www.ijarp.com ISSN 2456-9992 Page: 01-20
International Journal Advanced Research Publications
Research Article
Volume: 02
Issue: 07

ENERGY-AWARE QUANTUM SWARM OPTIMIZED ZERO TRUST FRAMEWORK FOR INTRUSION DETECTION AND PREVENTION IN MANET WITH 5G AND NXTG TECHNOLOGY

S. Kalaichelvi*[1], Dr. K. R. Ananth[2]

[1]*Research Scholar, Department of Computer Science, Nandha Arts and Science College (Autonomous), Erode - 638 052, Tamilnadu, India.*

[2]*Associate Professor & Head, Department of Computer Science, Nandha Arts and Science College (Autonomous), Erode - 638 052, Tamilnadu, India.*

Article Received: 26 May 2026, Article Revised: 14 June 2026, Published on: 04 July 2026

***Corresponding Author: S. Kalaichelvi**

Research Scholar, Department of Computer Science, Nandha Arts and Science College (Autonomous), Erode - 638 052, Tamilnadu, India.

Doi: https://doi-doi.org/101555/ijarp.8543

ABSTRACT

Mobile Ad Hoc Networks (MANETs) operating in 5G and Next-Generation (NxtG) environments require optimization techniques that can provide secure communication while minimizing energy consumption and computational overhead. To address the limitations of Golden Jackal Optimization (GJO), this paper introduces an Energy-Aware Quantum Swarm Optimized Zero Trust Framework (EAQSO-ZTF) to enhance security and energy efficiency in 5G and Next Generation MANET environments. The proposed EAQSO-ZTF employs a quantum-inspired swarm intelligence model in which mobile nodes in zero trust MANET environment are represented as particles within a probabilistic search space. An energy-aware initialization process selects nodes based on residual energy, trust level, and link stability, thereby reducing unnecessary participation of resource-constrained nodes. EAQSO-ZTF further incorporates a probabilistic position update mechanism that accelerates convergence and lowers computational cost compared with conventional iterative optimization approaches. To enhance adaptability, the swarm size is dynamically adjusted according to network density and mobility conditions. The fitness function integrates multiple performance metrics, including residual energy, packet delivery ratio, trust value, and link stability, ensuring balanced optimization of security and routing efficiency. A lightweight convergence criterion terminates the search process when further improvements become

negligible. From that,EAQSO-ZTF achieves improved energy efficiency, faster convergence, and reduced processing overhead, making it a suitable optimization solution for secure MANET operations in emerging 5G and NxtG communication environments.

KEYWORDS: MANETs, 5G Networks, NxtG, Swarm Intelligence, Energy Efficiency, Secure Routing, Link Stability.

I. INTRODUCTION

MANETs have emerged as a key communication paradigm for supporting dynamic and infrastructure-less connectivity in 5G and NxtG wireless environments. Their decentralized architecture enables flexible deployment in applications such as smart transportation, emergency response, military communications, and Internet of Things (IoT) networks. However, the highly dynamic topology, limited battery resources, and absence of centralized control make MANETs particularly vulnerable to routing attacks, malicious node behavior, and unauthorized access. Conventional intrusion detection and prevention mechanisms often struggle to maintain security while preserving energy efficiency, especially in large-scale and high-mobility network scenarios. Furthermore, existing optimization-based security approaches frequently incur significant computational overhead, resulting in increased energy consumption and reduced network lifetime.

In the state-of-the-art works, a Golden Jackal Cost Optimized Zero Trust Security framework integrated with blockchain technology (GJCOZTS-BCT)[1] was implemented for intrusion detection and prevention in MANETs operating in 5G and NxtG environments. The model enhances security through decentralized trust management and optimized attack detection. However, the application of blockchain and Golden Jackal Optimization increases computational complexity and energy consumption, which may affect resource-constrained mobile nodes.AHybrid Intelligence-Powered Secure Clustering and Trust-Optimized Routing (HISCTR) framework was implemented in [2] for next-generation MANET communications. This model enhances routing security, cluster stability, and network performance through intelligent decision-making mechanisms. But, it increased computational burden associated with hybrid optimization and trust evaluation processes.

A comprehensive review of machine learning and transfer learning approaches introduced for intrusion detection in 5G and beyond networks was presented in [3]. This study highlights the ability of advanced learning models to detect complex cyberattacks with high accuracy. However, most reviewed techniques depend on large training datasets and substantial

computational resources, limiting their applicability in lightweight MANET environments. A trust-aware intrusion detection and prevention system was planned in [4] for integrated 5G MANET-cloud networks. This framework strengthens network security by combining trust evaluation with intrusion prevention mechanisms. Though, it increases communication overhead and latency.An optimized fuzzy-based Ant Colony Optimization algorithm was presented in [5] for 5G-enabled MANETs. This approach improves route selection by considering multiple network parameters and fuzzy decision-making strategies. However, the algorithm may experience slower convergence when network size and node mobility increase significantly.The TFACR topology control algorithm was intended in [6] to enhance the performance of 5G-based MANETs through adaptive transmission coverage adjustment. This algorithm improves connectivity, throughput, and energy utilization under varying network conditions. Its limitation lies in the complexity of dynamically adjusting transmission ranges in rapidly changing topologies.

The survey of different trust-aware, optimization-assisted machine learning and deep learning intrusion detection systems designed for MANETs was investigated in [7]. Their study demonstrated that combining optimization algorithms with intelligent detection models can significantly improve attack detection rates. However, many of the surveyed methods suffer from high computational requirements and scalability challenges. A Dynamic Liquid Neural Network-based intrusion detection framework was implemented in [8] for zero trust environments. Thisframework adapts effectively to evolving attack patterns and provides improved detection capabilities in dynamic networks. But, the training and maintenance of neural architectures may require considerable processing resources and memory.

A hierarchical and privacy-preserving intrusion detection model was introduced in [9] for SAGIN-enabled Industrial IoT environments using Deep Q-Learning. Thismodel offers strong privacy protection and intelligent attack detection while supporting large-scale networks. However, the integration of multiple deep learning components increases implementation complexity and computational cost. An energy-efficient clustering and secure routing protocol based on hybrid evolutionary algorithms was developed in [10] for MANETs. Thisprotocol enhances network lifetime, routing security, and packet delivery performance through optimized cluster formation. However, hybrid evolutionary techniques often require extensive parameter tuning and may incur higher execution time in dense network scenarios.

II. LITERATURE SURVEY

An energy-efficient clustering mechanism combined with Enhanced Chicken Swarm Optimization and Adaptive Position Routing was presented in [11] for MANETs. Thismechanism improves cluster stability and reduces energy expenditure during route formation. However, the optimization process may become computationally intensive when the number of mobile nodes increases significantly. A secure optimization-based routing algorithm was designed in [12] that select reliable communication paths while maintaining network performance. Thisalgorithm enhances routing security and packet transmission efficiency in dynamic MANET environments. But, processing overhead required for continuous route optimization and security assessment was more.

A hybrid Osprey–Fire Hawk Optimization-based routing protocol was intended in [13] to achieve energy-efficient route selection in MANETs. This protocol improves routing quality by considering multiple constraints such as energy consumption and path reliability. However, integrating multiple optimization techniques increases algorithmic complexity and execution time.An ensemble optimization framework was designed in [14] for achieving secure, low-latency, and energy-efficient MANET communication with intrusion detection support. Thisframeworkimproves attack detection capability while reducing communication delays. However, the ensemble optimization strategy may require additional computational resources for real-time deployment.A hybrid adaptive clustering mechanism was planned in [15] for dynamic MANET environments. Thismechanismeffectively improves cluster maintenance, network scalability, and energy utilization under varying mobility conditions. Though, frequent cluster reconfiguration can formulate additional communication overhead. A trust-aware routing framework was developed in [16] that combine federated learning with multi-objective optimization to enhance MANET security. This framework strengthens privacy preservation and improves routing decisions without centralized data sharing. However, federated learning introduces synchronization and communication costs among participating nodes.

An energy-aware and trust-based secure routing approach was intended in [17] where it utilizes swarm intelligence techniques to improve routing reliability and network lifetime. The method effectively balances security and energy efficiency by selecting trustworthy nodes for communication. Nevertheless, the optimization process may require additional iterations under highly dynamic network conditions, resulting in increased processing overhead.A Zero Trust Architecture-based attack detection framework was presented in [18] for securing 6G edge computing environments. This framework provides continuous

verification and improved protection against sophisticated cyber threats. However, implementing Zero Trust principles may increase authentication overhead and resource consumption in highly dynamic networks.

A secure O-RAN optimization framework was designed in [19] that integrate Zero Trust principles with federated learning for 6G networks. This framework improves trustworthiness, privacy preservation, and intelligent network management. Nevertheless, the combination of federated learning and Zero Trust mechanisms can increase deployment complexity and operational costs. Zero Trust-based mobile network security architecture was introduced in [20] to strengthen access control and continuous authentication in modern wireless networks. The architecture enhances resilience against insider and external attacks while supporting flexible security management. However, it increased signaling and verification overhead associated with continuous trust assessment.

To address the aboveproblems, there is a need for an intelligent security framework capable of simultaneously improving threat detection accuracy, resource utilization, and network sustainability. Although Zero Trust security models provide continuous verification and access control, their integration into MANET environments remains limited due to resource constraints and frequent topology changes. In addition, many existing swarm-based optimization techniques suffer from slow convergence and excessive processing requirements. Motivated by these limitations, this work proposes an EAQSO-ZTF for intrusion detection and prevention in MANETs. The EAQSO-ZTFcombines energy-conscious optimization, trust-driven decision making, and quantum-inspired swarm intelligence to enhance security performance while reducing computational complexity and energy consumption in 5G and NxtG communication networks.The key contributions of EAQSO-ZTFis described as,

- ❖ The EAQSO-ZTF integrates energy-aware node selection, trust evaluation, and continuous authentication to strengthen intrusion detection and prevention capabilities.
- ❖ A quantum-inspired swarm optimization strategy is introduced to reduce computational complexity, accelerate convergence, and minimize energy consumption. The proposed mechanism dynamically adapts swarm size and optimization processes according to network conditions, improving network lifetime and resource utilization.
- ❖ The EAQSO-ZTF employs a multi-parameter fitness function incorporating residual energy, trust value, packet delivery ratio, and link stability to identify secure and reliable communication paths. This approach improves attack detection accuracy, routing efficiency,

and overall network resilience against malicious activities in highly dynamic MANET environments.

III. PROPOSED RESEARCH METHODOLOGY

The EAQSO-ZTF is introduced to achieve secure and energy-efficient intrusion detection and prevention in MANETs operating in 5G and NxtG communication environments. The EAQSO-ZTF combines energy-aware node selection, quantum-inspired swarm optimization, adaptive swarm management, and Zero Trust security principles to identify optimal routing paths while detecting and isolating malicious nodes. The primary contribution of this work lies in integrating an energy-aware node participation mechanism with a quantum-inspired swarm optimization strategy, which significantly reduces computational complexity and energy consumption while maintaining fast convergence during route optimization. The EAQSO-ZTF employs a multi-objective fitness evaluation function that considers key network parameters such as residual node energy, packet delivery ratio, communication delay, link stability, and trust value to identify optimal secure routing paths and detect malicious nodes effectively. In addition, the proposed EAQSO-ZTF incorporates a trust-based intrusion detection mechanism that continuously evaluates node behavior to isolate suspicious nodes and prevent malicious activities within the network. By combining energy-efficient optimization with intelligent security monitoring, the EAQSO-ZTF enhances network reliability, intrusion detection accuracy, and overall system performance, making it suitable for secure communication in highly dynamic 5G and Next-Generation MANET environments. The architecture diagram ofEAQSO-ZTF is presented in Figure 1.

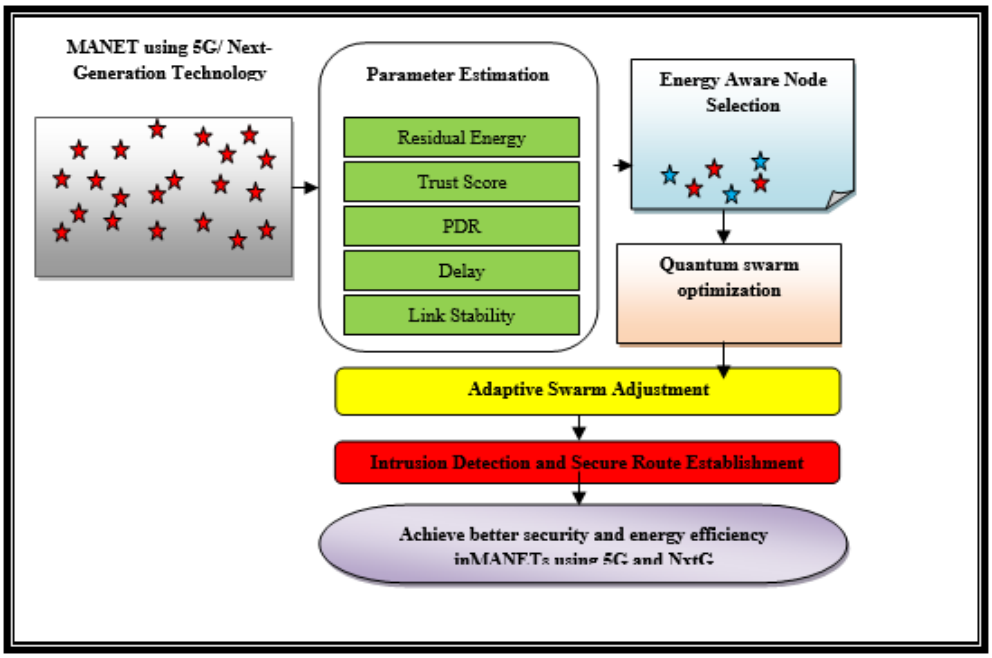

Figure 1 Overall Process of EAQSO-ZTF for Secure and Energy-Efficient Intrusion Detection.

As presented in above Figure 1, overall methodology ofEAQSO-ZTF consists of six phases: network initialization, parameter estimation, energy-aware node selection, quantum swarm optimization, adaptive swarm adjustment, and intrusion detection with secure route establishment.

Network Initialization and Parameter Estimation

Let consider zero trust MANET network using 5G and NxtG technology where it includes 'N' mobile node which mathematically described as,

$$M = n_1, n_2, n_3, \ldots, n_N \quad (1)$$

In equation (1),each mobile node (n_i) is characterized by key network parameters, including residual energy (RE), trust score (TS), packet delivery ratio (PDR), delay (D), and link stability ((LS).These parameters are continuously monitored to support secure and efficient routing decisions.The residual energy of node (i) is mathematically calculated with the support of below equation,

$$RE_i = E_{initial} - E_{consumed} \quad (2)$$

In equation (2), '$E_{initial}$' is the initial energy and '$E_{consumed}$' is the energy utilized during communication.Then, trust score of node (i) is determined based on its successful packet forwarding behavior using below mathematical formulation,

$$TS_i = \frac{N_{SF}}{N_{SF}+N_{UF}} \quad (3)$$

In equation (3), $N_{SF}$and N_{UF} denote the numbers of successfully and unsuccessfully forwarded packets respectively. Followed by,packet delivery ratio (PDR) is computed as,

$$PDR_i = \frac{N_{PR}}{N_{PS}} \quad (4)$$

In equation (4), N_{PR} is the number of packets successfully received and N_{PS} is the total number of transmitted packets. Subsequently, the transmission delay of node (i) is expressed as,

$$D_i = T_r - T_s \quad (5)$$

In equation (5),T_r and $T_s$represent packet transmission and reception times, respectively. After that, link stability between communicating nodes is calculated as,

$$LS_i = \frac{T_A}{T_O} \quad (6)$$

In equation (6),$T_A$denotes the duration for which the communication link remains active and $T_O$represents the total observation time.

Energy-Aware Node Selection

To reduce unnecessary computational burden and prolong network lifetime, only nodes possessing sufficient residual energy are considered for optimization. The candidate node set (CNS) is defined as,

$$CNS = \{n_i \in M | RE_i \geq E_{Th}\} \quad (7)$$

In equation (7), E_{Th} is the predefined minimum energy threshold. Nodes with energy levels below the threshold are excluded from optimization and routing participation, thereby preventing rapid battery depletion and network partitioning.

Quantum Swarm Initialization and Fitness Evaluation

Each feasible routing solution is represented as a particle in the swarm population.The particle population is represented as,

$$P = \{p_1, p_2, .., p_m\} \quad (8)$$

In equation (8),m denotes the swarm size.Each particle maintains its current position (X_j), personal best position ($PBest_j$), and the overall global best position ($GBest$) using,

$$PBest_j = X_j \quad (9)$$

$$GBest = arg\max_{1 \leq j \leq m}\{Fitness(X_j)\} \quad (10)$$

The quality of each routing solution is evaluated using a fitness function that jointly considers energy efficiency, trustworthiness, packet delivery performance, delay, and link reliability. From that, fitness function is formulated as,

$$Fitness(X_j) = \omega_{re} RE_i + \omega_{ts} TS_i + \omega_{pdr} PDR_i + \omega_{ls} LS_i - \omega_d D_i \quad (11)$$

Subject to $\omega_{re} + \omega_{ts} + \omega_{pdr} + \omega_{ls} + \omega_d = 1$

In equation (11), $\omega_{re}, \omega_{ts}, \omega_{pdr}, \omega_{ls}, \omega_d$ are weight coefficients assigned to each metric i.e.residual energy, trust score, packet delivery ratio, delay, and link stability.A larger fitness value indicates a more secure, reliable, and energy-efficient routing path.

Quantum-Inspired Position Update

On the contrary to conventional swarm algorithms that depend on velocity updates, EAQSO-ZTF employs a quantum-behavior-based search mechanism. The movement of particles is governed by probabilistic attraction toward promising regions of the search space.The mean best position of the swarm m_{best} is calculated as,

$$m_{best} = \frac{1}{m} \sum_{j=1}^{m} PBest_i \quad (12)$$

The particle position is mathematically updated using,

$$X_j^{(t+1)} = m_{best} + \beta \left| GBest^{(t)} - X_j \right| \ln \frac{1}{r_j^t} \quad (13)$$

In equation (13), $X_j^{(t)}$ describes the position of particle j at iteration t, $X_j^{(t+1)}$ denotes updated position of particle, β defines contraction–expansion coefficient, $r_j^t \in (0,1)$ refers uniform random number. The personal best position of the j^{th} particle is updated using,

$$PBest_j^{(t+1)} = \begin{cases} X_j^{(t+1)}, if\ Fitness\left(X_j^{(t+1)}\right) > Fitness(PBest_i^{(t)}) \\ PBest_i^{(t)}, otherwise \end{cases} \quad (14)$$

In equation (14), $PBest_i^{(t)}$ represents the personal best position of particle j at iteration t, $X_j^{(t+1)}$ describes the updated particle position, and $Fitness\ (.)$ refersfitness function.The global best solution is selected from all personal best particles based on the maximum fitness value and itobtained as,

$$GBest_j^{(t+1)} = arg \max_{1 \le j \le m} \left\{ F(PBest_i^{(t+1)}) \right\} \quad (15)$$

In equation (15), $GBest_j^{(t+1)}$ represents global best solution at iteration $t+1$, m refers the swarm size, $F(PBest_i^{(t+1)}$ defines the fitness value of the personal best position of particle j.

Adaptive Swarm Size Adjustment

To enhance energy efficiency and reduce computational overhead, the swarm population is dynamically adjusted according to the network stability factor. The network stability (NS) is calculated as,

$$NS = \frac{1}{N}\sum_{i=1}^{N} LS_i \quad (16)$$

Then, adaptive swarm adjustment rule is mathematically described as,

$$m_{new} = \begin{cases} m(1-\gamma), if NS > NS_{th} \\ m, \quad otherwise \end{cases} \quad (17)$$

In equation (17),m describes current swarm size, m_{new} refer updated swarm size, γ defines swarm reduction coefficient and$NS_{th}$is network stability threshold.This adaptive mechanism decreases computational complexity during stable network conditions while maintaining sufficient search diversity in dynamic environments.

Zero Trust-Based Intrusion Detection

Following the Zero Trust principle, every node is continuously evaluated before participating in routing operations.The intrusion detection decision is formulated as,

$$ID_i = \begin{cases} 1, if\ TS_i < T_{th} \\ 0, if\ TS_i \geq T_{th} \end{cases} (18)$$

In equation (18),$ID_i = 1$indicates a malicious node,$ID_i = 0$indicates a legitimate node whereas T_{th} defines trust threshold. Nodes identified as malicious are removed from routing operations and excluded from subsequent optimization iterations.After the optimization process, the routing path associated with the final global best particle is selected as the optimal secure route.As a result, the proposed EAQSO-ZTF optimizes routing efficiency, energy utilization, trust management, and intrusion detection for secure MANET communications in 5G and Next-Generation network environments.

The algorithmic steps of EAQSO-ZTF is demonstrated as,

Input: Number of nodes in MANET using 5G and Next generation technology
Output: Find optimal and secure routing path and intrusion detection decision
Step 1:Begin
Step 2: Initialize MANET with N mobile nodes
Step 3:For each node i in network
Step 4: Calculate residual energy, trustscore, PDR, D, LS
// **Energy-Aware Node Selection**
Step 5:For each node i
Step 6: If $RE_i \geq E_{Th}$

Step 7: Add node i to CandidateNodeSet
Step 8: End If
Step 9:End For
// Swarm Initialization
Step 10: Initialize particles randomly from CandidateNodeSet
Step 11: For each particle j
Step 12: Initialize position X_j
Step 13: Initialize $PBest_j$
Step 14: End For
// Determine $GBest$among all particles
Step 15: For $iter = 1\ to\ MaxIter$
Step 16: For each particle j
Step 17: Compute $Fitness = f(RE, TS, PDR, D, LS)$
Step 18: Quantum Position Update
Step 19: Update Position(X_j) using probabilistic quantum model
Step 20:If ($Fitness(X_j) > Fitness(PBest_j)$, then
Step 21:$PBest_j = Position(X_j)$
Step 22:End If
Step 23:End For
Step 24: Update $GBest$from all $PBest$ particles
Step 25: Adaptive Swarm Adjustment
Step 26:If network stability is high, **then**
Step 27: Reduce swarm size
Step 28:Else
Step 29: Maintain swarm size
Step 30:End If
Step 31:End For
// Intrusion Detection Decision
Step 32:If ($TS_i < T_{th}$)
Step 33: Find node as malicious
Step 34: Isolate node from routing path
Step 35:Else
Step 36: Find node as Legitimate
Step 37:End If
Step 38: Select GBest node as optimal for secure routing path
Step 39:End

Algorithm 1Energy-Aware Quantum Swarm Optimized Zero Trust Frameworks

As presented in the above algorithm, the process of EAQSO-ZTF starts by deploying a zero trust MANET environment composed of mobile nodes and assigning essential network attributes, including residual energy, mobility characteristics, and trust levels. To improve resource utilization and minimize processing overhead, only nodes that satisfy a predefined energy threshold are considered for the optimization process. Each feasible routing path is modeled as a particle within the swarm, and an initial set of particles is generated across the

search space. The quality of every particle is assessed through a fitness function that incorporates multiple performance indicators such as residual energy, packet delivery ratio, transmission delay, link stability, and trust score. Based on the computed fitness values, the personal best and global best solutions are determined. The particles are then updated using a quantum-inspired probabilistic search strategy that promotes efficient exploration of the solution space while guiding the search toward promising regions. The optimization procedure is repeated until the stopping criterion is reached. Upon convergence, the optimal solution is selected to establish a secure routing path. In addition, nodes exhibiting trust values below the specified threshold are classified as malicious and excluded from routing activities, thereby enabling effective intrusion detection and prevention within the network.

4. SIMULATION SETUP

.The performance of the proposed EAQSO-ZTF is evaluated using NS-3. A MANET environment is created to emulate dynamic wireless communication scenarios in 5G and NxtG networks. Mobile nodes are randomly distributed within a predefined simulation area and communicate through multi-hop wireless links. The Random Waypoint Mobility Model is employed to represent node movement, allowing the network topology to change dynamically during the simulation period.The simulation considers key network parameters such as residual energy, trust score, packet delivery ratio, transmission delay, and link stability for routing and intrusion detection decisions. The proposed EAQSO-ZTF is integrated with the MANET routing process, where energy-aware node selection and quantum swarm optimization are used to identify secure communication paths. To evaluate security performance, both legitimate and malicious nodes are introduced into the network. Nodes with trust values below the predefined threshold are classified as malicious and isolated from routing operations according to the Zero Trust policy.The metrics considered for simulation is shown in Table 2.

Table 1 Simulation Constraints.

Metrics	Values
Network Simulator	NS-3
Simulation Area	1000 m × 1000 m
Number of Mobile Nodes	250
Node Deployment	Random
Mobility Model	Random Waypoint
Speed of Nodes	1 – 20 m/s
Simulation Time	250 s
MAC Protocol	IEEE 802.11

Traffic Type	CBR (Constant Bit Rate)
Packet Size	512 bytes
Initial Battery Energy	100 J
Transmission Range	250

The performance of proposedEAQSO-ZTF is compared against with conventional GJCOZTS-BCT [1] and HISCTR [2]. The performance of proposed GJCOZTS-BCT is tested using metrics such as packet delivery rate, communication overhead,scalability.

5. RESULTS AND DISCUSSION

5.1 Packet Delivery Rate

Packet Delivery Rate (PDR)is a network performance metric that measures the effectiveness of data transmission by indicating the proportion of packets successfully delivered to their intended destination compared to the total number of packets transmitted. It reflects the reliability of the communication process and the ability of the network to maintain successful packet forwarding under varying network conditions. A higher Packet Delivery Rate signifies better routing performance, improved connectivity, and more efficient data communication within the network.

Table 2 Comparative Tabulation of PDR.

Number of data packets	PDR (%)		
	GJCOZTS-BCT	HISCTR	EAQSO-ZTF
25	92.14	89.62	93.05
50	93.54	90.02	93.91
75	94.28	90.86	95.19
100	95.34	91.98	95.78
125	95.98	92.54	96.20

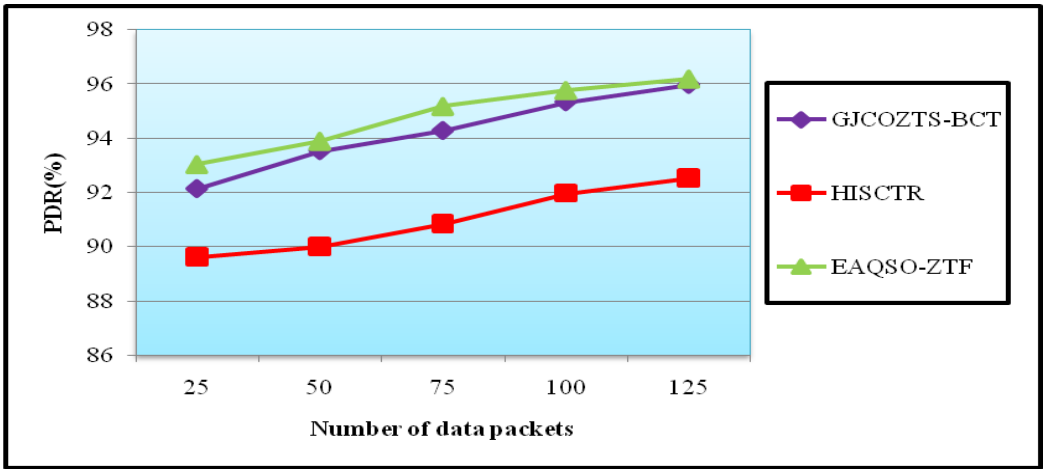

Figure 2 Graphical Performance of PDR

Table 2 and Figure 2 illustrate the PDR performance of the proposed EAQSO-ZTF framework compared with GJCOZTS-BCT [1] and HISCTR [2] under different numbers of data packets. As the packet load increases from 25 to 125 packets, all three approaches exhibit an improvement in PDR, indicating their ability to maintain communication reliability under increasing traffic conditions. However, the proposed EAQSO-ZTF consistently achieves the highest packet delivery performance throughout the evaluation. At 25 data packets, proposed EAQSO-ZTF attains a PDR of approximately 93.0%, outperforming GJCOZTS-BCT [1](92.1%) and HISCTR [2] (89.6%). As the number of packets increases to 75, the proposed method further improves its delivery performance to around 95.2%, demonstrating its capability to select stable and trustworthy routes even in dynamic network environments. This improvement can be attributed to the integration of energy-aware node selection and quantum swarm optimization, which efficiently identify reliable forwarding nodes while avoiding unstable communication links.

When the packet count reaches 125, proposed EAQSO-ZTF achieves the highest PDR of approximately 96.2%, whereas GJCOZTS-BCT [1]and HISCTR [2] achieve about 96.0% and 92.5%, respectively. The superior performance of EAQSO-ZTF indicates that the proposed framework effectively minimizes packet losses through intelligent route optimization and continuous trust assessment. Furthermore, the Zero Trust mechanism isolates malicious or unreliable nodes before they can affect data transmission, thereby enhancing routing reliability and network security.Overall, the results demonstrate thatproposed EAQSO-ZTF provides more dependable packet delivery than the existing methods across all traffic conditions. The combination of quantum-inspired optimization, energy-aware decision-making, and trust-based intrusion prevention contributes significantly to maintaining high packet delivery efficiency in 5G and Next-Generation MANET environments.

5.2 Communication Overhead

Communication overhead refers to the additional network resources consumed for transmitting control, routing, authentication, trust management, and security-related messages that support data communication in a network. In MANET environments, communication overhead is generated by activities such as route discovery, route maintenance, trust evaluation, intrusion detection, and node verification processes. Excessive communication overhead can increase bandwidth utilization, energy consumption, and network congestion, thereby reducing overall network performance. Therefore, minimizing communication

overhead is essential for achieving efficient and secure communication while preserving network resources and extending network lifetime.

Table 3 Comparative Tabulation of Communication Overhead

Number of data packets	Communication Overhead (ms)		
	GJCOZTS-BCT	HISCTR	EAQSO-ZTF
25	10	11.4	9
50	12	15.3	11
75	13	17	12
100	15	19	14
125	18	23	16

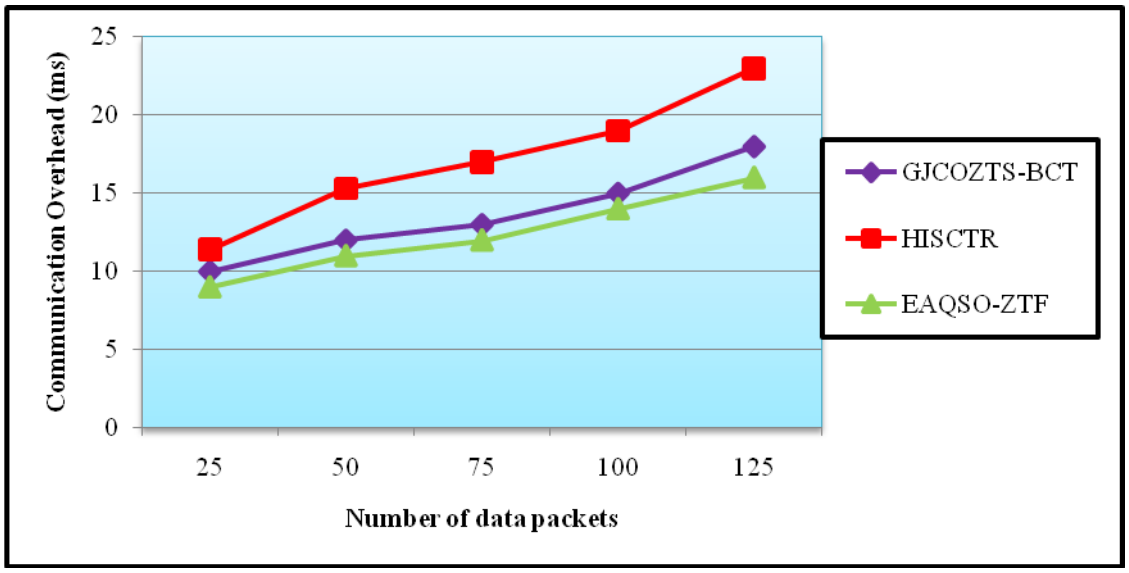

Figure 3 Graphical Performance of Communication Overhead.

Table 3 and Figure 3 illustrate the communication overhead incurred by the proposed EAQSO-ZTF framework and the existing GJCOZTS-BCT[1] and HISCTR[2] for different numbers of data packets. Communication overhead increases for all methods as the packet load grows from 25 to 125 packets because additional control messages, routing updates, and security-related operations are required to support network communication. Nevertheless, the proposed EAQSO-ZTF consistently produces the lowest overhead among the compared methods.At 25 data packets, proposed EAQSO-ZTF records a communication overhead of approximately 9 ms, which is lower than GJCOZTS-BCT [1] (10 ms) and HISCTR [2] (11.5 ms). As the traffic load increases to 75 packets, the overhead of proposed EAQSO-ZTF rises moderately to about 12 ms, while GJCOZTS-BCT and HISCTR reach nearly 13 ms and 17 ms, respectively. This behavior indicates that the proposed framework manages routing and security operations more efficiently, thereby reducing unnecessary control transmissions.

When the number of data packets reaches 125, proposed EAQSO-ZTF achieves an overhead of approximately 16 ms, whereas GJCOZTS-BCT [1] and HISCTR [2] exhibit significantly higher values of about 18 ms and 23 ms, respectively. The reduced overhead of EAQSO-ZTF can be attributed to its energy-aware node selection strategy and quantum swarm optimization mechanism, which limit participation to suitable nodes and accelerate route discovery. In addition, the Zero Trust-based intrusion detection process quickly identifies and isolates malicious nodes, preventing excessive routing updates and repeated communication attempts.Overall, the results demonstrate that proposed EAQSO-ZTF is more effective in controlling communication overhead under increasing network traffic conditions. By combining lightweight optimization, adaptive decision-making, and trust-based security management, the proposed framework minimizes control message exchanges while maintaining reliable and secure communication in 5G and Next-Generation MANET environments.

5.3 Scalability

Scalability refers to the capability of a network or system to maintain its performance and operational efficiency as the number of nodes, traffic load, or communication demands increase. In MANET environments, scalability indicates how effectively the network can accommodate growing node density and dynamic topology changes without causing significant degradation in routing performance, security, energy efficiency, or communication reliability. A highly scalable system can support larger network sizes while sustaining acceptable levels of throughput, packet delivery, delay, and resource utilization.

Table 4 Comparative Tabulation of Scalability.

Number of Mobile Nodes	Scalability (%)		
	GJCOZTS-BCT	HISCTR	EAQSO-ZTF
50	93.57	90.03	94.06
100	93.89	91.11	94.65
150	94.87	92.89	95.04
200	95.12	92.68	95.89
250	95.96	93.54	96.33

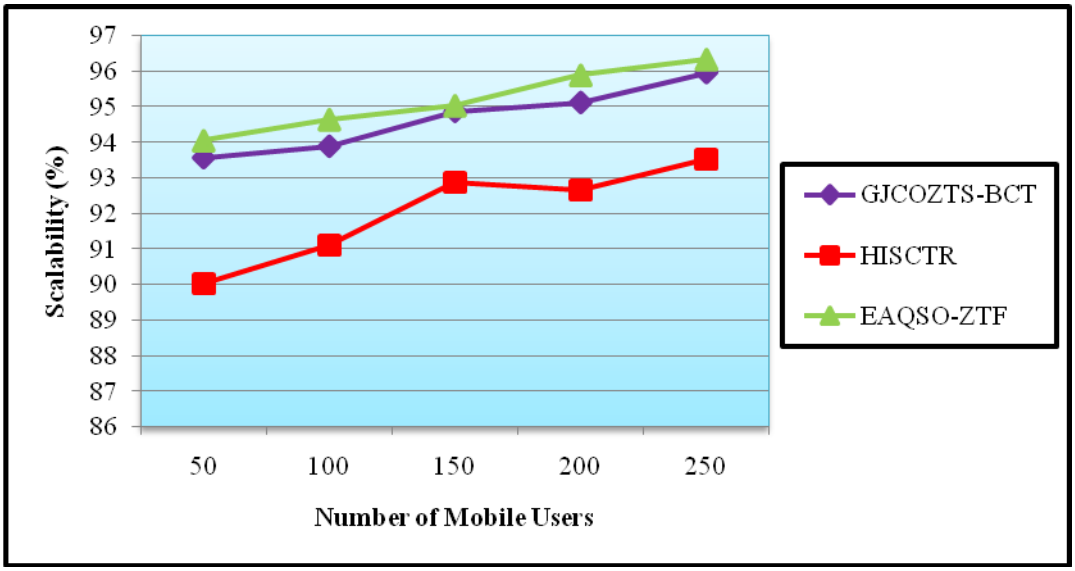

Figure 4 Graphical Performance of Scalability.

Table 4 and Figure 4depict the scalability performance of the proposed EAQSO-ZTF framework in comparison with GJCOZTS-BCT[1] and HISCTR[2] under varying numbers of mobile users. Scalability is evaluated by measuring the ability of the network to sustain efficient communication and security performance as the network size increases. The results show that all approaches exhibit improved scalability with the growth in the number of mobile users; however, proposed EAQSO-ZTFconsistently achieves superior performance throughout the evaluation.For a network comprising 50 mobile users, proposed EAQSO-ZTFattains a scalability value of approximately 94.0%, whereas GJCOZTS-BCT[1] and HISCTR[2] achieve about 93.6% and 90.0%, respectively. As the number of users increases to 150, the scalability of proposed EAQSO-ZTFimproves to nearly 95.0%, indicating its capability to effectively manage increasing routing demands and network dynamics. The performance improvement is mainly attributed to the energy-aware node selection process and adaptive optimization strategy, which reduce unnecessary resource utilization while maintaining efficient communication.

At 250 mobile users, the proposed EAQSO-ZTFreaches a scalability of approximately 96.3%, outperforming GJCOZTS-BCT [1] (96.0%) and HISCTR [2] (93.5%). The marginal increase in scalability with larger network sizes demonstrates the ability of EAQSO-ZTF to accommodate additional nodes without significant degradation in network performance. The quantum-inspired optimization mechanism efficiently identifies reliable routing paths, while the Zero Trust security model ensures that only trustworthy nodes participate in network operations.Overall, the results indicate that proposed EAQSO-ZTFprovides better scalability

than the existing methods under different network sizes. The combination of energy-aware optimization, adaptive swarm management, and trust-based intrusion prevention enables the framework to maintain stable performance and secure communication even as the number of mobile users increases, making it suitable for large-scale 5G and Next-Generation MANET deployments.

6. CONCLUSION

This paper presented an EAQSO-ZTF for secure and efficient intrusion detection and prevention in MANETs operating within 5G and NxtG communication environments. The proposed EAQSO-ZTF integrates energy-aware node selection, quantum-inspired swarm optimization, adaptive swarm management, and Zero Trust security principles to address the challenges of routing security, energy consumption, and network scalability. By considering residual energy, trust score, packet delivery performance, delay, and link stability during optimization, proposed EAQSO-ZTF effectively identifies reliable routing paths while minimizing resource utilization.The quantum-based optimization mechanism utilized in proposed EAQSO-ZTF accelerates convergence and reduces computational overhead compared with conventional swarm intelligence approaches. In addition, the Zero Trust model used in proposed EAQSO-ZTF continuously evaluates node behavior and isolates malicious entities, thereby strengthening network resilience against security threats. Simulation results demonstrate that the proposedEAQSO-ZTF achieves superior packet delivery performance, lower communication overhead, improved scalability, enhanced detection capability, and better energy efficiency when compared with existing methods. These improvements contribute to prolonged network lifetime and more reliable communication in highly dynamic MANET environments.Overall, proposed EAQSO-ZTF offers a lightweight, secure, and energy-efficient solution for next-generation mobile ad hoc networks. Future work may focus on integrating deep learning-based threat prediction, blockchain-assisted trust management, and real-time deployment in large-scale 6G-enabled intelligent network to further enhance security.

REFERENCES

1. S. Kalaichelvi, K. R. Ananth, “Golden Jackal Cost Optimized Zero Trust Security with Block-Chain for Intrusion Detection and Prevention in MANET with 5G and NxtG Technology”,

2. Anuprathibha, T., R. Maheswari, A. Suresh Babu, and S. Murugesan. "Hybrid intelligence-powered secure clustering with trust-optimized routing for next-generation MANET communication." *Scientific Reports* (2026).
3. Noor, Kinzah, Agbotiname Lucky Imoize, Chun-Ta Li, and Chi-Yao Weng. "A review of machine learning and transfer learning strategies for intrusion detection systems in 5G and beyond." *Mathematics* 13, no. 7 (2025): 1088.
4. Alghamdi, Saleh A. "Novel trust-aware intrusion detection and prevention system for 5G MANET–Cloud." *International Journal of Information Security* 21, no. 3 (2022): 469-488.
5. Nithya, R., K. Amudha, A. Syed Musthafa, Dilip Kumar Sharma, Edwin Hernan Ramirez-Asis, Priya Velayutham, V. Subramaniyaswamy, and Sudhakar Sengan. "An optimized fuzzy based ant colony algorithm for 5G-MANET." *Computers, Materials & Continua* 70, no. 1 (2022): 1069-1087.
6. Duong, Thuy-Van T., and Vuong M. Ngo. "TFACR: A novel topology control algorithm for improving 5G-based MANET performance by flexibly adjusting the coverage radius." *IEEE Access* 11 (2023): 105734-105748.
7. Shinde, Pradnya N., and Ankur Goyal. "A comprehensive review of trust aware and optimization assisted machine learning and deep learning intrusion detection systems for mobile ad hoc networks." *Discover Artificial Intelligence* (2026).
8. Soni, A., Nanda, S.K., Sahoo, P.K. *et al.* A dynamic liquid neural network based intrusion detection for zero trust systems. *Discov Computing* **29**, 170 (2026). https://doi.org/10.1007/s10791-026-10072-6
9. Uddin, Mueen, Sonia Khan, Fuhid Alanazi, Maha M. Althobaiti, Meshari Huwaytim Alanazi, and Mohammad N. Alanazi. "A hierarchical and privacy-preserving intrusion detection framework for SAGIN-enabled IIot using graph neural networks and deep Q-learning." *Neural Networks* (2026): 108876.
10. Selvakumar, Muru, and B. Sudhakar. "Energy efficient clustering with secure routing protocol using hybrid evolutionary algorithms for mobile adhoc networks." *Wireless Personal Communications* 127, no. 3 (2022): 1879-1897.
11. Reka, R., A. Manikandan, C. Venkataramanan, and R. Madanachitran. "An energy efficient clustering with enhanced chicken swarm optimization algorithm with adaptive position routing protocol in mobile adhoc network." *Telecommunication Systems* 84, no. 2 (2023): 183-202.

12. Srilakshmi, Uppalapati, Saleh Ahmed Alghamdi, Veera Ankalu Vuyyuru, Neenavath Veeraiah, and Youseef Alotaibi. "A secure optimization routing algorithm for mobile ad hoc networks." *IEEE Access* 10 (2022): 14260-14269.
13. Saravanan, N., Rajesh Arunachalam, A. Sahaya Anselin Nisha, and A. Karthikayen. "An innovative energy efficient routing protocol in MANET with hybridized osprey-fire hawk optimization algorithm to attain optimal routing constraints." *Wireless Networks* 31, no. 3 (2025): 2005-2026.
14. Vijayan, P., P. Anbalagan, and S. Selvakumar. "An Ensembled Optimization Algorithm for Secured and Energy Efficient Low Latency MANET with Intrusion Detection." *J. Internet Serv. Inf. Secur.* 12, no. 4 (2022): 156-163.
15. Yilmaz, Kudret, Resul Kara, and Ferzan Katircioglu. "Energy-efficient hybrid adaptive clustering for dynamic MANETs." *IEEE Access* (2025).
16. Hassan, Saad M., Mohd Murtadha Mohamad, Farkhana Binti Muchtar, and Firoz Bin Yusuf Patel Dawoodi. "Enhancing MANET security through federated learning and multiobjective optimization: A trust-aware routing framework." *IEEE Access* 12 (2024): 181149-181178.
17. Hemalatha, S., Nripendra Narayan Das, R. Arunkumar, and Charanjeet Singh. "Energy-aware and trust-based secure routing in manets using swarm intelligence techniques." *Scientific Reports* (2026).
18. Sedjelmaci, Hichem, and Nirwan Ansari. "Zero trust architecture empowered attack detection framework to secure 6G edge computing." *IEEE Network* 38, no. 1 (2023): 196-202.
19. El-Hajj, Mohammed. "Secure and trustworthy open radio access network (O-RAN) optimization: A zero-trust and federated learning framework for 6G networks." *Future Internet* 17, no. 6 (2025): 233.
20. Liu, Yiliang, Zhou Su, Haixia Peng, Yushan Xiang, Wei Wang, and Ruidong Li. "Zero trust-based mobile network security architecture." *IEEE wireless communications* 31, no. 2 (2024): 82-88.