Natural Resources for Human Health
eISSN: 2583-1194

Original Research

Received 14 April 2026
Revised 16 May 2026
Accepted 20 June 2026

Natural Resources for Human Health 2026, Vol. 6 (5s): 257–273

KEYWORDS:
wireless sensor networks, secure routing, trust-aware routing, energy-efficient routing, reinforcement-based path selection, malicious nodes.

Trust-Energy Path-Reinforcement Routing for Secure and Sustainable Wireless Sensor Networks under Dynamic Malicious-Node Conditions

Jyoti Saini*1, Ramesh Kait2

1,2Department of Computer Science and Applications
1,2Kurukshetra University, Kurukshetra, Haryana, India, 136119
*1jsaini089@gmail.com , 2rameshkait@kuk.ac.in

ABSTRACT: WSNs (wireless sensor networks) in hostile environments not only have limited energy resource but also have the existence of malicious node behaviour which significantly degrades both the routing reliability and network lifetime quality. To overcome this challenge, this study presents a trust-energy reinforced routing framework for secure and energy aware communication in WSNs with dynamic malicious-node conditions. The proposed method integrates residual energy, trust value as well as route-reinforcement memory into a single mechanism for next-hop selections, allowing routing decisions to adapt to both the earlier successful paths as well as the current network conditions. A MATLAB-based comparative simulation study through a network of 100 sensor nodes, malicious nodes being updated periodically, was conducted and the performance of the proposed simulated approach was evaluated against Grey Wolf Optimization (GWO)-, Harris Hawks Optimization (HHO)- and Whale Optimization Algorithm (WOA)-inspired routing approaches. In the experiments, the proposed method achieved best results in terms of final trust value, residual energy, alive-node fraction, and average routing cost. It finally produced a trust value of 0.8773, residual energy 0.242 Joule, alive-node fraction 0.94, and routing cost of 146.76. In addition, the first node death was delayed to round 28, while the half-nodes-dead and last-node-death conditions were not reached within the 50-round simulation horizon. These findings confirm that the proposed framework provides a more balanced and effective solution for secure, energy-efficient, and sustainable routing in adversarial WSN environments.

1. INTRODUCTION

Wireless sensor networks (WSNs) have become an important enabling technology for a wide range of applications, including environmental monitoring, healthcare systems, industrial automation, precision agriculture, military surveillance, and smart-city infrastructure. In these applications, a large number of small sensor nodes are deployed to sense, process, and transmit information to a base station[1]. Despite their broad usefulness, WSNs operate under severe resource constraints, particularly limited battery capacity, restricted communication range, and modest computational capability. As a result, routing is one of the most critical functions in WSN design, since an inefficient routing strategy can rapidly drain node energy, reduce data-delivery reliability, and shorten overall network lifetime.

In addition to energy limitations, WSNs are highly vulnerable to security threats because sensor nodes are often deployed in open or unattended environments[2]. Under such conditions, malicious or compromised nodes may participate in routing and disrupt the normal forwarding process. These interferences can weaken trust, raise routing costs, and precipitate node exhaustion [3]. That's why a practical routing mechanism for WSNs aims not only to minimize energy consumption but also to avoid unreliable nodes and make routing robust under changing network conditions[4]. In dynamic adversarial conditions where the set of malicious nodes are updated periodically, this challenge is more significant[5].

Traditional routing algorithms are typically having limited set of goals like, shortest path, minimizing energy consumption, or load balancing etc. neglecting the addressal of node trust values or dynamic malicious behaviour [6]. In recent years, the flexible and adapting behaviour of nature-inspired and metaheuristic approaches like Grey Wolf Optimization (GWO), Harris Hawks Optimization (HHO) and Whale Optimization Algorithm (WOA), captured the interest of researchers to optimize routing decisions[7]. While these approaches can aid routing decisions, they may yet be insufficient in case at the same time the above routing decisions have to consider for residual energy, node trust, route quality and changing patterns of malicious-nodes[8]. Hence, a more adaptive strategy is required to maintain secure communication as well as long-term network survivability.

In view of the above limitations, a trust-energy reinforced routing framework is proposed that can ensure security and energy efficiency in WSN communication systems. The proposed method combines three important aspects for the selection of next-hop: remaining energy, trust scores, and path reinforcement memory. This means that apart from considering the present state of the neighboring nodes, the routing algorithm will also consider previous success in route selection. This will make the routing algorithm less costly, energy efficient, enhance trust-awareness, and prolong the life of the network. The approach will be simulated within an environment where the malicious nodes are updated periodically and compared with other routing approaches inspired by the GWO, HHO, and WOA algorithms.

From the experimental results mentioned in this work, one can conclude that the proposed framework offers better performance than other methods taken into consideration. More specifically, higher residual-energy retention, better trust preservation, lower routing cost, higher alive node ratio, and prolonged network lifetime concerning the first node failure, half node failure, and final node failure. It appears to be a successful way to design routing schemes that consider trust, energy, and reinforcement learning in WSNs where resources are limited and there may be threats.

The main contributions of this study can be summarized as follows:

1. A simulation-based routing framework is developed for WSNs operating under dynamic malicious-node conditions.
2. A trust-energy reinforced routing strategy is proposed in which next-hop selection is guided by residual energy, trust value, and path-memory reinforcement.
3. The proposed method is evaluated against GWO, HHO, and WOA-inspired routing approaches using energy, trust, routing cost, alive-node ratio, and lifetime indicators.
4. The results show that the proposed framework leads to improved security, route efficiency, and long-term network sustainability.

The rest of the manuscript is structured as follows. Section 2 presents Background & Motivations. Section 3 illustrates the framework of proposed research method including network setting, the malicious-node simulation, routing strategy design framework and performance metrices. Section 4 discusses the experimental and comparative studies. Lastly, Section 5 provides conclusion and future research avenues.

2. LITERATURE REVIEW

Wireless sensor networks (WSNs) have been studied extensively with a focus on energy efficiency, routing reliability and communication security. Recent literature has shifted away from conventional shortest-path routing towards heuristic and optimization-based schemes that try to achieve a multi-objective trade-off simultaneously [9]. One important stream of work has aimed on energy-aware routing and clustering to reduce premature node depletion and improve network lifetime. In this case, an energy-warning-based routing strategy was proposed to keep sensor nodes connected even if the available energy is very low [10]. A metaheuristic-based multi-hop energy-aware cluster-based routing scheme was proposed for IoT-assisted WSNs which was reported to enhance the energy utilization by local optimization of clustering/ route discovery phases [11]. More recently this direction was strengthened by, NCRDAP, an AI-driven clustering, routing, and data aggregation protocol was proposed for energy-efficient WSNs[12]. A more comprehensive framework combining self-tuned fuzzy logic, adaptive palm tree optimization, and Stackelberg game-theoretic load balancing was then proposed to jointly improve the energy efficiency, reliability, and security of WSNs[13]. Similarly, a multi-objective energy-efficient routing using an adaptive black hole–tuna swarm optimization strategy was also addressed [14]. These studies clearly demonstrate the importance of energy-aware design, yet their main emphasis remains on efficiency, clustering, and load balancing rather than dynamic trust adaptation under malicious-node behaviour.

After energy efficiency became a well-established objective, the research focus moved toward trust-aware secure communication. A secure and trust-aware routing scheme demonstrated that route selection based on node trust can improve secure forwarding and reduce exposure to malicious nodes [15]. This idea was extended through trust-based clustering and best-route selection, in which trust and energy were jointly used to improve route quality [16] A further development combined trust-aware secure routing with attribute-based encryption, thereby integrating route security with data confidentiality [17]. Then TADR-EAODV, a trust-aware dynamic routing algorithm based on an extended AODV protocol for secure WSN communication was also introduces[18], while, a trust-aware secure routing protocol specifically designed to improve reliability in the presence of malicious forwarding behaviour was also introduced [19]. Collectively, these studies confirm that trust modelling has become a crucial component of modern WSN routing[20]. However, many existing trust-aware methods rely primarily on static trust handling, protocol-level modifications, or trust-clustering integration, with limited attention to route-memory reinforcement and dynamically changing malicious-node patterns.

As routing challenges became more complex, research shifted toward multi-objective optimization and metaheuristic-assisted secure route planning. A trust-and-energy-based multi-objective hybrid optimization approach showed that combining trust and residual energy can improve route selection quality[21]. Secure clustering and routing were also addressed through trust-aware cat swarm optimization, indicating that trust-guided metaheuristic search can improve forwarding decisions [22], while A secure and energy-aware multi-hop routing protocol based on a Taylor-inspired hybrid optimization algorithm further highlighted the usefulness of hybrid search strategies in WSN routing [23]. The problem of jointly satisfying energy efficiency, quality of service, and secure routing was also addressed through a dedicated QoS-aware secure routing algorithm [24]. In addition, a multi-objective trust-aware improved grey wolf optimization technique was proposed to uncover adversarial attacks and improve route robustness [25]. These studies highlight the growing importance of optimizer-based secure routing, but their routing decisions are still dominated by metaheuristic search behaviour and objective-function minimization, rather than by a lightweight route-memory mechanism that learns from previously successful paths.

The most recent stage of research has expanded secure routing into IoT, IIoT, and learning-assisted network environments. A secure multi-hop routing algorithm based on fuzzy logic was proposed for IoT communication, highlighting the role of intelligent inference in secure forwarding [26]. Heuristic and reinforcement learning-based survivable trust-aware virtual network embedding was then studied for IoT systems, showing that learning-assisted trust adaptation can improve resilience in networked environments [27]. Trustworthy sensor data collection for cyber-physical systems was further examined using genetic algorithms and differential privacy, demonstrating that trust and reliability must also be considered at the sensing and data-collection stage [28]. In the industrial IoT context, lightweight trust management was proposed for edge devices to improve secure cooperation under constrained resources [29], while, a security-driven routing architecture for industrial IoT environments also showed that secure routing increasingly requires integration with broader architectural and infrastructure-level defenses [30]. These contributions show that trust, learning, and survivability are becoming increasingly central in next-generation sensor and IoT systems. Nevertheless, many of these approaches are oriented toward IoT trust management, virtual embedding, or infrastructure-level security rather than lightweight hop-by-hop route construction in dynamic WSN attack environments.

The step-by-step evolution of the literature shows that meaningful progress has been achieved in energy-aware routing, trust-based secure forwarding, multi-objective optimization, and intelligent survivability-aware communication. However, an important gap remains. Most existing studies optimize energy efficiency, trust management, security, or clustering either independently or only partially in combination. In particular, there is still limited work on a lightweight routing mechanism that simultaneously integrates residual energy, trust value, and historical route preference while operating under periodically changing malicious-node conditions. This gap is especially important in practical WSN deployments, where routing decisions should adapt not only to instantaneous node state but also to evolving adversarial behaviour over time.

To address this gap, the present manuscript proposes a trust-energy reinforced routing framework for secure wireless sensor networks under dynamic malicious-node conditions. The proposed framework differs from prior studies in four important ways. First, it integrates residual energy, trust value, and path-reinforcement memory into a single next-hop decision mechanism.

Second, it introduces a dynamic malicious-node model, in which the malicious-node set is updated periodically rather than remaining fixed throughout the simulation. Third, it employs a unified routing-cost formulation that jointly accounts for distance, energy depletion, trust degradation, and malicious-node penalty. Fourth, it evaluates the proposed framework against GWO-, HHO-, and WOA-inspired routing methods using both routing-performance and network-survivability indicators, including residual energy, trust, routing cost, alive-node fraction, FND, HND, and LND. According to the current manuscript, this design enables the proposed method to achieve the highest final trust, highest residual energy, highest alive-node fraction, and lowest average routing cost among the compared methods, thereby demonstrating a balanced improvement in security, efficiency, and long-term network sustainability.

3. RESEARCH METHODOLOGY

3.1. Overview of the Proposed Framework

This study develops a simulation-based framework for secure and energy-aware routing in wireless sensor networks (WSNs) under dynamic malicious-node conditions. The overall methodology consists of four sequential phases: network initialization, state initialization, routing and dynamic update, and performance evaluation, as illustrated in *Figure 1*.

The main contribution of the research study is to evaluate a trust-energy reinforced routing mechanism that improve route quality, network reliability, and energy sustainability when compared with GWO, HHO, and WOA inspired routing strategies and jointly considers node residual energy, trust level, routing cost, malicious-node dynamics, and network lifetime indicators.

3.2. Network Initialization

A WSN consisting of 100 sensor nodes is deployed randomly in a two-dimensional sensing region of (100 X 100). The base station (BS) is positioned above the sensing field and acts as the final destination for all generated routes. After deployment, the network topology is modelled as a communication graph in which two nodes are connected if their Euclidean distance is less than the predefined communication radius.

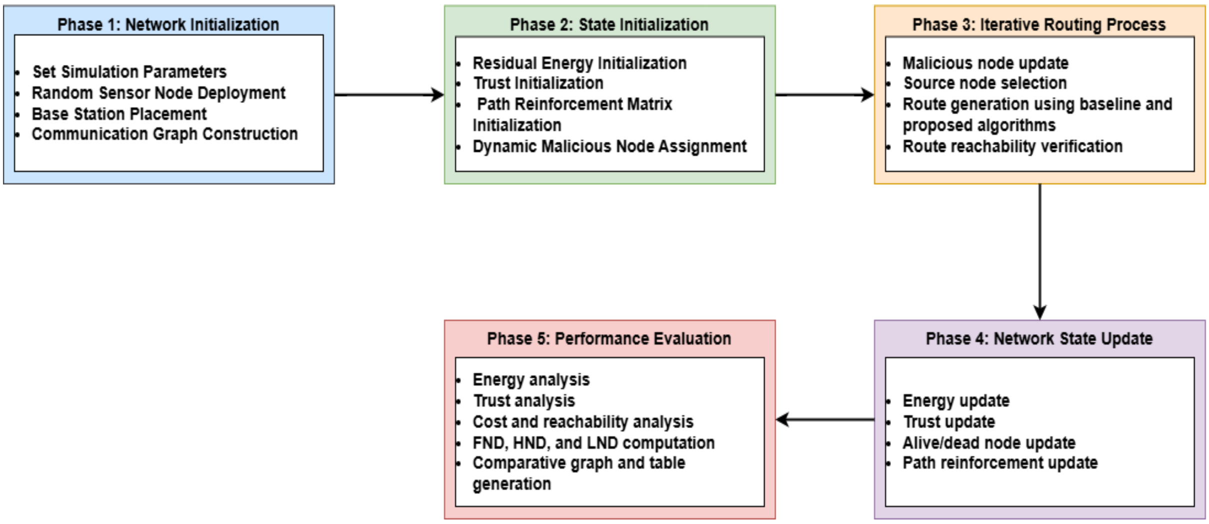

Figure 1:Overall research methodology framework for secure and energy-aware routing in wireless sensor networks under dynamic malicious-node conditions.

The simulation parameters used are:

- Number of nodes N=100
- Simulation rounds =50
- Initial node energy =0.5 J
- Communication radius =40 m
- Packet size =4000 bits
- Transmission/Reception energy cost $=50\times10^{-6}$ J/bit.

This simulation environment provides a controlled environment for evaluating the routing performance under limited-energy and adversarial conditions.

3.3. State Initialization

To enable fair comparisons among various routing approaches, similar initial energy and trust values are assigned to all the nodes for simulation. The initial residual energy level of 0.5 J and initial trust value of 0.9 is used. Energy and trust levels are kept separate for different routing policies so that the impact of routing decisions on the energy and trust state is independent of one another.

The proposed routing algorithm also initializes the path reinforcement matrix. The path reinforcement matrix keeps track of the preferred routes and acts as a lightweight memory mechanism for improving favorable routing paths over time. Initially, all entries of the path memory matrix are assigned equal preference values.

3.4. Iterative Routing Process

To simulate an adversarial routing environment, 20% of the sensor nodes are designated as malicious. Unlike a static attack model, the malicious-node set is updated periodically every three rounds. This periodic update reflects changing hostile conditions and enables the framework to assess the adaptability of each routing algorithm under dynamic security threats.

The malicious-node model affects the routing process in two ways. First, the presence of malicious nodes increases the routing cost through an explicit penalty factor. Second, trust values of malicious nodes degrade when they participate in routing paths, thereby influencing future route selection.

Four routing strategies are evaluated in this study: GWO-inspired routing, HHO-inspired routing, WOA-inspired routing, and the proposed trust-energy reinforced routing strategy. In each simulation round, one source node is selected randomly, and all four methods independently generate a route from the source node to the base station.

The GWO-inspired method chooses the next hop from highly ranked candidate nodes based on the combined effect of residual energy and trust. The HHO-inspired and WOA-inspired methods employ a mixed exploration-exploitation mechanism in which next-hop selection is influenced by energy-trust suitability as well as stochastic search behaviour. These three methods serve as comparative baselines for evaluating the proposed approach.

3.5. Network State Update

The proposed routing strategy illustrated in *Figure 2,* performs hop-by-hop path construction by considering neighbour availability, direct reachability to the base station, and a weighted next-hop selection rule.

Energy is deducted from transmitting and receiving nodes according to the communication energy model. Trust values are updated to penalize malicious or unreliable nodes participating in routing paths. The alive-node status is also recalculated based on the remaining residual energy of each node. Furthermore, the path-reinforcement matrix is updated by decaying older route preferences and reinforcing successful routing links. This mechanism allows the proposed framework to balance route exploitation and adaptability under dynamic malicious-node conditions.

3.5.1. Proposed Trust-Energy Reinforced Routing Strategy

At each routing step, the neighbouring nodes of the current node are identified from the communication graph. Nodes with zero residual energy are removed from the candidate set, while the base station is retained if it is directly reachable. If no valid neighbour exists, the route is terminated by forcing the final hop toward the base station. If the base station is already a direct neighbour, it is immediately appended to the route.

Otherwise, the next-hop node is selected using a weighted function that combines path memory, trust, and residual energy[21]:

$$w_{ij} = (p_{ij})^{0.5}(T_j)^{1.2}(E_j)^{1.1} \qquad (1)$$

where:

w_{ij} denotes the routing weight from current node (i) to candidate node (j),

p_{ij} is the reinforcement-based path preference,

T_j is the trust value of candidate node (j), and

E_j is its residual energy.

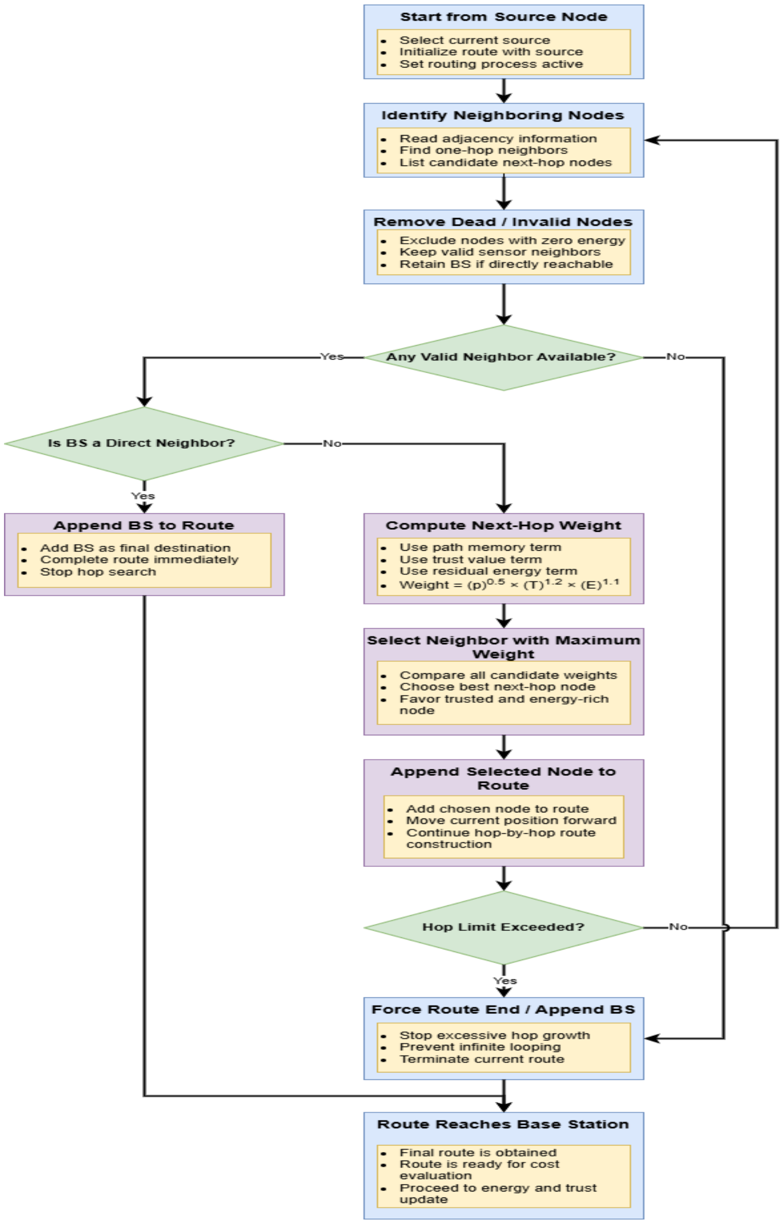

Figure 2: Proposed trust-energy reinforced routing algorithm for next-hop selection and route construction toward the base station.

The candidate with the highest weight is selected as the next hop. To prevent excessive route growth and potential looping, a maximum hop limit is imposed. If the hop count exceeds the limit, the route is terminated by appending the base station.

After each round, the path memory matrix is updated in two stages. First, the existing memory values are decayed by a factor of 0.9 in order to avoid overdependence on older routes. Second, the links belonging to the selected route are reinforced by increasing their corresponding matrix values. This mechanism allows the algorithm to preserve beneficial routing history while still adapting to changing network conditions.

3.5.2 Routing Cost Formulation

The quality of each generated route is evaluated using a routing cost function that combines transmission distance, energy condition, trust level, and malicious-node participation. For a route (R), the cost is computed as[21] :

$$C(R) = \sum_{i=1}^{L-1} \alpha d_{i,i+1} + \beta(1 - E_i) - \gamma(1 - T_i) \qquad (2)$$

where $d_{i,i+1}$ is the Euclidean distance between consecutive nodes, E_i is the residual energy of the transmitting node, and T_i is the trust value of that node. In this study, (α=0.5), (β=0.3), and (γ=0.2).

To reflect adversarial influence, the route cost is further penalized when malicious nodes appear in the selected path:

$$C_{final}(R) = C(R)(1 + 0.25\, M_R) \qquad (3)$$

where M_R denotes the number of malicious nodes present in route R. A lower routing cost indicates a more favourable path in terms of distance efficiency, energy condition, and trustworthiness.

3.5.3 Energy and Trust Update Mechanism

Once a route is generated, node states are updated according to packet forwarding activities. The transmitting nodes lose energy according to the transmission model, while the receiving nodes lose energy according to the reception model. The update rules are defined as[23]:

$$E^{tx} = \max(E - E_{tx} \times pkt, 0) \qquad (4)$$

$$E^{rx} = \max(E - E_{rx} \times pkt, 0) \qquad (5)$$

where $E^{tx} = E^{rx}$ =50×10^{-6} J/bit. and pkt =4000 bits. The max operator ensures that energy values do not become negative.

Trust is also updated dynamically. If a malicious node appears in the selected route, its trust value is reduced according to

$$T_{new} = 0.85 T_{old} \qquad (6)$$

This update mechanism allows the routing framework to reflect unreliable behaviour over time and reduces the future attractiveness of compromised nodes.

3.6. Simulation Procedure

The simulation is executed for 50 rounds. A malicious-node set is periodically updated in each round, one source node randomly selected from 100 nodes and four routing strategies generate routes independently. After each round, we store the route reachability status, routing cost, residual energy, trust values and alive-node ratio. In the proposed method, at the end of each round, we decay and reinforce path memory matrix in our model. After completion of all rounds, the framework calculates final trust, final residual energy, average routing cost, final alive-node fraction and lifetime measure (FND, HND and LND) of each algorithm. The results are then summarized using comparative graphs and a final performance table for detailed analysis.

3.7. Performance Evaluation

The effectiveness of the routing strategies is assessed using multiple performance indicators. These include average residual energy, average trust, average routing cost, route reachability to the base station, and alive-node fraction. In addition, network lifetime is analyzed using three standard milestones: first node death (FND), half nodes dead (HND), and last node death (LND). Average residual energy measures the overall energy preservation capability of a routing strategy, whereas average trust reflects its ability to avoid unreliable nodes. Routing cost quantifies route quality based on distance, energy, and trust. The alive-node fraction indicates the proportion of functional nodes remaining in the network. FND, HND, and LND provide a broader view of short-, medium-, and long-term network survivability.

4. RESULTS & DISCUSSION

4.1. Experimental Setup

To check the applicability and performance of the proposed trust-energy reinforced routing strategy, a comparative simulation study is presented in MATLAB using the framework presented in section 3. Four routing methods were studied and evaluated:

GWO-inspired routing, HHO-inspired routing, WOA-inspired routing, and the proposed method. The experiments were performed on a WSN consisting 100 randomly deployed sensor nodes in the 100 × 100 sensing area with the base station placed out of this sensing field. The communication radius was fixed at 40 m, the initial node energy was set to 0.5 J, and the simulation was executed for 50 rounds. In addition, 20% of the nodes were treated as malicious, and the malicious-node set was updated every three rounds to emulate a dynamic adversarial environment.

The performance of the routing algorithms was assessed using average residual energy, average trust, average routing cost, final alive-node fraction, and three standard lifetime indicators: FND, HND, and LND. For the lifetime indicators, a value of **51** does **not** represent an actual event occurring in the 51st round. Instead, it is used as a reporting marker, when the corresponding event is not observed within the 50-round simulation horizon. Thus, a value of 51 indicates that the event remained unreached during the entire experiment.

4.2. Residual Energy Analysis

The residual-energy evolution of the four routing methods is illustrated in *Figure 3*. All methods start with the same average energy level of 0.5 J, but their depletion trends differ substantially over the simulation horizon. The proposed method exhibits the slowest energy decay, maintaining a smooth and gradual decline throughout the 50 rounds. In contrast, HHO and WOA show rapid energy depletion, while GWO demonstrates intermediate behaviour.

At the end of the simulation, the proposed method retained **0.242 J** of average residual energy, whereas GWO retained only **0.015 J**, and both HHO and WOA depleted their average energy to **0 J**.

It signifies indicates that the proposed routing mechanism is substantially more effective in balancing forwarding decisions across trustworthy and energy-efficient nodes. With the gradually declining proposed curve, this indicates that reinforcement-based path memory successfully reduces repeated use of weak or unreliable routes.

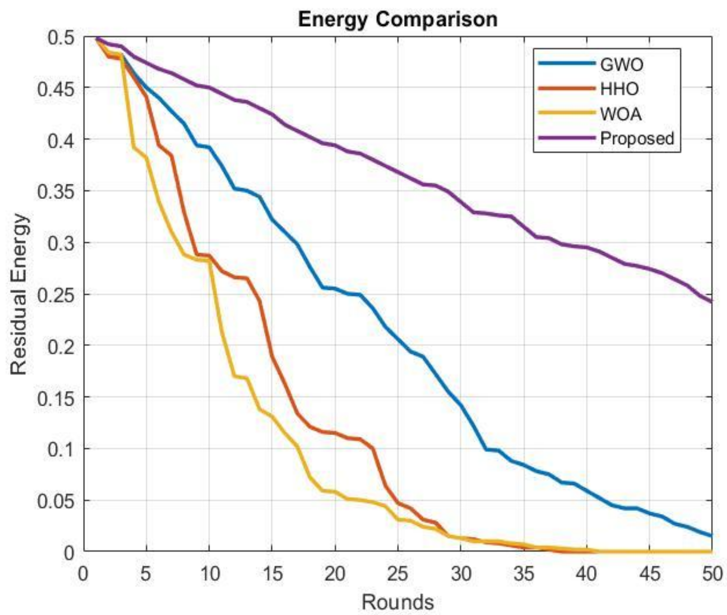

Figure 3: Residual energy comparison of GWO, HHO, WOA, and proposed routing methods over 50 simulation rounds.

4.3. Trust Evolution Analysis

Trust evolution of all methods is compared. While trust preservation is an essential metric for routing robustness under dynamic attack conditions since the malicious-node set updates periodically, The proposed method retains the highest trust level over time, and exhibits the smallest decline over time.

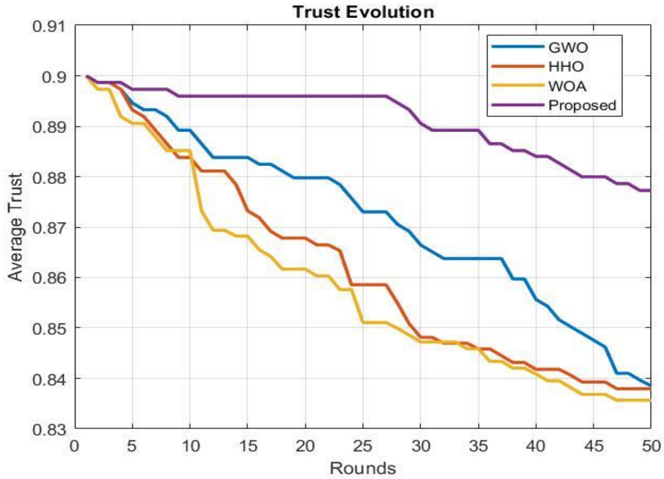

Figure 4: Trust evolution of the compared routing methods under dynamic malicious-node conditions across 50 rounds.

The trust evaluation of composite routing methods in comparison is presented in *Figure 4*. The final average trust values were 0.8773 for the proposed method, 0.8385 for GWO, 0.8379 for HHO, and 0.8357 for WOA. The numerical differences may seem relatively small; however, the trust curve of our approach remains consistently higher than baseline methods for the entire duration of the experiment. Such a behavior indicates that the next-hop selection rule proposed is superior in terms of evading both unreliable routing paths and maintaining secure forwarding performance when malicious nodes are periodically updated.

4.4. Routing Cost Analysis

The routing-cost comparison shows that GWO has the largest fluctuations and the highest cost spikes, which indicates an unstable route selection with many costly paths being used. Optimizations based on HHO and WOA mitigate some of these fluctuations, but their cost curves still exhibit sharp increases. In contrast, the routing cost for the proposed method is much lower and stable across most rounds. *Figure 5* depicts the routing-cost comparison of all methods.

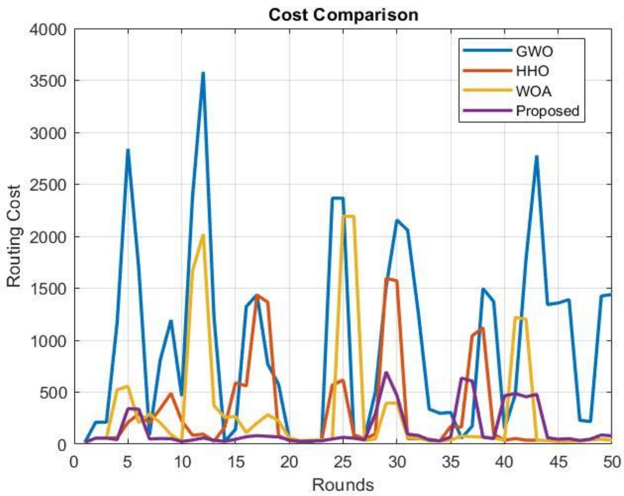

Figure 5: Routing cost comparison of GWO, HHO, WOA, and proposed methods during the simulation period.

The average routing costs of GWO, HHO, WOA and the proposed method were 986.30, 285.48, 323.03 and 146.76 respectively. Thus, the proposed approach obtained the least overall cost among all competitors. Compared to GWO, HHO and WOA the average routing cost of in proposed method reduced by 85.12%, 48.59% and 54.57%, respectively It also confirms that the combining of trust, residual energy and path reinforcement is a better heuristic routing policy under the given cost model.

4.5. Final Comparative Performance

The final performance indicators are summarized in Table 1. The proposed method outperformed the baseline methods in final trust, final residual energy, alive-node fraction, average routing cost, and most lifetime indicators.

Table 1:Final comparative performance of GWO, HHO, WOA, and Proposed Routing methods in terms of trust, residual energy, alive-node fraction, routing cost, and lifetime metrics.

Algorithm	Final_Trust	Final_Energy_J	Final_Alive_Frac	Avg_Cost	FND_Round	HND_Round	LND_Round
GWO	0.838508	0.015	0.15	986.3041	7	42	51
HHO	0.837937	0	0	285.479	5	23	38
WOA	0.835673	0	0	323.029	6	18	41
Proposed	0.877253	0.242	0.94	146.7586	28	51	51

From the *Table 1*, two observations are especially important. First, the proposed strategy preserved **94%** of the nodes alive at the end of the simulation, whereas GWO retained only **15%**, and HHO and WOA retained **0%**. Second, the proposed method delayed the first node death to round **28**, compared with rounds **7**, **5**, and **6** for GWO, HHO, and WOA, respectively. Moreover, the proposed approach did not reach either half nodes dead or last node death within the simulated horizon, while HHO and WOA experienced complete node depletion by rounds **38** and **41**, respectively.

4.6. Network Lifetime Analysis

The proposed method achieved the strongest network survivability among all evaluated approaches. Specifically, the FND value increased to 28 rounds, which is four times greater than GWO and substantially higher than HHO and WOA. Similarly, the HND and LND results show that the proposed method sustained network operation throughout the full experimental duration. The lifetime comparison based on FND, HND, and LND is further illustrated in *Figure 6, Figure 7 and Figure 8*.

Although, GWO also achieved partial survivability up to the end of the simulation, but with a low fraction of alive-nodes: only 0.15 and nearly empty residual energy. Thus, while GWO exhibits relatively better performance than HHO and WOA in terms of total collapse delay, it is still obviously inferior to the proposed method in terms of energy preservation, route quality and trust maintenance. In comparison, the HHO and WOA performed worse than others due to the earlier depletion of their nodes thus directly reduced their long-term routing viability.

The experimental results are in accordance with this analysis and all the comparisons prove that the proposed trust-energy reinforced routing strategy achieves a better trade-off between enhanced network security, energy economy and route stability. Significantly, the energy results demonstrate that the proposed approach is capable of distributing routing decisions more uniformly throughout the network, thereby avoiding excessive burden on weak nodes. The results of trust show that the proposed method is more capable of bypassing the unreliable nodes and adapting to dynamic malicious-node effects as well. The routing-cost results additionally validate that the proposed decision-rule leads lower-cost and more stable paths, as compared to the bio-inspired baselines. These results validate the effectiveness of combining trust awareness, energy awareness and reinforcement-based route preference for secure WSN routing.

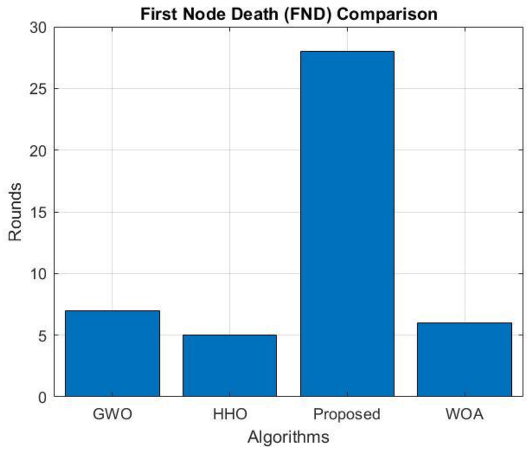

Figure 6: First node death (FND) comparison of the routing methods, indicating the early-stage network lifetime performance.

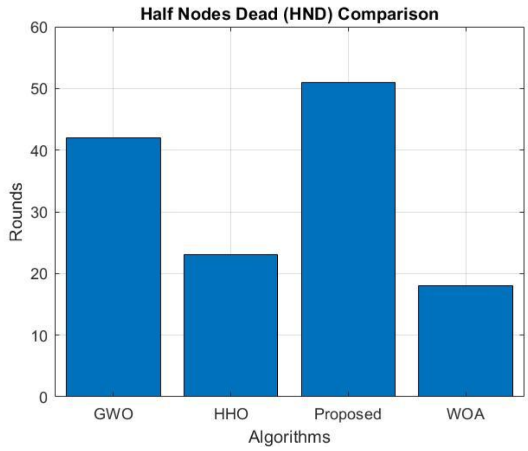

Figure 7:Half nodes dead (HND) comparison of the routing methods, representing the mid-stage network lifetime behaviour.

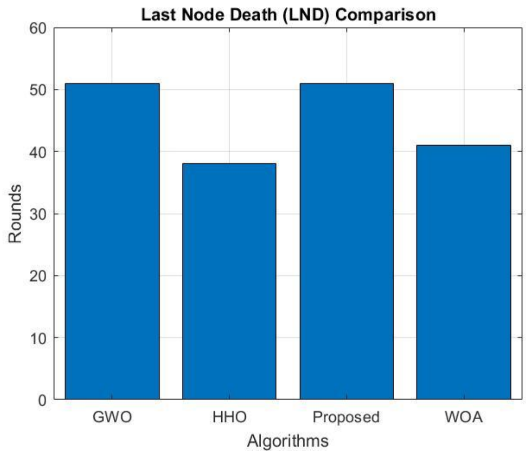

Figure 8:Last node death (LND) comparison of the routing methods, reflecting the overall network lifetime of the compared approaches.

4.7. Comparative Analysis

Table 2 presents a consolidated comparative assessment of the proposed trust–energy–path memory routing framework against recent WSN routing approaches reported in the literature. The comparison is based on key performance indicators, including energy or residual energy, network lifetime, first node death (FND), half nodes dead (HND), last node death (LND), alive/dead node status, trust/security, routing cost, and number of simulation rounds. It can be observed that most existing methods emphasize energy efficiency and lifetime enhancement, which remain the primary optimization goals in resource-constrained WSNs. For example, ABTSO, SWARAM, EOAMRCL, HGWO-Firefly, and HZ-BFOA mainly focus on energy-aware clustering, residual-energy preservation, or optimal cluster-head selection. However, several of these studies do not explicitly report complete lifetime milestones such as FND, HND, and LND, which limits their ability to describe early, intermediate, and complete network degradation. Similarly, some works report alive/dead node trends graphically but do not provide exact numerical values, making direct quantitative comparison difficult.

Security-oriented approaches such as EEOTSR and SECR introduce trust, attack resilience, encryption, or secure routing mechanisms, but their performance reporting is often centered on packet delivery ratio, latency, security robustness, or lifetime improvement rather than a unified evaluation of trust, residual energy, node survivability, and routing cost. In contrast, the proposed method evaluates all major routing dimensions simultaneously within a single simulation framework. The proposed trust–energy–path memory routing method achieves a final residual energy of 0.242 J, an alive-node fraction of 0.94, a final trust value of 0.877253, and an average routing cost of 146.7586 over 50 simulation rounds. Moreover, the proposed method delays FND to round 28, while HND and LND are not reached within the 50-round simulation horizon, demonstrating strong network survivability. This result indicates that the proposed framework is not limited to energy optimization alone but also maintains trustworthiness, route stability, and node availability under dynamic malicious-node conditions. The inclusion of path-memory reinforcement further differentiates the proposed approach from conventional metaheuristic routing schemes because it allows successful historical routes to influence future next-hop selection. Therefore, Table 2 clearly establishes that the proposed framework provides a more comprehensive and balanced solution by jointly addressing energy efficiency, security, routing cost, and lifetime sustainability. This comparative evidence strengthens the novelty and suitability of the proposed method for secure and sustainable WSN routing applications.

Table 2:Comparative analysis of existing WSN routing approaches and the proposed trust–energy–path memory routing framework based on energy, lifetime, security, survivability, and routing-cost indicators.

Reference	**Algorithm / Model**		**Energy / Residual Energy**	**Network Lifetime**	**FND**	**HND**	**LND**	**Alive / Dead Nodes**	**Trust / Security**	**Routing Cost**
Sheeja et al. [14]	AB TSO	Case 1: 50 Rounds	NE mean: 0.000654	NR	NR	NR	NR	Alive-node mean: 0.015508	NR	Objective/path-loss mean: 94.673
		Case 2: 100 Rounds	0.000641					0.043272		95.843
		Case 3: 150 Rounds	0.000634					0.069785		94.089
Roberts and Thangavel[31]	Dual-phased SFO-SHO routing		Mean residual energy: 0.5081	Mean network lifetime: 482.1 rounds	NR	NR	NR	Alive nodes improved 3-20%; dead nodes reduced 9-17%	NR	NR
Somula et al.[32]	Osprey Optimization / SWARAM (4000 rounds)		Energy consumption: 0.35 J	Alive until 4000 rounds	3250 rounds*	3750 rounds*	4000 rounds*	Alive nodes: 0	NR	NR
Kaddi et al. [33]	GWO-based EOAMRCL		Highest remaining energy; numeric NR	FND/HND/LND evaluated graphically	Graphical NR	Graphical NR	Graphical NR	Live-node percentage reported graphically	NR	NR; clustering overhead reported

Dev and Mishra [34]	Hybrid GWO + Firefly		Residual energy: 0.3335 J after 1000 rounds	High lifetime reported	NR	NR	NR	Alive nodes: 130; dead nodes: 0	NR	Route-cost function used; final cost NR
Singh et al. [35]	EEOTSR using ACO		Energy-efficient routing; exact residual NR	Network lifetime +23%	NR	NR	NR	NR	PDR +17%; latency -14%; PDR >90% with 30% compromised nodes	NR
Dixit et al.[36]	Security-aware RFO routing / SECR		Network energy starts from 140 J; residual trend reported	Case-1: 40153 rounds; Case-2 lifetime +134.34% over DECEM	Case-1: 19478 rounds; Case-2: 53 rounds	Case-1 HND improvement: 288.10% / 100.30% / 86.57%	NR	Alive/dead-node curves reported	Adaptive AES + DDoS detection; trust-based CH selection	NR
Godi et al. [37]	Secure multi-objective routing / HZ-BFOA	Case 1: 50 Rounds	Energy efficiency 0.010339	Stability-period metric reported; exact lifetime NR	NR	NR	NR	NR	Security: 89.910493	Cost function reduced by 5.8%
		Case 2: 100 Rounds	0.007429						87.202933	3.41%
		Case 3: 150 Rounds	0.0023779						82.870668	4.2%
		Case 4: 200 Rounds	0.0116201						85.336909	5.04%

Proposed Method	Trust-Energy-Path Memory Routing	Final residual energy: 0.242 J	Sustained through 50 rounds	28 rounds	51**	51**	Alive-node fraction: 0.94	Final trust: 0.877253	Average routing cost: 146.7586

Note: NR = not reported as an explicit numerical value in the cited article. Graphical NR = metric shown only in figures/plots without tabulated numerical values. *FND/HND/LND values for SWARAM are inferred from the alive-node table. **In the proposed method, 51 denotes that HND/LND were not reached within the 50-round simulation horizon.

5. CONCLUSION

This study proposed a trust–energy reinforced routing framework to improve secure, energy-efficient, and reliable communication in wireless sensor networks under dynamic malicious-node conditions. The proposed strategy integrates residual energy, node trust, and path-reinforcement memory to support adaptive next-hop selection and reduce dependence on unreliable or energy-depleted nodes. The experimental results show that the proposed method consistently outperformed GWO-, HHO-, and WOA-inspired routing methods across all major performance indicators. It achieved the highest final trust value of 0.8773, retained the highest average residual energy of 0.242 J, preserved the highest alive-node fraction of 0.94, and obtained the lowest average routing cost of 146.76. In contrast, the baseline methods showed faster energy depletion, lower trust preservation, and earlier node failures. The proposed method also delayed the first node death to round 28, while half-node-death and last-node-death conditions were not reached within the 50-round simulation period. These findings confirm that combining trust awareness, energy awareness, and reinforcement-based route preference provides a balanced and effective routing solution for adversarial WSN environments. The proposed methodology can be extended to larger and heterogeneous networks, coordinated attack scenarios, node mobility, dynamic base-station placement, multiple simulation runs with statistical validation, and real-time implementation using advanced network simulators or testbeds.

6. CONFLICT OF INTEREST:

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

7. FUNDING INFORMATION

No funding is available for this research.

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

8. AUTHOR CONTRIBUTION

Jyoti Saini contributed to the conceptualization, methodology, simulation design, implementation, data analysis, result interpretation, and manuscript drafting. Ramesh Kait contributed to supervision, research guidance, methodology refinement, critical review, validation of results, and final manuscript revision. Both authors reviewed and approved the final version of the manuscript.

9. DATA AVAILABILITY STATEMENT

The data used in this study were generated through MATLAB-based simulation experiments. No publicly available benchmark dataset was used. The simulation data, MATLAB code, and supporting materials are available from the corresponding author upon reasonable request.

REFERENCE

[1] B. M. C. Silva and E. Ladeira, “A weighted reputation-based cooperative model to optimize internet connectivity in intermittent IoT networks,” *Computer Networks*, vol. 282, no. February, p. 112278, 2026, doi: 10.1016/j.comnet.2026.112278.

[2] H. Alhulayyil, T. Alzahrani, and H. Alsagri, "Intrusion detection system framework for cyber-physical systems," *Egyptian Informatics Journal*, vol. 30, no. December 2024, p. 100600, 2025, doi: 10.1016/j.eij.2024.100600.

[3] J. Sengendo, "From prediction to protection : A network digital twin framework for traffic monitoring and anomaly detection," *Computer Networks*, vol. 282, no. February, 2026.

[4] S. Gaba, M. Gupta, and H. Singh, "A comprehensive survey on VANET security attacks," in *AIP Conference Proceedings*, AIP Publishing LLC, 2023, p. 20029.

[5] B. Achaal, M. Adda, M. Berger, and A. Awde, "An Intelligent Authentication & Intrusion Detection System for Securing Advanced Metering Infrastructure," *Cyber Security and Applications*, p. 100115, 2025, doi: 10.1016/j.csa.2025.100115.

[6] I. Lahmar *et al.*, "Adaptive Type-2 Fuzzy Unequal Clustering With Energy-Aware Routing For Efficient WSNs," in *Procedia Computer Science*, Elsevier B.V., 2025, pp. 1022–1031. doi: 10.1016/j.procs.2025.09.223.

[7] V. K. R. M and A. C, "Secure Clustering and Routing Based Multi Objective Walrus Optimization Algorithm for Wireless Sensor Networks," *International Journal of Electrical and Electronics Engineering*, vol. 12, no. 1, pp. 211–221, Jan. 2025, doi: 10.14445/23488379/IJEEE-V12I1P121.

[8] R. Kait and J. Saini, "ADAPTIVE INTRUSION DETECTION SYSTEMS FOR WIRELESS SENSOR NETWORKS: A HYBRID MACHINE LEARNING APPROACH," *Int. J. Appl. Math. (Sofia).*, vol. 38, no. 4s, pp. 1054–1081, 2025.

[9] D. Gupta, J. Saini, and M. Rana, "Unraveling the potential of machine learning in lung cancer prediction," in *2023 International conference on advanced computing & communication technologies (ICACCTech)*, IEEE, 2023, pp. 245–250.

[10] B. Saoud, I. Shayea, M. H. Azmi, and A. A. El-Saleh, "New scheme of WSN routing to ensure data communication between sensor nodes based on energy warning," *Alexandria Engineering Journal*, vol. 80, pp. 397–407, Oct. 2023, doi: 10.1016/j.aej.2023.08.058.

[11] R. Jangra, A. Chhikara, J. Saini, and R. Kait, "DEEC Protocol with ACO-Based Cluster Head Selection in Wireless Sensor Network BT - Mobile Radio Communications and 5G Networks," N. Marriwala, C. C. Tripathi, S. Jain, and D. Kumar, Eds., Singapore: Springer Nature Singapore, 2023, pp. 53–61.

[12] J. Hoque, S. Islam, and I. Ahmed, "Engineering Science and Technology , an International Journal NCRDAP : An AI-driven clustering routing and data aggregation protocol for energy-efficient wireless sensor networks," *Engineering Science and Technology, an International Journal*, vol. 71, no. February, p. 102184, 2025, doi: 10.1016/j.jestch.2025.102184.

[13] F. B. D and N. Kumaresan, "Enhancing wireless sensor network performance through self-tuned fuzzy logic , adaptive palm tree optimization , and Stackelberg Game-Theoretic load balancing : A comprehensive approach for energy efficiency , reliability , and security," *Egyptian Informatics Journal*, vol. 32, no. July, p. 100767, 2025, doi: 10.1016/j.eij.2025.100767.

[14] R. Sheeja, M. M. Iqbal, and C. Sivasankar, "Multi-objective-derived energy efficient routing in wireless sensor network using adaptive black hole-tuna swarm optimization strategy," *Ad Hoc Networks*, vol. 144, p. 103140, May 2023, doi: 10.1016/j.adhoc.2023.103140.

[15] A. Beheshtiasl and A. Ghaffari, "Secure and Trust-Aware Routing Scheme in Wireless Sensor Networks," *Wirel. Pers. Commun.*, vol. 107, no. 4, pp. 1799–1814, Aug. 2019, doi: 10.1007/s11277-019-06357-3.

[16] G. Sudha and C. Tharini, "Trust-based clustering and best route selection strategy for energy efficient wireless sensor networks," *Automatika*, vol. 64, no. 3, pp. 634–641, Jul. 2023, doi: 10.1080/00051144.2023.2208462.

[17] M. Selvi, S. V. N. Santhosh Kumar, K. Thangaramya, and H. Abdul Gaffar, "Energy efficient trust aware secure routing algorithm with attribute based encryption for wireless sensor networks," *Sci. Rep.*, vol. 15, no. 1, p. 19724, Jun. 2025, doi: 10.1038/s41598-025-03558-8.

[18] Z. Yang, L. Li, F. Gu, X. Ling, and M. Hajiee, "TADR-EAODV: A trust-aware dynamic routing algorithm based on extended AODV protocol for secure communications in wireless sensor networks," *Internet of Things*, vol. 20, p. 100627, Nov. 2022, doi: 10.1016/j.iot.2022.100627.

[19] H. Hu, Y. Han, H. Wang, M. Yao, and C. Wang, "Trust-aware secure routing protocol for wireless sensor networks," *ETRI Journal*, vol. 43, no. 4, pp. 674–683, Aug. 2021, doi: 10.4218/etrij.2020-0147.

[20] A. K. Shukla and H. Singh, "Your OTP is also not secure: Security Issues of Mobile Apps in the E-Commerce," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 1, 2019.

[21] S. C. Veerabadrappa, K. and Lingareddy, "Trust and Energy Based Multi-Objective Hybrid Optimization Algorithm for Wireless Sensor Network," *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 5, pp. 71–80, Oct. 2022, doi: 10.22266/ijies2022.1031.07.

[22] P. Vennam and S. K. Mouleeswaran, "Secure clustering and routing based on multi Objective – trust aware average inertia weighted cat swarm optimization for Wireless Sensor Networks," *Journal of Intelligent & Fuzzy Systems*, vol. 45, no. 4, pp. 5401–5408, Oct. 2023, doi: 10.3233/JIFS-230564.

[23] A. Vinitha, M. S. S. Rukmini, and Dhirajsunehra, "Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 5, pp. 1857–1868, May 2022, doi: 10.1016/j.jksuci.2019.11.009.

[24] H. Fei *et al.*, "A novel energy efficient QoS secure routing algorithm for WSNs," *Sci. Rep.*, vol. 14, no. 1, p. 25969, Oct. 2024, doi: 10.1038/s41598-024-77686-y.

[25] V. P. Bannikuppe Srinivasiah, R. H. Ranganathasharma, and V. Ramanna, "Multi-objective-trust aware improved grey wolf optimization technique for uncovering adversarial attacks in WSNs," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 36, no. 1, p. 375, Oct. 2024, doi: 10.11591/ijeecs.v36.i1.pp375-391.

[26] T. Fu, G. Han, X. Qin, J. Li, and W. Lin, "Engineering Science and Technology , an International Journal A secure multi-hop routing algorithm based-on fuzzy logic for IoT communication," *Engineering Science and Technology, an International Journal*, vol. 72, no. October, p. 102208, 2025, doi: 10.1016/j.jestch.2025.102208.

[27] P. Rezaeimoghaddam and I. Al-anbagi, "Ad Hoc Networks Heuristic and reinforcement learning-based survivable trust-aware virtual network embedding for IoT networks," *Ad Hoc Networks*, vol. 177, no. March, p. 103898, 2025, doi: 10.1016/j.adhoc.2025.103898.

[28] M. Ejazulghaffar, M. Arif, and A. Jaffar, "Reliable , trustworthy sensor data collection for event detection in Cyber-Physical Systems using Genetic Algorithm and Differential Privacy," *Array*, vol. 30, no. April, p. 100761, 2026, doi: 10.1016/j.array.2026.100761.

[29] I. Ud Din, A. Bano, K. A. Awan, A. Almogren, A. Altameem, and M. Guizani, "LightTrust: Lightweight Trust Management for Edge Devices in Industrial Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 2776–2783, Feb. 2023, doi: 10.1109/JIOT.2021.3081422.

[30] J. Cao, X. Wang, M. Huang, B. Yi, and Q. He, "A security-driven network architecture for routing in industrial Internet of Things," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, Apr. 2021, doi: 10.1002/ett.4216.

[31] M. K. Roberts, J. Thangavel, and H. Aldawsari, "An improved dual-phased meta-heuristic optimization-based framework for energy efficient cluster-based routing in wireless sensor networks," *Alexandria Engineering Journal*, vol. 101, pp. 306–317, 2024, doi: https://doi.org/10.1016/j.aej.2024.05.078.

[32] R. Somula, Y. Cho, and B. K. Mohanta, "SWARAM: Osprey Optimization Algorithm-Based Energy-Efficient Cluster Head Selection for Wireless Sensor Network-Based Internet of Things," 2024. doi: 10.3390/s24020521.

[33] M. Kaddi, M. Omari, K. Salameh, and A. Alnoman, "Energy-Efficient Clustering in Wireless Sensor Networks Using Grey Wolf Optimization and Enhanced CSMA/CA," 2024. doi: 10.3390/s24165234.

[34] J. Dev and J. Mishra, "Energy Efficient Routing in Cluster Based Heterogeneous Wireless Sensor Network Using Hybrid GWO and Firefly Algorithm," *Wirel. Pers. Commun.*, vol. 137, no. 2, pp. 997–1028, Jul. 2024, doi: 10.1007/s11277-024-11447-y.

[35] A. Singh *et al.*, "Resilient wireless sensor networks in industrial contexts via energy-efficient optimization and trust-based secure routing," *Peer. Peer. Netw. Appl.*, vol. 18, no. 3, p. 132, 2025, doi: 10.1007/s12083-025-01946-5.

[36] S. Dixit and S. Qureshi, "Security-aware, Red fox optimization-based cluster-based routing in wireless sensor network," *Peer. Peer. Netw. Appl.*, vol. 18, no. 3, p. 128, 2025, doi: 10.1007/s12083-025-01951-8.

[37] R. K. Godi, S. R. P, Shobha. N, B. V. Bhoothpur, and A. Das, "A highly secure and stable energy aware multi-objective constraints-based hybrid optimization algorithms for effective optimal cluster head selection and routing in wireless sensor networks," *Peer. Peer. Netw. Appl.*, vol. 18, no. 2, p. 97, 2025, doi: 10.1007/s12083-025-01918-9.