I. J. Computer Network and Information Security, **2026, 2, 126-148**
Published Online on April 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2026.02.08

Adaptive Tangent Homomorphic Encryption with Equivariant Quantum Neural Networks for Secure Data Transmission Routing in MANET

I. V. Ravi Kumar*
Department of Electronics and Communication Engineering, GIET University., Gunupur, Odisha, -765022, India
Department of Electronics and Communication Engineering, Swarnandhra College of Engineering and Technology., Narsapur – 534 280., West Godavari District., Andhra Pradesh., India
E-mail: iv.ravikumar@giet.edu
ORCID iD: https://orcid.org/0009-0003-0613-988X
*Corresponding author

Prasada Reddy. M. M.
Dept. of ECE, GIET University, Gunupur, Odisha - 765022., India
E-mail: maruthiprasadareddy@gmail.com
ORCID iD: https://orcid.org/0000-0002-7994-7023

B. Nancharaiah
ECE Department, Usha Rama College of Engineering and Technology, Telaprolu- 521 109, A.P.
E-mail: nanch_bn@yahoo.com
ORCID iD: https://orcid.org/0000-0001-6079-5480

Received: 11 October 2025; Revised: 02 December 2025; Accepted: 27 January 2026; Published: 08 April 2026

Abstract: Due to the dynamic nature of the network architecture, resource constraints, and susceptibility to security attacks, securing data transmission in Mobile Ad-hoc Networks (MANETs) is a significant problem. This work proposes a novel Equivariant Quantum Neural Networks with Adaptive Tangent Brakerski-Gentry Vaikuntanathan Homomorphic Encryption algorithm (EQNN-ATBGVHEA)- based secure routing in MANET. The suggested approach comprises three steps: cluster head (CH) selection, optimal path selection, and secure data transfer. Initially, the Bowerbird Optimization Algorithm chooses the CH and sends the message through the constructed path. Once the clusters are established, data is transferred between the sender and receiver. For optimal route selection, developed the EQNNs technique which incorporates a neural network for quick route selection. EQNN resolves the issues of local optimality by constructing a new fitness process based on residual energy (RE) and delay. After the optimal path selection, Data transfer is secured by the innovative ATBGVHEA technique. Furthermore, this method is built using NS3, and the variables are determined. Additionally, the acquired results are contrasted with existing approaches for validating the efficiency of the suggested strategy. The developed method achieved a clustering accuracy of 98.5%, a computational time of 55ms, and a residual energy of 0.44.

Index Terms: Cluster Head, Optimal Route Selection, Data Transmission, Encryption, Tangent Search, Residual Energy.

1. Introduction

A MANET lacks a fixed infrastructure and consists entirely of mobile nodes. An access point, base station (BS), and wired network are not required for setting up the network [1]. Because host mobility is unrestricted, it may be quickly and inexpensively created. The rapid growth of wireless networks and the proliferation of mobile terminals have enabled the use of MANET in scenarios where network design is challenging [2]. The mobile nodes that make up the MANET function as routers in addition to carrying out the data transmission and reception tasks now completed by the host [3]. Because the mobile nodes function as routers, they can allow multipathing to neighbour nodes and execute dynamic routing in route settings. However, due to the dynamic topology and node migration within the wireless

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

network, it is vulnerable to numerous security flaws [4]. Numerous routing strategies for reliable data transmission and reception between nodes have been explored to address this issue. The demand-based AODV protocol has demonstrated exceptional performance across a range of traffic, density, and mobility patterns, outperforming the current routing protocol under study [5].

Nevertheless, there is an issue whereby more control packets are required to keep the routing to the destination intact. It has also been researched in relation to several malicious node routing attacks. Techniques that rely on the dependability of nodes participating in routing or employ authentication nodes to route by providing certificates to nodes have been researched to counter such routing attacks [6]. Rebuilding a new path from the source to the destination will take a while, increase the count of control packets, and raise the overhead if packet loss or route connection failure is caused by several attacks already present on the route [7]. Therefore, research into more effective and safe routing strategies is required to raise MANET's reliability.

The widespread use of mobile access networks, or MANETs, has led to an increase in their use in Internet of Things applications, such as pollution and environmental monitoring. However, the lack of infrastructure in MANETs makes routing difficult [8]. Efficiency problems with routing protocols like DSR and AODV include selecting the optimal path, assessing routes, ensuring fast data delivery, reducing retransmissions, and handling route breaks caused by mobility [9]. Routing takes network dynamics into account, with mobility being a key indicator, in order to address these problems. Data transmission efficiency is increased when measurements for route selection are combined. The network structure is closely linked to routing, and when the network is structured correctly, routing becomes easier and more efficient. For effective data transfer, MANETs can be clustered into several groups. Conventional algorithms, however, simply take the distance measure into account, which is inefficient. Data transmission can be optimized by combining cluster-based routing techniques. Given that MANETs are frequently installed in open, isolated locations, where there is a greater possibility of tampering, data manipulation, and theft, security is a top priority [10].

This paper proposes a secure routing technique based on encryption models to enhance the efficiency and performance of secure data transmission. The proposed EQNN–ATBGVHEA framework is particularly suitable for real-world MANET scenarios such as disaster recovery, IoT sensor networks, and military communications. In these contexts, nodes exhibit high mobility, limited battery power, and dynamic topology changes, making secure and efficient routing a critical challenge. The proposed framework addresses these challenges by striking a balance among routing efficiency, energy consumption, and encryption security.

The key contributions of this research are given below,

- The developed method consists of three phases: CH selection, Optimal path selection, and secured data transmission.
- Initially, the Bowerbird Optimization Algorithm selects the CH and transmits the message through the selected path.
- After the formation of clusters, the data is transmitted between the sender and the recipient. For optimal route selection, we presented the Equivariant Quantum Neural Networks approach, which integrates a neural network for fast route selection. Equivariant Quantum Neural Networks resolve the issues of local optimality by formulating new fitness processes based on routing overhead, residual energy (RE), clustering accuracy, and delay
- After the optimal path selection, Data transmission is secured by a novel Adaptive Tangent Brakerski-Gentry Vaikuntanathan Homomorphic Encryption algorithm.
- Finally, Network Simulator 3 is used to execute this model and calculate various characteristics such as clustering accuracy, energy consumption, packet delivery ratio, network lifetime, delay, and throughput. Furthermore, the obtained results are contrasted with existing techniques to assess the efficiency of the developed methodology.

The research study presented is structured as follows: Section 2 provides an overview of the most recent related work. Section 3 provides more details on the recommended approach. The outcome of the novel approach is described in Section 4. The research justifications are provided in Section 5 to support the conclusion.

2. Literature Survey

Some of the recent papers related to data transmission in MANET are given below,

In 2024, Murugan, V.S, and Unhelkar, B [11] have presented a novel model for energy prediction called Convolutional layer in a deep convolutional neural network concatenated with a max-average pooling layer (CCMAP-DCNN). It creates clusters based on energy, trust, distance, and latency limitations by adding layers to the current DCNN architecture. The NBO technique is used in the hybrid algorithm known as Namib Beetle Upgraded Jellyfish Search Optimization (NBUJSO) for cluster head selection and optimal routing. Taking network quality and mobility into account, the optimal routing approach selects the best path. To eliminate duplicate transmissions, the data aggregation technique is employed.

In 2023, Rajeshkumar, G., et al. [12] presented a MOPSO method for detecting intrusions in MANET. This research article explores the use of Dynamic Source Routing (DSR) in MANETs to combat blackhole attacks. Unauthorized nodes in a MANET system are located using the Cluster Trust Adaptive Acknowledgment (CTAA) technique. The use of Kalman Filters (KF) helps to prevent synchronization issues and predict node trustworthiness. Network traffic is reduced and the number of clustered MANETs is maximized by utilizing Multi-Objective Particle Swarm Optimization (MOPSO) in route optimization. By 3.5% at 30% malware, the suggested CTAA-MPSO outperforms the CTAA-PSO by 3.3% in terms of packet delivery ratio.

In 2023, Ravi, S, et al, [13] have presented an ATSORS-HFO model to select the best route for packet transmission in a Multi-Agent Network (MANET). The Adaptive Chaotic Grey Wolf Optimisation (ACGWO) method underpins the Advanced Encryption Standard, while the Fuzzy Butterfly Optimisation method (FBOA) is evaluated in the study to determine the best pathways for both untrusted and trusted nodes from the source. The trust-based ACGWO method is employed to optimally select the resulting K-paths, and the AES-ACGWO technique is utilized to validate the shared code and node keys.

In 2024, Selvaraj, S and Chakkaravarthy, M [14] presented a unique deep learning architecture designed for effective sequential data categorization in MANETs: the Convolutional Gated Recurrent Unit Network (CGRUN). The Artificial Gorilla Troops Optimizer (AGTO), a novel optimization model, is proposed with the explicit purpose of enhancing weight reduction procedures within the CGRUN framework. To address the challenges of effective resource utilization and network performance enhancement in MANETs, AGTO demonstrates potential in optimizing and refining the categorization model. Additionally, this study introduces a Python-based program specifically designed for processing and analyzing the WSN-DS dataset. The technology outperforms existing alternatives with an amazing accuracy rate of 99.81%.

In 2023, Jose, M.R and Vigila, S.M, [15] have presented the F-CAPSO technique to increase security and energy effectiveness in MANET wireless networks with constrained mobility and battery life. The method integrates the Sine Cosine algorithm search and Salp Swarm Algorithm with Replacement Method (SSARM-SCA) for optimal routing and safe data transfer. The Fuzzy-based CAPSO algorithm is used to choose the optimal Cluster Head (CH). Secure pathways are established using encryption that is based on trust. In terms of energy usage and network longevity, the methodology outperforms four state-of-the-art methods, with improvements seen for up to 3500 rounds. Applications in tracking and military settings benefit from this strategy.

In 2023, Manthiramoorthy, C, et al. [16] proposed the Effective Trusted Knowledge Algorithm (HETKA), which ensures the security of data as it is transmitted between nodes by utilizing trust estimation. The reliable node is identified using one of the two components of the proposed method. In the next step, an effective value of dependability was determined using a hybrid method after the promiscuous node was seen. After conducting extensive simulation experiments, we have concluded that the suggested technique offers an effective way to secure data across the Internet from unreliable routers and unstable Distributed Anomaly Networks (MANET).

In 2022, Singh, P., et al. [17] provided an innovative method that utilizes the modified Ad hoc On-demand Multipath Distance Vector (AOMDV) protocol to ensure safe and dependable data transfer in MANETs against black hole attacks. AOMDV is used for multiple route discoveries, KNN is used to select the nearest neighbor node, and False Key Build Advanced Encryption Standard (FAES) encryption is employed for cryptography within the system. IoT data and devices are protected against network and hardware intrusions using the FAES algorithm. The simulation results demonstrate that, even in the presence of hostile nodes, the FAES-AOMDV protocol ensures secure data transmission with minimal energy consumption.

2.1. Problem Statement

In MANETs, where nodes can move about and topology changes often, the challenge of secure data transmission routing is to maintain dependable and effective data communication in a decentralized and dynamically changing network environment. Creating routing protocols that effectively find and preserve the best routes for data transfer while guarding against various security risks, including spoofing, denial-of-service attacks, and eavesdropping, is the fundamental challenge. To accomplish reliable and secure communication in resource-constrained MANETs, the solution must strike a balance between security, energy efficiency, and network efficiency.

2.2. Motivation

MANETs are wireless networks composed of numerous peer nodes, and their mobility introduces challenges such as unpredictable connectivity, security vulnerabilities, reliability issues, path maintenance, and limited battery life, all of which impact network quality of service (QoS). Effective routing protocols are critical for maintaining reliable communication paths, while multicast routing can enhance network dependability and reduce transmission costs by delivering data from one node to multiple recipients simultaneously. Despite prior studies, a lack of approaches remains that integrate advanced techniques, such as quantum graph neural networks, or address real-world deployment challenges in dynamic MANET environments. This gap motivates the proposed work, which introduces a novel Adaptive Tangent Homomorphic Encryption algorithm combined with Equivariant Quantum Neural Networks to enable secure, efficient, and robust routing in MANETs.

2.3. Research Gap in Quantum Routing and MANET Encryption

Recent research has explored the integration of quantum computing and advanced cryptographic models in MANETs. For instance, Zhang et al. (2022) [18] introduced a Quantum-Inspired Routing Protocol (QIRP) that leverages quantum state representation for optimizing path discovery, but it suffers from scalability issues under high mobility scenarios, while on the encryption side, Zu et al. (2023) [19] suggested a modified CKKS-based homomorphic encryption scheme for IoT-enabled MANETs, enabling partial secure computation but with significant noise growth. From this survey, it is evident that while quantum models enhance routing and homomorphic encryption enhances security, no prior work has jointly optimized both aspects. The proposed EQNN–ATBGVHEA framework uniquely integrates equivariant quantum neural networks for efficient and robust routing with adaptive tangent homomorphic encryption for secure end-to-end data transmission in MANETs. Therefore, the proposed work not only fills this gap but also establishes a unified framework that simultaneously optimizes routing efficiency and data security in MANETs.

3. Proposed Methodology

In this section, describe the suggested EQNN-ATBGVHEA scheme for MANET. The key procedures involved in the EQNN-ATBGVHEA scheme, including secure cluster creation, secure routing, and secure data transmission, are explained in detail in this section. The Bowerbird Optimization Algorithm (BOA) is utilized to select the CH for data transmission. The Equivariant Quantum Neural Networks (EQNN) approach is utilized for rapid route selection, incorporating a neural network to expedite path selection. Data transmission is secured using the Adaptive Tangent Brakerski-Gentry Vaikuntanathan Homomorphic Encryption algorithm (ATBGVHEA). The workflow of the proposed work is given in Figure 1.

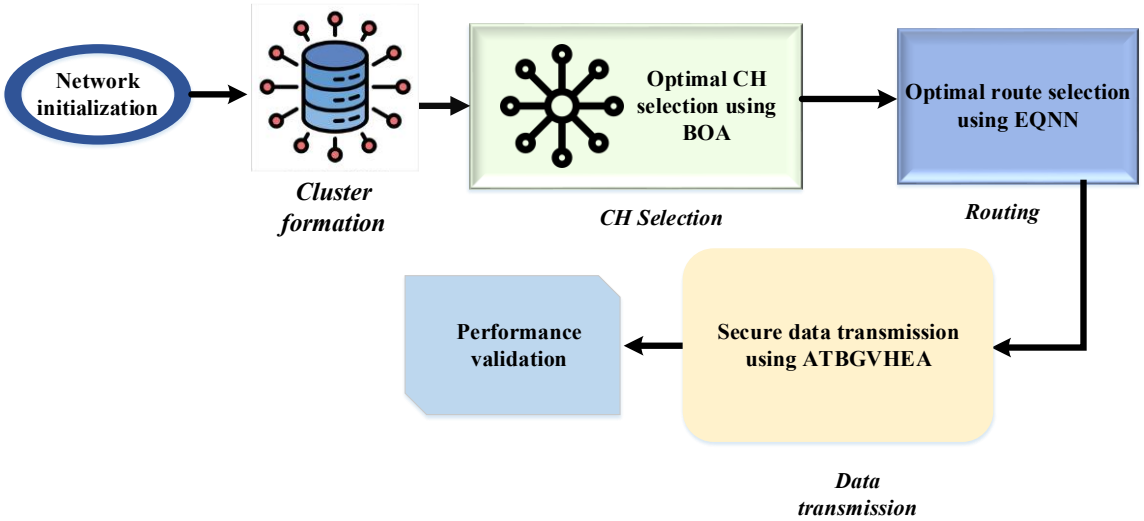


Fig.1. Process of the proposed approach

3.1. System and Network Model

In this section, provide the system and network model for secure data transfer in MANETs. The system features a collection of mobile nodes that connect wirelessly, providing a decentralized and self-configuring network.

A. MANET System Model

Data transmission from one MANET node to another is depicted in figure 2 of the MANET system concept. Taking into account the nodes' dynamic topology changes, its primary goal is to estimate the power needed to maintain network communication throughout. Let us take the MANET system model represented by graph $G = \{A, B\}$, which consists of A nodes and B links. In this case, the node-set is represented by $A = \{a_1, a_2, \ldots . a_m, \ldots a_n\}; 1 \leq m \leq n$denotes the total amount of nodes employed. The set of connections utilized to connect two nodes is denoted by $B = \{b_1, b_2, \ldots . b_z\}$, while the total number of links used is indicated by z . Many factors, including power, the quantity of transmissions and retransmissions, and the total count of neighbours engaged, are taken into account when designing the MANET system.

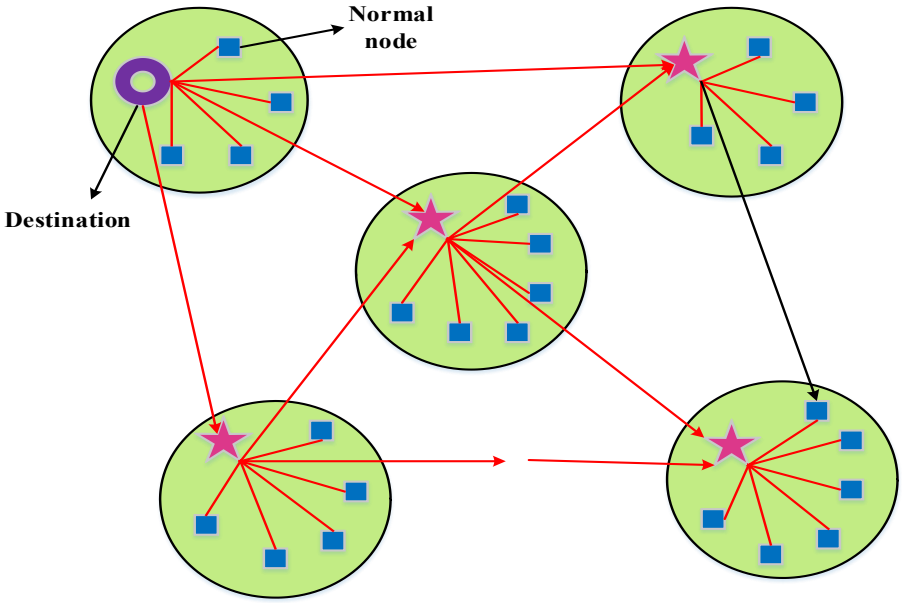


Fig.2. MANET system model

Assume O to be a source node sending data packets to destination T. $C = \{c_1, c_2, \ldots . c_r, \ldots c_v\}; 1 \leq r \leq v$ denotes the cluster headset; v denotes the overall amount of cluster heads employed. Every node uses a lot of power to send a packet from one node to another, and the cluster head selection procedure is covered in the next section. To solve this issue, the power-centric dependable CH selection approach is applied. The transmission path that uses the least amount of power to forward packets is chosen. The criteria of distance, node battery level, and connection connectivity are deemed significant in determining the node's lifespan.

B. Network Model

The mobility range of the n nodes $(M_1, M_2, \ldots . M_n)$ in the suggested mobile network indicates the lowest and upper bounds of the mobility range, respectively. Within the range, all mobile nodes are free to roam the network at different speeds. Several clusters have been created inside the entire network to facilitate management. Prior to cluster formation, each node in the network is granted authorization. The distributed validation of the nodes is facilitated by the MANET. Data transmission is accomplished via the network's optimal route selection. Encryption algorithm approaches are used to secure data transport overall.

3.2. Optimal CH Selection Using Bowerbird Optimization Algorithm (BOA)

In this section, the optimal CH has been selected using BOA. The Bowerbird Optimization Algorithm (BOA) [20] is a useful method for resolving challenging optimization issues. It was inspired by the courtship behaviour of satin bowerbirds. It can be modified to select the best CH in a MANET. In order to maintain effective communication, reduce EC, and increase the NL, choosing the best CH for a MANET is essential. Applying the same content structure and supplied equations, the BOA can be used to solve this problem in the phases that follow:

Step 1: Generating a set of random bowers (Initial CHs)

An initial population of possible cluster heads is generated, akin to the process of creating initial bowers in the BOA. Every potential CH is depicted as an n-dimensional vector, with each dimension denoting a network feature that affects the choice of CH, such as connectedness, RE, and distance to other nodes. Within the defined parameters, these initial candidates are generated randomly.

Step 2: Measuring the probability of each population member

Each candidate CH's attractiveness is computed based on its fitness, which is established by a cost function that takes into account node degree, connection, and energy efficiency. The probability equation utilized in the BOA method is also employed to determine the fitness of every candidate CH, which is given in equation (1).

$$Pr\,o\,b_i = \frac{fit_i}{\sum_{n=1}^{NC} fit_n} \tag{1}$$

where, fit_i indicates the fitness of the i^{th} candidate CH, NC indicates the number of candidate CHs. The fitness function is defined in equation (2).

$$fit_i = \begin{cases} \frac{f(s_i)}{1+f(x_i)}, \overrightarrow{\leftarrow}\overrightarrow{\leftarrow}\overrightarrow{\leftarrow}\overrightarrow{\leftarrow}\overrightarrow{\leftarrow}\overrightarrow{\leftarrow}\overrightarrow{\leftarrow}\overrightarrow{\leftarrow} iff(s_i) \geq 0 \\ \frac{1}{1+|f(s_i)|}, iff(s_i) < 0 \end{cases} \quad (2)$$

where, the value of the cost function for the i^{th} candidate CH is denoted by $f(s_i)$. Node density, communication distance, and energy usage are possible components of this cost function.

Step 3: Elitism (preserving the best candidate CH)

The "elite" CH, or the best candidate CH, is identified in this step and saved for the next iteration. With the greatest fitness value, this candidate CH sets the standard for all other candidate CHs. The elite CH is comparable to the BOA algorithm's most alluring bower, which influences the choices of other CHs in later iterations.

Step 4: Determining new changes in any position

As in the SBO method, candidate CH positions are changed according to their attractiveness, as given in equation (3).

$$s_{ik}^{new} = s_{ik}^{old} + \gamma_k \left(\frac{s_{jk}+s_{elitek}}{2} - s_{ik}^{old} \right) \quad (3)$$

where, s_{ik} indicates the k^{th} parameter of the i^{th} candidate CH, s_{elite} indicates the position of the elite CH, s_{jk} indicates the target solution, selected based on the probability calculated earlier, and γ_k determines the step size and is calculated in equation (4).

$$\gamma_k = \frac{\beta}{1+p_j} \quad (4)$$

where, β indicates the increasing step size, and p_j indicates the probability associated with the target solution.

Step 5: Mutation

The candidate CHs are subjected to random mutations to add diversity and prevent the algorithm from becoming stuck in local optima. The new location of a candidate CH is determined using the following equation (5), which is analogous to the BOA algorithm in the mutation process.

$$s_{ik}^{new} \sim N(s_{ik}^{old}, \sigma^2) \quad (5)$$

where, N indicates a normal distribution, and σ^2 indicates the variance, calculated in equation (6).

$$\sigma = z \times (\text{var}_{\max} - \text{var}_{\min}) \quad (6)$$

In this case, the variable range's upper and lower boundaries are denoted by the parameters $\text{var}_{\max}$ and $\text{var}_{\min}$, respectively, and z z is a percentage of the difference between them.

Step 6: Combining the Old Population and the Population Obtained from Changes

The modified population of candidate CHs is combined with the previous population created prior to the modifications. The top-performing candidates are selected to form the new population for the next iteration, once the merged populations have been evaluated. To select the best CHs for the MANET, this process continues until the termination requirements are met. The step-by-step procedure of BOA is given in Figure 3.

By following these steps, the BOA algorithm effectively identifies the optimal CHs in a MANET, enhancing network performance by ensuring energy-efficient and reliable communication across the network.

3.3. Optimal Path Selection Using Equivariant Quantum Neural Network (EQNN)

After selecting the CH, the optimal path for data transmission is determined. Ensuring effective routing and communication within a MANET requires an appropriate path selection algorithm. Utilizing the concepts of equivariance and quantum computation, an EQNN [21] is applied for this purpose in order to improve the path selection algorithm performance. The Equivariant Graph Neural Network (EGNN) and Quantum Graph Neural Network (QGNN) ideas are employed in the EQNN. Integrating equivariant transformations with representations of quantum states is the goal in order to determine optimal pathways. Path selection is enhanced by this method, which considers quantum state development, translational, and rotational equivariance. Algorithm 1 presents the Pseudocode for EQNN.

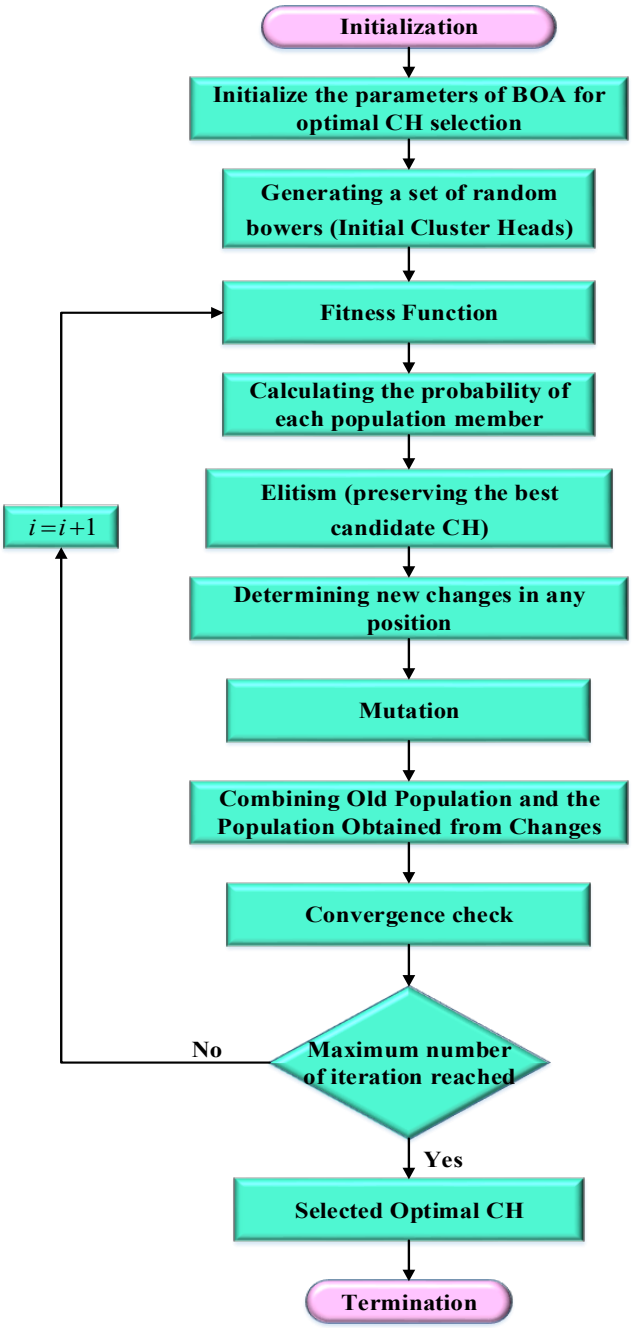


Fig.3. The step-by-step procedure of BOA

In the proposed EQNN framework, all mathematical concepts are grounded in practical MANET behavior, reflecting real-world network conditions. Node features capture important metrics such as residual energy, buffer occupancy, and connectivity, while edge attributes represent link quality, distance, or signal strength between nodes. Neighbor relationships define which nodes are directly connected, and message aggregation ensures that no single node is overused. Quantum states and transformations are employed to model complex interactions among nodes, enabling robust route selection under dynamic topologies. By integrating these concepts, the EQNN method ensures energy-efficient, reliable, and topology-invariant path selection, directly linking the abstract model to tangible MANET routing decisions.

By incorporating equivariance, which accounts for changes in 2D space (including rotations and translations), an EGNN outperforms conventional GNNs. An EGNN's message sending function is made to update node coordinates and features in an equivariant way. The message m_{ij} is calculated for nodes i and j as follows in equation (7).

$$m_{ij} = \varphi_e(f_i^l, f_j^l, e_{ij}, |s_i^l - s_i^l|) \tag{7}$$

where, f_i^l and f_j^l indicates the features of nodes i and j, e_{ij} indicates the edge attributes, and $|s_i^l - s_j^l|$ indicates the distance between nodes i and j in the current layer l. The aggregated message for node i is given in equation (8).

$$m_i = \sum_{j \in N(i)} m_{ij} \tag{8}$$

where, $N(i)$ indicates the set of neighbours of node i.The discrepancies between node i coordinates and those of its neighbours are taken into account when updating node i coordinates. The person providing this update is given in equation (9).

$$s_i^{l+1} = s_i^l + C \sum_{j \neq i} (s_i^l - s_j^l) \varphi_s(m_{ij}) \tag{9}$$

here, C indicates suppression factor, defined as $C(n_\alpha) = \frac{1}{ln(2n_\alpha)}$ and $\varphi_s$is an MLP that processes the messages. The node feature update is performed in equation (10).

$$f_i^{l+1} = \varphi_f(f_i^l, m_i) \tag{10}$$

where, φ_f is an MLP that combines the node features and aggregated messages. Using quantum states and Hamiltonians, a QGNN models the graph and offers a framework for inference and learning in quantum space. Node properties are embedded into qubit states to create the first quantum state in equation (11).

$$|\phi_0^\alpha\rangle = \overset{i=1}{\underset{N}{\otimes}} \left|\varphi_{|\phi_0\rangle}(f_i)\right\rangle \tag{11}$$

where, $\left|\varphi_{|\phi_0\rangle}(f_i)\right\rangle$ indicates the quantum state corresponding to node features f_i, and $|\phi_0^\alpha\rangle$indicates the product state for all nodes in the graph. The interactions between nodes are described by the Hamiltonian H. It consists of node characteristics f_i and coupling terms based on the adjacency matrix e_{ij} is given in equation (12).

$$H(e_{ij}) = \sum_{(i,j) \in E} e_{ij} \left(\frac{\hat{D}_i - \sigma_z^i}{2} - \frac{\hat{D}_j - \sigma_z^j}{2} \right) + \sum_{i \in V} \sigma_s^i \tag{12}$$

where, σ_z^i and σ_z^j are the Pauli operators acting on the Hilbert space of qubit i, and $\hat{D}_i$ indicates the identity operator. Unitary transformations with learnable coefficients as parameters lead to the evolution of the quantum state given in equation (13) and (14).

$$U_{ij} = \varphi_u(e_{ij}) = exp\left(-i \sum_{q=1}^{Q} \gamma l q H_q(e_{ij})\right) \tag{13}$$

$$|\phi^{l+1}\rangle = \varphi_{|\phi\rangle}(|\phi^l\rangle, U_{ij}) = U_\theta^l U_{ij} U_\theta^{l+} |\phi^l\rangle \tag{14}$$

where, U_θ^l indicates the parameterized unitary transformation. The EQNN combines quantum state processing with equivariance principles: Following the evolution of quantum states, mean pooling is used to aggregate the final quantum state given in equation (15).

$$Output = \frac{1}{2^n} \sum_{k=1}^{2^n} \left|\phi_P^k\right\rangle \tag{15}$$

The global characteristics of the graph are captured by this combined quantum state. To generate forecasts or judgments, the combined state is fed through a traditional neural network. The best path is determined by this classical network, which processes the aggregated quantum state. By following these procedures, the EQNN method tackles the problem of optimal path selection in MANETs by fusing quantum computing and EGNN. The EQNN framework is a promising approach to enhancing routing efficiency and flexibility in dynamic network situations by utilizing quantum state processing and equivariance.

Algorithm 1: Pseudocode for EQNN

Input: MANET graph with node features and edge attributes
Output: Optimal path for data transmission
1. Initialize cluster heads (CH) and construct initial clusters
2. For each node in the cluster:
    a. Aggregate messages from neighboring nodes

// Combines neighbor information such as energy, connectivity, and link quality
b. Update node features based on aggregated messages
// Ensures balanced energy usage and prevents node overloading
3. Encode node features into quantum states
// Captures complex node interactions for robust routing
4. Evolve quantum states using Hamiltonian and unitary transformations
// Models network dynamics and interactions
5. Aggregate final quantum states using mean pooling
// Extracts global network characteristics
6. Feed aggregated quantum state into classical neural network
// Predicts optimal routing path considering delay, energy, and reliability
7. Return the path with the highest routing score

It is important to note that the proposed EQNN differs significantly from conventional Graph Neural Networks (GNNs) and standard Quantum Neural Networks (QNNs). While GNNs are effective in processing graph-structured data, they often converge to local optima in highly dynamic MANET topologies. QNNs, on the other hand, leverage quantum state representations but lack structural equivariance, making them sensitive to node reordering or variations in topology. The proposed EQNN integrates equivariance within a quantum framework, ensuring that routing decisions remain invariant under such transformations. This design allows EQNN to achieve higher robustness, stability, and adaptability in MANET environments compared to existing GNN and QNN models.

3.4. Secure Data Transmission using a Novel ATBGVHEA

After selecting the optimal path, data can be transmitted securely. Secure data transfer is crucial in MANETs to prevent breaches, especially when data may reside in cloud storage. To protect non-malicious data, the proposed ATBGVHEA [22] encrypts and preserves benign data, while malicious data is discarded. This homomorphic encryption-based approach enables computations on encrypted data without revealing the underlying plaintext, ensuring privacy and security during transmission and storage.

A. Homomorphic Encryption (HE) with BGV

Mathematical operations can be done on encrypted data thanks to homomorphic encryption (HE). By doing this, computation privacy is guaranteed without requiring data decryption beforehand.

Addition under Homomorphic Encryption: Equation (16) states that the following relation applies if the operation is addition.

$$H_E(a+b) = H_E(a) \oplus H_E(b) \tag{16}$$

where, H_E indicates the encryption function, and $\oplus$ indicates the operation determined by the encryption cipher.

Multiplication under Homomorphic Encryption: Equation (17) represents the multiplication operation in a similar manner.

$$H_E(a+b) = H_E(a) \oplus H_E(b) \tag{17}$$

where, a and b are plaintext messages.

Key generation using SHA-512: The SHA-512 hash function creates a new secret key by utilizing the error vectors associated with the public and private keys to produce the encryption and decryption key, which is given in equation (18).

$$Key_{secret} = SHA_{512}(Errorvector(Private Key).Errorvector(PublicKey) \tag{18}$$

The non-malicious data kept in the cloud is then encrypted and decrypted using this key.

BGV Ciphertext Format: An enhanced homomorphic encryption method is called Brakerski-Gentry-Vaikuntanathan (BGV). Elements in a ring $\Re$ are represented by the plaintexts and ciphertexts, which are as follows in equation (19).

$$\Re = F[S]/(S^P + 1) \tag{19}$$

here, P indicates the power of 2, and the elements are decreased modulo $S^P + 1$. The ciphertext $(M_0, M_1) \in \Re_r^2$ indicates the encrypted plaintext $p \in \Re_t$, with secret key $Key_{secret}$and public key P_k, as represented in equation (20).

$$(M_0 + M_1).SecretKey = n + x_{error}.M_k \, mod(r) \tag{20}$$

where, the noise that determines whether decryption yields the proper plaintext is represented by x_{error}. In the event that the error coefficient is less than $r/2^y$, the plaintext can be uniquely recovered as follows in equation (21).

$$[(P_0 + P_1).SecretKey]_r^y \tag{21}$$

B. Key Management Optimization using ATSA

Optimizing key management presents issues for the ATBGVHEA. The best key with the fastest key-breaking time is chosen using the ATSA to resolve this.

- ***Key initialization:*** To get the best answers, first initialize the AHEBGV's initial key management variables and create the ATSA populations. Equation (22), which distributes the starting solution equally throughout the search space, is used to calculate it.

$$S_0 = L_b + (U_b - L_b) \times rand(D) \tag{22}$$

where, U_b and L_b indicate upper and lower boundaries, and $rand(D)$ generate random values in the interval [0, 1]

- ***Random key generation:*** After initialization, generate the ATSA's input variables at random.
- ***Fitness function (FF):*** To obtain optimal solutions, the (FF) is utilized to choose the best key from the AHEBGV. The FF of the algorithms is determined by the following equation, which is presented in Equation (23).

$$FitnessFunction = select_{Max}(Optimum_{(key)} with key breaking time) \tag{23}$$

Using the aforementioned equation, the ideal key is determined in terms of the maximum key-breaking time. Therefore, an ATSA based on FF is proposed to discover the best option. Equation (23) selects the optimal key as the best option based on the truncated key breakage time. The previous equation generates the ideal key with the quickest key breakup time (23).

- ***Intensification search for selecting optimal keys (OK):*** Here, the optimal key with the shortest breaking time is chosen using ATSA's intensification search approach. The variables in the acquired solution are then compared to the equivalent variables in the current best solution. The best-chosen equation is provided in equations (24) and (25).

$$S_j^{t+1} = S_j^t + Step * tan(\varphi) * (S_j^t - optimizationKey_{secret_j}^t) \tag{24}$$

$$S_j^{t+1} = optimalKey_{secret_j}^t if \; variablejisselected \tag{25}$$

This leads to a final solution S_j^{t+1} that improves the best existing solution locally by deviating from it by less than 50%. The ideal keys are chosen using equations (24) and (25).

From the collection of random keys produced by an ATBGVHE, an ATSA chooses the optimal key with the highest time breakage. Ultimately, encrypted data stored in a very secure cloud is the outcome of ATBGVHE. If the user wishes to retrieve the data, it is recovered using an encrypted key.

Algorithm 1: ATSA

Input: Data to share
Output: Data transferred securely
Step 1: Generation of key
Step 2: Selecting OK utlizing equation (24) and (25) by the ATSA
Step 3: Output of key generation

secret key $Key_{secret}$and public key P_k

Step 4: Encryption

Encrypt output(Ciphertext $(M_0, M_1) \in \Re_r^2$)

Step 5: Decryption

Decrypt output(Plain text ($[(P_0 + P_1).SecretKey]_r^y$))

Step 6: Termination

- ***Termination:*** The ATBGVHE is a secure cloud storage solution that utilises the ASSA to select the optimal key in real-time. Algorithm 1 gives the pseudocode of the optimal key management.

By following these procedures, the data can be transmitted using the novel ATBGVHEA.

In the proposed ATBGVHEA, encryption keys are dynamically selected to balance security and computational overhead in mobile MANET nodes. The adaptive noise mechanism ensures that repeated operations do not compromise precision or increase latency, while homomorphic encryption allows secure computation directly on encrypted data without exposing plaintext. Together, these features enable real-time, robust, and energy-efficient data transmission in dynamic and resource-constrained MANET environments.

It is important to emphasize how the proposed ATBGVHEA differs from conventional homomorphic encryption schemes. The Brakerski–Gentry–Vaikuntanathan (BGV) scheme enables exact operations but suffers from rapid noise growth, making repeated computations impractical without costly bootstrapping. The Cheon–Kim–Kim–Song (CKKS) scheme supports approximate arithmetic but introduces rounding errors, which reduce precision and make it less suitable for secure routing. In contrast, ATBGVHEA incorporates an adaptive tangent-based mechanism that dynamically controls noise accumulation, thereby reducing bootstrapping overhead while retaining precision. This adaptation lowers encryption and decryption latency, making the scheme efficient for resource-constrained MANET devices. Furthermore, ATBGVHEA preserves confidentiality, integrity, and resistance against eavesdropping, replay, and tampering attacks, ensuring robust and real-time secure data transmission in dynamic MANET environments.

4. Result and Discussion

This section discusses the evaluation of the planned work based on simulation observations. The Network Simulator simulation tool is utilised to create the suggested MANET network. Ns-3 is a discrete-event system simulator designed for Internet networks, primarily for research and educational reasons. Table 1 lists all the parameters used in the simulation.

Table 1. Simulation parameters

Parameter	Value
Tool	NS-3.38
Area	1000x1000
Data rate	2048bps
Simulation time	200s
Mobility	20 m/s
Mobility model	Random waypoint
Mobile nodes	20, 40, 60, 80, 100
Netnanim	3.109
Maximum clusters	15
Initial energy of nodes	750J
Packet size	64
Transmission energy	50nJ
Reception energy	50nJ
Dissipation energy	10pJ/bit/m^2

4.1. Performance Analysis of the Proposed Method

The performance study of the suggested EQNN-ATBGVHEA method compares it to other approaches and assesses its efficacy using specific measures. Numerous key performance indicators, including energy consumption, routing overhead, packet delivery ratio, network lifetime, encryption time, decryption time, and computational time, can be used to assess the suggested approach.

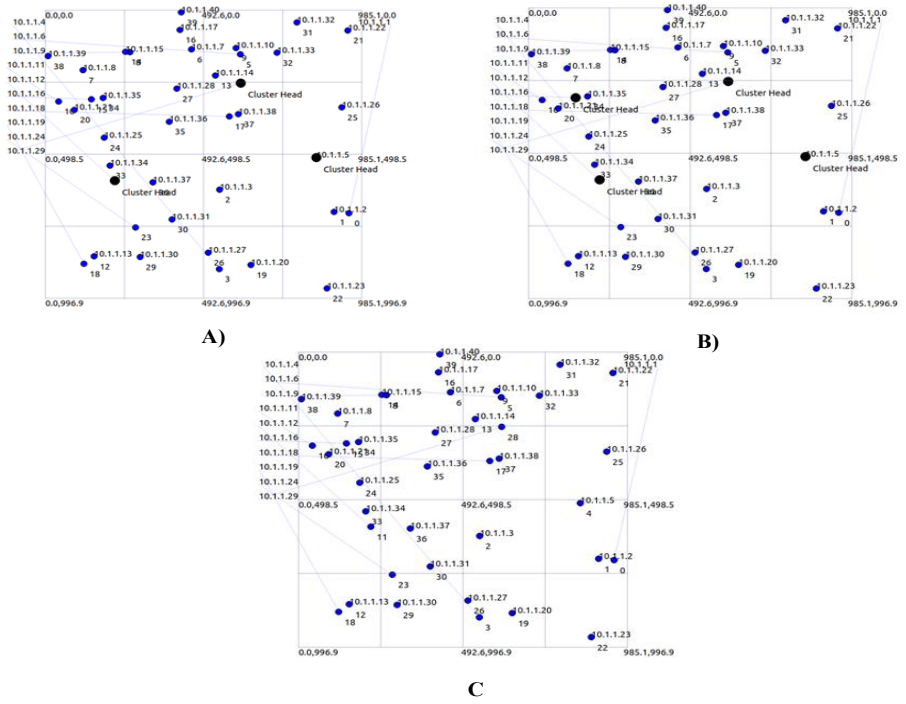


Fig.4. A) Node initialization B) Cluster head selection and C) Data transmission

Three steps in the MANET process are depicted in Figure 4: A) Data transmission, B) cluster head selection, and C) node initialisation. Nodes are initialised and their locations within the network are determined in the first step (A). The cluster head selection procedure is depicted in stage (B) of the second picture. Larger markers designate particular nodes as cluster heads, who oversee communication both inside and between clusters. Data transmission occurs in the final stage (C), where data is efficiently routed through the selected cluster heads to reach their destination. The hierarchical clustering mechanism in MANETs minimises direct communication between remote nodes, which increases communication efficiency and lowers energy consumption. This sequence demonstrates how it works.

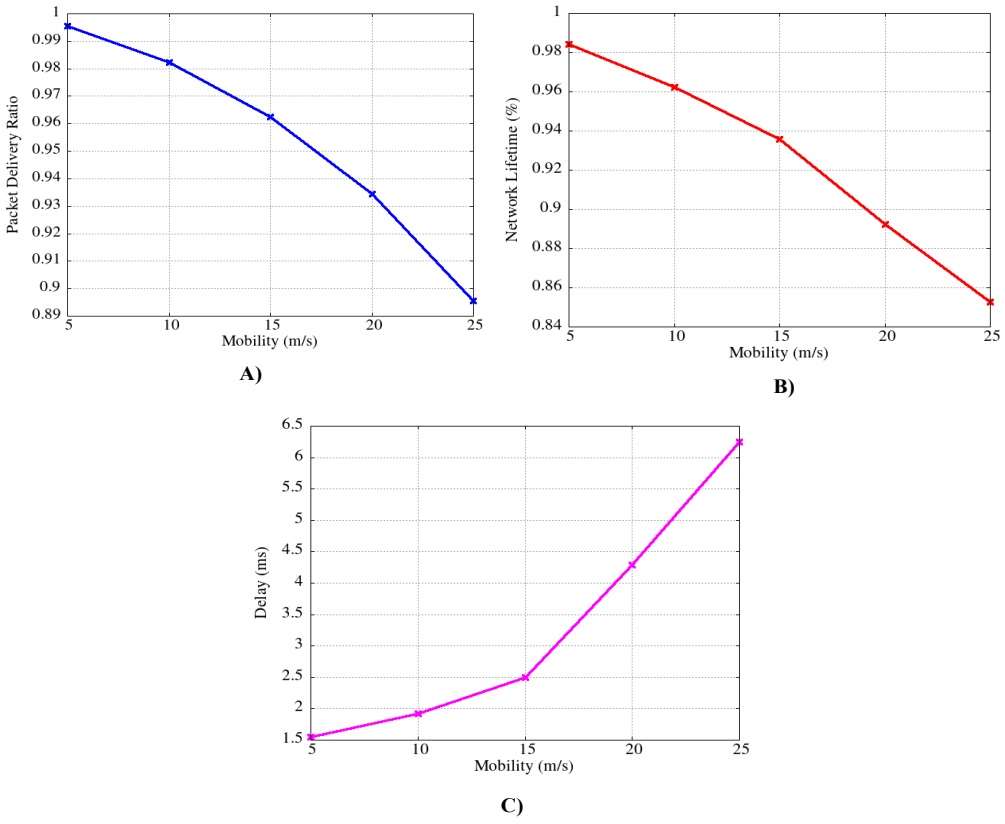


Fig.5. Performance of proposed method A) PDR B) Network Lifetime and C) Delay

The performance analysis of the suggested EQNN-ATBGVHEA method is shown in Figure 5, which presents the results as a function of three key metrics: (A) PDR, (B) network lifetime, and (C) Delay, all expressed as a function of mobility (measured in m/s). Higher node mobility results in increased packet losses, as seen by the PDR declining as mobility rises in Figure 5 (A). The network lifetime is also seen in Figure 5(B) to decrease with node mobility. This is likely because frequent route discoveries result in increased energy usage. Finally, Figure 5(C) shows the latency, which increases with mobility and reflects the longer data transmission times. Overall, the analysis demonstrates how network performance and node mobility are traded off, with the suggested approach maintaining a comparatively high level of efficiency under varying condition.

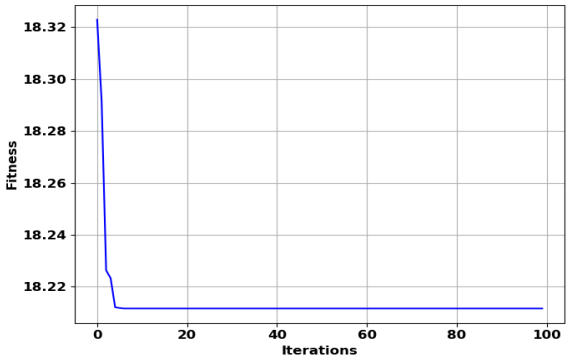


Fig.6. Fitness evaluation

The convergence of a fitness function over 100 iterations is represented in Figure 6. Initially, the fitness value starts at roughly 18.32 and rapidly drops, stabilising at approximately 18.22 after around 10 rounds. This shows that the optimization algorithm made great progress in the early iterations, reaching a point where future iterations caused small changes in the fitness value. The figure suggests that the solution has converged and no further improvement in fitness is achieved after a certain point, indicating that the algorithm has likely identified a near-optimal solution.

4.2. Performance Analysis of the Proposed Model Compared with the Previous Methods

The proposed EQNN–ATBGVHEA technique is implemented and tested on the NS3 simulation platform (version 3.38) and a wireless sensor network environment. Nodes are deployed in a 1000 m × 1000 m area, following the Random Waypoint mobility model with speeds ranging from 0 to 10 m/s. The network consists of N nodes, with clustering performed using BOA, and optimal paths selected using EQNN. Data is encrypted with ATBGVHEA before transmission along selected paths. Traffic is modelled as CBR flows with 512-byte packets, and the simulation runs for 500 seconds. Each experiment is repeated five times with different random seeds, and the results are averaged for statistical validity. The following metrics are measured: clustering accuracy, encryption/decryption time, computational time, routing overhead, throughput, delay, packet delivery ratio, network lifetime, and energy consumption. The performance of EQNN–ATBGVHEA is compared against existing methods: MOPSO, NBUJSO-DCNN, ATSORS-HFO, and AGTO. This setup ensures reproducibility and demonstrates the advantages of integrating EQNN-based routing with ATBGVHEA-secured transmission under realistic MANET conditions.

- ***Routing overhead (RO):*** The extra communication or control packets that are sent back and forth between nodes in a network in order to create, update, and maintain routes are referred to as RO. These control packets are crucial for establishing and preserving network topology and node-to-node pathways in MANETs. This can be expressed in equation (26).

$$R_o = \frac{P_{total}}{D_{delivered}} \tag{26}$$

where, P_{total} indicates the overall count of control packets, and $D_{delivered}$ indicates the overall count of data packets successfully delivered.

A comparison of the RO of five distinct routing algorithms is shown in Figure 7: AGTO, ATSORS-HFO, NBUJSO-DCNN, MOPSO, and a suggested approach. Routing overhead is plotted on the y-axis, with values ranging from 0.1 to 0.6. The suggested approach outperforms the other algorithms by a considerable margin and has the lowest routing overhead. The highest overhead is reported by NBUJSO-DCNN, followed by MOPSO, AGTO, and ATSORS-HFO. This shows that when compared to the other strategies offered, the proposed strategy is very effective at minimising routing overhead.

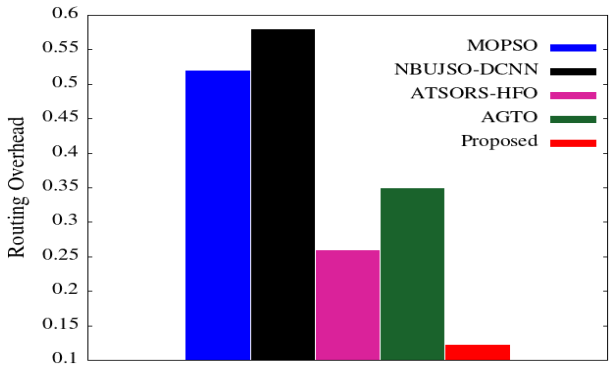


Fig.7. Comparison of RO

- ***Clustering Accuracy (CA):*** For a specific number of nodes in the network, the count of overlaps generated by the algorithm determines the clustering accuracy of the algorithm. It was measured using equation (27).

$$ClusteringAccuracy = \frac{Noofoverlaps}{Totalnoofnodes} \tag{27}$$

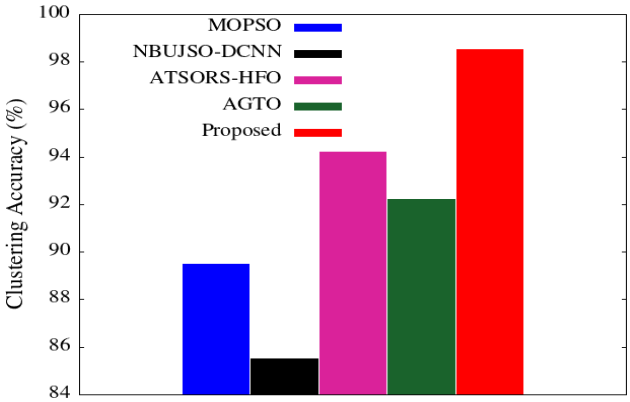


Fig.8. Comparison of clustering accuracy

The suggested algorithm is compared with the MOPSO, NBUJSO-DCNN, ATSORS-HFO, and AGTO clustering algorithms in Figure 8 based on their percentage clustering accuracy. The NBUJSO-DCNN method earned 85% of clustering accuracy. The clustering accuracies of MOPSO and ATSORS-HFO are lower; MOPSO is approximately 89% and ATSORS-HFO is approximately 94%. The clustering accuracy of AGTO is roughly 92%, which falls between these two. With a clustering accuracy of roughly 98.5%, the proposed algorithm outperforms the existing methods.

- ***Encryption time (ET):*** ET is the length of time needed to use a certain encryption algorithm to transform plaintext data into ciphertext. It is a vital indicator for assessing how well an encryption scheme works, especially in real-time applications where speedy data encryption is required to preserve system security and efficiency.

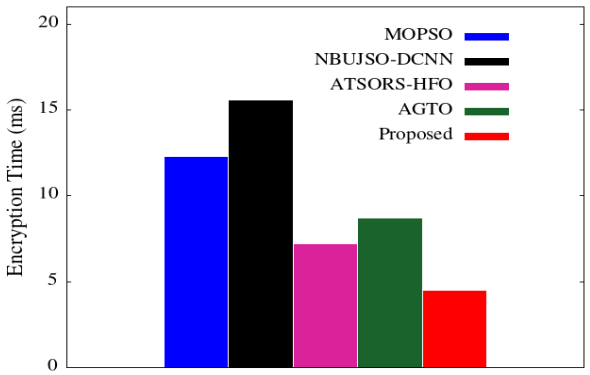


Fig.9. Comparison of encryption time

The suggested algorithm is compared with MOPSO, NBUJSO-DCNN, ATSORS-HFO, and AGTO encryption algorithms in Figure 9, based on their percentage of encryption time. The NBUJSO-DCNN has the largest encryption time, at about 15.5 milliseconds. Between these two extremes are the encryption times of MOPSO and ATSORS-HFO, with MOPSO having a slightly longer time at around 12 milliseconds, ATSORS-HFO having a somewhat shorter time at about 7.5 milliseconds and the AGTO method earned 8 ms. When compared to the previous methods, the presented model achieved the lowest encryption time of 5 ms.

- ***Decryption time (DT):*** DT is the amount of time needed to use the appropriate decryption key and algorithm to transform encrypted data (ciphertext) back into plaintext. It is a crucial indicator for assessing the effectiveness of a decryption process, particularly in secure communication systems where instant access to the original data is essential.

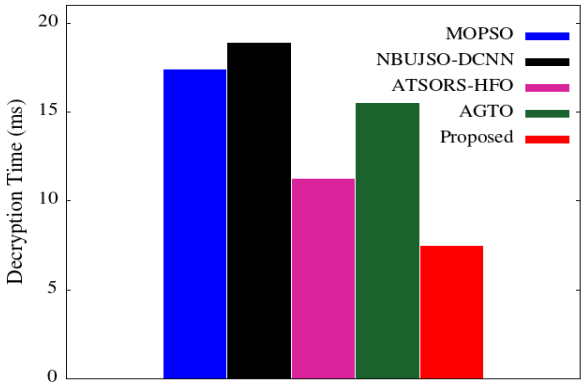


Fig.10. Comparison of decryption time

The decryption times (in milliseconds) of five distinct decryption algorithms — MOPSO, NBUJSO-DCNN, ATSORS-HFO, AGTO, and the suggested algorithm — are compared in Figure 10. Out of all of them, NBUJSO-DCNN takes the longest to decode data, at roughly 18.5 ms. The ATSORS-HFO method earned 12.9 ms, and the AGTO method earned 15.5 ms. In comparison, the proposed method achieved the lowest decryption time of 7 ms.

- ***Computational time (CT):*** The overall amount of time needed for a computer or system to complete a certain task or set of activities is referred to as computational time. It shows how long it takes to process an algorithm, carry out computations, or finish a particular software action.

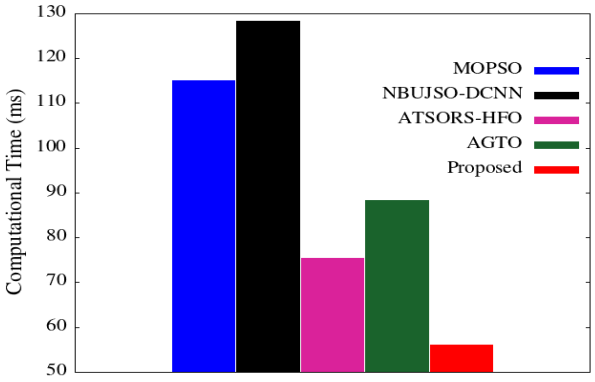


Fig.11. Comparison of computational time

The computational times (in milliseconds) of four distinct methods MOPSO, NBUJSO-DCNN, ATSORS-HFO, AGTO, and the suggested algorithm are compared in the figure 11. The NBUJSO-DCNN has the maximum roughly 127 milliseconds. The computation times for MOPSO and ATSORS-HFO are in the middle of these ranges; MOPSO is a little bit faster at around 115 milliseconds, while ATSORS-HFO is a little bit slower at about 75 milliseconds. The computation time of AGTO is approximately 85 milliseconds. Out of all of them, the suggested approach has the lowest computational time roughly 55 milliseconds.

Table 2. Overall performance analysis of proposed with existing method

Methods	RO	CA (%)	ET (ms)	DT (ms)	CT (ms)	PDR (%)	Energy (J)
MOPSO	0.51	89	1.0	17.0	115	90.5	1.45
NBUJSO-DCNN	0.559	85	15.5	18.5	127	87.2	1.62
ATSORS-HFO	0.25	94	7.5	12.9	75	93.4	1.28
AGTO	0.32	92	8.0	15.5	85	92.0	1.33
QIRP	0.41	90	6.8	14.5	97	91.7	1.38
CKKS	0.35	91	6.5	13.0	100	92.5	1.30
Proposed EQNN–ATBGVHEA	0.13	98.5	5.0	7.0	55	97.8	1.05

Table 2 presents a comparison of the overall performance of the proposed EQNN–ATBGVHEA method with several existing MANET routing and encryption approaches. Metrics such as Routing Overhead (RO), Clustering Accuracy (CA), End-to-End Transmission Time (ET), Data Transfer Time (DT), Computation Time (CT), Packet Delivery Ratio (PDR), and Energy Consumption (J) are considered. The proposed method achieves the lowest RO (0.13), highest CA (98.5%), and the fastest ET, DT, and CT values among all compared methods, demonstrating efficient and rapid routing. Furthermore, it ensures the highest PDR (97.8%) while consuming the least energy (1.05 J), highlighting its effectiveness in secure, energy-efficient, and reliable data transmission. In comparison, quantum-inspired routing (QIRP) and homomorphic encryption-based schemes (CKKS) improve either routing or security individually, but the proposed EQNN–ATBGVHEA simultaneously optimizes both, establishing its superiority over conventional and recent approaches.

- ***Throughput:*** Throughput refers to the number of packets delivered via the system within a specified time frame. The throughput rate in the proposed model is expressed in kilobits per second (Kbps). Equation (28) provides the formulation defined for the throughput calculation.

$$Throughput = \frac{Sentpackets + Packetsize}{Time} \tag{28}$$

The suggested method is compared with the previous methods like ATSORS-HFO, NBUJSO-DCNN, MOPSO, and AGTO whose throughput (measured in Mbps) and compared in the figure 12 as the count of nodes increases from 20 to 100. While it continues to lag behind the suggested method, NBUJSO-DCNN likewise exhibits a consistent rise in throughput. AGTO, ATSORS-HFO, and MOPSO all function differently, with MOPSO exhibiting the lowest throughput overall. The suggested EQNN-ATBGVHEA technique achieves the maximum throughput at all node counts, routinely outperforming the others. Table 3 gives the comparison of throughput for different mobility.

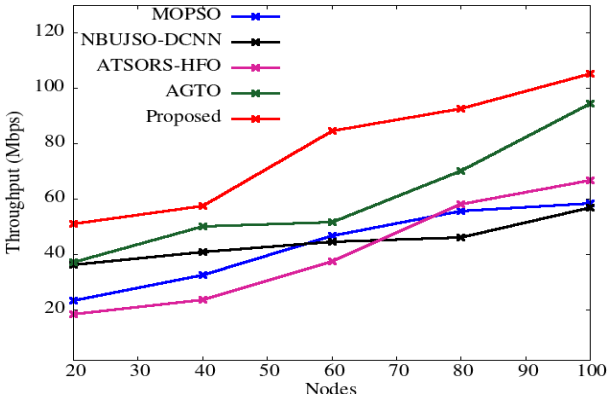


Fig.12. Throughput comparison for different nodes

Table 3. Comparison of throughput for different mobility

Methods	Node mobility (ms)			
	5	10	15	20
MOPSO	22	28	41	46
NBUJSO-DCNN	37	38	39	42
ATSORS-HFO	18	20	50	60
AGTO	42	41	61	92
Proposed	56	81	85	100

- ***Residual energy (RE):*** The crucial performance metric known as residual energy indicates the nodes' present energy status within the network. The RE for the i^{th} node is calculated in equation (29).

$$R_{Ei} = (\sum_i = 1^n E_i(Ini) - E_i(cur))/n \tag{29}$$

here, $E_i(Ini)$ indicates the initial energy level and $E_i(cur)$ denotes the current energy level of the i^{th} node.

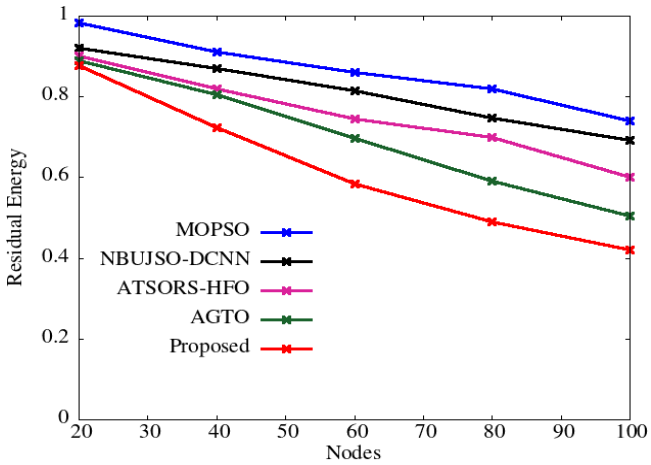


Fig.13. Residual energy comparison for different nodes

As the count of nodes rises from 20 to 100, the figure 13 compares the residual energy of exiting methods like MOPSO, NBUJSO-DCNN, ATSORS-HFO, AGTO, with the proposed EQNN-ATBGVHEA approach. As the number of nodes increases, MOPSO and ATSORS-HFO show a sharp fall in residual energy, but NBUJSO-DCNN and AGTO show a steadier decline. The suggested approach routinely performs greater than the others in terms of residual energy preservation. All things considered, the suggested algorithm exhibits exceptional energy efficiency. Table 4 give the comparison of RE for different mobility.

Table 4. Comparison of RE for different mobility

Methods	Node mobility (ms)			
	5	10	15	20
MOPSO	0.99	0.78	0.85	0.75
NBUJSO-DCNN	0.91	0.84	0.8	0.79
ATSORS-HFO	0.92	0.79	0.76	0.65
AGTO	0.82	0.79	0.65	0.57
Proposed	0.71	0.6	0.5	0.44

- ***Packet Delivery Ratio (PDR):*** The effectiveness and dependability of data transmission are gauged by the PDR, a critical network communications performance statistic. It is the percentage of source packets that are transferred to destination packets that are delivered. The PDR can be calculated using equation (30).

$$PDR = \frac{P_{received}}{P_{sent}} \tag{30}$$

where, $P_{received}$ indicates quantity of packets received by destination and P_{sent} indicates the count of packets sent by the source.

The packet delivery ratio (PDR) comparison of MOPSO, NBUJSO-DCNN, ATSORS-HFO, AGTO methods, and the proposed algorithm is presented in Figure 14 as the number of nodes increases from 20 to 100. MOPSO has the lowest PDR, particularly as the number of nodes increases. The PDR levels of NBUJSO-DCNN, ATSORS-HFO, and AGTO vary, with ATSORS-HFO typically outperforming NBUJSO-DCNN and AGTO. Maintaining a high PDR is regularly achieved by the suggested EQNN-ATBGVHEA method better than the others. Table 5 provides a comparison of PDR for different mobility levels.

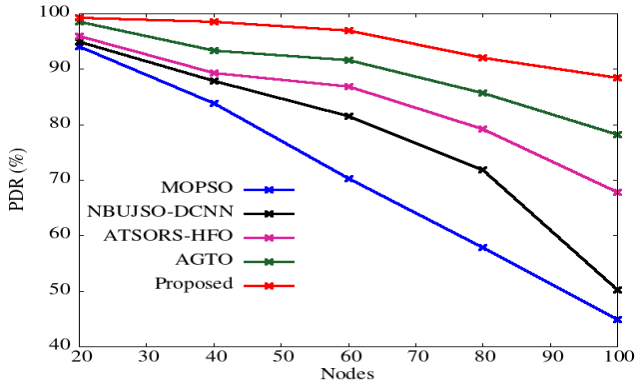


Fig.14. PDR comparison for different nodes

Table 5. Comparison of PDR for different mobility

Methods	Node mobility (ms)			
	5	10	15	20
MOPSO	83	70	55	45
NBUJSO-DCNN	89	85	75	53
ATSORS-HFO	90	89	85	68
AGTO	95	92	89	79
Proposed	99	98	95	89

- ***Delay:*** A delay is the amount of time it takes for packets to travel from their source to their destination. If not, it is the amount of the time required by the server to handle the request. In this case, the seconds delay is computed. Equation (31) gives a description of the expression for the delay calculation.

$$Delay = packetdeparttime - arrivedtime \tag{31}$$

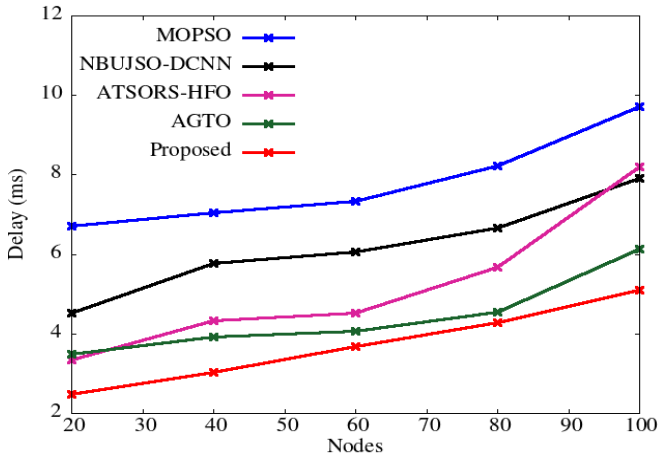


Fig.15. Delay comparison for different nodes

Table 6. Comparison of delay for different mobility

Methods	Node mobility (ms)			
	5	10	15	20
MOPSO	6.8	7	7.9	9.7
M,	5.6	5.9	6.2	6.9
ATSORS-HFO	4.2	4.4	5.2	7
AGTO	3.9	4	4.2	5.2
Proposed	3	3.6	4	4.2

The delay comparison of MOPSO, NBUJSO-DCNN, ATSORS-HFO, AGTO methods, and the proposed EQNN-ATBGVHEA algorithm is presented in Figure 15 as the number of nodes increases from 20 to 100. As the number of nodes increases, MOPSO exhibits the greatest latency. While ATSORS-HFO typically outperforms NBUJSO-DCNN

and AGTO, all three models exhibit differing degrees of latency. When it comes to minimizing delay, the suggested algorithm continuously beats the others. Table 6 gives the comparison of delay for different mobility.

- ***Network Lifetime (NL):*** In WSN, where nodes are frequently powered by finite energy sources like batteries, network longevity is crucial phrase. It is usually refers to the amount of time that a network may continue to function and do its intended duties before the first node or a sizable portion of nodes run out of energy.

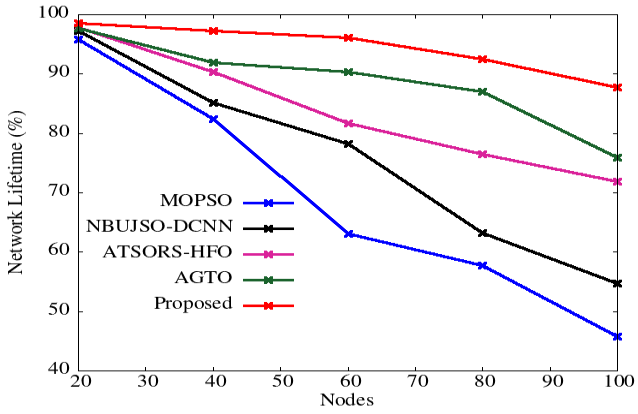


Fig.16. NL comparison for different nodes

The network lifetime comparison of MOPSO, NBUJSO-DCNN, ATSORS-HFO, AGTO methods, and the suggested EQNN-ATBGVHEA algorithm is given in the figure 16 as the number of nodes rises from 20 to 100. In particular, when there are more nodes, MOPSO shows the shortest network lifetime. Network lifespan is displayed differently by NBUJSO-DCNN, ATSORS-HFO, and AGTO; in general, ATSORS-HFO outperforms NBUJSO-DCNN and AGTO. In terms of prolonging NL, the suggested algorithm consistently outperforms the others. Table 7 give the comparison of NL for different mobility.

Table 7. Comparison of NL for different mobility

Methods	Node mobility (ms)			
	5	10	15	20
MOPSO	82	64	59	45
NBUJSO-DCNN	86	80	65	55
ATSORS-HFO	93	84	78	72
AGTO	94	92	90	78
Proposed	98	97	94	89

4.3. Statistical Analysis

To validate the performance of the proposed EQNN–ATBGVHEA framework, each experiment was repeated five times using different random seeds and the mean values of all metrics were calculated. The standard deviation (SD) was computed for each metric to quantify variability and assess consistency. A paired t-test was conducted to compare the proposed method against each baseline (MOPSO, NBUJSO-DCNN, ATSORS-HFO, and AGTO) and evaluate statistical significance at a 95% confidence level ($p < 0.05$). All results demonstrate that the improvements in routing overhead, clustering accuracy, encryption/decryption time, throughput, PDR, and network lifetime are statistically significant. Error bars in the figures for ET, DT, CT, PDR, and RE further illustrate the reproducibility and robustness of the proposed approach under varying MANET conditions. To ensure fair comparisons, all baseline methods were implemented with parameters optimized according to the original studies, and hyperparameter tuning was applied uniformly to avoid bias toward the proposed model. This controlled setup guarantees that observed performance improvements are attributable to the EQNN–ATBGVHEA framework rather than differences in parameter selection or experimental conditions.

Table 8 presents a comparison of the overall performance of the proposed EQNN–ATBGVHEA method with existing MANET routing and encryption techniques, including MOPSO, NBUJSO-DCNN, ATSORS-HFO, AGTO, QIRP, and CKKS. Each metric Routing Overhead (RO), Clustering Accuracy (CA), Encryption Time (ET), Decryption Time (DT), Computation Time (CT), Packet Delivery Ratio (PDR), and Energy Consumption is reported as the mean ± standard deviation (SD) over five repeated simulation runs to ensure statistical reliability. The proposed EQNN–ATBGVHEA consistently achieves the lowest RO (0.13 ± 0.008), highest CA ($98.5 \pm 0.7\%$), fastest ET, DT, and CT, along with the highest PDR ($97.8 \pm 0.6\%$) and minimal energy consumption (1.05 ± 0.03 J), demonstrating statistically significant improvements ($p < 0.05$) over baseline and recent methods. This confirms the robustness, reproducibility, and effectiveness of integrating EQNN-based routing with ATBGVHEA-secured transmission under realistic MANET

conditions.

Table 8. Statistical analysis of the proposed approach

Methods	RO	CA (%)	ET (ms)	DT (ms)	CT (ms)	PDR (%)	Energy (J)
MOPSO	0.51 ± 0.02	89 ± 1.5	12.0 ± 0.8	17.0 ± 1.2	115 ± 5	90.5 ± 1.0	1.45 ± 0.05
NBUJSO-DCNN	0.559 ± 0.03	85 ± 1.8	15.5 ± 1.0	18.5 ± 1.5	127 ± 6	87.2 ± 1.2	1.62 ± 0.07
ATSORS-HFO	0.25 ± 0.01	94 ± 1.2	7.5 ± 0.5	12.9 ± 0.7	75 ± 4	93.4 ± 0.8	1.28 ± 0.04
AGTO	0.32 ± 0.015	92 ± 1.0	8.0 ± 0.6	15.5 ± 0.8	85 ± 5	92.0 ± 0.9	1.33 ± 0.05
QIRP	0.41 ± 0.02	90 ± 1.3	6.8 ± 0.5	14.5 ± 0.7	97 ± 4	91.7 ± 1.0	1.38 ± 0.05
CKKS	0.35 ± 0.018	91 ± 1.4	6.5 ± 0.4	13.0 ± 0.6	100 ± 5	92.5 ± 0.9	1.30 ± 0.04
Proposed EQNN–ATBGVHEA	0.13 ± 0.008	98.5 ± 0.7	5.0 ± 0.3	7.0 ± 0.4	55 ± 3	97.8 ± 0.6	1.05 ± 0.03

4.4. Discussion

The results of the proposed EQNN–ATBGVHEA framework demonstrate its practical applicability in real-world MANET scenarios, such as disaster response, IoT sensor networks, and military communications, where nodes are highly mobile, battery-constrained, and network topology changes frequently. By simulating the network in NS3 under realistic mobility patterns and traffic loads, and repeating experiments with multiple random seeds, we ensured robustness and reproducibility. Statistical analysis, including standard deviations and paired t-tests, confirms that improvements in routing overhead, clustering accuracy, encryption/decryption time, and packet delivery ratio are significant. Error bars further highlight the consistency of the proposed method across varying conditions. Importantly, baseline comparisons were conducted under identical settings to ensure fairness, demonstrating that EQNN–ATBGVHEA achieves a superior balance between secure routing, energy efficiency, and overall network performance.

5. Conclusions

Secure data transmission routing is crucial in MANETs (Mobile Ad Hoc Networks) to ensure data integrity and confidentiality in the face of dynamic network conditions. This work proposes a novel Equivariant Quantum Neural Networks with Adaptive Tangent Brakerski-Gentry Vaikuntanathan Homomorphic Encryption algorithm (EQNN-ATBGVHEA) - based secure routing in MANET. The suggested approach comprises of three steps: CH selection, optimal path selection, and secure data transfer. Initially, the BOA chooses the CH and sends the message through the constructed path. Once the clusters are established, data is transferred between the sender and receiver. To achieve the best route selection, we developed the EQNN technique, which incorporates a neural network for rapid route selection. EQNN resolves the issues of local optimal by constructing new FF based on RE, CA, and delay. After the optimal path selection, Data transfer is secured by innovative ATBGVHEA technique.Furthermore, this method is built using NS3, and the variables are determined. Additionally, the acquired results are compared with previous approaches to validate the efficiency of the proposed strategy. The presented method achieved a clustering accuracy of 98.5%, a computational time of 55ms, and a residual energy of 0.44. In future, explore mechanisms to counteract potential attacks or adversarial threats specific to quantum-enhanced encryption and routing.

Author Contributions Statement

V. Ravi Kumar, Prasada Reddy. M.M.-Conceptualization, Methodology, Software, Formal analysis, Investigation, Resources, Validation, Data Curation, Writing - Original Draft, Writing - Review & Editing, Supervision, Project administration.

B. Nancharaiah -Conceptualization, Methodology, Software, Formal analysis, Writing - Original Draft, Writing - Review & Editing, Visualization.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

Authors do not have any conflict of interest to declare.

Funding Declaration

No funding is provided for the preparation of manuscript.

Data Availability Statement

Data sharing not applicable to this article.

Ethical Declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Acknowledgments
Not applicable.

Declaration of AI Generative in Scholarly Writing
AI tools were used only for minor grammar checking and language refinement. All methodological development, analysis, and technical content were entirely carried out by the authors without AI assistance.

Abbreviations
ACGWO -Adaptive Chaotic Grey Wolf Optimisation
AGTO - Artificial Gorilla Troops Optimizer
AOMDV - Ad hoc On-demand Multipath Distance Vector
ATBGVHEA- Adaptive Tangent Brakerski-Gentry Vaikuntanathan Homomorphic Encryption algorithm
BOA - Bowerbird Optimization Algorithm
BS - Base station
CA - Clustering Accuracy
CCMAP-DCNN - Convolutional layer in a deep convolutional neural network concatenated with a max-average pooling layer
CGRUN - Convolutional Gated Recurrent Unit Network
CH - Cluster head
CT - Computational time
CTAA - Cluster Trust Adaptive Acknowledgment
DSR - Dynamic Source Routing
DT - Data Transfer Time
DT - Decryption time
EQNN - ATBGVHEA Equivariant Quantum Neural Networks with Adaptive Tangent Brakerski-Gentry Vaikuntanathan Homomorphic Encryption algorithm
ET - End-to-End Transmission Time
ET - Encryption time
FAES - False Key Build Advanced Encryption Standard
FF - Fitness function
HETKA - Hybrid Effective Trusted Knowledge Algorithm
KF - Kalman Filters
MANETs - Mobile Ad-hoc Networks
NBUJSO - Namib Beetle Upgraded Jellyfish Search Optimization
NL - Network Lifetime
OK - Optimal Keys
PDR - Packet Delivery Ratio
QIRP - Quantum-Inspired Routing Protocol
QoS - Quality of service
RE - Residual energy
RO - Routing Overhead
SSARM-SCA - Sine Cosine algorithm search and Salp Swarm Algorithm with Replacement Method

References

[1] S. Singh, A. Pise, O. Alfarraj, A. Tolba, B. Yoon, “A cryptographic approach to prevent network incursion for enhancement of QoS in sustainable smart city using MANET”. Sustainable Cities and Society. Vol.79, p.103483, 2022.
[2] S. Dalal, B. Seth, V. Jaglan, M. Malik, Surbhi, N. Dahiya, U. Rani, DN. Le, YC.Hu, “An adaptive traffic routing approach toward load balancing and congestion control in Cloud–MANET ad hoc networks”. Soft Computing. Vol.26, No.11, pp.5377-88, 2022.
[3] B. Reddy, B. Dhananjaya, “The AODV routing protocol with built-in security to counter blackhole attack in MANET”. Materials Today: Proceedings. Vol.50, pp.1152-8, 2022.
[4] A. Ali, A. Ali, F. Masud, MK. Bashir, AH. Zahid, G. Mustafa, Z. Ali, “Enhanced fuzzy logic zone stable election protocol for cluster head election (E-FLZSEPFCH) and multipath routing in wireless sensor networks”. Ain Shams Engineering Journal. Vol.15, No.2, p.102356, 2024.
[5] S. Li, B. Gong, “Developing a reliable route protocol for mobile self-organization networks”. High-confidence computing. Vol.4, No.3, p.100194, 2024.
[6] S. Shafi, DV. Ratnam, “Ant-colony optimization based energy aware cross layer routing protocol to improve route reliability in MANETs”. Wireless Personal Communications. Vol.129, No.3, pp.1865-79, 2023.

[7] SA. Alghamdi, Novel trust-aware intrusion detection and prevention system for 5G MANET–Cloud. International Journal of Information Security. Vol.21, No.3, pp.469-88, 2022.
[8] X. Wang, Y. Weng, H. Gao, "A low-latency and energy-efficient multimetric routing protocol based on network connectivity in VANET communication". IEEE Transactions on Green Communications and Networking. Vol.5, No.4, pp.1761-76, 2021.
[9] OT. Abdulhae, JS. Mandeep, M. Islam, "Cluster-based routing protocols for flying ad hoc networks (FANETs)". IEEE access. Vol.10, pp.32981-3004, 2022.
[10] K. Manasa, LM. Leo Joseph, "IoT security vulnerabilities and defensive measures in Industry 4.0". InArtificial Intelligence and Cyber Security in Industry 4.0 2023 Jun 14 (pp. 71-112). Singapore: Springer Nature Singapore.
[11] V. S. Murugan, B. Unhelkar, "Optimizing Mobile Ad Hoc Network cluster based routing: Energy prediction via improved deep learning technique". International Journal of Communication Systems, p.e5777, 2024.
[12] G. Rajeshkumar, M. V. Kumar, K. S. Kumar, S. Bhatia, A. Mashat, P. Dadheech, "An Improved Multi-Objective Particle Swarm Optimization Routing on MANET". Computer Systems Science & Engineering, Vol.44, No.2, (2023).
[13] S. Ravi, S. Matheswaran, U. Perumal, S. Sivakumar, S. K. Palvadi, "Adaptive trust-based secure and optimal route selection algorithm for MANET using hybrid fuzzy optimization". Peer-to-Peer Networking and Applications, Vol.16, No.1, pp.22-34, 2023.
[14] S. Selvaraj, M. Chakkaravarthy, "Enhancing security and efficiency in MANETs: a clustering-based approach with CGRUN and AGTO optimization for intrusion detection and path establishment". International Journal of Information Technology, pp.1-11, 2024.
[15] MR. Jose, SM. Vigila, "F-CAPSO: Fuzzy chaos adaptive particle swarm optimization for energy-efficient and secure data transmission in MANET". Expert Systems with Applications. Vol.234, p.120944, 2023.
[16] C. Manthiramoorthy, KM. Khan, "A Hybrid Effective Trusted Knowledge Algorithm for Effective Integrated Internet MANET based on Secure Data Transmission". In2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) 2023 (pp. 1-6). IEEE.
[17] P. Singh, M. Khari, S. Vimal, "EESSMT: an energy efficient hybrid scheme for securing mobile ad hoc networks using IoT". Wireless Personal Communications. Vol.126, No.3, pp.2149-73, 2022.
[18] Zhang, L. and Liu, Q., 2022. Optimisation of the routing protocol for quantum wireless Ad Hoc network. IET Quantum Communication, 3(1), pp.5-12.
[19] Su, Y., Wang, X.A., Du, W., Ge, Y., Zhao, K. and Lv, M., 2023. A secure data fitting scheme based on CKKS homomorphic encryption for medical IoT. Journal of High Speed Networks, 29(1), pp.41-56.
[20] S. Zhang, Y. Zhou, Q. Luo, "A complex-valued encoding satin bowerbird optimization algorithm for global optimization". Evolving Systems. Vol.12, pp.191-205, 2021.
[21] RT. Forestano, M. Comajoan Cara, GR. Dahale, Z. Dong, S. Gleyzer, D. Justice, K. Kong, T. Magorsch, KT. Matchev, K. Matcheva, EB. Unlu, "A comparison between invariant and equivariant classical and quantum graph neural networks". Axioms. Vol.13, No.3, p.160, 2024.
[22] S. Ahmad, S. Mehfuz, J. Beg, "An efficient and secure key management with the extended convolutional neural network for intrusion detection in cloud storage". Concurrency and Computation: Practice and Experience. Vol.35, No.23, p.e7806, 2023.

Authors' Profiles



I. V. Ravi Kumar was born in Kakinada, East Godavari district, India, in 1978. He received his BTech. degree in Electronics and Communication Engineering from JNTU, Kakinada Engineering College, JNTU University, Andhra Pradesh, India, in 2007, his M.Tech degree in VLSI System Design from JNTUK University, Kakinada in 2011. He is currently Research scholar, Department of ECE, GIET University, Gunupur-765022, Odisha, India. And also working as Assistant Professor, Department of ECE, Swarnandhra College of Engineering and Technology, Narsapur-534280, AP, India.



Prasada Reddy M. M. has established himself as a leading figure in Electronics and Computer Science Engineering through his impactful research and scholarly contributions. His extensive body of work includes over 50 published research papers and presentations at 40 conferences, highlighting his active engagement with the academic community. Dr. Reddy's innovative contributions are further recognized through the 2 patents he has been granted. As a prolific author, he has penned more than 10 influential books covering a broad spectrum of topics, including Antennas and Wave Propagation, Cloud Computing, Machine Learning, Internet of Things, Data Structures, Signals and Systems, Electromagnetic Theory and Transmission Lines, Embedded Real Time Systems, Artificial Intelligence, and Computer Communication. These books serve as key learning resources for students in numerous universities, demonstrating the significant impact of his work on engineering education. The translation of his book, Embedded Real Time Systems, into an impressive 14 languages, including Mandarin, further attests to the global relevance and impact of his scholarship. Dr. Reddy's current research interests are at the forefront of technological advancement, focusing on wireless communications, innovative 5G antenna design, and the rapidly evolving field of Natural Language Processing. Also, Mr. Reddy Worked as a Principal for reputed Engineering Colleges in Andhra and Telangana states, India.



B. Nancharaiah was born in Bhattiprolu, Guntur district, India, in 1976. He received his B.E. degree in Electronics and Communication Engineering from SRKR Engineering College, Bhimavaram, Andhra University, Andhra Pradesh, India, in 1999, his M.Tech degree in Electronics and Communication Engineering from Pondicherry Engineering College, Pondicherry Central University, in 2003, and his Ph.D. degree in Electronics and Communication Engineering from Jawaharlal Nehru Technological University Hyderabad, India, in 2017.

He is currently working as Professor and Head of the Department of Electronics and Communication Engineering at Usha Rama College of Engineering and Technology, Telaprolu, Vijayawada, Andhra Pradesh, India. With 23 years of teaching experience, he has published over 81 research papers in reputable national and international journals and conferences. He has also filed and published 37 patents. His research interests include wireless communications, VLSI, IoT, and networks.

How to cite this paper: I. V. Ravi Kumar, Prasada Reddy. M. M., B. Nancharaiah, "Adaptive Tangent Homomorphic Encryption with Equivariant Quantum Neural Networks for Secure Data Transmission Routing in MANET", International Journal of Computer Network and Information Security(IJCNIS), Vol.18, No.2, pp.126-148, 2026. DOI:10.5815/ijcnis.2026.02.08