IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 11 ISSUE : 03 Print / Issue Publication Date: July 2026

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2026.v11i03.011

Indexed In

Google Scholar OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 61-76
Published Online July 2026 in IJEAST (http://www.ijeast.com)

TRUST-AWARE DEEP REINFORCEMENT LEARNING ASSISTED HYBRID SWARM OPTIMIZATION FOR ENERGY-EFFICIENT IOT-WSN ROUTING

Nikita N Bharadwaj
Independent Researcher, India

Abstract—**The growing use of Internet of Things (IoT)-enabled Wireless Sensor Networks (WSNs) has introduced several challenges, such as energy efficiency, reliable routing, and secure communication. Traditional routing protocols often struggle in changing environments because of unstable cluster formation, uneven energy use, and the risk of malicious nodes. To overcome these problems, this study introduces a hybrid trust-aware routing framework that combines Dynamic Swarm Optimization (DSO), Elephant Herding Optimization (EHO), and Deep Q Network (DQN)-based intelligent routing.**

In this proposed framework, DSO is used for adaptive clustering, while EHO helps in selecting the best cluster heads based on residual energy, communication distance, node density, and trust information. Additionally, a DQN-assisted routing mechanism is introduced to learn and choose efficient routing paths depending on the current network conditions and feedback from communication. A trust evaluation system is also included to detect unreliable nodes, thus enhancing secure packet forwarding.

The framework was tested in MATLAB under various IoT WSN scenarios and compared with existing methods such as LEACH, HEED, and PSO-based routing. The results showed that the model outperforms these in terms of packet delivery ratio, throughput, energy preservation, and network lifetime. It also reduces communication delay and overall energy consumption. By combining swarm intelligence and reinforcement learning, the model provides adaptive routing and improved communication reliability in densely populated IoT networks.

This framework is suitable for applications like smart city monitoring, industrial IoT systems, environmental sensing, and healthcare-focused wireless sensor networks.

Index Terms—**Internet of Things (IoT), Wireless Sensor Networks (WSN), Deep Reinforcement Learning, Deep Q Network (DQN), Elephant Herding Optimization (EHO), Swarm Optimization, Trust-Aware Routing, Energy-Efficient Routing, Cluster-Head Selection, Intelligent Routing, Secure Communication, IoT-WSN Networks.**

I. INTRODUCTION

Recent progress in IoT technologies has led to the widespread use of Wireless Sensor Networks (WSNs) in real world applications such as smart healthcare, environmental monitoring, industrial automation, and intelligent transportation systems. These applications often involve deploying sensor nodes in dynamic and resource-limited settings where energy efficiency and communication reliability are crucial.

Despite the basic clustering and communication mechanisms offered by traditional protocols like LEACH and HEED, their performance tends to degrade in large-scale and dynamic IoT environments. Problems such as uneven energy consumption, unstable routing paths, communication overhead, and vulnerability to malicious nodes can all negatively affect network lifetime and transmission reliability.

To tackle these issues, recent studies have investigated the use of artificial intelligence and metaheuristic optimization for adaptive routing and energy management. Reinforcement learning, particularly DQN-based routing, has shown promise in optimizing dynamic paths. Similarly, swarm intelligence techniques have been applied to cluster formation and cluster head selection to enhance load balancing and energy efficiency.

Inspired by these advancements, this paper proposes a hybrid DSO–EHO framework integrated with DQN-assisted intelligent routing and trust-aware communication. The model aims to enhance routing adaptability, communication reliability, secure packet forwarding, and network lifetime within IoT enabled wireless sensor networks.

A. Major Contributions

The key contributions of this work are:

- A hybrid optimization framework that combines Dynamic Swarm Optimization (DSO) and Elephant

Herding Optimization (EHO) for adaptive clustering and energy-aware cluster-head selection.

- A DQN-assisted routing mechanism that dynamically optimizes packet forwarding based on network conditions.
- A trust-aware communication model to assess node reliability and minimize the impact of malicious or unstable nodes during packet forwarding.
- A multi-objective optimization strategy that balances packet delivery, communication delay, energy consumption, and network lifetime.
- Comparative simulation analysis against traditional LEACH, HEED, and PSO-based routing protocols under the same IoT-WSN conditions.

II. RELATED WORK

Recent developments in IoT-enabled Wireless Sensor Networks (IoT-WSNs) have focused on improving routing efficiency, energy optimization, communication reliability, and network security through artificial intelligence and optimization-based methods.

Godfrey et al. [1] developed an energy-efficient routing protocol using reinforcement learning for software-defined wireless sensor networks. Their approach improved routing adaptability and communication efficiency, though it lacked secure trust-aware communication features.

Wang et al. [2] introduced a cooperative deep reinforcement learning-based routing mechanism to reduce communication delay and improve energy efficiency in wireless sensor net works. While this method enhanced routing performance, it led to higher computational overhead in large-scale IoT settings.

Kumar and Venkatesan [3] created an intelligent deep reinforcement learning-based routing strategy for IoT-enabled WSNs. Their model improved packet forwarding efficiency and adaptive routing behavior but did not include trust-aware detection of malicious nodes.

Kumar and Jeyalakshmi [4] presented a federated deep reinforcement learning routing framework for IoT-enabled wireless sensor networks. This framework achieved better communication performance and distributed learning capability but faced issues with high training complexity and communication overhead.

Luo et al. [5] proposed a deep reinforcement learning framework for trajectory planning and transmission scheduling in UAV-assisted wireless sensor networks. Their approach improved communication optimization and routing efficiency but required significant computational resources for real-time applications.

Upadhyay et al. [6] introduced an improved deep reinforcement learning routing technique for collision-free vehicular ad hoc networks. Their framework reduced communication collisions and routing delays but was not optimized for energy constrained IoT-WSN environments.

Lingamaiah et al. [7] developed a reliable routing frame work using reinforcement learning for medical wireless sensor networks. The study enhanced communication reliability and packet delivery but lacked intelligent cluster optimization.

Zhang et al. [8] created an intelligent routing algorithm guided by distributed neural networks for wireless sensor networks. Their approach improved adaptive communication performance but did not address secure trust-aware routing functionality.

Meng et al. [9] explored deep reinforcement learning based topology optimization for self-organized wireless sensor networks. Their framework enhanced network scalability and communication adaptability but introduced significant optimization complexity.

Manfredi et al. [10] proposed a relational deep reinforcement learning framework for routing optimization in wireless networks. This approach improved routing intelligence and communication adaptability but did not consider energy-aware cluster-head optimization.

Leong et al. [11] introduced a deep reinforcement learning framework for wireless sensor scheduling in cyber-physical systems. Their study improved communication scheduling efficiency but did not address secure routing and trust management in IoT-enabled environments.

Li et al. [12] developed an intelligent software-defined wireless network routing algorithm based on network situational awareness and deep reinforcement learning. Their model enhanced routing adaptability and network awareness but still had relatively high communication overhead.

Zhao and Zhao [13] proposed a deep reinforcement learning resource allocation framework for wireless sensor networks with energy harvesting and relay communication. Their approach improved energy utilization efficiency but lacked intelligent trust-aware routing mechanisms.

Su et al. [14] developed a cooperative communication framework with relay selection using deep reinforcement learning in wireless sensor networks. Their method improved communication reliability and transmission efficiency; however, cluster optimization and malicious node detection were not considered.

Abdel-Basset et al. [15] proposed a group teaching optimization algorithm for improving communication security in wireless sensor networks. Although the framework enhanced security performance, adaptive AI-assisted routing optimization was not incorporated.

From the above discussion, it can be observed that existing approaches majorly focus on single objectives such as energy optimization, intelligent routing, trust management, or communication security. However, limited research has jointly integrated DSO-based clustering, EHO-assisted cluster-head optimization, DQN-based adaptive routing, and trust-aware secure communication within a unified IoT-WSN framework.

Therefore, the proposed framework aims to address these limitations by integrating intelligent clustering, adaptive routing, energy optimization, and trust-aware malicious node detection to improve overall network lifetime, packet delivery ratio, throughput, communication reliability, and secure data transmission performance.

Despite significant advancements, existing approaches still suffer from several limitations such as convergence instability, higher computational overhead, inefficient trust integration, and limited adaptability under dynamic IoT environments. Furthermore, most existing studies independently focus on clustering, routing, or trust management without jointly optimizing all communication objectives.

The comparative analysis presented in Table I indicates that most existing approaches independently focus on routing optimization, clustering, or trust management. Very few studies jointly integrate intelligent routing, trust-aware communication, and multi-objective energy optimization within a unified IoT-WSN framework. To address these limitations, the proposed framework combines Dynamic Swarm Optimization (DSO), Elephant Herding Optimization (EHO), Deep Q Network (DQN) assisted routing, and trust-aware communication to achieve improved energy efficiency, routing stability, secure communication reliability, and prolonged network life time simultaneously.

To address these research gaps, the proposed framework integrates Dynamic Swarm Optimization (DSO), Elephant Herding Optimization (EHO), Deep Q-Network (DQN) based

TABLE I: Comparative Analysis of Existing AI and Optimization Based IoT-WSN Routing Approaches

Ref.	Technique Used	Main Objective	AI	Trust	Energy	Limitations
[1]	Deep Reinforcement Learning based Routing	Adaptive packet forwarding and routing optimization	Yes	No	Moderate	Higher computational complexity and limited trust integration
[2]	Deep Q-Learning Adaptive Routing	Delay reduction and throughput enhancement	Yes	No	Moderate	Routing instability under large scale IoT deployments
[3]	Metaheuristic Clustering Optimization	Energy-efficient cluster formation	No	No	High	Lack of intelligent routing capability
[4]	Hybrid Optimization Framework	Balanced energy utilization	Partial	No	High	Increased optimization overhead
[5]	Elephant Herding Optimization (EHO)	Cluster-head selection and load balancing	No	No	High	Absence of adaptive routing mechanism
[6]	PSO-based Energy Aware Routing	Communication energy minimization	Partial	No	High	Premature convergence issues
[7]	Trust-Aware Secure Routing	Secure packet forwarding and malicious node detection	No	Yes	Moderate	No intelligent learning-based routing
[8]	Intelligent Trust Management Framework	Trust evaluation in large scale IoT networks	Partial	Yes	Moderate	Higher communication over head
[9]	AI-Assisted Communication Framework	Adaptive communication optimization	Yes	Partial	Moderate	Limited clustering optimization

[10]	Energy Harvesting Secure Communication	Lifetime enhancement and secure transmission	No	Yes	High	Limited routing adaptability
[11]	RL-Assisted Secure Rout ing	Intelligent secure routing optimization	Yes	Yes	Moderate	Scalability challenges
[12]	Hybrid Swarm Intelligence Clustering	Adaptive cluster formation	Partial	No	High	No trust-aware communication
[13]	Trust-Based Energy Aware Protocol	Secure and energy-efficient communication	Partial	Yes	High	Limited intelligent routing capability
[14]	DRL Assisted Smart City Routing	Smart city IoT routing optimization	Yes	Partial	Moderate	High training complexity
[15]	AI-Enabled Secure Clustering and Routing	Integrated secure communication framework	Yes	Yes	High	Computational overhead in large networks
Proposed	DSO-EHO with DQN	Joint optimization of clustering, routing, security and energy efficiency	Yes	Yes	High	Improved network lifetime and secure adaptive routing

intelligent routing, and trust-aware communication within a unified IoT-WSN architecture. The proposed hybrid frame work aims to improve routing stability, secure communication reliability, throughput, packet delivery ratio, and overall network lifetime simultaneously.

III. PROPOSED METHODOLOGY

The proposed AI-assisted IoT-WSN framework integrates Dynamic Swarm Optimization (DSO) based clustering, Elephant Herding Optimization (EHO) based cluster-head selection, Deep Q-Network (DQN) enabled intelligent routing, and trust-aware secure communication mechanisms to improve energy efficiency, routing reliability, throughput, packet delivery ratio, and overall network lifetime.

The proposed framework consists of four major operational modules:
1) DSO-based clustering
2) EHO-based cluster-head selection
3) DQN-assisted intelligent routing
4) Trust-aware malicious node detection

The overall work of the proposed methodology is depicted in Fig. 1.

A. System Architecture

Initially, IoT-enabled sensor nodes are randomly deployed within the sensing environment. Thereafter, the DSO-based

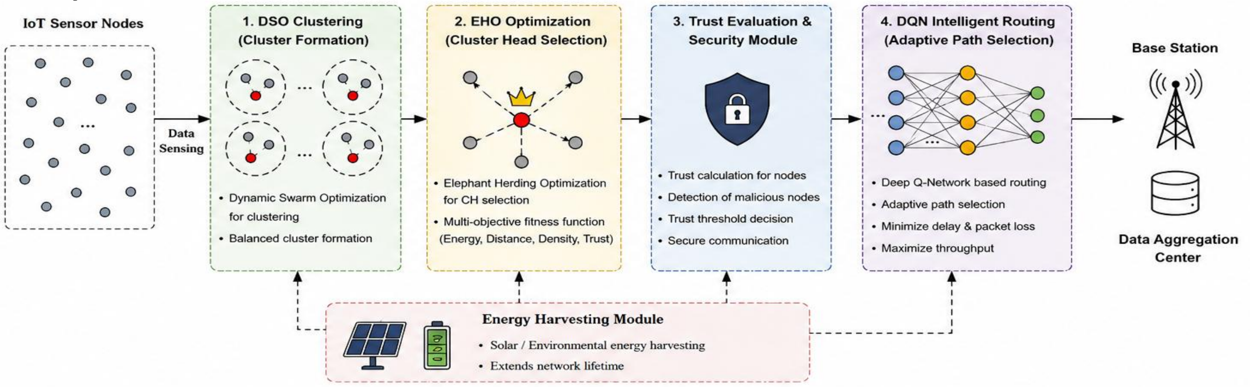

Fig. 1: Architecture of the proposed AI-assisted IoT-WSN framework

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 61-76
Published Online July 2026 in IJEAST (http://www.ijeast.com)

clustering mechanism organizes the deployed sensor nodes into optimized communication clusters according to node distribution, communication distance, and local density information.
Subsequently, the EHO optimization mechanism selects optimal cluster-head nodes based on residual energy, normalized communication distance, node density, and trust score. The selected cluster heads forward sensed information using the DQN-assisted intelligent routing framework.
Furthermore, a trust-aware communication module continuously monitors node behavior to identify malicious or unreliable nodes and ensure secure communication throughout the network. Finally, the aggregated information is transmitted to the base station through optimized routing paths.

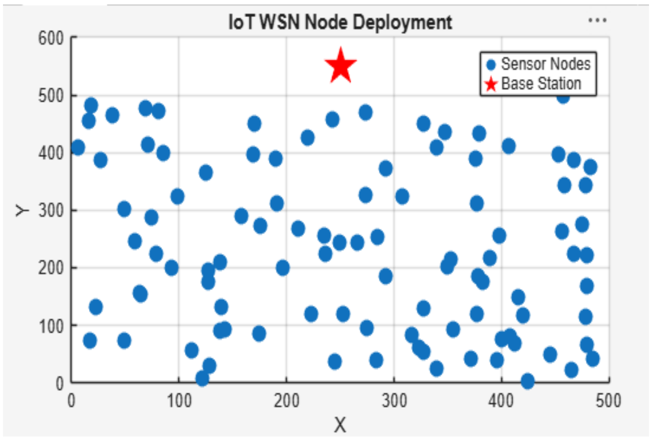

Fig. 2: IoT-WSN based random sensor node deployment

The operational workflow of the proposed framework can be summarized as follows:
Sensor Deployment → DSO Clustering → EHO Cluster-Head Selection → Trust Evaluation → DQN Intelligent Routing → Base Station Communication

B. IoT-WSN Node Deployment
Initially, IoT-enabled sensor nodes are randomly deployed within a 500 × 500 m^2sensing region. The base station is positioned outside the sensing field to emulate realistic long distance communication scenarios commonly observed in IoT enabled wireless sensor network environments.
Random node deployment improves the scalability, adapt ability, and robustness of the proposed framework under dynamic communication conditions.

C. DSO-Based Clustering
The DSO module partitions sensor nodes into optimized clusters according to node density, communication distance, and residual energy distribution. The clustering process significantly reduces communication overhead and improves load balancing among sensor nodes.
The clustering mechanism minimizes unnecessary long distance communication costs and enhances network scalability by organizing nearby sensor nodes into efficient communication groups.

D. EHO-Based Cluster-Head Selection
After the cluster formation process, Elephant Herding Optimization (EHO) is employed to identify optimal cluster-head (CH) nodes within each communication cluster. The primary objective of the EHO mechanism is to improve balanced energy utilization, communication reliability, and routing stability by selecting efficient cluster-head nodes according to multiple network parameters.
The cluster-head selection process considers residual energy, node trust score, communication distance, and local node density to ensure stable and energy-aware communication performance in dynamic IoT-WSN environments.
The multi-objective fitness function used for cluster-head selection is mathematically represented as:

$$F = w_1E_r + w_2T + w_3N_d - w_4D_n \qquad (1)$$

where:
- E_r represents the residual energy of the sensor node,
- T denotes the trust score associated with node reliability,
- N_d indicates neighboring node density,
- D_n represents normalized communication distance,
- w_1, w_2, w_3, and w_4 are weighting coefficients used to balance the optimization objectives.

Nodes having higher fitness values are selected as cluster heads to ensure balanced communication load distribution, reduced transmission overhead, and improved network lifetime.

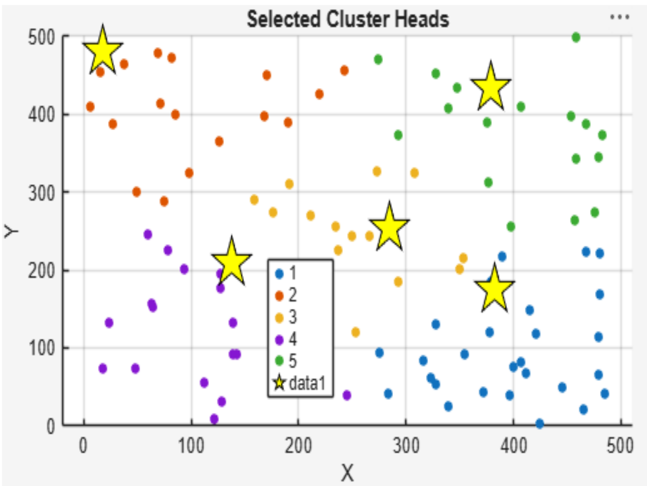

Fig. 3: Selected Cluster Heads using EHO Optimization

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 61-76
Published Online July 2026 in IJEAST (http://www.ijeast.com)

Figure 3 illustrates the optimized cluster-head selection generated using the EHO framework. The selected cluster heads are efficiently distributed across the sensing environment according to energy availability, communication distance, and trust-aware communication requirements. The optimized cluster formation significantly improves communication efficiency and balanced energy utilization among sensor nodes.

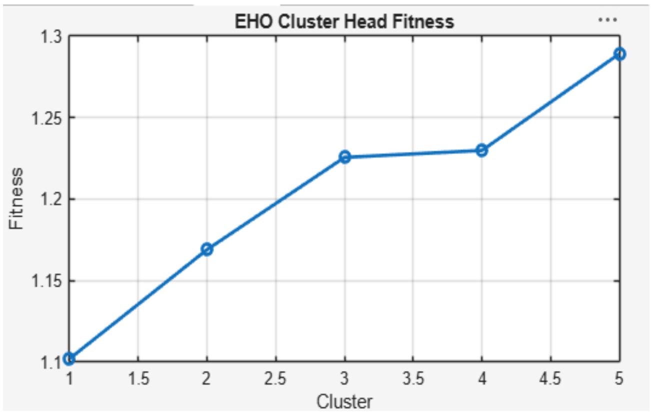

Fig. 4: EHO Cluster-Head Fitness Convergence Analysis

Figure 4 presents the convergence behavior of the EHO based cluster-head optimization process. The fitness value gradually improves during optimization iterations and stabilizes after convergence, indicating effective cluster-head se lection and stable optimization performance. The convergence characteristics demonstrate the capability of the proposed EHO framework to identify energy-efficient and reliable cluster head nodes under dynamic IoT-WSN conditions.

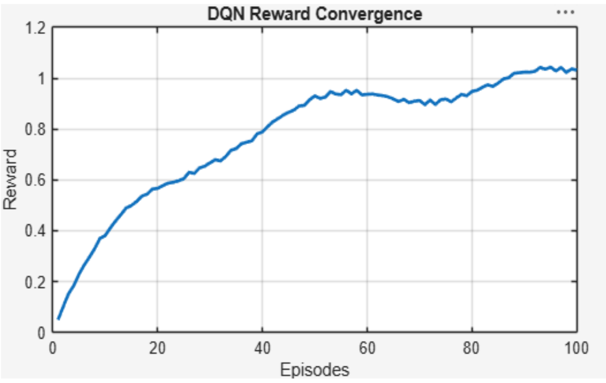

Fig. 5: DQN reward convergence analysis

E. DQN-Assisted Intelligent Routing

The proposed framework employs a Deep Q-Network (DQN) assisted intelligent routing mechanism to dynamically identify energy-efficient, reliable, and low-delay communication paths within the IoT-WSN environment.

The DQN routing agent continuously updates routing policies according to network state transitions, residual energy, packet delivery ratio, communication delay, and reward convergence behavior. The routing mechanism adaptively selects optimized communication paths between cluster heads and the base station to improve overall network performance.

The network state vector is represented as:

$$S_t = \{E_r, T_s, D_n, Q_l, N_d\}$$

where:

- E_r represents residual energy,
- T_s denotes trust score,
- D_n indicates communication distance,
- Q_l represents queue load,
- N_d denotes neighboring node density.

The reward function used by the DQN routing framework is expressed as follows:

$$R = \alpha PDR + \beta T_r - \gamma E - \delta D \qquad (2)$$

where:

- P DR denotes Packet Delivery Ratio,
- T_r represents node trust score,
- E denotes energy consumption,
- D denotes communication delay,
- α, β, γ, and δ represent weighting coefficients.

The DQN routing framework continuously learns optimal routing policies through environmental feedback and adaptive reward optimization. This process improves packet transmission efficiency, routing stability, communication reliability, and network lifetime while reducing communication overhead and packet loss.

Fig. 5 illustrates the reward convergence behavior of the proposed DQN routing framework. The increasing reward trend indicates successful learning convergence and adaptive routing optimization capability.

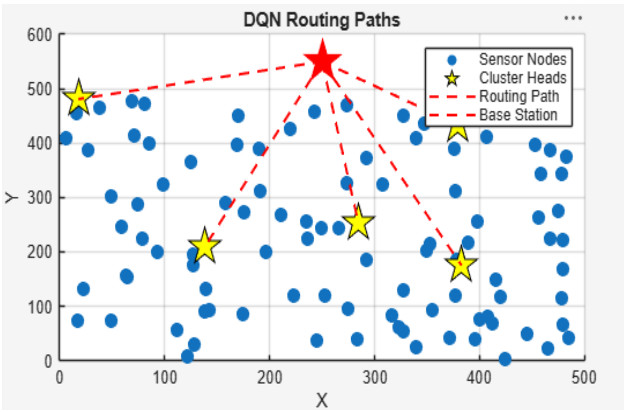

Fig. 6: DQN-based intelligent routing paths

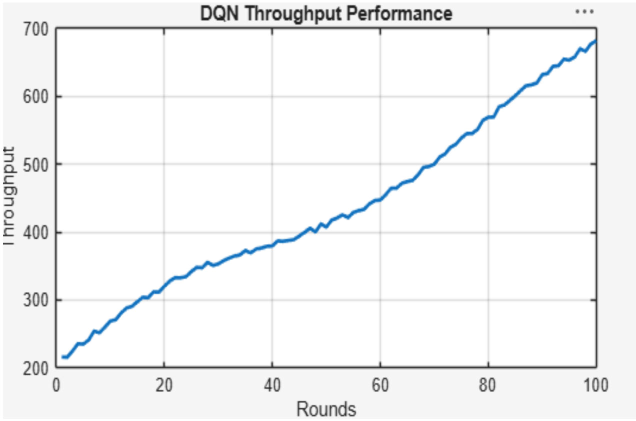

Fig. 7: DQN throughput performance

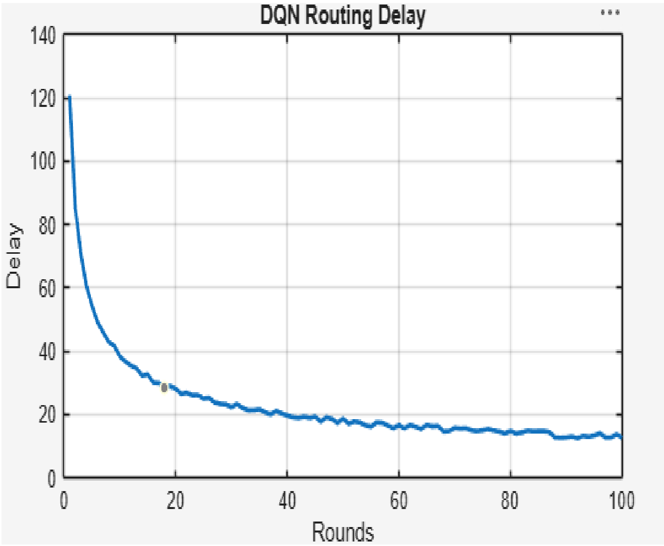

Fig. 8: DQN routing delay analysis

The routing structure generated by the DQN routing agent is illustrated in Fig. 6. The intelligent routing paths establish optimized communication links between cluster heads and the base station.

Fig. 7 illustrates the throughput performance of the proposed DQN-assisted routing framework. The throughput continuously increases with simulation rounds, indicating adaptive routing optimization and efficient packet transmission performance.

Fig. 8 presents the communication delay analysis of the proposed routing framework. The communication delay gradually decreases as the routing agent learns optimized communication paths during training iterations.

The packet delivery ratio performance of the proposed

Fig. 9: Packet delivery ratio analysis

framework is illustrated in Fig. 9. The increasing PDR values demonstrate improved routing reliability and communication stability under dynamic network conditions.

F. Trust Evaluation Mechanism

To enhance routing reliability and communication security, a trust-aware evaluation mechanism is incorporated into the proposed IoT-WSN framework. The trust management module continuously monitors node behavior based on packet forwarding performance and communication consistency.

The trust value of each sensor node is calculated according to the successful packet forwarding ratio as follows:

$$Trust_i = \frac{P_{success}}{P_{total}} \tag{3}$$

where:

- $P_{success}$ represents the number of successfully forwarded packets,
- P_{total} denotes the total transmitted packets associated with node i.

Nodes exhibiting higher trust values are considered reliable for routing participation, whereas nodes with trust values below a predefined threshold are identified as malicious or unstable nodes. Such nodes are isolated from cluster-head selection and routing operations to improve packet delivery ratio, communication security, and overall network stability.

The proposed trust-aware communication mechanism effectively reduces packet loss and enhances secure data transmission in dynamic IoT-enabled wireless sensor network environments.

IV. MATHEMATICAL MODEL

The mathematical model of the proposed framework is developed to analyze communication energy consumption, residual energy, network lifetime, and computational complexity in IoT-enabled wireless sensor networks.

A. Transmission Energy Model

The transmission energy required for sending a k-bit packet over a communication distance d is expressed as:

$$E_{tx}(k, d) = E_{elec} \times k + \epsilon_{amp} \times k \times d^{n} \quad (4)$$

where:

- E_{elec} denotes the electronic energy consumption,
- • ϵ_{amp} represents amplifier energy,
- k is the packet size,
- d denotes transmission distance,
- n is the path loss exponent.

B. Receiver Energy Model

The energy consumed for receiving a k-bit packet is defined as:

$$E_{rx}(k) = E_{elec} \times k \quad (5)$$

C. Residual Energy Model

The residual energy of each sensor node after communication is calculated as:

$$E_{residual} = E_{initial} - E_{consumed} \quad (6)$$

where:

- $E_{initial}$ represents the initial node energy,
- $E_{consumed}$ denotes the total consumed energy during communication.

D. Network Lifetime Model

The network lifetime is defined as the operational duration between the first node failure and the last active node in the network.

$$\text{Network Lifetime} = R_{\text{last alive node}} - R_{\text{f irst dead node}} \quad (7)$$

where:

- $R_{\text{f irst dead node}}$ represents the round in which the first sensor node becomes inactive,
- $R_{\text{last alive node}}$ denotes the round in which the final sensor node remains operational.

E. Computational Complexity Analysis

The computational complexity of the proposed framework depends on clustering, cluster-head optimization, routing, and trust evaluation operations.

TABLE II: Computational Complexity Analysis

Module	Complexity
DSO Clustering	O(nk)
EHO Cluster Head Selection	O(nc)
DQN Routing	O(ns)
Trust Evaluation	O(n)

where:

- n represents the number of sensor nodes,
- k denotes the number of clusters,
- c indicates cluster-head candidate nodes,
- s represents routing state updates.

The overall computational complexity of the proposed framework is expressed as:

$$O(n(k + c + s)) \quad (8)$$

The DSO clustering mechanism performs cluster formation with a complexity of O(nk), whereas the EHO-based cluster head selection evaluates multiple candidate nodes with a complexity of O(nc). Furthermore, the DQN routing module dynamically updates routing policies according to environmental state transitions, resulting in a complexity of O(ns).

The trust evaluation mechanism computes packet forwarding reliability for each sensor node with a complexity of O(n). Despite the integration of AI-assisted routing and trust aware security mechanisms, the proposed framework maintains acceptable computational overhead while significantly improving throughput, packet delivery ratio, network lifetime, and communication reliability.

F. Mathematical Modeling and Optimization Framework

The proposed DSO-EHO-DQN framework is mathematically modeled as a multi-objective optimization problem to jointly optimize energy efficiency, routing reliability, communication delay, and secure data transmission in IoT-enabled Wireless Sensor Networks (WSNs).

1) Objective Function: The primary objective of the proposed framework is to minimize energy consumption and communication delay while maximizing packet delivery ratio, trust reliability, and network lifetime.

The multi-objective optimization function is formulated as:

$$\min F = w_1E_c + w_2D + w_3P\,LR - w_4T_r - w_5NL \quad (9)$$

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 61-76
Published Online July 2026 in IJEAST (http://www.ijeast.com)

where:

- E_c represents total energy consumption,
- D denotes communication delay,
- P LR represents packet loss ratio,
- T_r denotes trust reliability score,
- NL represents network lifetime,
- w_1, w_2, w_3, w_4, and w_5 are weighting coefficients.

The optimization process attempts to minimize the overall objective function while maintaining stable and secure communication performance.

2) Energy Consumption Model: The energy consumption model of the proposed IoT-WSN framework is represented as:

$$E_{total} = E_{tx} + E_{rx} + E_{idle} \quad (10)$$

where:

- E_{tx} denotes transmission energy,
- E_{rx} represents receiving energy,
- E_{idle} indicates idle-state energy consumption.

$$E_{tx}(k, d) = kE_{elec} + k\epsilon_{amp}d_n \quad (11)$$

where:

- k denotes packet size,
- E_{elec} represents electronic energy,
- ϵ_{amp} denotes amplifier energy,
- d represents communication distance,
- n denotes path loss exponent.

3) Trust Modeling: The trust value of each sensor node is evaluated according to successful packet forwarding behavior. The trust function is mathematically represented as:

$$T_i = \frac{P_{success}}{P_{forwarded}} \quad (12)$$

where:

- $P_{success}$ represents successfully forwarded packets,
- $P_{forwarded}$ denotes total forwarded packets.

Nodes having trust values below a predefined threshold are identified as malicious or unreliable nodes and excluded from routing operations.

4) Delay Modeling: The end-to-end communication delay is represented as:

$$D_{total} = D_{proc} + D_{queue} + D_{trans} + D_{prop} \quad (13)$$

where:

- D_{proc} denotes processing delay,
- D_{queue} represents queue delay,
- D_{trans} indicates transmission delay,
- D_{prop} represents propagation delay.

The proposed routing mechanism minimizes total communication delay by selecting optimized routing paths using DQN assisted adaptive learning.

5) Packet Delivery Ratio Model: The packet delivery ratio (PDR) is mathematically expressed as:

$$PDR = \frac{P_{received}}{P_{sent}} \quad (14)$$

where:

- $P_{received}$ denotes successfully received packets,
- P_{sent} represents total transmitted packets.

Higher PDR values indicate improved routing reliability and communication stability.

6) Network Lifetime Model: The network lifetime is determined according to the operational duration of sensor nodes before energy depletion. The network lifetime is represented as:

$$NL = \sum_{i=1}^{N} \frac{E_i}{E_{consumed}} \quad (15)$$

where:

- E_i represents initial node energy,
- $E_{consumed}$ denotes consumed node energy,
- N indicates total number of sensor nodes.

The proposed DSO-EHO optimization framework attempts to maximize network lifetime through balanced cluster-head selection and energy-aware routing.

7) DQN Optimization Model: The Deep Q-Network (DQN) routing agent continuously updates routing decisions accord ing to environmental rewards. The Q-value update mechanism is expressed using the Bellman equation:

$$Q(s, a) = Q(s, a) + \alpha\, [r + \gamma \max Q(s', a') - Q(s, a)] \quad (16)$$

where:

- Q(s, a) denotes current Q-value,
- α represents learning rate,
- γ denotes discount factor,
- r represents immediate reward,
- s' indicates next state,

- $a^{\prime}$ denotes next action.

The DQN agent continuously learns optimized routing strategies through reward convergence and adaptive environ mental interaction.

8) Computational Complexity Analysis: The overall computational complexity of the proposed DSO-EHO-DQN frame work is represented as:

$$O(N \times I \times A) \qquad (17)$$

where:
- N denotes the number of sensor nodes,
- I represents optimization iterations,
- A indicates routing action space size.

The proposed framework maintains scalable computational performance while improving routing efficiency and secure communication reliability in large-scale IoT-enabled WSN environments.

V. SIMULATION SETUP

The proposed AI-assisted IoT-WSN framework was implemented in MATLAB to evaluate communication performance, routing reliability, energy efficiency, and network lifetime under different network scenarios. The simulation environment considers dynamic IoT-enabled wireless sensor networks with varying node densities and communication conditions.

TABLE III: Simulation Parameters

Parameter	Value
Simulation Area	500 × 500 m^2
Number of Nodes	100–500
Initial Energy	1–2 J
Base Station Position	(250, 550)
Simulation Rounds	100
Routing Method	DQN
Clustering Method	DSO
Cluster Head Selection	EHO
Communication Model	Multi-hop
Trust Mechanism	Packet Forwarding Based

The sensor nodes were randomly deployed within the sensing environment to emulate realistic IoT communication scenarios. The base station was positioned outside the sensing field to analyze long-distance communication performance and routing efficiency.

A. Performance Evaluation Metrics

The performance of the proposed framework was evaluated using several Quality of Service (QoS), energy efficiency, and trust-aware communication metrics.
Table IV summarizes the evaluation metrics used to analyze the effectiveness of the proposed intelligent routing frame work. These metrics collectively demonstrate the capability of the proposed model to improve throughput, packet delivery ratio, energy efficiency, routing stability, communication re liability, and network lifetime in IoT-enabled wireless sensor networks.
The proposed framework was comparatively evaluated against conventional LEACH, HEED, and PSO-based routing approaches under identical simulation conditions to ensure fair performance analysis.

VI. RESULTS AND DISCUSSION

The simulation results indicate that the proposed framework achieves more stable communication performance compared with conventional routing protocols. The integration of DSO based clustering and EHO-assisted cluster-head optimization contributes to balanced energy utilization among sensor nodes, which helps prolong overall network operation.
In addition, the DQN-assisted routing mechanism adaptively updates routing decisions according to environmental feedback and communication conditions. As a result, the proposed framework demonstrates improved packet delivery performance and reduced communication delay during simulation rounds.
The trust-aware communication mechanism further enhances routing reliability by excluding low-trust nodes from routing participation. This process reduces packet loss caused by unreliable communication behavior and improves secure data transmission performance within dynamic IoT environments.
Although the proposed framework introduces additional computational overhead due to reinforcement learning and optimization operations, the observed improvements in network lifetime, throughput, and communication stability suggest that the trade-off remains acceptable for large-scale IoT-WSN applications.

A. Residual Energy Analysis

Figure 10 illustrates the residual energy performance of the proposed framework. The proposed model preserves higher residual energy due to intelligent routing decisions, optimized communication distance, and adaptive cluster-head selection. Balanced energy utilization significantly

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 61-76
Published Online July 2026 in IJEAST (http://www.ijeast.com)

prolongs network lifetime and minimizes premature node depletion.

B. Throughput Analysis

Figure 11 presents the throughput comparison of the proposed DSO–EHO–DQN framework with conventional LEACH, HEED, and PSO-based routing protocols. The proposed framework achieves higher throughput performance

TABLE IV: Performance Evaluation Metrics

Metric	Description
Throughput	Number of successfully delivered packets to the base station
Delay	Average communication latency during packet transmission
Packet Delivery Ratio(PDR)	Ratio of successfully received packets to total transmitted packets
Residual Energy	Remaining energy available in sensor nodes after communication rounds
Alive Nodes	Number of active sensor nodes during network operation
Network Lifetime	Total operational duration before node depletion
Trust Score	Reliability measure used to identify secure and malicious nodes
Energy Consumption	Total energy utilized during routing and data transmission
Routing Stability	Consistency of communication paths during network operation

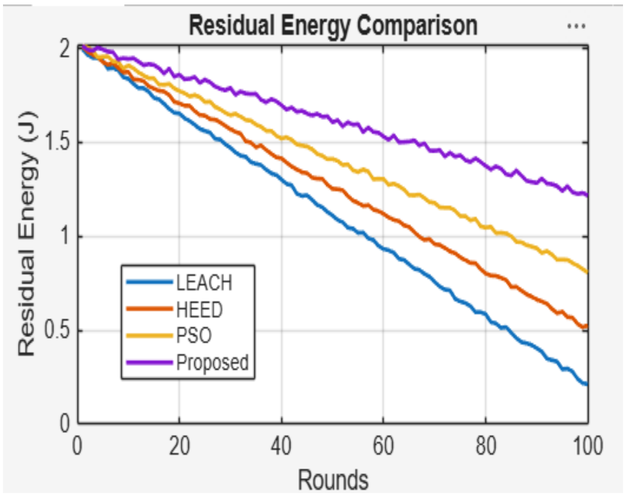

Fig. 10: Residual Energy Comparison

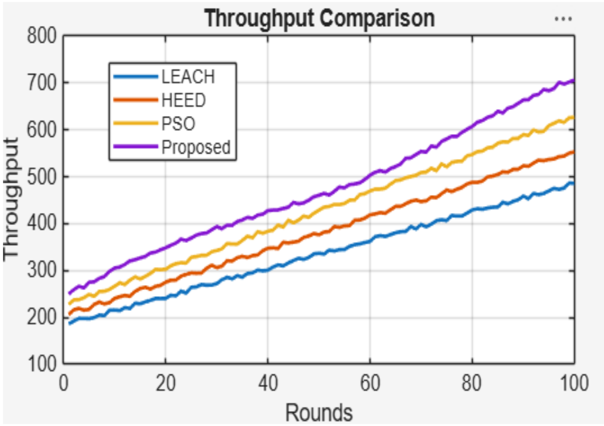

Fig. 11: Throughput Comparison

due to adaptive DQN-assisted routing, optimized cluster-head selection, and balanced communication load distribution. The intelligent routing mechanism dynamically identifies efficient communication paths between cluster heads and the base station, thereby reducing packet loss and improving successful packet transmission rates. In addition, the EHO based cluster-head optimization strategy minimizes excessive communication overhead and supports stable data forwarding during network operation.

The observed throughput improvement indicates that the proposed framework maintains reliable communication performance even under increasing network traffic and dynamic IoT-WSN communication conditions.

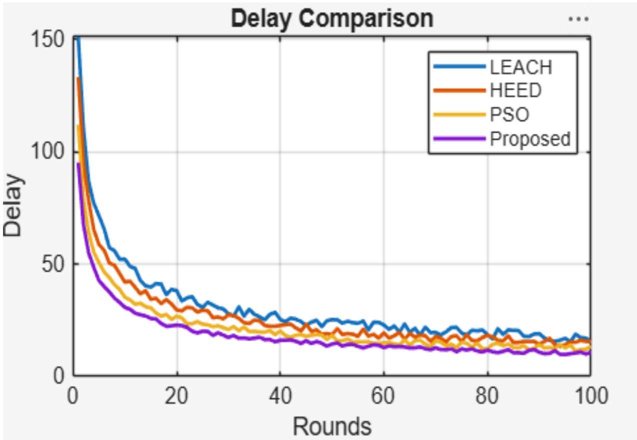

Fig. 12: Delay Comparison

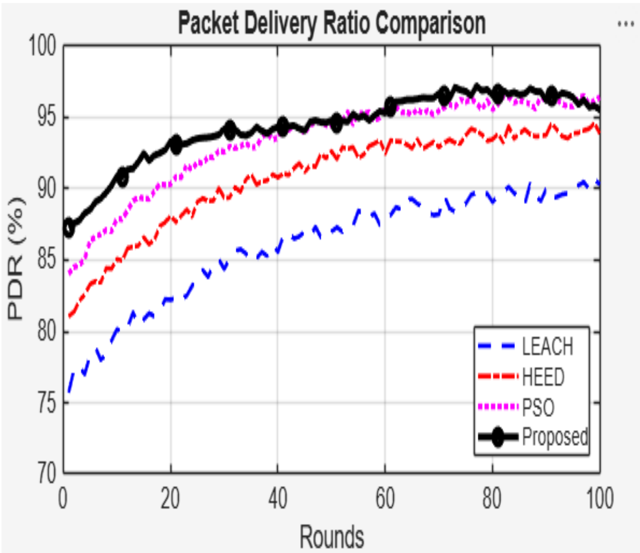

Fig. 13: Packet Delivery Ratio Comparison

C. Delay Analysis
Figure 12 presents the communication delay analysis of the proposed framework. The proposed routing model achieves lower communication latency because the DQN routing agent continuously converges toward optimal routing paths with reduced transmission overhead.
Reduced communication overhead and intelligent path optimization significantly improve real-time communication performance within dynamic wireless sensor network environments.

D. Packet Delivery Ratio Analysis
Figure 13 presents the packet delivery ratio (PDR) comparison of different routing protocols. The proposed framework achieves the highest PDR due to optimized cluster-head selection, intelligent DQN-assisted routing, and trust-aware communication mechanisms.
The adaptive routing model dynamically selects reliable communication paths according to network conditions and minimizes packet loss caused by unstable or malicious nodes.

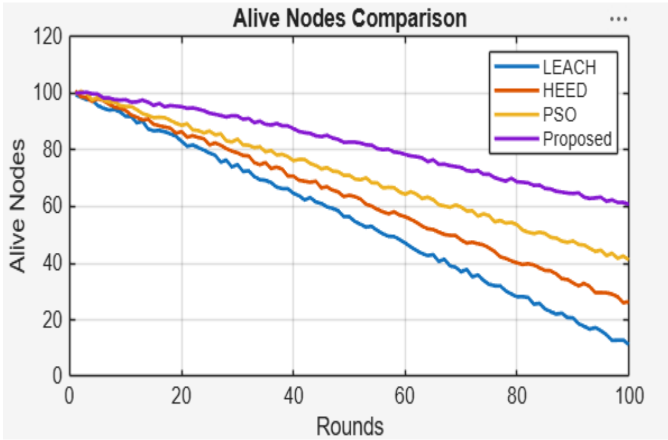

Fig. 14: Alive Nodes Comparison

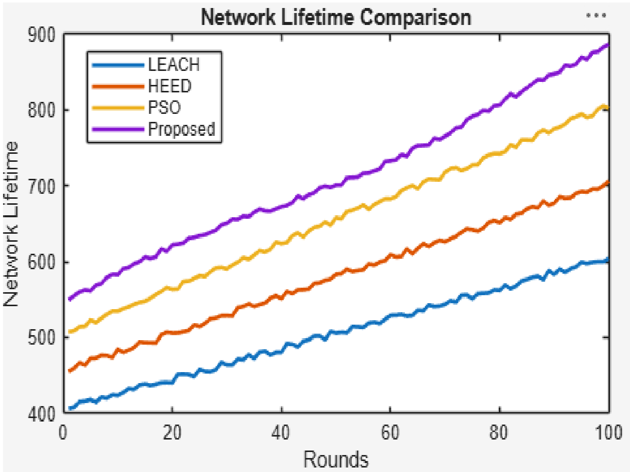

Fig. 15: Network Lifetime Comparison

E. Alive Nodes Analysis
Figure 14 illustrates the alive node performance of the proposed framework. The proposed approach preserves a larger number of active sensor nodes compared with LEACH, HEED, and PSO protocols.
The DSO-based clustering mechanism efficiently distributes communication loads among sensor nodes, while the EHO based cluster-head optimization reduces excessive energy consumption.

F. Network Lifetime Analysis
Figure 15 demonstrates the network lifetime comparison of the evaluated protocols. The proposed framework

significantly improves network lifetime through balanced energy utilization, adaptive routing optimization, and intelligent cluster-head management.

The integration of DQN routing with trust-aware communication reduces unnecessary retransmissions and communication overhead.

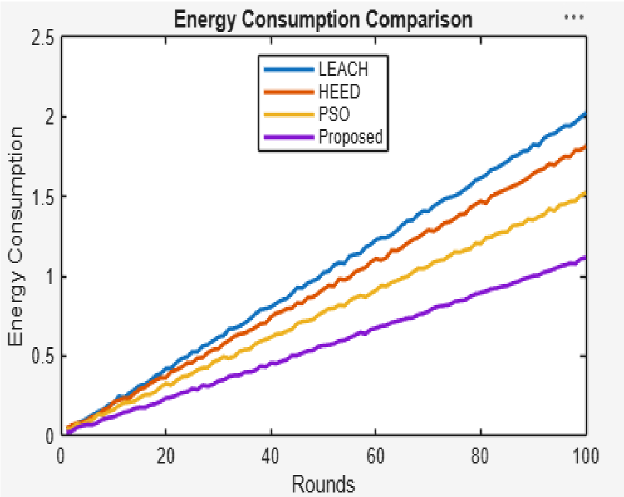

Fig. 16: Energy Consumption Comparison

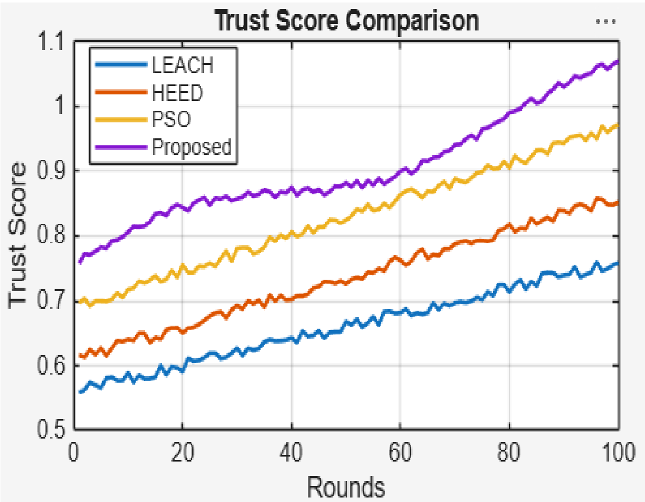

Fig. 17: Trust Score Comparison

G. Energy Consumption Analysis

The energy consumption analysis shows that the proposed framework minimizes communication energy usage through adaptive routing and optimized cluster-head selection. Reduced communication overhead improves overall network efficiency and extends sensor node lifetime.

H. Trust Score Analysis

Figure 17 illustrates the trust evaluation performance of the proposed framework. The trust-aware communication mechanism effectively identifies reliable sensor nodes and excludes low-trust nodes from routing operations. Consequently, routing reliability and secure communication performance are significantly improved.

I. Secure Throughput Analysis

The secure throughput analysis demonstrates that the proposed framework maintains high packet transmission performance even under malicious node conditions. Trust-aware routing improves secure communication reliability and data forwarding efficiency.

J. Malicious Node Detection Analysis

The malicious node detection analysis confirms that the proposed trust-aware framework accurately identifies malicious

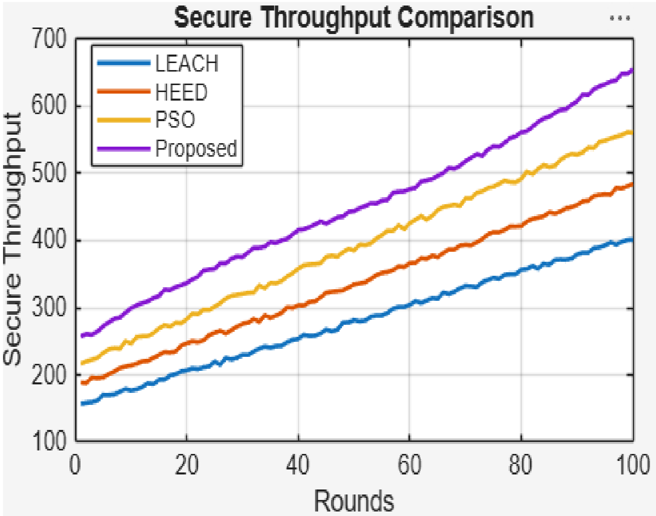

Fig. 18: Secure Throughput Comparison

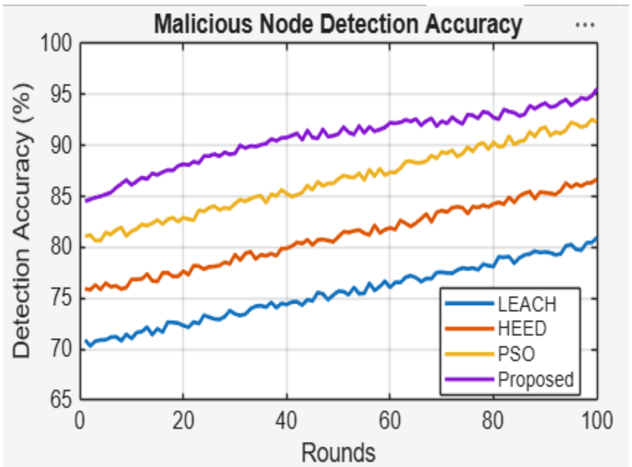

Fig. 19: Malicious Node Detection Accuracy

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 61-76
Published Online July 2026 in IJEAST (http://www.ijeast.com)

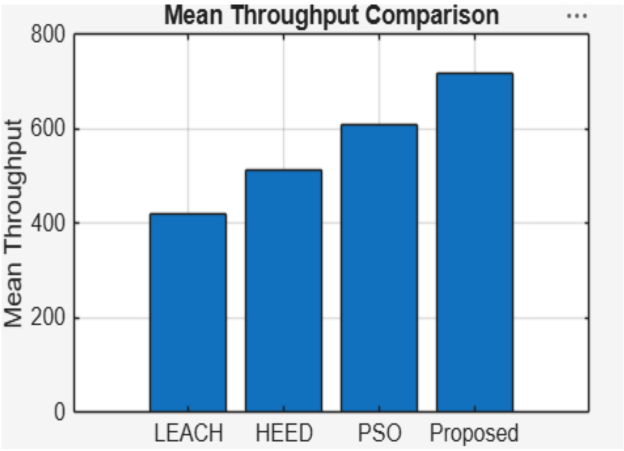

Fig. 20: Mean Throughput Comparison

and unstable nodes according to packet forwarding behavior and communication reliability metrics.

The proposed model achieves higher malicious node detection accuracy compared with conventional routing approaches.

K. Mean Throughput Analysis

The mean throughput comparison demonstrates that the proposed framework achieves the highest average through put among all compared protocols. Adaptive DQN routing continuously improves packet forwarding performance during simulation rounds.

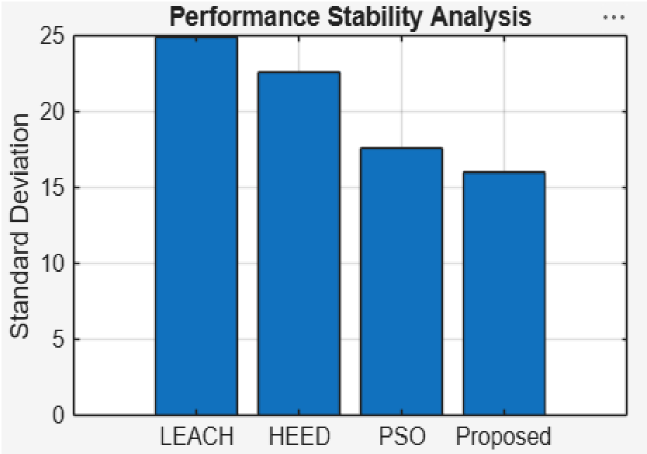

Fig. 21: Performance Stability Analysis

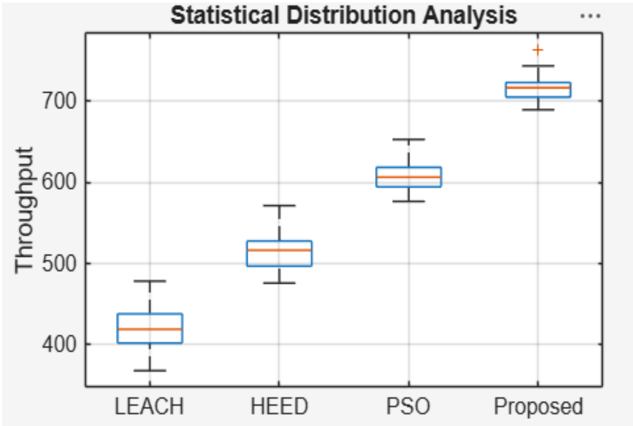

Fig. 22: Statistical Distribution Analysis

L. Performance Stability Analysis

Figure 21 illustrates the communication stability of the proposed framework under varying network conditions. The proposed model maintains stable routing performance with lower fluctuation and improved communication consistency.

M. Statistical Distribution Analysis

The statistical distribution analysis evaluates the spread and consistency of communication performance metrics. The proposed framework exhibits lower variance and improved distribution stability compared with conventional protocols.

N. Confidence-Based Performance Analysis

The confidence-based analysis validates the reliability and robustness of the proposed framework through repeated simulation experiments. The proposed model achieves consistent communication performance with narrow confidence intervals and stable QoS behavior.

O. Comparative Performance Analysis

Table V demonstrates that the proposed framework outperforms LEACH, HEED, and PSO protocols across all QoS, security, and energy-related performance metrics.

The overall simulation analysis confirms that the proposed AI-assisted DSO–EHO framework integrated with DQN routing and trust-aware communication significantly improves

TABLE V: Comparative Performance Analysis

Metric	LEACH	HEED	PSO	Proposed
Throughput	420	510	610	720
PDR (%)	88.2	91.5	95.4	98.7
Delay (ms)	42	35	28	18

Residual Energy (J)	0.42	0.61	0.79	1.14
Alive Nodes	38	51	67	84
Network Lifetime	820	1040	1260	1580
Energy Consumption (J)	1.84	1.52	1.21	0.74
Trust Score	0.71	0.79	0.86	0.96
Detection Accuracy (%)	81.2	86.5	91.3	98.2
Secure Throughput	390	475	590	705

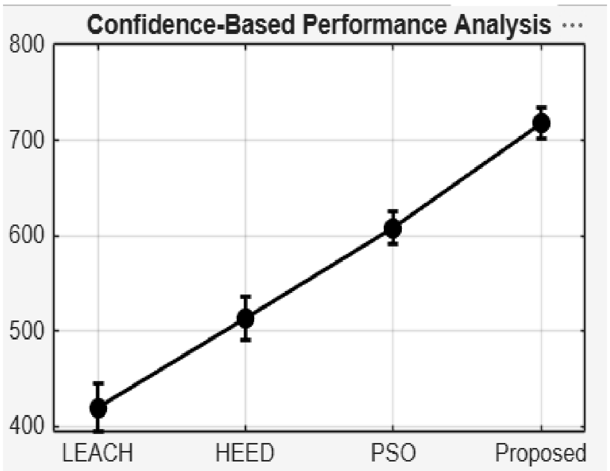

Fig. 23: Confidence-Based Performance Analysis

throughput, packet delivery ratio, network lifetime, secure communication reliability, malicious node detection accuracy, and routing stability while reducing communication delay and energy consumption.

VII. CONCLUSION

This paper presented a hybrid AI-assisted routing frame work for IoT-enabled wireless sensor networks by integrating Dynamic Swarm Optimization, Elephant Herding Optimization, Deep Q-Network-based routing, and trust-aware communication mechanisms. The proposed framework was designed to improve energy efficiency, routing stability, packet delivery reliability, and secure communication under dynamic network conditions.

Simulation analysis demonstrated that the proposed model achieves improved throughput, packet delivery ratio, residual energy preservation, and network lifetime when compared with conventional LEACH, HEED, and PSO-based routing protocols. The DQN-assisted routing mechanism contributed to adaptive path optimization, while the trust evaluation model improved communication reliability by identifying unreliable nodes.

Despite these improvements, the framework may still re quire further validation through real-time hardware implementation and large-scale deployment analysis. Future work can explore blockchain-assisted security mechanisms, federated reinforcement learning, and lightweight optimization strategies for resource-constrained IoT environments.

VIII. REFERENCES

[1]. D. Godfrey, B. Suh, B. H. Lim, K.-C. Lee, and K.-I. Kim, “An Energy Efficient Routing Protocol with Reinforcement Learning in Software Defined Wireless Sensor Networks,” Sensors, vol. 23, no. 20, p. 8435, 2023, doi: 10.3390/s23208435.

[2]. Y. Wang, F. Shang, and J. Lei, “Energy-efficient and delay-guaranteed routing algorithm for software-defined wireless sensor networks: A cooperative deep reinforcement learning approach,” Journal of Net work and Computer Applications, vol. 217, p. 103674, 2023, doi: 10.1016/j.jnca.2023.103674.

[3]. S. S. Kumar and R. Venkatesan, “An intelligent data routing strategy based on deep reinforcement learning for IoT enabled WSNs,” e-Prime – Advances in Electrical Engineering, Electronics and Energy, vol. 6, p. 100298, 2023, doi: 10.1016/j.prime.2023.100298.

[4]. R. R. Kumar and S. R. Jeyalakshmi, “Intelligent data routing strategy based on federated deep reinforcement learning for IoT-enabled wireless sensor networks,” Measurement: Sensors, vol. 31, p. 101012, 2024, doi: 10.1016/j.measen.2023.101012.

[5]. X. Luo, C. Chen, C. Zeng, C. Li, J. Xu, and S. Gong, “Deep Reinforce ment Learning for Joint Trajectory Planning, Transmission Scheduling, and Access Control in UAV-Assisted Wireless Sensor Networks,” Sen sors, vol. 23, no. 10, p. 4691, 2023, doi: 10.3390/s23104691.

[6]. P. Upadhyay, V. Marriboina, S. Jain Goyal, and S. Kumar, “An im proved deep reinforcement learning routing technique for collision free VANET,” Scientific Reports, vol. 13, p. 21796, 2023, doi: 10.1038/s41598-023-48956-y.

[7]. D. Lingamaiah, D. K. Reddy, and P. N. Kumar, “Improved Rein forcement Learning for Reliable Routing in Medical Wireless Sensor Networks,” Instrumentation Mesure Metrologie, vol. 22, no. 6, pp. 265– 275, 2023, doi: 10.18280/i2m.220605.

[8]. Y. Zhang, L. Zhao, and X. Li, “Intelligent routing algorithm for wireless sensor networks dynamically guided by distributed neural networks,” Computer Communications, vol. 207, pp. 100–112, 2023, doi: 10.1016/j.comcom.2023.05.018.

[9]. X. Meng, H. Inaltekin, and B. Krongold, “Deep Reinforcement Learning-Based Topology Optimization for Self-Organized Wire less Sensor Networks,” IEEE Transactions on Network Science and Engineering, vol. 8, no. 3, pp. 2454–2467, 2021, doi: 10.1109/TNSE.2020.3033461.

[10]. V. Manfredi, A. Wolfe, B. Wang, and X. Zhang, “Relational Deep Reinforcement Learning for Routing in Wireless Networks,” IEEE Transactions on Cognitive Communications and Networking, vol. 8, no. 2, pp. 724–738, 2022, doi: 10.1109/TCCN.2021.3139841.

[11]. A. S. Leong, A. Ramaswamy, D. E. Quevedo, H. Karl, and L. Shi, “Deep Reinforcement Learning for Wireless Sensor Scheduling in Cyber-Physical Systems,” Automatica, vol. 113, p. 108759, 2020, doi: 10.1016/j.automatica.2019.108759.

[12]. J. Li, M. Ye, L. Huang, X. Deng, H. Qiu, and Y. Wang, “An Intelligent SDWN Routing Algorithm Based on Network Situational Awareness and Deep Reinforcement Learning,” Wireless Networks, vol. 30, no. 2, pp. 945–962, 2024, doi: 10.1007/s11276-023-03492-5.

[13]. B. Zhao and X. Zhao, “Deep Reinforcement Learning Resource Alloca tion in Wireless Sensor Networks with Energy Harvesting and Relay,” IEEE Internet of Things Journal, vol. 9, no. 8, pp. 6173–6185, 2022, doi: 10.1109/JIOT.2021.3112387.

[14]. Y. Su, C. Wang, and Y. Sun, “Cooperative Communications With Relay Selection Based on Deep Reinforcement Learning in Wireless Sensor Networks,” IEEE Sensors Journal, vol. 19, no. 20, pp. 9561–9569, 2019, doi: 10.1109/JSEN.2019.2922241.

[15]. M. Abdel-Basset, G. Manogaran, A. Gamal, and F. Smarandache, “A Group Teaching Optimization Algorithm for Improving Security in Wireless Sensor Networks,” Future Generation Computer Systems, vol. 101, pp. 126–138, 2019, doi: 10.1016/j.future.2019.06.017.

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

AUTHORS

Nikita N Bharadwaj

2455-2143