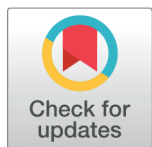


ORIGINAL ARTICLE



OPEN ACCESS

Received: 27/05/2026

Accepted: 10/06/2026

Published: 07/07/2026

Citation: Sruthi S, Hemalatha M (2026) HTER-ACOA: A Hybrid Trust-Energy Optimized Routing Framework Using Adaptive Coyote Optimization, Blockchain Consensus, and Fuzzy Deep Neural Network-Driven Anomaly Detection for Secure Hierarchical Wireless Sensor Networks. Indian Journal of Science and Technology 19(23): 1593-1610. <https://doi.org/10.17485/IJST/v19i23.sruthi>

* **Corresponding author.**sruthiwalyar@gmail.com**Funding:** None**Competing Interests:** None

Copyright: © 2026 Sruthi & Hemalatha. This is an open access article distributed under the terms of the [Creative Commons Attribution License](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Published By Indian Society for Education and Environment ([iSee](#))

ISSN

Print: 0974-6846

Electronic: 0974-5645

HTER-ACOA: A Hybrid Trust-Energy Optimized Routing Framework Using Adaptive Coyote Optimization, Blockchain Consensus, and Fuzzy Deep Neural Network-Driven Anomaly Detection for Secure Hierarchical Wireless Sensor Networks

S Sruthi^{1*}, M Hemalatha¹

¹ Department of Information Technology, Hindusthan College of Arts & Science, Coimbatore, Tamil Nadu, India

Abstract

Objectives: To develop a secure, adaptive, and energy-efficient routing framework for hierarchical Wireless Sensor Networks that enhances trust management, routing reliability, and communication performance in environments vulnerable to malicious attacks. **Method:** A Hybrid Trust-Energy Optimized Routing framework was developed by integrating Adaptive Coyote Optimization for cluster-head and relay-node selection based on residual energy and trust values. A Fuzzy Deep Neural Network was employed for anomaly detection and trust evaluation, while a lightweight Directed Acyclic Graph blockchain with Proof-of-Authority consensus was incorporated for secure and low-latency trust validation. The framework was implemented in Network Simulator-2 and evaluated against existing routing protocols using packet delivery ratio, throughput, network lifetime, end-to-end delay, trust detection accuracy, and routing overhead. **Findings:** The proposed framework achieved a packet delivery ratio of 96.9%, throughput of 223 kbps, and trust detection accuracy of 98.5%, outperforming all comparison methods. The network lifetime was extended to 1245 rounds, representing a 25.1% improvement over the best-performing baseline method. In addition, end-to-end delay was reduced to 128 ms and routing overhead to 12.2%. The integrated anomaly detection and blockchain-based trust validation mechanisms improved secure communication while maintaining low energy consumption and efficient routing performance. **Novelty:** This study introduces a unified trust-energy routing framework that combines Adaptive Coyote Optimization, Fuzzy Deep Neural Network-based anomaly detection, and lightweight blockchain validation. The proposed approach simultaneously enhances security, trust management, routing stability, and energy efficiency, providing a robust solution for hierarchical Wireless Sensor Networks.

Keywords: Wireless Sensor Networks; Secure Routing; Trust Management; Energy Efficiency; Anomaly Detection; Blockchain Validation

1 Introduction

Wireless Sensor Networks (WSNs) have emerged as a fundamental technology for a wide range of applications, including environmental monitoring, industrial automation, healthcare systems, smart agriculture, and military surveillance. A WSN consists of numerous sensor nodes that cooperatively monitor physical phenomena and transmit sensed data to a base station. Despite their broad applicability, WSNs face several challenges, including limited battery energy, dynamic network conditions, communication overhead, and vulnerability to security attacks. Consequently, designing secure and energy-efficient routing protocols remains a critical research issue in WSNs^{(1), (2), (3)}.

To improve energy utilization and prolong network lifetime, several hierarchical and cluster-based routing protocols have been proposed. Energy-aware routing approaches organize sensor nodes into clusters and employ Cluster Heads (CHs) to aggregate and forward data, thereby reducing communication overhead. Recent studies have introduced dynamic energy-aware routing, load-balanced clustering mechanisms, and adaptive cluster management techniques to enhance network performance and lifetime^{(4), (5), (6)}. Although these approaches effectively reduce energy consumption, they generally focus on energy optimization and often neglect security and trust management aspects.

To address security concerns, trust-aware routing mechanisms have been developed to identify reliable nodes and prevent malicious activities within the network. These methods evaluate node behavior using parameters such as packet forwarding ratio, communication reliability, residual energy, and interaction history. Trust-based routing frameworks have demonstrated significant improvements in routing reliability and attack mitigation by isolating suspicious nodes from routing decisions^{(7), (8), (9)}. However, most existing trust models rely on static trust updating mechanisms and limited behavioral analysis, resulting in inaccurate trust estimation under dynamic network conditions and sophisticated attack scenarios.

Recent advancements have also explored intelligent optimization and anomaly detection techniques to strengthen routing security and efficiency. Adaptive optimization algorithms, explainable anomaly detection models, and hybrid clustering approaches have been employed to improve route selection, malicious node identification, and network sustainability^{(10), (11), (12)}. Furthermore, adaptive routing strategies based on dynamic clustering and intelligent optimization have shown promising results in balancing energy consumption and enhancing communication reliability in heterogeneous WSN environments⁽¹³⁾.

Blockchain technology has recently attracted considerable attention as a decentralized mechanism for trust management and secure data validation in WSNs. By maintaining immutable transaction records, blockchain can improve routing transparency and prevent trust manipulation. However, conventional consensus mechanisms such as Proof-of-Work (PoW) and Proof-of-Stake (PoS) introduce significant computational complexity, communication overhead, and energy consumption, making them unsuitable for resource-constrained sensor nodes^{(7), (8)}.

Although existing protocols such as trust-based routing, energy-aware clustering, and secure optimization frameworks have achieved notable improvements, they still exhibit several limitations. Most approaches focus on either security enhancement or energy conservation rather than addressing both objectives simultaneously. Trust-based schemes often suffer from delayed trust adaptation and limited attack detection capability, while energy-aware protocols lack comprehensive trust assessment. Additionally, current anomaly detection methods may fail to accurately identify complex nonlinear attack patterns, and blockchain-based solutions frequently incur excessive resource overhead^{(14), (9), (10), (11), (12), (13)}.

1.1 Research Gap

Current schemes for WSN routing focus on improving one aspect alone, which is either security improvement or energy consumption. Trust-based routing methods have the drawback of inflexibility in handling threats, delayed computation process, and insufficient flexibility. Energy-based routing methods lack consideration of node behavior and security assessment. Furthermore, current blockchain-oriented designs consume a lot of system resources, and anomaly detection techniques are inefficient in detecting attacks that do not follow a definite pattern. Therefore, a unified routing strategy should be designed to integrate the features of adaptive trust management, intelligent detection, effective security verification, and energy efficiency in hierarchical WSNs^{(10), (11), (12), (13)}.

2 Methodology

For WSN with hierarchical clustering, HTER-ACOA (Hybrid Trust–Energy–Optimized Routing Framework) ensures secure, flexible, and balanced energy-based data transmission. The system design includes ACOA for global CH and relay election, FDNN for detecting anomalies and calculating trust dynamically, and DAG blockchain technology using Proof of Authority method for validating routes. The complete process flow diagram is provided in Figure 1, and the process involves five

steps: network initialization, trust and anomaly assessment, CH and relay optimization, route establishment, and blockchain validation.

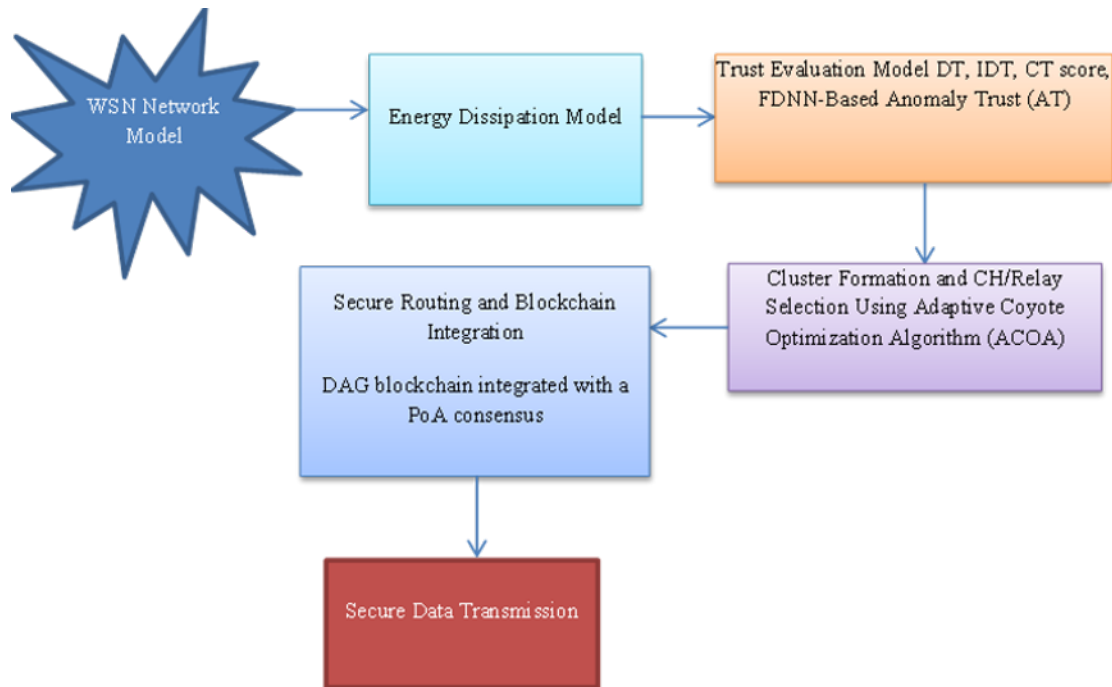


Fig 1. Proposed Block Diagram

2.1 Network-model

In the proposed HTER-ACOA framework, sensor nodes with unique IDs are randomly deployed in the sensing field and organized into clusters consisting of Cluster Heads (CHs) and Cluster Members (CMs). CHs perform data aggregation and transmit information to the Base Station (BS) through direct or multi-hop communication. The Adaptive Coyote Optimization Algorithm (ACOA) dynamically selects CHs and relay nodes by jointly evaluating residual energy, trustworthiness, and FDNN-based anomaly scores derived from direct and indirect interactions. This trust-aware and energy-efficient clustering mechanism enables adaptive CH rotation, balanced energy consumption, secure routing, and prolonged network lifetime.

Network Assumptions

- All nodes, including the BS, remain stationary after deployment.
- Each node has equal initial energy, processing capability, and sensing range.
- The BS can communicate directly with any node and has unlimited energy and high processing power.
- MH communication is supported between CHs and the BS.
- The trust model computes DT, IDT, and FDNN-based AT to identify reliable nodes and prevent routing through malicious ones.
- Energy efficiency, trust reliability, and secure routing decisions are jointly optimized in each round using the ACOA algorithm.

2.2 Energy dissipation model

Since WSN nodes are typically used in inaccessible or hostile environments, battery recharging or replacement is impractical. Therefore, minimizing energy consumption (EC) during communication is essential to prolong network lifetime. A first-order radio energy model that takes both multipath and free-space fading effects is used in the HTER-ACOA.

It ensures accurate estimation of transmission cost between communicating nodes. Distance d of transmitting x data bits from the EC of node n_i to node n_j is

$$ET_{(i,j)} = \begin{cases} x * E_{elec} + x * \varepsilon_{fs} * d^2 & d < d_0 \\ x * E_{elec} + x * \varepsilon_{mp} * d^4 & d \geq d_0 \end{cases} \quad (1)$$

To receive x bits of data, EC at node n_j is calculated as follows:

$$ER_{(i,j)} = x * E_{elec} \quad (2)$$

Here $d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}$, For modulation and digital coding d_0 , the EC of electronic circuit is denoted as E_{elec} . When $d \geq d_0$, $d < d_0$ is a threshold. The amplification parameters of transmitter hardware circuit is represented as ε_{fs} and ε_{mp} .

The following represents the EC for aggregating x data bits:

$$E_{agg} = x * E_{DA} \quad (3)$$

The radio energy per packet is denoted by E_{DA} .

Assume E_{ini} as an initial energy. The following equation expresses the residual energy (RE) of all node,

$$RE = E_{ini} - ET_{(i,j)} - ER_{(i,j)} - E_{agg} \quad (4)$$

The energy Trust Value E_{tv} is expressed as follows:

$$E_{tv} = \frac{RE}{E_{ini}} \quad (5)$$

This energy metric is integrated with the comprehensive trust model and used by ACOA for adaptive CH and relay selection. Nodes with higher E_{tv} and trust value are prioritized as CHs or routing intermediates. Consequently, energy-aware routing paths are formed dynamically to balance node utilization and extend network lifetime while maintaining secure and trustworthy data delivery.

2.3 Trust Evaluation Model

The HTER-ACOA framework employs an enhanced hybrid trust model derived from the earlier T-BMESR formulation. It estimates the reliability of each node through DT, IDT, and an integrated CT score, which jointly reflect behavioral consistency, interaction history, and neighborhood feedback. These values are periodically updated and used by the optimization module for adaptive routing.

1. Direct trust (DT)

A node's DT value is determined by looking at the behavior of neighboring nodes. The DT function is established by examining the neighbor's transmitting and receiving packet status. The calculation of DT between node n_i and neighbour n_j is:

$$DT_{(i,j)}^n = \varphi * HT_{(i,j)}^n + (1 - \varphi) * NT_{(i,j)}^n \quad (6)$$

Here, the historical TV of node n_i as assessed by node n_j in the past is represented by $HT_{(i,j)}^n$. In the current cycle, node n_i evaluates the TV of neighbour n_j , that is denoted as $NT_{(i,j)}^n$. $NT_{(i,j)}^n = r_j^n + s_j^n$.

The factors are measured by φ and $1 - \varphi$, the historical TV and current TV. These values, $0 < \varphi < 1$, are set for fairness in particular settings. Then, 0.5 is a common value of φ . r_j^n and s_j^n reflect the percentage of packets received and sent by node n_j to the total amount of packets:

$$r_j^n = \frac{\tau * rn_j - \mathcal{Z}n_j}{\ln_j} \quad (7)$$

$$s_j^n = \frac{\tau * sn_j - un_j}{\ln_j} \quad (8)$$

Node n_j denied to receive and send data, as indicated by $\mathcal{Z}n_j$ and un_j . $\ln_j$ is the over-all count of packets transmitted and received by n_j . Misbehaviour nodes' trust value decreases more quickly due to the adaptive penalty factor τ .

$$\tau = \frac{-p}{1 + t^{-q^*(XY_{n_j} + w)}} + 1 \quad (9)$$

$$XY_{n_j} = \frac{MX_{n_j}}{NX_{n_j}} \quad (10)$$

Here, the ratio of misbehaviour MX_{n_j} to normal behaviour NX_{n_j} across the previous five trust computation cycles is denoted by XY_{n_j} . The variable parameters of τ are q and w . MX_{n_j} rises quickly when a misbehaviour node is caught, which lowers the ratio of XY_{n_j} and, in turn, the τ values was reduced. The current assessment can be limited by MN's previous TV, which can be difficult to identify throughout the evaluation cycle. Prior to being recognised as a misbehaviour node, MN was a normal node with a higher TV. In practice, it requires more evaluation cycles to determine whether something is suspicious. The volatilisation factor Δ is included to increase the recognition speed and lessen the impact of historical TV. For the current evaluation cycle, historical TV is calculated using the formula below:

$$HT_{(i,j)}^n = \Delta * (DT_{(i,j)}^{n-1} + HT_{(i,j)}^{n-1}) \quad (11)$$

2. Indirect trust (IDT)

If there is insufficient information sharing between nodes or if the channel is impacted, IDT can be assessed for the node to progress the precision of the trust evaluation. IDT provides the TV between the node and the target nodes by using common nodes. The IDT between n_i and n_j is computed as follows:

$$IDT_{(i,j)}^n = \sum_{m \in q} (\varphi_m * DT_{(i,m)}^n * DT_{(j,m)}^n) \quad (12)$$

Here, n_i and n_j jointly hold a collection of trusted nodes denoted by q . To filter neighbour nodes and stop third-party node m from launching attacks, common neighbours of n_i and n_j may have trusted or untrusted nodes.

The following expression is provided to improve security and filter false evaluations:

$$dt_m^n = \sqrt{\frac{\sum_{V_x \in V} (\bar{D} - DT_{mV_x}^n)^2}{L}} \quad (13)$$

Here, node V_x is evaluated by node n_i . The median is denoted by D . V_x represents the nodes that n_i and the third-party node m jointly own. Whereas the common neighbours are represented by L . When the recommended threshold value of m is set to 0.5, its correspondence value is dt_m^n . The misbehaviour of m rises by L if dt_m^n is $>$ the threshold, and node n_i does not accept the m suggestion value. To increase trust accuracy, node m is given weights, which are stated as follows:

$$\varphi_m = \frac{DT_{(i,m)}^n}{\sum_{m \in q} DT_{(i,m)}^n} \quad (14)$$

3. Comprehensive trust

Comprehensive trust combines DT and IDT to indicate if a node is trustworthy or not, resulting in strong security and reliable nodes.

$$CT_{(i,j)}^n = \begin{cases} (1 - \beta) * DT_{(i,j)}^n + \beta * IDT_{(i,j)}^n & \text{if } n_j \neq m \\ (1 - \beta) * IDT_{(i,j)}^n + \beta * DT_{(i,j)}^n & \text{else } n_j = m \end{cases} \quad (15)$$

$$\beta = \begin{cases} 0.5 & \text{if } dt_m^n < \mu \\ DT_{(i,j)}^n - IDT_{(i,j)}^n \big| DT_{(i,j)}^n & \text{else } dt_m^n \geq \mu \end{cases} \quad (16)$$

The outcomes of the evaluators' assessments are the primary focus of comprehensive trust the weight coefficient is denoted by β .

4. FDNN-Based Anomaly Trust (AT)

Traditional fuzzy-SVM-based detectors in earlier frameworks such as T-BMESR and TBSEER perform inadequately when node behavior becomes nonlinear, overlapping, or uncertain under dynamic attack scenarios. To overcome this limitation, the proposed HTER-ACOA introduces a Fuzzy Deep Neural Network (FDNN) to evaluate Anomaly Trust (AT), providing high-precision trust deviation detection in uncertain network environments.

Each node n_i continuously monitors its neighboring nodes and extracts behavioral attributes that reflect communication reliability and energy stability. The observed features are represented as a multidimensional vector:

$$x_i = [PDR_i, RED_i, Delay_i, Density_i, TC_i] \quad (17)$$

where

- PDR_i : PDR,
- RED_i : Residual Energy Deviation,
- $Delay_i$: Mean end-to-end latency,
- $Density_i$: Neighborhood density, and
- TC_i : Trust Consistency across recent rounds.

The FDNN employs fuzzy membership functions in its input layer to quantify the uncertainty associated with each observation. For a given feature vector x_i , the fuzzy membership $\mu_i \in [0, 1]$ defines the reliability of the input, where values close to 1 denote highly consistent and trustworthy node behavior.

The network is trained with labeled data (normal and malicious node states) to minimize the following regularized cost function:

$$\min_{W, b, \xi} \frac{1}{2} \|W\|^2 + C \sum_{i=1}^N \mu_i \xi_i, \quad (18)$$

subject to

$$y_i (W^T \phi(x_i) + b) \geq 1 - \xi_i, \xi_i > 0. \quad (19)$$

Here,

- The deep network's weight and bias parameters are W and b .
- $y_i \in +1, -1$ represents the node class label (normal or malicious),
- $\phi(x_i)$ is the nonlinear deep-feature mapping,
- ξ_i is the slack variable handling misclassification, and
- C is the regularization constant.

The network output yields an anomaly confidence score $\hat{y}_i$, which is transformed into the Anomaly Trust (AT) value as follows:

$$AT_i = \frac{1}{1 + e^{-\hat{y}_i}} \quad (20)$$

The FDNN model was trained using labelled node-behaviour data consisting of normal and malicious node activities generated from the simulation environment. The dataset was divided into 70% training, 15% validation, and 15% testing samples. The network employed three hidden layers with ReLU activation and a sigmoid output layer. Training was performed using the Adam optimizer with a learning rate of 0.001 and a batch size of 64 for 100 epochs.

where higher AT_i implies greater behavioral normality and thus higher trust. If a node's predicted label is malicious ($y_i = -1$), its AT_i is set to a penalized minimum value ($AT_i = 0$), and it is excluded from routing and CH candidacy.

5. Final Hybrid Trust–Energy Metric (HTE)

The proposed trust architecture fuses DT, IDT, and AT into the CT (Eq. 15), which is then integrated with the node's residual energy (RE) ratio to generate the HTE score:

$$HTE_i = \alpha \frac{RE_i}{E_{ini}} + (1 - \alpha) CT_i, \quad (21)$$

where $\alpha \in [0, 1]$ controls the weighting between energy efficiency and trustworthiness.

Nodes with higher HTE_i are prioritized during ACOA processing for CH and relay selection, ensuring that routing decisions simultaneously satisfy energy-balance, reliability, and security constraints.

2.4 Cluster Formation and CH/Relay Selection Using ACOA

In Wireless Sensor Networks (WSNs), a large number of energy-constrained sensor nodes (SNs) are organized into clusters to reduce communication overhead and improve network efficiency. Each cluster is managed by a Cluster Head (CH), which performs data aggregation and forwards the processed information to the Base Station (BS) either directly or through relay nodes. To enhance network lifetime, balance energy consumption, and ensure routing security, the proposed HTER-ACOA framework dynamically forms clusters and intelligently selects CHs based on network conditions, enabling efficient data aggregation, secure multi-hop communication, and optimized energy utilization across the network.

1. Cluster Formation Phase

Using RSSI measurements, nodes estimate their distance from the Base Station (BS) and neighboring nodes to form clusters within the communication range. Each node calculates a Cluster Head (CH) threshold based on residual energy, comprehensive trust value, and FDNN anomaly score. Nodes with high threshold values that have not recently served as CHs broadcast ADV messages, and sensor nodes select the most reliable and energy-efficient CH by evaluating the received advertisements. This process ensures that Cluster Members (CMs) connect to CHs with strong trustworthiness and sufficient energy reserves, improving network stability and secure communication.

2. Enhanced CH threshold calculation

Each node computes its Cluster Head eligibility threshold $T(n)$ based on its energy, trust, and previous CH participation:

$$T(n) = \begin{cases} \frac{P}{1 - P \times (r \bmod (\frac{1}{P}))} \times \left(\alpha \cdot \frac{RE_n}{E_{ini}} + \beta \cdot HTE_{(n)} \right), & \text{if } n \in G \\ 0, & \text{otherwise} \end{cases} \quad (22)$$

Here:

- P: The optimal % of CHs in each round (e.g., 5%).
- r: Current round number.
- G: Collection of nodes that wasn't CHs in the past 1/P rounds.
- RE_n : RE of node n.
- HTE_n : Hybrid Trust–Energy value of node n,
- α, β : Weights (typically $\alpha + \beta = 1$) to balance energy and trust contributions.

The self-adaptive HTER-ACOA mechanism selects only nodes with high residual energy, strong trust levels, and low FDNN anomaly scores as Cluster Heads (CHs), effectively reducing the impact of selective forwarding, blackhole, and Sybil attacks by assigning low trust values to malicious nodes. Sensor nodes evaluate received ADV messages using RSSI and Hybrid Trust Evaluation (HTE) values and join the CH with the highest trust and strongest signal strength as Cluster Members (CMs). Subsequently, each CH creates a TDMA schedule to ensure collision-free and energy-efficient data transmission within the cluster.

To prevent early depletion of energy, CH roles are rotated periodically based on updated RE_i and HTE_i values, ensuring balanced energy distribution among nodes.

3. Adaptive Cluster Head (CH) and Relay Node Selection

Unlike traditional protocols such as LEACH, T-BMESR, and TBSEER that rely on static or probability-based cluster head selection, HTER-ACOA employs the Adaptive Coyote Optimization Algorithm (ACOA) for dynamic CH and relay node selection. Inspired by the social behavior and adaptability of coyote packs, each coyote represents a potential routing solution, enabling the algorithm to continuously adapt to changing network conditions. By considering factors such as hop-to-energy ratio, residual energy, trust reliability, routing stability, and distance to the base station, ACOA optimizes node assignment, balances energy consumption, enhances network lifetime, supports secure data transmission, and reduces communication delay.

Representation of a Coyote and Pack Formation

Each coyote in the population represents a candidate solution vector:

$$C_k = [CH_1, CH_2, \dots, CH_m, R_1, R_2, \dots, R_l], \quad (23)$$

where CH_i and R_j denote selected Cluster Heads and relay nodes, respectively.

The entire population of coyotes is divided into P packs, each containing N_c coyotes. The population is initialized randomly based on network topology and node energy constraints.

Fitness Function Formulation

Each node's candidacy for CH or relay role is determined by the fitness value computed through ACOA, which jointly considers the node's HTE score, RE, and distance to the BS. The fitness function:

$$F_i = \omega_1 HTE_i + \omega_2 \frac{E_{res,i}}{E_{ini}} - \omega_3 \frac{D_i}{D_{max}}, \quad (24)$$

where $\omega_1 + \omega_2 + \omega_3 = 1$.

Here,

- HTE_i = Hybrid Trust–Energy value combining trust and residual energy;
- $E_{res,i}$ = current RE of node i ;
- D_i = distance of node i to the BS;
- D_{max} = maximum distance among all nodes.

Nodes with higher fitness scores are prioritized as CH or relay candidates. ACOA simulates adaptive social learning among “coyotes” (candidate nodes), allowing the system to converge rapidly toward an energy-balanced and secure CH configuration while preventing premature node exhaustion.

Social Adaptation and Coyote Position Update

Within each pack, coyotes adapt by learning from both the best (α -coyote) and the mean (social trend) of the group. For a coyote C_k at iteration t , the position update rule is given as:

$$C_k^{t+1} = C_k^t + r_1 \cdot (C_\alpha^t - |r_2 \cdot C_{mean}^t|), \quad (25)$$

Where

- C_α^t : The best-performing coyote in the pack (highest fitness),
- C_{mean}^t : Mean position vector of the pack,
- r_1, r_2 : Random numbers in $[0,1]$ controlling exploration and exploitation.

After each iteration, if the new position C_k^{t+1} yields a higher fitness, it replaces the old one. This mechanism ensures continuous adaptation and avoids premature convergence.

Adaptive Mechanism

To enhance convergence stability, unlike the standard Coyote Optimization Algorithm (COA), the proposed Adaptive Coyote Optimization Algorithm (ACOA) incorporates an adaptive coefficient λ_t to dynamically balance global exploration and local exploitation:

$$\lambda_t = \lambda_{max} - \frac{(\lambda_{max} - \lambda_{min}) \cdot t}{t_{max}} \quad (26)$$

where

- t : Current iteration,
- t_{max} : Maximum iterations,
- λ_{max} and λ_{min} : Upper and lower limits of adaptation rate.

The updated coyote position is refined using this adaptive factor:

$$C_k^{t+1} = C_k^t + \lambda_t \cdot (C_\alpha^t - C_{mean}^t) \quad (27)$$

This mechanism ensures fast convergence in early iterations and fine-tuning in later stages.

Algorithm: Adaptive Coyote Optimization Algorithm for CH and Relay Selection

Input: Node set N , residual energy E_{res} , HTE values, maximum iteration t_{max}

Output: Optimal CH and relay node sets

- (a) **Initialize** network parameters and coyote population.
- (b) **Evaluate** each coyote using fitness function (Eq. 24).
- (c) **Identify** the α -coyote (best fitness) and compute pack mean.
- (d) **Update** positions using Eq. (25) and adaptive coefficient Eq. (27).
- (e) **Recalculate** fitness; replace weaker coyotes if new fitness improves.
- (f) **Iterate** until $t = t_{max}$ or convergence.
- (g) **Select** final CHs and relays based on highest HTE_{*i*} and F .
- (h) **Broadcast** CH–relay assignments to nodes for data transmission.

4. Relay Node Selection and Load Balancing

After cluster head (CH) formation, ACOA selects relay nodes for inter-cluster communication by minimizing transmission energy while maximizing end-to-end trust. The protocol continuously monitors residual energy and link quality, periodically rotating CH and relay roles to balance energy consumption and enhance network lifetime. CHs collect data from cluster members, remove redundant packets through aggregation, and forward the processed data to higher-level CHs or the base station via the most trusted relay nodes. Routing paths are established based on the highest Hybrid Trust Evaluation (HTE) value and Routing Priority Score (RPS), ensuring secure communication, energy-efficient routing, and long-term network stability.

2.5 Secure Routing and Blockchain Integration

After selecting optimal CH and relay nodes through the Adaptive Coyote Optimization Algorithm (ACOA), the next objective of the HTER-ACOA framework is to establish secure, trustworthy, and energy-efficient routing.

This is achieved through a dual mechanism:

1. Hybrid Trust–Energy (HTE)-driven Routing, ensuring data flows only through reliable and energy-sufficient nodes.
2. Directed Acyclic Graph (DAG) blockchain integrated with a Proof-of-Authority (PoA) consensus, which performs distributed validation of routing activities and trust updates with minimal delay and energy overhead.

1. Hybrid Trust–Energy (HTE)-Based Routing

Routing in the HTER-ACOA framework contains 2 sequential phases: Intra-Cluster Communication and Inter-Cluster Communication.

Intra-Cluster Phase:

- Every CM transmits its detected data to the associated CH via a single-hop link following the TDMA schedule assigned by the CH.
- The CH aggregates all received data packets, eliminates redundancy, and produces a compressed packet using an aggregation function:

$$D_{agg} = f_{agg}(D_1, D_2, \dots, D_k) \quad (28)$$

where D_i represents data from CM i .

- This aggregation reduces overall traffic, minimizes transmission energy, and lowers the risk of congestion or packet collisions within the cluster.

Inter-Cluster Phase:

- After aggregation, either directly or through multi-hop relays, each CH is required to forward the packet to the BS.
- The next hop is determined using a Routing Priority Score (RPS) that integrates trust, energy, and distance parameters:

$$RPS_i = \gamma_1 \frac{HTE_i}{HTE_{\max}} + \gamma_2 \frac{E_{res,i}}{E_{\max}} + \gamma_3 \frac{D_i}{D_{\max}} \quad (29)$$

where:

- HTE_i : Hybrid Trust–Energy value of node i ,
- $E_{res,i}$: Current RE of node i ,
- D_i : Distance between node i and the next hop or BS,
- $\gamma_1 + \gamma_2 + \gamma_3 = 1$: Normalized weighting coefficients.

The node with the highest RPS among trusted neighbors is chosen as the next-hop relay. This ensures that every transmission step prioritizes:

- Security: only trusted nodes (validated by FDNN and blockchain) are selected,
- Energy balance: nodes with higher residual energy are preferred,
- Low latency: shorter routes with better link quality are chosen.

Routing continues until the aggregated data reaches the BS. Each transmission generates a trust-update event, logged in the distributed ledger for validation.

2. DAG–PoA Blockchain Validation Mechanism

Conventional blockchain frameworks mainly use Proof-of-Work (PoW), which requires high computational power and energy consumption, making them unsuitable for wireless sensor networks. To address this issue, the HEART-ACOA framework employs a Directed Acyclic Graph (DAG) structure along with a Proof-of-Authority (PoA) consensus mechanism. These approaches enable parallel transaction validation while reducing latency, computational complexity, and energy usage.

(a) DAG Ledger Construction

- Each CH acts as a blockchain node and generates a transaction vertex v_t whenever a trust update, anomaly detection, or routing event occurs.
- Unlike linear blockchains, DAG allows multiple blocks (vertices) to be appended simultaneously, increasing throughput and reducing propagation delay.
- Each new vertex references two existing parent vertices, maintaining causal order while enabling concurrent validation.

Each transaction vertex v_t is expressed as:

$$H(v_t) = Hash(ID_t \parallel T_t \parallel \sigma_t \parallel H(v_1) \parallel H(v_2)) \quad (30)$$

Where:

- $H(v_t)$: Hash of the current transaction,
- ID_t : Node ID performing the transaction,
- T_t : Type of event (e.g., CH election, route forwarding, anomaly report),
- σ_t : Digital signature of the validator node,
- $H(v_1), H(v_2)$: Hashes of the parent nodes (past events).

This hashing model maintains cryptographic integrity and prevents double-spending or trust forgery.

(b) **Proof-of-Authority (PoA) Consensus**

- Some of high-trust CHs, validated by the FDNN and trust assessment model, are selected as PoA Validator.
- Validators verify lightweight signatures and add transactions to the DAG if they are valid.
- The validation process includes:
 - Verifying the validity of the node's ID and signature $\sigma_t \sigma_t \sigma_t$;
 - Check energies and trust levels of the reporter node;
 - While the transaction does not duplicate or contradict existing records.
- After validating the vertex, it is permanently added to the DAG, and this update will be propagated to other CHs.
 - High-trust cluster heads identified through the FDNN and trust evaluation process are chosen as PoA validators.
 - These validators verify lightweight signatures and approve valid transactions before adding them to the DAG structure.
 - The validation process includes:
 - i. The system verifies the node identity and validates the signature σ_t .
 - ii. The energy level and trust value of the reporting node are then examined.
 - iii. The transaction is checked to ensure that it does not duplicate or conflict with existing records.
 - Once verified, the transaction is permanently stored in the DAG and shared with other cluster heads in the network.

The PoA scheme eliminates the need for heavy computation (as in PoW) or token staking (as in PoS), making it highly energy-efficient and suitable for constrained WSN environments.

3. **Secure Routing Workflow**

The integration of routing and blockchain validation follows these steps:

- (a) **Initialization:** CHs and relays selected by ACOA broadcast their HTEHTEHTE and residual energy values.
- (b) **Route Formation:** Each CH computes RPSiRPS_iRPSi for nearby nodes and chooses the best next hop.
- (c) **Data Transmission:** Aggregated data is forwarded securely through high-RPS nodes toward the BS.
- (d) **Event Logging:** Each CH logs routing and trust events as transaction vertices in the DAG ledger.
- (e) **PoA Validation:** Designated validators verify and sign transactions; validated vertices are appended concurrently.
- (f) **Ledger Update:** All CHs synchronize the updated DAG locally for future trust decisions.
- (g) **Re-Optimization:** ACOA re-runs in the next round using the updated HTEHTEHTE and trust scores, adapting to energy or topology changes.

This cyclic interaction between optimization, trust computation, and blockchain verification ensures continuous network self-adaptation and long-term resilience against malicious activity.

After this phase, the HTER-ACOA framework achieves:

- (a) Secure data delivery through verified and immutable routing records,
- (b) Energy efficiency by avoiding redundant re-validation and costly computations,
- (c) Dynamic adaptability where trust and route updates are continuously integrated,
- (d) Resilience to attacks like selective forwarding, on-off, Sybil, and bad-mouthing, through distributed anomaly detection and PoA consensus.

2.6 Experimental Setup and Reproducibility

2.6.1. Dataset and Network Configuration

The suggested HTER-ACOA architecture was modeled and analyzed through NS-2.35 simulation tool. A hierarchy WSN comprising 100 to 500 nodes was randomly deployed within a sensing region of 1000 m × 1000 m. All nodes in the network had the same initial energy level, transmission range, and sensing capacity. In addition, normal as well as malicious nodes were present in the simulation environment.

2.6.2. Baseline Methods for Comparison

The performance of HTER-ACOA was compared with the following state-of-the-art routing frameworks:

- T-BMESR
- TBSEER
- ETOR
- MSCR
- EASR

All algorithms were evaluated under identical network conditions and simulation settings to ensure a fair comparison.

2.6.3. Statistical Validation

In order to increase the reliability of our experimental process, we repeated each simulation run 30 times for a number of random network configurations. The results we provided are the averages for all simulation runs. We performed standard deviations and 95% confidence intervals calculations in order to assess the variance in our results. The statistical significance of differences between HTER-ACOA and other approaches was checked by the one-way ANOVA test.

2.6.4. Reproducibility Statement

All simulation parameters, routing strategies, trust metric equations, ACOA optimization techniques, FDNN training parameters, and blockchain validation methods used in this study are all clearly stated here to aid in replication efforts by future researchers.

3 Results and Discussion

The network simulator NS2 tool is used in this part to simulate and perform T-BMESR performance with an experimental setup. A BS is situated on top of the sensing region, and 100 nodes are arranged at random throughout a 1000×1000 m network space as part of the simulation setup. The trust model is used to introduce and identify MN like BH and SFA. Table 1 displays all of the simulation parameters. Every SN has the same energy level and is uniform and static. Performance indicators including network T, packet deliver ratio (PDR), NL, and EC are calculated and the suggested HTER-ACOA is compared with ETOR, MSCR, TBSEER, EASR and T-BMESR.

Table 1. Simulation parameters

Parameter	Value
System configuration region	1000 × 1000 mts
SN installed in system	100 nodes
Initial energy allocated	2J
DA energy	20 nJ
Transmission energy	30 nJ
Receiver Energy	20 nJ
Packet Size	256
MAC	802.11
TV	(0 to 1)
Rounds Count	50
BS	1

1. Network Throughput

It is the proportion at which valid DP are successfully distributed to the destination (BS) over the communication channel. It reveals the data delivery capacity of the routing protocol.

$$Throughput = \frac{\sum_{i=1}^N P_i \times S_i}{T_{Sim Time}} \quad (31)$$

Where:

- P_i : Number of successfully received packets by node iii
- S_i : Size of each packet (in bits or bytes)
- $T_{Sim Time}$: Total simulation time (in seconds)
- Units: kbps or bps

2. PDR

When compared to the total packet count that are *sent* by the source nodes, PDR is the proportion of DP that are effectively *received* by the destination. It assesses the RP's dependability.

$$PDR (\%) = \left(\frac{P_{received}}{P_{sent}} \right) \times 100 \quad (32)$$

Where:

- $P_{received}$: Over-all count of DP received by the BS
- P_{sent} : Over-all count of DP sent by all SN

3. NL

The amount of time (rounds) until a specific proportion of nodes run out of energy is known as NL. It is a crucial indicator of the protocol's sustainability and EE.

$$Network Lifetime = R_{last alive} \quad (33)$$

The count of simulation rounds until all nodes are dead or the first threshold is achieved is denoted by $RR_{last alive}$.

4. EC

Throughout the entire simulation, the total EC by all nodes. It helps measure the efficiency of the RP in using battery power.

$$Energy Consumption = \sum_{i=1}^N (E_{init}^i - E_{rem}^i) \quad (34)$$

Where:

- E_{init}^i : node i's initial energy
- E_{rem}^i : Remaining energy of node i at the termination of experiment
- Units: Joules (J)

The results demonstrate that HTER-ACOA consistently outperforms ETOR, MSCR, TBSEER, EASR, and T-BMESR throughout network operation. The framework achieves superior packet delivery, throughput, network lifetime, and trust detection accuracy while reducing energy consumption, end-to-end delay, and routing overhead. These improvements are enabled by the integration of Adaptive Coyote Optimization for efficient cluster-head and relay selection, FDNN-based trust evaluation for accurate malicious node detection, and lightweight DAG-PoA blockchain validation for secure routing. Overall, HTER-ACOA provides a stable, scalable, energy-efficient, and secure routing solution for hierarchical wireless sensor networks operating in dynamic and hostile environments.

Packet Delivery Ratio (PDR): Figure 2 compares the Packet Delivery Ratio (PDR) of different routing protocols, where a higher PDR indicates more reliable data delivery and better network performance. Although packet delivery generally decreases with increasing rounds due to congestion and energy depletion, HTER-ACOA consistently achieves the highest PDR, ranging from 94.6% to 96.9%, outperforming ETOR, MSCR, TBSEER, EASR, and T-BMESR. This superior performance is achieved through adaptive routing and trust-aware path selection, which reduce packet loss and avoid unreliable or malicious nodes.

Throughput: Figure 3 compares the throughput of different routing protocols, where throughput represents the rate of successful data packet delivery and indicates communication efficiency. As network operation progresses, throughput generally improves due to increased routing stability and reduced packet loss. Among the evaluated methods, HTER-ACOA achieves the highest throughput, demonstrating superior data transmission efficiency and effective utilization of network resources.

Figure 3 shows that HTER-ACOA achieves the highest throughput, increasing from 205 kbps to 223 kbps, outperforming ETOR, MSCR, TBSEER, EASR, and T-BMESR. The improved performance is attributed to adaptive routing, efficient cluster-head and relay selection, reduced packet loss, and reliable communication paths, which minimize congestion and enhance overall data transmission efficiency.

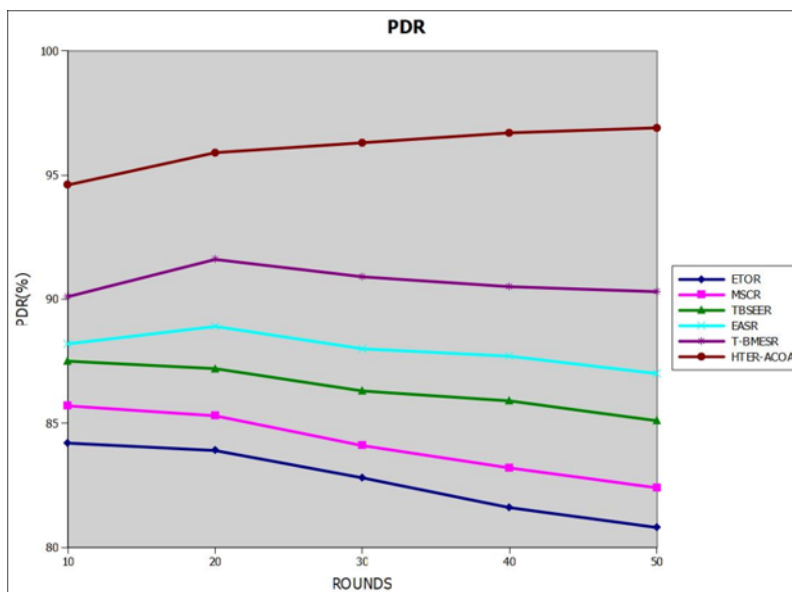


Fig 2. Packet Delivery Ratio Comparison

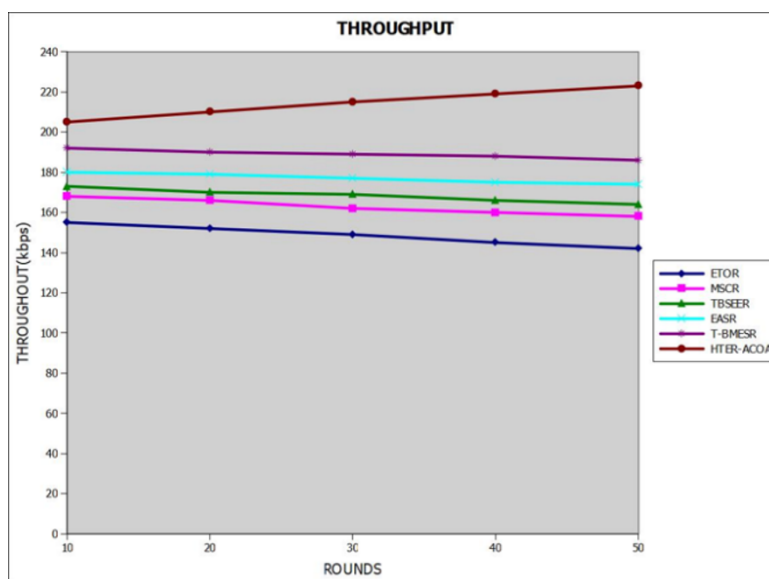


Fig 3. Comparison Chart of Throughput

Average Energy Consumption: Figure 4 shows that HTER-ACOA achieves the lowest energy consumption, decreasing from 1.28 J/node to 0.86 J/node, compared to ETOR, MSCR, TBSEER, EASR, and T-BMESR. Through adaptive optimization, intelligent route selection, and efficient packet forwarding, the proposed protocol minimizes redundant transmissions and energy wastage, resulting in improved energy efficiency and prolonged network operation.

Network Lifetime: Figure 5 shows that HTER-ACOA achieves the longest network lifetime, increasing from 1045 to 1245 rounds, outperforming ETOR, MSCR, TBSEER, EASR, and T-BMESR. The improvement is achieved through efficient traffic distribution, adaptive cluster-head selection, and balanced energy utilization, which prevent premature node depletion and significantly extend the operational lifetime of the wireless sensor network.

End-to-End Delay: Figure 6 demonstrates that HTER-ACOA achieves the lowest end-to-end delay, reducing it from 138 ms to 128 ms, compared to ETOR, MSCR, TBSEER, EASR, and T-BMESR. By selecting the most reliable and shortest routing paths

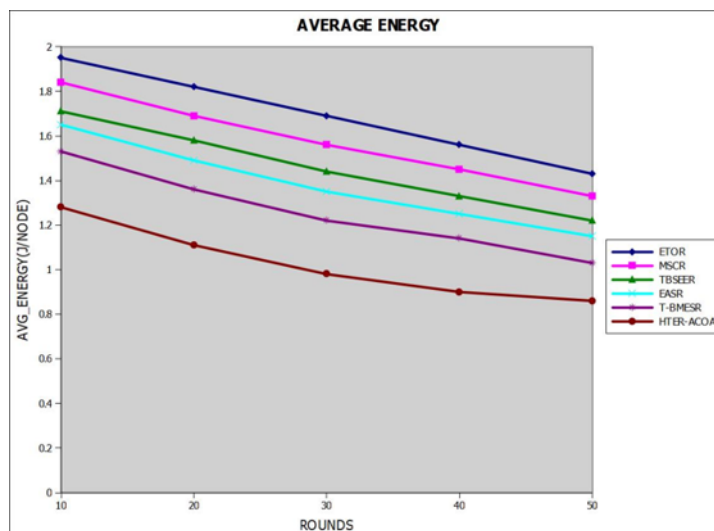


Fig 4. Average Energy Comparison

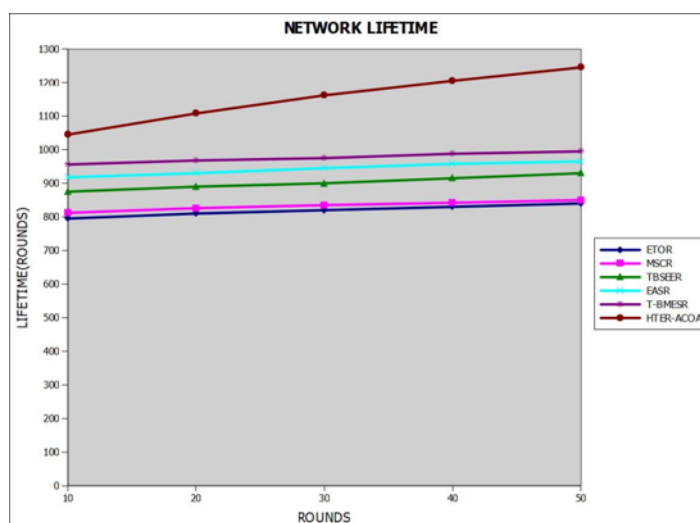


Fig 5. Network Lifetime Comparison

while avoiding congested nodes, the proposed protocol enables faster packet delivery, improved network responsiveness, and enhanced real-time communication performance.

Trust Detection Accuracy: Figure 7 shows that HTER-ACOA achieves the highest trust detection accuracy, improving from 96.2% to 98.5%, outperforming ETOR (80.9–81.3%), MSCR, TBSEER, EASR, and T-BMESR. The superior performance is attributed to its FDNN-based adaptive trust evaluation mechanism, which effectively identifies malicious and unreliable nodes, ensuring secure routing and reliable network communication.

Routing Overhead: Figure 8 shows that HTER-ACOA achieves the lowest routing overhead, decreasing from 13.5% to 12.2%, compared to ETOR, MSCR, TBSEER, EASR, and T-BMESR. By maintaining stable routes, optimizing route discovery, and reducing unnecessary control messages, the proposed protocol minimizes communication overhead and improves overall network resource utilization and routing efficiency.

The performance achieved by HTER-ACOA is consistent with recent trust-aware routing studies in WSNs. For example, TBSEER reported improvements in secure routing through trust evaluation, while ETOR focused on energy-aware route selection. However, the proposed HTER-ACOA achieved a higher Packet Delivery Ratio (96.9%) and Trust Detection Accuracy (98.5%) due to the integration of FDNN-based trust assessment and Adaptive Coyote Optimization. Similar findings were

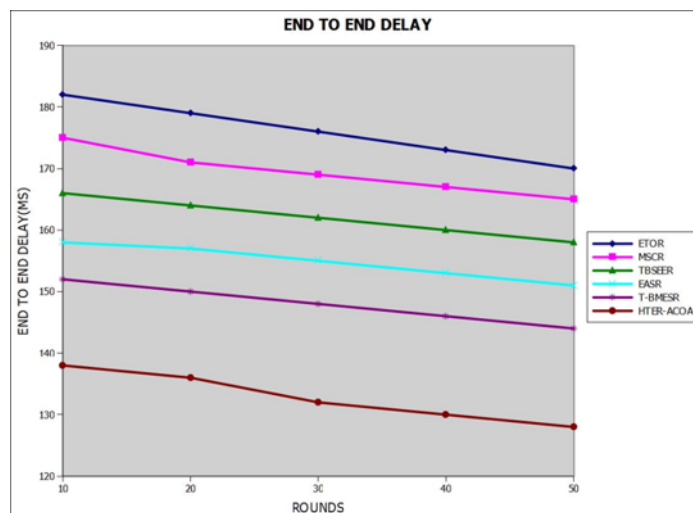


Fig 6. End to End delay Comparison

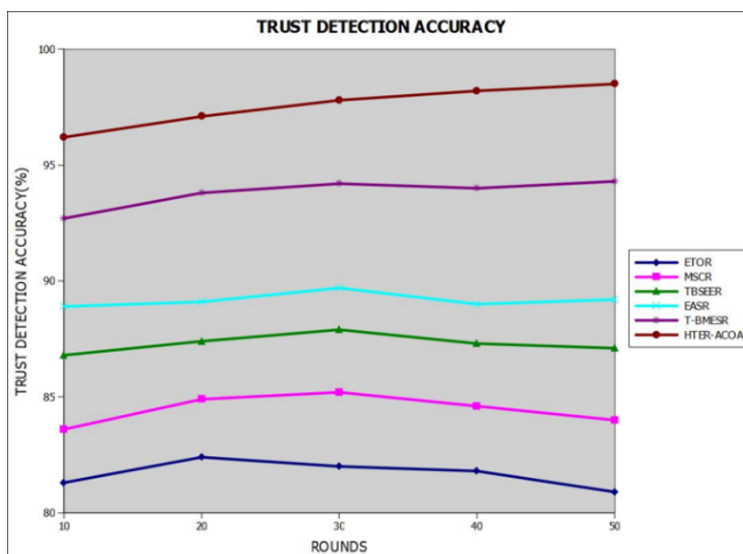


Fig 7. Trust Detection Accuracy Comparison

reported in recent blockchain-enabled routing studies, where decentralized route verification improved routing security and reliability.

3.1 Discussion

The results indicate that HTER-ACOA outperforms ETOR, MSCR, TBSEER, EASR, and T-BMESR in terms of Packet Delivery Ratio (96.9%), throughput (223 kbps), network lifetime (1245 rounds), and trust detection accuracy (98.5%), while reducing energy consumption, end-to-end delay, and routing overhead. These improvements are mainly attributed to the integration of Adaptive Coyote Optimization Algorithm (ACOA), FDNN-based anomaly detection, and DAG-PoA blockchain validation. The ACOA mechanism enables efficient cluster-head and relay-node selection based on trust and residual energy, resulting in stable routing and balanced energy utilization. Similar findings have been reported by Wang *et al.*⁽⁶⁾ and Zhang *et al.*⁽¹³⁾, who highlighted the effectiveness of intelligent optimization for enhancing network performance. Furthermore, the FDNN model improves malicious node detection compared with traditional trust-based approaches, consistent with the observations of TITAN⁽¹¹⁾ and HEXADWSN⁽¹²⁾. Unlike existing protocols that focus primarily on either security or energy efficiency, HTER-

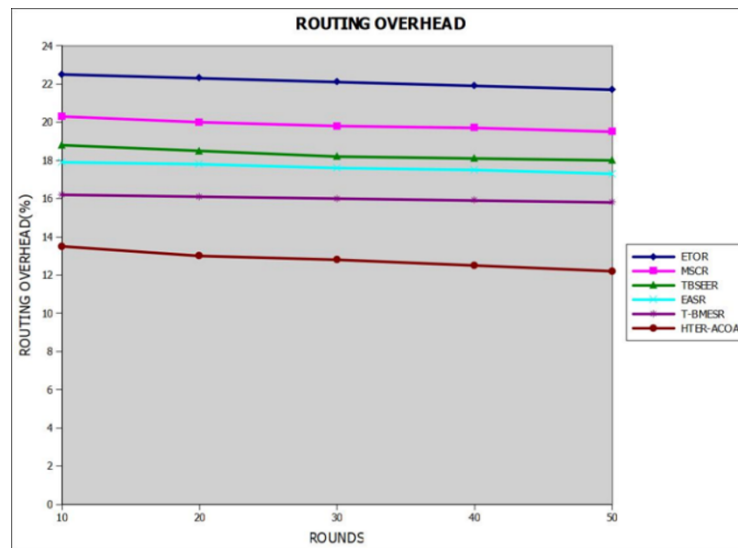


Fig 8. Routing Overhead Comparison

ACOA jointly optimizes both objectives while maintaining low routing overhead through lightweight DAG-PoA blockchain validation. Therefore, the proposed framework provides a secure, reliable, and energy-efficient routing solution for hierarchical wireless sensor networks operating in dynamic and hostile environments.

4 Conclusion

This study proposed HTER-ACOA, a hybrid trust-energy optimized routing framework for hierarchical Wireless Sensor Networks that integrates Adaptive Coyote Optimization, Fuzzy Deep Neural Network-based anomaly detection, and lightweight DAG-PoA blockchain validation. By jointly optimizing trust, energy efficiency, and routing stability, the framework overcomes the limitations of existing routing protocols. Simulation results demonstrated superior performance, achieving 96.9% packet delivery ratio, 223 kbps throughput, 98.5% trust detection accuracy, extended network lifetime, reduced energy consumption, lower routing overhead, and minimized delay compared to existing methods. The findings confirm that HTER-ACOA provides a secure, reliable, scalable, and energy-efficient solution for next-generation WSN and IoT applications, with future potential for enhancement through federated learning, edge computing, and intelligent autonomous routing techniques.

References

- 1) Saidi KA, Benahmed K, Seddiki N. Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks. *Ad Hoc Networks*. 2020;106:102215. <https://doi.org/10.1016/j.adhoc.2020.102215>.
- 2) Mathapati M, Kumaran TS, Muruganandham A, et al. Secure routing scheme with multi-dimensional trust evaluation for wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*. 2020. <https://doi.org/10.1007/s12652-020-02169-7>.
- 3) Sajjan RI, Jasper J. Trust-based secure routing and the prevention of vampire attack in wireless ad hoc sensor network. *International Journal of Communication Systems*. 2020;33(8). <https://doi.org/10.1002/dac.4341>.
- 4) Nori MK, Sharifian S. EDMARA2: A hierarchical routing protocol for EH-WSNs. *Wireless Networks*. 2020;26:4303–4317. <https://doi.org/10.1007/s11276-020-02328-w>.
- 5) Qureshi KN, Bashir MU, Lloret J, Leon A. Optimized cluster-based dynamic energy-aware routing protocol for wireless sensor networks in agriculture precision. *Journal of Sensors*. 2020. <https://doi.org/10.1155/2020/9040395>.
- 6) Wang C, Liu X, Hu H. Energy-efficient and load-balanced clustering routing protocol for wireless sensor networks using a chaotic genetic algorithm. *IEEE Access*. 2020;8:158082–158096. <https://doi.org/10.1109/ACCESS.2020.3020158>.
- 7) Patil PA, Deshpande RS, Mane PB. Trust and opportunity based routing framework in wireless sensor network using hybrid optimization algorithm. *Wireless Personal Communications*. 2020;115(1):415–437. <https://doi.org/10.1007/s11277-020-07579-6>.
- 8) Fang W, Zhang W, Chen W, Liu J, Ni Y, Yang Y. MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*. 2021;2021(1). <https://doi.org/10.1186/s13638-020-01884-1>; <https://doi.org/10.1186/s13638-021-01911-5>.
- 9) Hajiee M, Fartash M, Eraghi NO. An energy-aware trust and opportunity-based routing algorithm in wireless sensor networks using multipath routes technique. *Neural Processing Letters*. 2021;53(4):2829–2852. <https://doi.org/10.1007/s11063-021-10490-2>.

- 10) Goel S, Sharma KP, Mittal N, Mittal V, Khafaga DS, Abouhawwash M. Energy efficient clustering protocol in wireless sensor networks using an adaptive hybrid optimization algorithm. *Scientific Reports*. 2026;16:6300. <https://doi.org/10.1038/s41598-026-36957-6>.
- 11) Tripathi K, Shalu, Kaushik S, Vyas S, Khan MA, Ahmadian A. TITAN: Logarithm-based trust-aware integrated technique for robust anomaly neutralization in industrial WSNs. *Peer-to-Peer Networking and Applications*. 2026;19(79):1–21. <https://doi.org/10.1007/s12083-026-02222-w>.
- 12) Mishra R, Jha SK, Prakash S, Rathore RS. HEXADWSN: Explainable ensemble framework for robust and energy-efficient anomaly detection in WSNs. *Future Internet*. 2025;17(11):520. <https://doi.org/10.3390/fi17110520>.
- 13) Zhang Y, Yang L, Tan Y. Energy-efficient adaptive routing in heterogeneous wireless sensor networks via hybrid PSO and dynamic clustering. *Journal of Cloud Computing*. 2025;14(46):1–22. <https://doi.org/10.1186/s13677-025-00768-3>.
- 14) Hu H, Han Y, Yao M, Xue S. Trust-based secure and energy-efficient routing protocol for wireless sensor networks. *IEEE Access*. 2021;9:72805–72819. <https://doi.org/10.1109/ACCESS.2021.3075959>.