



ISSN ONLINE: 2447-0228



RESEARCH ARTICLE

OPEN ACCESS

MULTI-ATTACK RESILIENT TRUST-EMBEDDED ROUTING ARCHITECTURE FOR ENERGY-AWARE IOT WIRELESS SENSOR NETWORKS

Prajakta Sudhirkumar Khelkar¹, Gautam M. Borkar^{2*}

¹Department of Computer Engineering, Ramrao Adik Institute of Technology, DY Patil Deemed to be University, Nerul, Navi Mumbai, India.

^{2*}Department of Information Technology, Ramrao Adik Institute of Technology, DY Patil Deemed to be University, Nerul Navi Mumbai Maharashtra India 700708.

¹<https://orcid.org/0009-0009-9383-8905>, ²<https://orcid.org/0000-0002-6339-5295>

E-mail: *gautam.borkar@rait.ac.in

ARTICLE INFO

Article History

Received: March 12, 2026

Reviewed: April 11, 2026

Accepted: May 15, 2026

Published: September 30, 2026

Keywords:

Wireless Sensor Network,
Internet of Things,
Metaheuristic Optimization,
Evolutionary Routing Protocol,
Trust Assessment.

ABSTRACT

The growth of wireless sensor networks that are enabled with IoT technologies has increased the demand for routing methods that are secure, low-power, and can scale through dynamic and adversarial environments. Many traditional routing protocols are limited to a single-metric optimization strategy or a static trust model which creates problems with energy imbalance, improper selection of nodes, and vulnerability to coordinated attacks. This study proposes a Hybrid Trust-Metaheuristic Secure Routing Framework that includes an adaptive trust fusion approach to build trust among network nodes, a multi-objective clustering paradigm for optimization of cluster head selection, evolutionary based routing mechanisms and a multi-layered defense against a variety of attack types as components to create unified architecture for routing in WSNs. The framework uses dynamic trust models to evaluate the reliability of each node; employs multiple fitness criteria to optimize the decision-making process for both clustering and routing; and employs a continual monitoring process to evaluate and isolate malicious nodes within the wireless sensor network. By conducting simulations of large-scale IoT-enabled WSN scenarios (100-500 nodes), it can be demonstrated that compared to current methods, improvements were found in the areas of PDR (3 - 5%), Network Lifetime (12 - 18%), Energy Efficiency (10 - 15%) and Attack Detection Accuracy (4-6%). The proposed architecture provides for balanced energy use throughout the WSN, reduced latency and increased security against attacks, and improved communication performance. Thus, the proposed routing framework is a significant enhancement for the deployment of secure and sustainable large-scale IoT-enabled WSNs.



Copyright ©2026 by authors and Galileo Institute of Technology and Education of the Amazon (ITEGAM). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are a key technology for use across many different application domains to obtain information through monitoring, sensing, and collecting data including environmental monitoring, smart agriculture, industrial automation, military surveillance, and healthcare systems [1]. A WSN consists of many small battery operated sensors that work together to detect physical events or conditions. When they do so, they relay that data back to one or more central base stations [2]. Most batteries for sensors in WSNs cannot be easily replaced or recharged due to the location (remote/inaccessible) [3]. Therefore, [4] [5] the need for energy-efficient designs in communication algorithms of WSN is critical (especially routing algorithms) because they directly affect a WSN's performance (energy consumption, communication delay, packet delivery assurance, and network lifetime) [6]. The typical routing methods used to design and implement routing protocols for other networks do not take into consideration the unique limitations on sensor nodes (i.e., limited battery life, limited processing capability, limited memory, and low bandwidth) [7].

Communication protocols that route data through a WSN are therefore designed specifically to limit energy use while transmitting data reliably, provide uniform load distribution, limit redundancy due to excessive or unnecessary communication, and ensure that overhead costs remain as low as possible for each transmission [8]. The main challenge with energy-efficient routing is the way that the energy of nodes in a network is being used and therefore depleted at an inconsistent rate. This inconsistency can result in partitioning of the network, as well as the early failure of critical nodes in the network [9]. Nodes that are located close to the base station or that relay information will consume energy at a faster rate than nodes further away from the base station, creating ‘energy holes’ and therefore disrupting communication paths [10]. Figure 1 outlines the primary components of an energy-efficient routing algorithm: 1) Energy and residual energy monitoring; 2) Clustering techniques for effective network organization; 3) Selection and optimization of cluster heads; and 4) Data aggregation to reduce duplication of data [11]. To solve this problem, researchers have looked at different types of techniques including clustering, multi-hop routing, data aggregation, duty cycling and adaptive transmission power control. Of these techniques, clustering-based routing protocols have received significant research interest, because they reduce transportation distances and allow cluster heads to efficiently manage local data aggregation within a group of collected nodes [12].

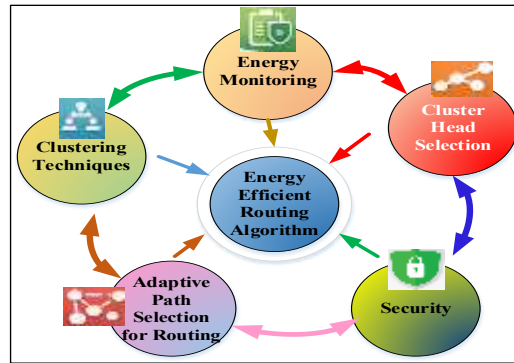


Figure 1: Core components of an energy-efficient routing algorithm in wireless sensor networks.

Source: Authors, (2026).

Routing algorithms in WSNs should also be flexible to changes in the network environment since routing may be significantly impacted by different types of environmental interference, node malfunction, alterations in the overall network topology and variation in the load of node traffic [13]. Energy-efficient routing algorithms should therefore be able to alter their routing paths and to find alternative forwarding node(s) when necessary; they will also balance energy loads across the WSN [14]. Intelligent and optimization-based routing methodologies have been investigated recently to facilitate enhanced routing decisions through the use of many simultaneous metric inputs, rather than using a distance-based routing metric alone; e.g., bio-based algorithms, metaheuristics, and trust-based models have been developed to enable routing algorithms to efficiently utilize diverse information to make the best routing decisions possible [15]. Accordingly, designing advanced energy-efficient routing algorithms has become a major focus of current research since this will allow for longer network lifetimes and reliable data delivery within a WSN. Recent trends in routing algorithm design have integrated additional input parameters, such as node reliability, scalability of the WSN, security and quality of service, into energy-based routing algorithm design. By designing intelligent algorithms for selecting transmission paths based on a number of performance parameters, researchers are developing robust WSN communication networks that can efficiently adapt to large-scale deployment across complex environments [16].

While there has been an increase in routing methods for Wireless Sensor Networks, the ability to balance energy efficiency, security, scalability and reliability of these methods still presents a challenge that is made worse in larger deployments of IoT devices because they contain more nodes and have very complicated network communications, leading to greater performance limits than with smaller deployments. In addition, routing protocols designed for Wireless Sensor Networks continue to exhibit poor performance when trying to achieve all four goals simultaneously largely because most of the emerging protocols only emphasize energy consumption and do not consider other important elements (node trust, conditions on the network, vulnerability to attack) which results in decreased packet delivery and overall shorter lifetimes for the networks. Also, current methods are mostly built around static metrics, cooperative node behavior, and simplistic cluster head selection processes that do not factor in trust, centrality, and communications reliability - thus creating an energy imbalance, vulnerable routing paths, and possible network failure. The vast majority of existing frameworks treat security, energy optimization, and routing as completely separate processes instead of interrelated elements. Therefore, current approaches do not effectively adapt to real world variations in networks, thus revealing a dire need for a unified adaptive routing framework which takes into account: trust, energy, delay, and stability of the network. The major contributions of a research proposal are:

- Proposes a hybrid trust-based routing architecture that combines direct trust with indirect trust metrics to provide a reliable level of trust evaluation and detection of malicious nodes.
- Develops a metaheuristic cluster head selection mechanism by means of hybrid PSO–GA optimization to achieve balanced clustering with better energy distribution and stable network operation.
- The routing strategy introduced in the paper is a trust embedded evolutionary multi-objective-based routing where the path for communication is initiated based on multiple objectives namely trust continuity, residual energy, hop count and delay.
- It designs a multi-attack adaptive defense model that can detect and isolate different types of routing attacks such as packet dropping, the identity spoofing, and tunneling attacks based on behaviors.
- It implements an energy-aware routing decision that ensures nodes with the highest trust levels also have enough residual battery capacity to avoid early node death.

- Incorporates an adaptive load balancing scheme that reallocates traffic, performs cluster head rotation, and triggers multipath routing, ensuring the eradication of energy hotspots.
- Scalable framework was presented and validated under dense large-scale networks conditions resulting in higher packet delivery ratio with reduced end-to-end latency, high resilience to security attacks, and longer network lifetime.

The rest of this paper is organized as follows. Section 2 reviews related work and research gaps. Section 3 presents the proposed framework. Section 4 covers the simulation setup and metrics, results, and comparisons. Section 5 ends with contributions and future research directions and implications for real-world deployment scenarios.

II. RECENT RESEARCHES

This study reviews existing state-of-the-art energy-efficient, secure, and intelligent routing protocols for Wireless Sensor Networks, with a focus on trust-based routing, clustering optimization protocols, metaheuristic techniques, and adaptive communication and routing protocols, as well as a critical analysis of their limitations to identify research gaps that the proposed framework fills. Sirajuddin et al. [17] proposed a hybrid trust-based framework that combined Ant Colony Optimization with trust probability to compute routing decisions in dynamic wireless sensor networks. The approach was based on applying local and global updating policies for better reliable route discovery. In addition, they proposed a non-linear integrity-based intrusion detection model combined with a hybrid encryption protocol to secure node-to-node communication. Other results for runtime, packets delivered, delay, throughput, and security were improved when compared to conventional approaches. However, the model relied on fixed trust evaluation parameters, limiting its capacity to capture dynamic node behavior and coordinated insider attacks, potentially misclassifying malicious nodes. Building on hybrid trust-routing, Ganta et al. [18] developed a similar ACO-based trust-aware routing mechanism coupled with a non-linear integrity intrusion detection model and hybrid security protocol. Route reliability was enhanced based on trust probability-guided path planning to secure communication and performance. The protocol demonstrated measurable improvements in routing efficiency and network security performance. However, the framework adopted static trust thresholds without real-time adaptability, limiting its effectiveness against adaptive attacks and dynamic network performance. To further improve energy-aware routing, Zhang et al. [19] introduced an intelligent clustering mechanism based on Harris Hawks Optimization and reinforcement learning. Clustering considered node distance, dispersion, and energy balance, while selecting cluster heads was done using fuzzy logic trained by reinforcement learning using energy, number of neighbors, and distance as inputs. The experiments showed efficient clustering and increased network lifetime. However, cluster head selection was solely based on energy and proximity without considering trust and clustering based on topology dynamics, which could lead to unreliable nodes being selected as cluster heads and destabilizing network performance.

Building upon secure routing research, Sirajuddin et al. [20] later proposed a hybrid cryptographic framework combined with trust-based routing protocol to improve quality of service and security in the network. The system coupled logistic-map-based encryption with a routing scheme that could identify multiple attacks and guarantee confidentiality, integrity, and authentication. The performance analysis confirmed the enhancement of secure communication performance metrics. Besides this, the main emphasis was placed on cryptographic protection, disregarding adaptive routing optimization, thus posing limitations in preventing energy imbalance and optimizing dynamic routing. Focusing on behavioral reliability, Hasan et al. [21] formulated a trust-route optimization framework using Bayesian inference based on Jeffrey's conditioning to calculate composite trust values for intermediate nodes. The proposed solution was evaluated via simulations against random, greedy, and AI routing protocols, with results indicating improved routing reliability. However, the model did not include an adaptive packet redistribution mechanism based on traffic pattern changes and lacked a real-time energy balancing framework that could redistribute service loads to minimize skewed energy depletion and premature node death. Similarly, Mata et al. [22] proposed composite routing, which is based on trust and congestion-aware routing to improve performance and security in the network. Their protocol used behavioral trust to avoid malicious nodes and congestion-aware routing to improve throughput and reduce delay. Results indicated better resource utilization and network lifetime. However, the routing decision-making process was based on predefined metrics without employing multi-objective optimization dynamically, thereby limiting adaptability to rapidly changing network conditions. In the context of intelligent routing, Priyadarshi et al. [23] proposed a modular AI-based routing framework that combines reinforcement learning, supervised learning, and swarm intelligence routing algorithms with GA and PSO. Hence the modular decision pipeline adaptively took care of the varying routing topology, traffic, and energy parameters, with each module responsible for a particular optimization endeavor. The experimental results demonstrated an adaptability and improvement in the routing efficiency.

However, the framework lacked a specialized trust management strategy, leaving it susceptible to insider threats and untrustworthy node behavior. Focusing on adaptive energy balancing, Soltani et al. [24] have come up with reinforcement learning-based cluster-head selection and multi-hop routing scheme using Q-learning in the case of a multi-agent system. Each node acted as an autonomous agent selecting routing actions based on local parameters such as residual energy and distance to sink. Classical graph algorithms were combined to optimize the economic consumption and balance the load. However, the method was purely focused on energy optimization, ignoring trust evaluation and detection of coordinated attacks for enhanced robustness in adversarial environments. Manogaran et al. [25] proposed an energy-efficient routing framework using an ADDQL model that enabled intelligent high-speed routing in dynamic WSN scenarios. The performance was measured in a variety of metrics such as delay and scalability, energy consumption, and others, to demonstrate superiority against existing approaches. However, routing decisions rely on performance metrics rather than behavioral trust, implying a limitation in identifying malicious nodes. To combat cluster stability issues, Alomari et al. [26] introduced the Meta-Heuristic Algorithms-based Collaborative Dynamically Clustered Routing Protocol that combined Genetic Algorithms and Whale Optimization to adaptively select cluster heads. The protocols consider several parameters, including but not limited to distance, velocity, residual energy, and packet delivery ratio to guarantee fair energy consumption and stability in communication. However, there was no trust monitoring in real-time and no dynamic detection of attacks, allowing compromised nodes to route packets. Prince et al. [27] developed the Energy-Efficient Mega-Cluster-Based Routing protocol for large coverage areas, with centralized clustering and mega-cluster heads to counter hotspot problems and balance the traffic load. To reduce the communication overheads and energy consumption, the protocol used multi-level aggregation and, mobile data mules.

Simulative analysis showed enormous improvement in network life span and traffic balance. However, scalability and adaptability to real-time network changes were limited by the centralized architecture, especially in highly dynamic large-scale environments. Finally, Visalatchi et al. [28] developed the Energy-Efficient Consonance-Based Adaptive Routing algorithm. This algorithm selected routes dynamically based on energy levels, connectivity, and reliability with consonance-based decision principles. The adaptive routing method improved the packet delivery ratio, network stability, and also the lifetime of the respective network, especially under conditions where there was a critical mission to be completed. However, it was limited in the consideration of energy-aware routing and did not have integrated security and trust evaluation, therefore leaving it vulnerable to a participating malicious node or coordinated attacks on the routing mechanisms used within that network. Prior studies have shown many areas of improvement within Wireless Sensor Networks when it came to routing efficiency, clustering methods, and energy efficiency. However, the majority of existing research tends to look at only individual performance areas instead of developing a recognizable overall framework. This has led to some critical issues still remaining such as static/single parameter trust evaluations, single objective optimization models, limited capability to detect coordinated attacks, lack of adaptive load balancing and validation only being done on small scale scenarios. All of these issues combined resulted in decreased Routing reliability, Routing adaptability, and decreased Network lifetime; therefore, there is a need for an ALL-IN-ONE trust-aware routing framework that is unified, scalable and intelligent and can address security, energy efficiency and dynamic network conditions all at the same time thus motivating the development of this proposed methodology.

III. PROPOSED METHODOLOGY

The development of the Hybrid Trust & Metaheuristic Secure Routing Framework aims to overcome the major obstacles that traditional ways of doing things have in large IoT-enabled Wireless Sensor Networks in particular when trying to provide energy efficiency, routing reliability, scalability and secure routing all at the same time. Many traditional protocols are based on using static trust models, single objective optimization and shortest paths which do not react appropriately to changes in the network, energy variations, and malicious node behaviour. Each of these issues often results in unreliable path selection, increased packet losses, imbalance of energy burning rate and ultimately poor network lifetime. In addition, many of the traditional clustering methods do not consider the trustworthiness of a node and have no concept of a dynamic network, both of which would make clusters unstable and vulnerable to insiders, as well as static security measures being of minimal benefit for identifying coordinated or developing security issues. To address these limitations, a unified multi-phase architecture is being proposed as an integrated framework to provide a systematic approach to topology-aware deployment, hybrid trust calculation, metaheuristic cluster head optimization, evolutionary secure data routing, adaptive attack detection, and energy-aware load balancing. The first step includes the creation of a realistic large-scale network topology in order to model high-density IoT sensing environments and to validate routing decisions within real-world conditions. The next step involved evaluating the reliability of nodes by creating a hybrid trust fusion method that incorporates the behavior of nodes from both direct observation and indirect recommendations.

Based on this trust value and remaining energy, an advanced metaheuristic optimization strategy selects optimal cluster heads, thus ensuring that clustering is stable, communication is balanced, and re-clustering is reduced. Following this process, a secure data routing method using evolutionary fitness was conducted by selecting data paths based on the following criteria: degree of trust continuity, amount of remaining energy, efficiency of number of hops, degree of delay; thus ensuring data transmission reliability and efficiency. The processes within the proposed methodology are illustrated in Figure 2. The framework established an adaptive defense mechanism which constantly observed network activities to identify abnormal behavior and separate harmful nodes from the system to safeguard routing security against organized attacks. The energy-aware routing strategy required nodes to meet two conditions of energy capacity and dependable performance before they could start their forwarding activities, which helped to avoid early node breakdowns. The system used an adaptive load balancing mechanism to distribute communication activities while it used automatic cluster head rotation to manage load balancing requirements. The system used trust reliability and residual energy and delay and network stability to make routing decisions which enabled it to adjust to current network conditions while blocking access to untrustworthy and compromised nodes. The proposed system achieved better routing stability for network operation through its combined and collaborative system design which achieved longer network operational life and improved protection against attacks while maintaining performance efficiency for dense heterogeneous IoT-WSN systems.

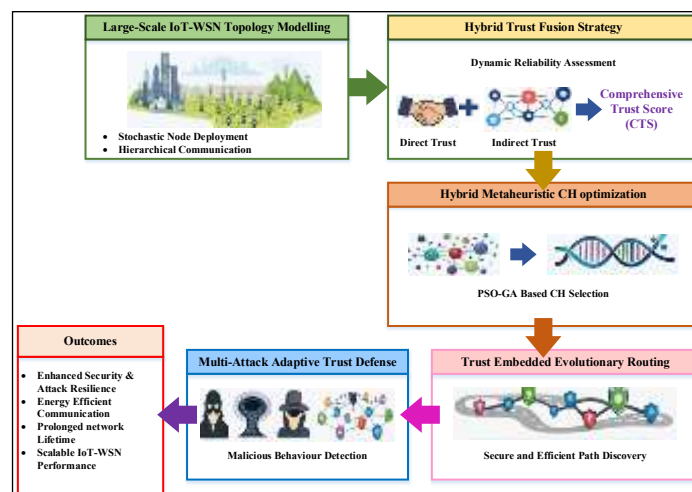


Figure 2: Overall flow diagram of the proposed Hybrid Trust–Metaheuristic Secure Routing methodology.

Source: Authors, (2026).

III.1 LARGE-SCALE IOT-WSN TOPOLOGY MODELLING

The initial phase of the proposed framework begins with this stage, which establishes a realistic sensor network environment that contains various sensor types to simulate actual deployment conditions. In this stage, sensor nodes are distributed across the monitoring area through random placement, while multiple energy capacity and transmission range and sensing capacity attributes are given to the nodes and distance-based and channel-condition-based communication links are established. The system begins with a hierarchical multi-hop framework, which uses cluster heads and relay nodes, to enable scalable communication testing, while network density and interference and link reliability testing, which maintains IoT-WSN testing conditions, enables trust evaluation and clustering and routing optimization testing in the forthcoming evaluation process. Let the network be defined as a graph $G = (N, L)$, where $N = \{n_1, n_2, \dots, n_k\}$ denotes the set of sensor nodes and $L \subseteq N \times N$ represents communication links. Nodes are deployed using a stochastic spatial distribution modelled through a two-dimensional Poisson point process:

$$P(X = x) = \frac{\lambda^x e^{-\lambda}}{x!} \quad (1)$$

Where λ represents the spatial density of nodes and x is the number of nodes in a given area. Stochastically deploying nodes allows for realistic simulations of random node placement typically seen in monitoring the environment, sensing industry, and smart city infrastructures. Stochastic node placement provides an opportunity to test the robustness of a routing algorithm against variations in random topology as opposed to deterministic node-placement models. Incorporating heterogeneity into a node is included by assigning each node variable attributes, such as residual energy (E_i), transmission range (R_i), and processing capability (C_i). The initial energy distribution is uniformly distributed randomly.

$$E_i \sim U(E_{min}, E_{max}) \quad (2)$$

By omitting uniform energy assumptions, it allows for simulating real devices with various battery capacities. To check whether there is connectivity between nodes i and j , the connectivity function is used to determine the feasibility of communication:

$$L_{ij} = \begin{cases} 1 & \text{if } d_{ij} \leq R_i \\ 0 & \text{otherwise} \end{cases} \quad (3)$$

Where d_{ij} is the distance between two nodes in Euclidean space. This adaptive link formation mechanism captures dynamic communication over wireless networks rather than assuming all nodes have fixed neighbor sets. Scalable communication will use a hierarchical multi-hop topology. The nodes will self-organize into clusters with a cluster formation probability of,

$$P_{CH}(i) = \alpha \frac{E_i}{E_{max}} + (1-\alpha) \frac{Deg_i}{Deg_{max}} \quad (4)$$

Where Deg_i is the degree of node i and $\alpha \in [0,1]$ is a constant between 0 and 1 that balances energy consumption with topological centrality. This model provides an innovative way of initializing the clusters so that low-energy nodes are not chosen as cluster heads, while high-degree nodes provide an efficient routing capability. Relay nodes will be determined based on a minimum-cost path from node i to node j , which is determined by:

$$Cost_{path} = \sum_{(i,j) \in path} \left(w_1 d_{ij} + w_2 \frac{1}{E_j} + w_3 \eta_{ij} \right) \quad (5)$$

Where η_{ij} represents the link error rate between nodes i and j , and w_1, w_2, w_3 represent the adaptive weights of each link. are adaptive weights. The interference between nodes and reliability of each link will be modelled to reflect realistic wireless channel conditions. The calculation for signal-to-interference-plus-noise ratio (SINR) from node i to node j is as follows:

$$SINR_{ij} = \frac{P_i h_{ij}}{\sum_{k \neq i} P_k h_{kj} + N_0} \quad (6)$$

Where P_i is transmission power, h_{ij} is channel gain and N_0 is noise power. A communication link is considered stable only if:

$$SINR_{ij} \geq \gamma_{th} \quad (7)$$

Topology formation will benefit from SINR-based validation as this process will eliminate links that are unstable; helping to create stable routing within that topology and reducing the number of retransmissions required. The initialization phase of creating the topology uses a dynamic construction method rather than using an initial given topology; this means that the protocol will create an active, non-homogeneous, and interference-aware network model. This protocol combines the stochastic deployment, heterogeneous node properties, probabilistic cluster head initialization, multi-criteria relay selection, and SINR-based link validation variables into a single mathematical model, providing much more realistic topologies than traditional methods and being more easily scalable and adaptable due to its ability to model large scale IoT-WSN deployments closely to the characteristics of these types of deployments. The entire process can be visualized throughout this process and includes stochastic node placement, heterogeneous profiling, adaptive link creation, and hierarchical multi-hop communication shown in Figure 3.

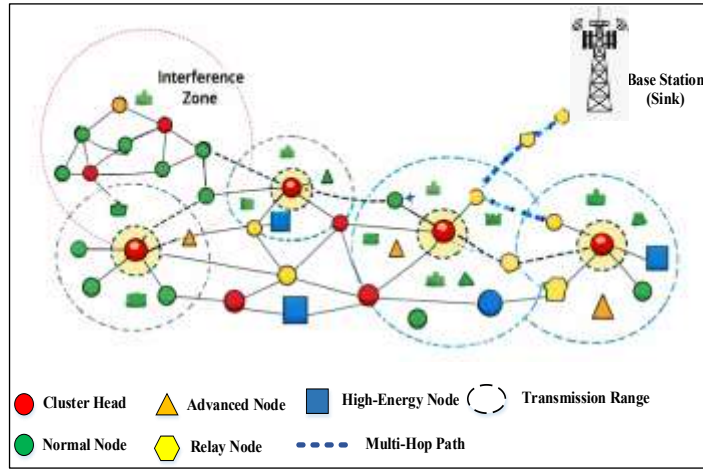


Figure 3: Large-scale heterogeneous IoT-WSN topology model.
Source: Authors, (2026).

III.2 HYBRID TRUST FUSION MECHANISM

Following the creation of a realistic heterogeneous large-scale topology, the next critical step in the proposed framework is to evaluate the reliability of each node prior to clustering and routing in the network. Routing decisions in large-scale IoT-WSNs cannot be based on connectivity or residual energy alone, especially because a node's behavior may change dynamically due to device failures, congestion, depleted batteries, or malicious interference. Trust models generally rely on an individual metric for evaluation or use a static evaluation method, both of which will be inadequate for detecting any coordinated insider attacks or dishonest recommendation propagation. The consequences of these deficiencies will be inaccurate route selection, packet losses, untrustworthy amplification and unstable operation of the whole network. The proposed framework will provide a Hybrid Trust Fusion Mechanism to assess trust on dynamic, multiple sources by the following way: The Hybrid Trust Phase consists of two complementary components, Direct Trust (DT) and Indirect Trust (IT), in order to evaluate behavior comprehensively. DT reflects the first-hand experience between two nodes from previous interactions. DT is determined using measurable indicators related to the performance of communications between two nodes, e.g., a node's success in forwarding packets, consistent acknowledgments, the stability of the link, and historical cooperation. Node j 's DT as assessed by node i is defined as:

$$DT_{ij} = \frac{F_{ij} + \beta H_{ij}}{T_{ij} + \epsilon} \quad (8)$$

Where F_{ij} is the successful forwarding of packets, H_{ij} is the historical consistency of cooperation, T_{ij} is the total number of 0 interaction, β is the control parameter for the impact of long-term behavior, and ϵ is a small constant to avoid division instability. This model is more focused on long-term cooperation rather than short-term cooperation, thus reducing the impact of occasional malicious behavior. Indirect Trust takes into consideration the recommendations of the neighboring nodes that have previously interacted with node j . To avoid false reporting attacks, each recommendation is weighted based on the credibility of the recommending node. The Indirect Trust is given by:

$$IT_{ij} = \frac{\sum_{k \in N_i} w_k DT_{kj}}{\sum_{k \in N_i} w_k} \quad (9)$$

The function N_i identifies all neighboring nodes that connect to node i whereas w_k defines the trustworthiness rating for recommender node k . The system updates credibility weights in response to changes in each recommender's past performance of truthful and consistent behavior. The weighted fusion mechanism retains valid recommendations while blocking dishonest feedback and protecting against collusion attacks. The system calculates the Comprehensive Trust Score (CTS) through adaptive fusion methods which produce the final score.

$$CTS_{ij} = \alpha DT_{ij} + (1 - \alpha) IT_{ij} \quad (10)$$

The equation shows that the value of α exists within the interval which ranges from 0 to 1 to create a balance between personal knowledge and network-wide standing. The system combines real-time user behavior data with network user agreement to create a trust measurement system that outperforms traditional single-source methods. The system uses a dynamic threshold τ to authenticate nodes which will participate in routing activities.

$$Node_j = \begin{cases} Trusted & CTS_{ij} \geq \tau \\ Malicious & CTS_{ij} < \tau \end{cases} \quad (11)$$

The system uses network trust values through τ which adjusts to their statistical distribution whereas static thresholds remain fixed. The hybrid trust system creates a security layer that uses behavior recognition technology developed through the topology model described in Section 3.1. The framework identifies compromised nodes through its combination of direct behavioral evidence and credibility-weighted reputation and adaptive fusion and dynamic thresholding. The system reduces malicious participation while improving routing integrity and decreasing false packet propagation and enhancing decision accuracy. The design enables large-scale IoT-WSN deployments to achieve scalability and robustness and adaptability while preserving mathematical clarity and practical applicability.

III.3 HYBRID METAHEURISTIC CLUSTER HEAD OPTIMIZATION

The system proceeds to its next phase after completing topology building and hybrid trust assessment through its process of forming clusters, which selects its best Cluster Heads (CHs). The selection process for CHs stands as the most crucial element because CHs handle both intra-cluster communication and data gathering while they send information to the base station. The selection of CHs through low-energy nodes and unreliable nodes leads to faster energy consumption and cluster instability plus security breaches. The usual methods use single-objective metrics like residual energy and distance to measure requirements, which create an incomplete understanding of large-scale IoT-WSN requirements. The proposed method solves existing issues by developing CH selection through multi-objective optimization, which combines trust energy topology and communication efficiency into a single fitness assessment system. Each node i is evaluating using:

$$F_i = w_1 \cdot CTS_i + w_2 \cdot \frac{E_i}{E_{max}} + w_3 \cdot C_i + w_4 \cdot \left(1 - \frac{D_i}{D_{max}}\right) \quad (12)$$

Where CTS_i represents the comprehensive trust score which derives from eq (12), E_i represents the remaining energy, C_i represents the centrality of the node, D_i represents the typical distance to neighboring nodes, and $\sum w = 1$. A node can become CH only when it meets four criteria which include trustworthiness, energy capacity, central position in the network, and ability to communicate effectively. The objective of this system combines two different evaluation methods which assess both performance results and security requirements. The proposed framework uses Hybrid Evolutionary Swarm Optimization Mechanism as its main solution for the optimization problem. The system achieves its objectives through metaheuristic system which combines cooperative population-based search with evolutionary refinement to deliver fast results while maintaining system diversity. The goal of this process is to conduct global solution space exploration without encountering early process halts. The candidate solutions function as potential CH configurations. The position of candidate i at iteration t is denoted by x_i^t , and its adaptive search direction is represented by v_i^t . The update mechanism is defined as:

$$v_i^{t+1} = \omega v_i^t + c_1 r_1 (p_i^{best} - x_i^t) + c_2 r_2 (g^{best} - x_i^t) \quad (13)$$

$$x_i^{t+1} = x_i^t + v_i^{t+1} \quad (14)$$

The best solution which a candidate has discovered previously exists as p_i^{best} while g^{best} represents the most successful solution which the entire population ω, c_1, c_2 has discovered. The cooperative learning system enables candidates to use their personal knowledge together with worldwide information to investigate CH configurations which show promise. The adaptive recombination process treats elite candidate solutions:

$$x_{offspring} = \lambda Parent_1 + (1 - \lambda)x_{Parent_2} \quad (15)$$

The parameter $\lambda \in (0,1)$ controls the distribution of contributions. This recombination approach combines effective solution parts which boosts the system's ability to search for solutions that are close to optimality.

$$x_{new} = x_{old} + \sigma \cdot \mathcal{N}(0,1) \quad (16)$$

The mutation intensity is represented by σ while Gaussian noise is denoted by $\mathcal{N}(0,1)$. This step introduces controlled random elements which help the system to escape local optimum points while maintaining its convergence stability. The multi-objective fitness function (Eq. 14) evaluates each candidate solution after its respective updates. The configuration that achieves maximum objective value is selected for retention.

$$x^* = \arg \max F(x_i) \quad (17)$$

The Hybrid Evolutionary Swarm Optimization mechanism provides organizations with an adaptable solution to handle their multi-objective Cluster Head selection needs in large-scale IoT-WSNs environments. The system achieves efficient exploration because it applies three methods, which are cooperative global search and evolutionary refinement and controlled diversification, to maintain balance between exploration and prevention of early stopping. The system creates secure cluster leadership through its fitness framework, which combines trustworthiness and residual energy and node centrality and communication efficiency into a unified system. The adaptive update strategy enables the system to respond to changing network conditions, which results in improved system scalability and network security. The system achieves better clustering stability through its design, which also maintains energy balance and enhances security while doubling the operational time of the entire network. The workflow, shown in Figure 4, shows the steps of starting the process, assessing fitness, using hybrid optimization, refining solutions, and creating the final cluster.

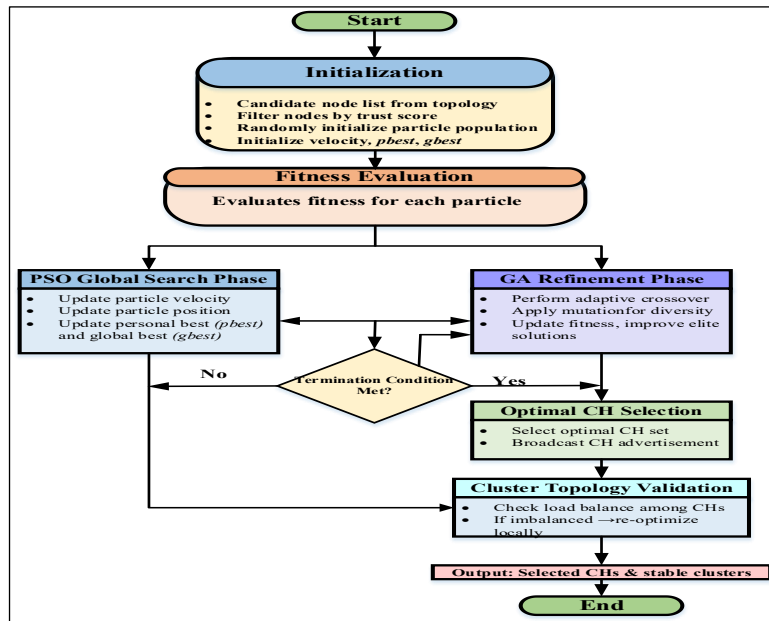


Figure 4: Flowchart representation of the proposed Hybrid PSO–GA–based Cluster Head Optimization algorithm.

Source: Authors, (2026).

III.4 TRUST-EMBEDDED EVOLUTIONARY ROUTING MODEL

The process begins with creating trustworthy and stable clusters which lead to the establishment of secure energy-efficient routes. The conventional routing protocols which most systems use depend on two methods: shortest-path and minimum-hop. These methods fail to account for dynamic trust changes and residual energy shifts and quality-of-service (QoS) requirements. The presence of compromised nodes in routing paths results in packet loss and extended delays and decreased network lifespan. The proposed framework uses multi-objective evolutionary optimization to solve routing problems because it enables complete route evaluation through security and performance assessment. The system uses the following route R_k representation method which shows all possible routes from source S to destination D .

$$R_k = [n_1, n_2, n_3, \dots, n_m] \quad (18)$$

The variable n_i represents the i^{th} forwarding node. The method of encoding routes into structured sequences allows for systematic testing of different forwarding paths instead of using fixed path selection. The evaluation of candidate routes uses the following assessment criteria:

$$F(R_k) = w_1 T_k + w_2 E_k + w_3 H_k + w_4 D_k \quad (19)$$

Where

- T_k =Trust continuity score
- E_k =Residual energy factor
- H_k =Hop efficiency metric
- D_k =Delay efficiency metric

The unified method evaluates four elements which are reliability, energy stability, communication expenses and delay restrictions. Trust continuity ensures that all intermediate nodes are reliable:

$$T_k = \frac{1}{m} \sum_{i=1}^m CTS(n_i) \quad (20)$$

Where $CTS(n_i)$ is the comprehensive trust score of node n_i . The process guarantees that all intermediate nodes work together to protect their secure forwarding operations. The system calculates energy availability through the complete path.

$$E_k = \frac{1}{m} \sum_{i=1}^m \frac{E_i}{E_{max}} \quad (21)$$

The system uses residual energy resources E_i of all nodes i to assess their remaining operational time until system shutdown occurs. The scoring system assigns lower values to routes which contain low-energy nodes because these routes lead to early system breakdowns. The hop efficiency metric establishes routing paths which require less data transfer through intermediate points as the most effective transmission method to reduce network transmission expenses and communication costs.

$$H_k = \frac{H_{min}}{H_k^{actual}} \quad (22)$$

The actual hop count for route k is represented by H_k^{actual} . The metric gives better results to paths which transmit data fewer times. An end-to-end delay estimation model exists to evaluate candidate routing paths because the system needs to meet quality-of-service standards. Therefore, end-to-end delay is modelled as

$$D_k = \frac{D_{min}}{\sum_{i=1}^m (d_i^{proc} + d_i^{trans})} \quad (23)$$

Where d_i^{proc} and d_i^{trans} denotes the processing and transmission delay at node i . The optimal route is determined as:

$$R^{best} = \arg \max_{R_k \in P} F(R_k) \quad (24)$$

The population of candidate routes exists as the value P throughout the process. The system develops candidate routes through two methods: guided recombination and controlled stochastic variation which together protect against early system shutdowns while supporting system changes that occur during node outages and traffic overloads and security trust system failures. The Trust-Embedded Evolutionary Routing Model advances conventional routing by transforming deterministic path selection into an adaptive, multi-objective optimization framework. The model achieves secure data forwarding through trust continuity and residual energy awareness and hop minimization and delay optimization which also results in balanced energy usage and scalable system performance. The adaptive refinement mechanism improves network resilience against both network disruptions and attacks while creating better packet delivery performance and extended network duration and constant communication in IoT and WSNs that operate under heavy device and environmental diversity.

III.5 MULTI-ATTACK ADAPTIVE DEFENCE MECHANISM

The network requires protection from runtime threats after secure route establishment because node behavior will change when nodes face compromise or failure or when adversaries apply their influence. The routing paths become insecure despite their optimization and trust-based design because malicious activities can occur during system operation. The proposed framework establishes a Multi-Attack Adaptive defence Mechanism which functions as an ongoing monitoring system that works in close association with both routing and clustering operations. The system detects threats through three components which include its unified framework that handles dynamic behavior assessment and threshold adjustment and anomaly-based system separation. The system continuously tracks each node's current trust value $CTS_i(t)$ while comparing it against its previous trust value $\overline{CTS}_i$. The deviation is computed as:

$$\Delta T_i = |CTS_i(t) - \overline{CTS}_i| \quad (25)$$

If a node's deviation is greater than the dynamically timed $\theta(t)$, then it gets kind of categorized as a rogue nod.:

$$Node_i \rightarrow \text{Malicious if } \Delta T_i > \theta(t) \quad (26)$$

Then the adaptive threshold determine as:

$$\theta(t) = \mu_T + \lambda \sigma_T \quad (27)$$

The formula uses network trust distribution which is measured through its mean value μ_T and standard deviation value σ_T while λ serves as the parameter for adjusting detection precision. The system uses a dynamic thresholding mechanism which adapts to changing network conditions in order to detect insider attacks that occur both immediately and progressively. The detection accuracy is enhanced through the concurrent assessment of multiple runtime indicators.

$$A_i = \alpha_1 P_i + \alpha_2 R_i + \alpha_3 C_i + \alpha_4 F_i \quad (28)$$

The packet drop anomaly routing inconsistency index communication deviation feedback credibility factor are represented by the variables P_i, R_i, C_i and F_i . All nodes which exceed the established anomaly threshold must undergo immediate isolation. The integrated scoring method enables unified detection of Sybil attacks wormhole attacks blackhole attacks selective forwarding attacks impersonation attacks. The combined trust–energy prioritization score protects routing stability after all malicious nodes have been isolated.:

$$Score_i = \beta_1 CTS_i + \beta_2 \frac{E_i}{E_{max}} \quad (29)$$

Higher scores of nodes are preferred for forwarding. Load redistribution is triggered when:

$$E_i < E_{th} \rightarrow \text{Trigger Load Redistribution} \quad (30)$$

The security measure leads to active load balancing operations which create an energy hotspot solution while extending the operational period of the network. The Multi-Attack Adaptive Defense Mechanism introduces a new approach to WSN security which combines continuous trust assessments with advanced statistical analysis methods and multiple anomaly detection techniques and live statistical thresholding and energy-efficient routing protection inside one operational framework. The system enables instant detection of security breaches because its design allows for tracking of damaged nodes while maintaining network operation stability. The framework achieves continuous communication stability together with better packet transmission results and stronger protection against attacks and increased operational duration through its security system combined with its dynamic load distribution system and its energy-efficient decision-making process. The operation sequence of the Multi-Attack Adaptive Defense Mechanism is shown in Algorithm 1 which presents the ongoing monitoring system that tracks node activity together with trust value changes and suspicious behavior identification and dangerous node removal and energy-efficient routing and dynamic load management.

Algorithm 1: Multi-Attack Adaptive Defense Mechanism for IoT-WSNs

Input:

- Clustered network topology with nodes $N = \{n_1, n_2, \dots, n_m\}$
 - The node performance metrics which operate in real time measure three aspects of packet processing and routing information and communication stability between nodes.
-

- The Hybrid Trust Fusion system calculates the node trust score for each node at time t using the formula $CTS_i(t)$

- The node residual energy E_i represents the remaining power which resides within the system.

Output:

- Isolation of malicious nodes
- Balanced load distribution and safe, energy-conscious routing

Step 1: Initialize Monitoring

- The system should track various behavior metrics which include packet drop ratio and routing consistency and neighbor feedback reliability and communication deviations for every node n_i which belongs to set N .

- The system needs to obtain current Comprehensive Trust Score (CTS) $CTS_i(t)$ and residual energy E_i .

Step 2: Compute Trust Deviations using eq (27) and (29)

- If $\Delta T_i > \theta(t)$ mark node n_i as suspect.

Step 3: Evaluate composite Anomaly score using eq (30)

Step 4: Routing update and node isolation

- Remove identified malicious nodes from cluster and routing tables.
- Trigger recalculation of routing paths using Trust-Embedded Evolutionary Routing to avoid compromised nodes.

Step 5: Energy-Aware Trust Routing using eq (31)

- Prioritize forwarding nodes with high trust and sufficient energy.
- Update forwarding paths dynamically to maintain QoS and energy balance.

Step 6: Adaptive Load Balancing

- The system requires monitoring of cluster head energy levels and relay node energy levels to determine their energy thresholds E_i which should not fall below E_{th} threshold.
- The system will distribute network traffic to different trusted nodes to stop the creation of energy hotspots.
- The system will activate its dynamic cluster head rotation system together with its multipath routing system whenever the situation requires such functions.

Step 7: Continuous Monitoring

- Repeat these tasks on routine basis for real time threat detection, node trust assessment, and energy-aware re-routing modification.

Step 8: Termination

- The algorithm operates throughout the entire network life to achieve three objectives which include maintaining secure communication and resilient communication and energy-efficient communication.

The proposed methodology establishes a unified and well-coordinated framework that integrates trust evaluation, multi-objective clustering, adaptive routing, and real-time defense mechanisms to address energy efficiency, security, and scalability challenges in IoT-WSNs. The system establishes reliable node selection and secure cluster formation and optimized route discovery and continuous threat monitoring through its components which operate in sequential and collaborative modes. The strong interaction among modules enhances routing stability, prevents malicious participation, balances energy consumption, and adapts to dynamic network conditions. The framework produces extended network lifespan, greater system dependability, and secure communication channels which withstand attacks and function effectively in extensive and diverse IoT-WSN environments.

IV. RESULTS AND DISCUSSION

The section provides a complete performance assessment of the Hybrid Trust–Metaheuristic Secure Routing framework which operates across various network environments and security breach situations. The study conducted multiple simulations to test the system's performance which included measuring its energy consumption, routing accuracy, security strength, and ability to handle increased workloads. Additionally, present their results as a formal comparison to established routing protocols which demonstrates the better performance of their developed method. Through in-depth evaluation of essential performance indicators how trust modeling, hybrid optimization, evolutionary routing, and adaptive defense systems work together to increase network lifespan and improve packet delivery and boost protection against attacks.

IV.1 SIMULATION SETUP AND EXPERIMENTAL CONFIGURATION

This study used MATLAB R2021b to conduct their simulations which tested the Hybrid Trust–Metaheuristic Secure Routing framework in large-scale IoT-WSN environments. The study deployed between 100 and 500 different sensor nodes across a $1000 \times 1000 m^2$ area. All nodes started with 50 J energy and a 0.5 trust score. The researchers established data packet sizes at 4000 bits while control packets were set to 1000 bits. The system operated for 200 to 1000 rounds which used 500 ms intervals to perform its functions of dynamic clustering and routing and trust evaluation and adaptive defense. The researchers implemented various attack scenarios while they conducted their experiments to compute results which they tested for statistical validity through 20 independent runs.

The simulation setup is summarized in Table 1, providing a clear overview of the experimental configuration and implementation environment.

Table 1: Simulation parameters and Configuration.

Parameter	Value
Number of Sensor Nodes	100- 500 nodes
Network Area	1000 × 1000 m ²
Packet Size (Data)	4000 bits
Packet Size (Control)	1000 bits
Initial Node Energy	50 J per node
Transmission Power	0.500 J
Receiving Power	0.050 J
Initial Power	0.5 J
Initial Trust Value	0.5
Time Interval	500 ms
Simulation Duration	500 ms
Number of Rounds	200–1000 rounds

Source: Authors, (2026).

IV.2 METRICS USED FOR EVALUATION

The evaluation of the Hybrid Trust–Metaheuristic Secure Routing framework used multiple metrics which measured energy efficiency and routing reliability and security strength and total network performance. The following metrics were considered: The proposed framework performance evaluation in large-scale dynamic IoT-enabled WSN environments which face security threats uses the metrics listed in Table 2 to deliver complete results.

Table 2: Performance Evaluation Metrics.

Metric	Definition / Formula	Description
Packet Delivery Ratio (PDR)	$PDR = \frac{\text{Number of packets received at sink}}{\text{Number of packet sent}} \times 100\%$	The system tests data transmission reliability through its measurement system which shows higher values when data transmission succeeds.
Packet Loss Ratio (PLR)	$PLR = \frac{\text{Number of packets lost}}{\text{Total packets sent}} \times 100\%$	The system shows transmission failures which happen because of network congestion and attacks and link failures. The system operates better when it achieves lower results.
Throughput	$\text{Throughput} = \frac{\text{Total successfully received data (bits)}}{\text{Simulation time (s)}}$	The system calculates the effective data transmission rate which the network can achieve.
Average Residual Energy (ARE)	$ARE = \frac{\sum_{i=1}^N E_i^{\text{residual}}}{N}$	The system displays average remaining energy of each node which shows the system's energy efficiency and load balancing capacity.
Network Lifetime	Time/rounds until first, half, or last node dies	The system tests how long the network can operate while maintaining its efficiency.
End-to-End Delay	$\text{Delay} = \frac{\sum_{i=1}^P (t_{\text{received}} - t_{\text{sent}})}{P}$ Where P is the total number of packets successfully delivered.	The system calculates time required for successful packet delivery which results in faster communication when its value decreases.
Trust Reliability (CTS Accuracy)	Accuracy of malicious node detection via CTS	The system measures how well CTS-based trust evaluation methods can identify dangerous nodes and unreliable nodes.
Attack Detection Rate (ADR)	$ADR = \frac{\text{Number of attacks detected}}{\text{Total number of attacks launched}} \times 100\%$	The security mechanism shows success in attack detection through its ability to identify unauthorized access attempts.
Routing Overhead (RO)	$RO = \frac{\text{Number of control packets transmitted}}{\text{Number of data packets delivered}}$	The system calculates protocol efficiency through its measurement system which shows lower overhead values that produce reduced control expenses.
Energy Consumption per Round	Total energy consumed by all nodes in each round	The system calculates total energy consumption which all nodes use during every communication session.
Computational Efficiency	Time / resources used for trust, clustering, and routing calculations	The system requires specific time and processing resources for trust evaluation and clustering and routing operations.

Source: Authors, (2026).

IV.3 RESULTS ANALYSIS

The evaluation of the Hybrid Trust–Metaheuristic Secure Routing framework took place through its testing on large-scale IoT–WSN environments across 200 to 1000 simulation rounds. The team evaluated performance through a complete set of energy and security metrics which included packet delivery ratio, packet loss, throughput, delay, residual energy, network lifetime, trust reliability, detection rate, routing overhead, and computational efficiency. The research showed that the new system outperformed existing routing and trust-based protocols through its improved secure data transmission and balanced clustering and adaptive routing stability.

The system achieved better performance through the integration of dynamic trust evaluation and multi-objective optimization which enabled reliable node selection while reducing energy hotspots and maintaining operational capability during multiple attack situations.

IV.4 NETWORK TOPOLOGY AND CLUSTER FORMATION VISUALIZATION

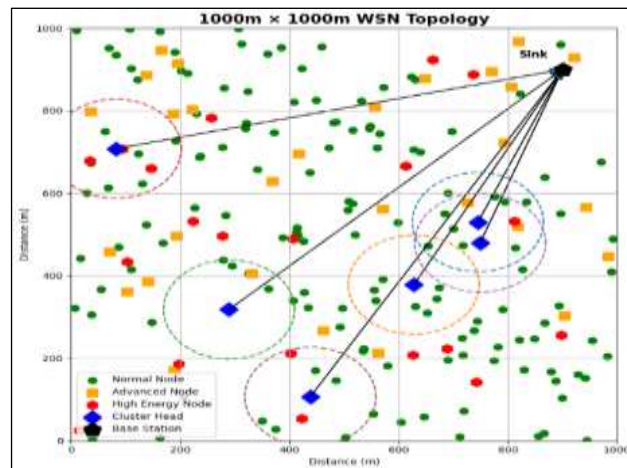


Figure 5: Simulated IoT-WSN topology illustrating node deployment, cluster head selection, and multi-hop communication toward the sink.

Source: Authors, (2026).

The simulated IoT-enabled Wireless Sensor Network topology was created through the experimental configuration according to Figure 5. The proposed work distributed sensor nodes across a 1000 by 1000 meter area to create an authentic representation of large-scale deployment conditions. The different node types which include normal nodes advanced nodes and high-energy nodes display their distinct abilities and energy capacities through visual differentiation. The system shows dynamically selected Cluster Heads through dashed coverage regions which demonstrate the hierarchical clustering that resulted from the implemented optimization method. The system displays multi-hop communication paths which lead to the sink while implementing secure and energy-efficient forwarding methods. The active distribution of Cluster Heads throughout the area shows that the system achieves effective load handling while stopping energy accumulation at specific points and expanding network capacity and operational efficiency.

IV.4.1 Performance Evaluation Results

This work assessed the proposed energy-efficient, trust-aware routing framework through tests which required different node densities between 100 and 500 nodes in dynamic IoT-WSN environments. The performance metrics which include Packet Delivery Ratio and Packet Loss and Throughput and Routing Overhead and Computational Efficiency show that the system maintains operational stability while providing performance scalability. The system achieves dependable data transmission through its combination of trust assessment and dynamic clustering and enhanced routing methods which enable energy-efficient operations during both normal and hostile situations.

Packet Delivery Ratio:

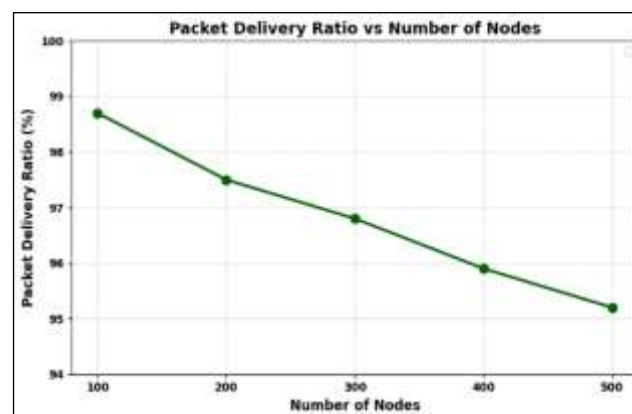


Figure 6: PDR (%) of the proposed routing framework across varying network sizes (100–500 nodes).

Source: Authors, (2026).

As illustrated in Figure 6, the performance of the proposed routing framework for Packet Delivery Ratio is shown, where sensor nodes are increased from 100 to 500. The results show that delivery rates are consistently very high, with only a slight decrease in delivery rate (98.7% to 95.2%). Delivery rates will be decreased in dense networks due to contention, interference, collisions, and routing complexity, but that slight decrease is to be expected. This shows that the proposed routing framework still has good scalability and capability under heavy traffic.

The three methods that provide these performance levels are coordinated trust-based node filtering, hybrid metaheuristic cluster head selection, and evolutionary route optimization, which ensure that only nodes with high trust and low power are used to forward packets. Furthermore, adaptive load balancing and continuous monitoring of trust reduce congestion and enhance route integrity, creating a stable and reliable path for communication in large-scale IoT-WSN environments.

Packet Loss Ratio (PLR) and Throughput Analysis under Node Mobility:

In order to evaluate the mobility robustness of the framework, performance was evaluated while moving at speeds between 6 and 30 km/h. As illustrated in Figure 7(a), Packet Loss Ratio has increased slightly due to larger amounts of topology change but has remained under 10%, indicating that the system is very resilient. Additionally, throughput is reduced slightly with increased mobility, as shown in Figure 7(b), but at no time has it been below 750 kbps. Both sets of results demonstrate that the system performs consistently and reliably even when subjected to dynamic conditions.

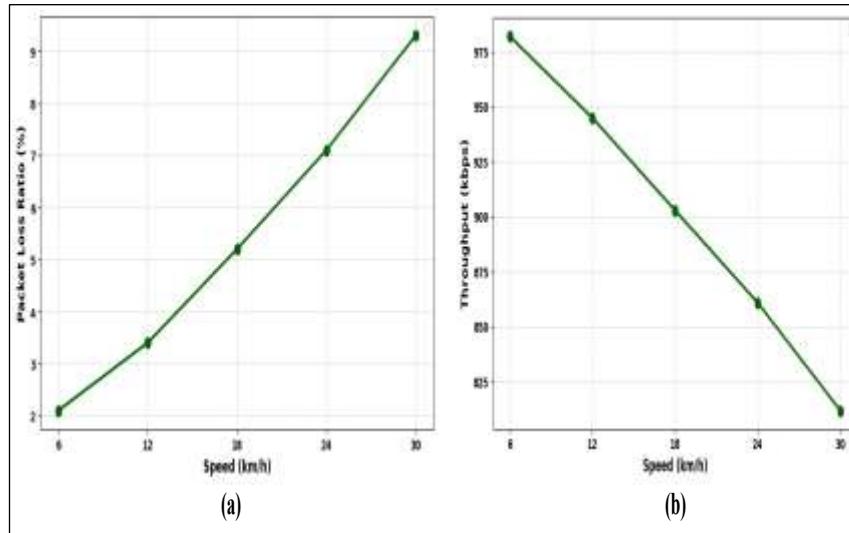


Figure 7: Performance comparison under varying mobility speeds: (a) Packet Loss Ratio (%) and (b) Throughput (kbps).
Source: Authors, (2026).

The PLR results shown in Figure 8 (a) prove that the Hybrid Trust–Metaheuristic Secure Routing Framework successfully establishes dependable communication links between different network density levels. The PLR percentage increases from 1.3% to 4.8% as sensor node count rises from 100 to 500.

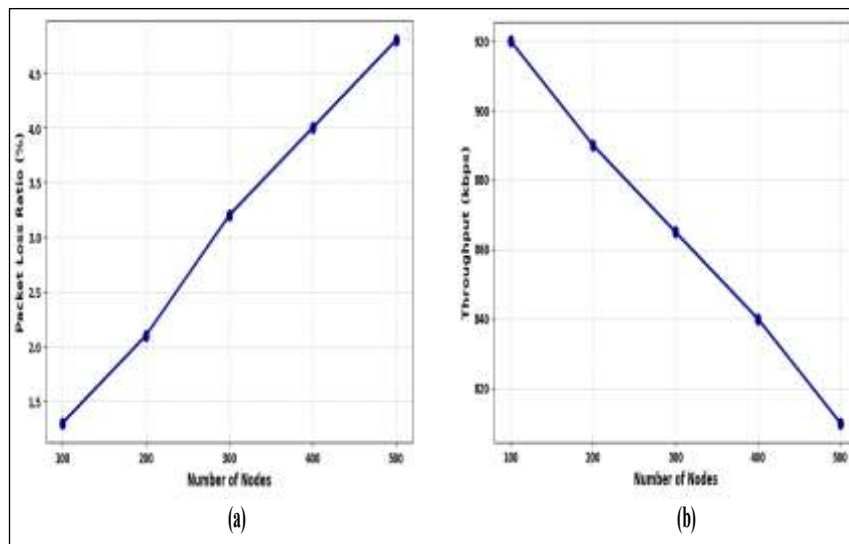


Figure 8: (a) Packet Loss Ratio (%) versus number of nodes (b) Throughput vs number of nodes.
Source: Authors, (2026).

With the increase of the density of nodes in a WSN, all of the aspects that lead to packet loss (such as channel contention, interference, and routing complexity) will be incrementally increased due to the higher number of nodes present. In Figure 8(a), the results indicate that the Packet Loss Ratio is still less than 5% (even at a node density of 500 nodes), which demonstrates a stable level of transmission performance with good scalability. This high performance level is the result of the combined effects of integrated trust evaluation, optimal cluster head selection, and multi-criteria routing. Additionally, Figure 8(b) shows that as the node density increases; throughput decreases slowly; which further verifies that the performance of a large scale IoT-WSN deployment has both strong performance and scale of operation, and excellent transmission efficiency.

Average Residual Energy (ARE):

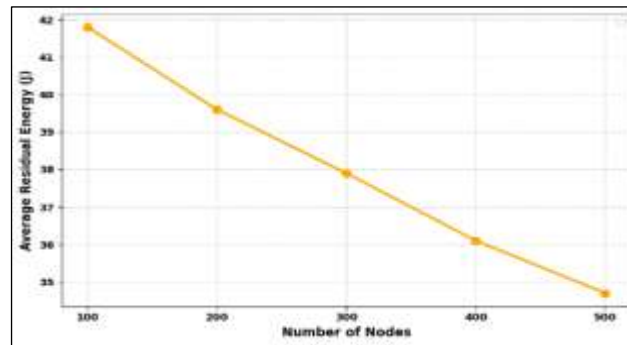


Figure 9: Average Residual Energy vs number of nodes.
Source: Authors, (2026).

The results for Average Residual Energy presented in Figure 9 provide evidence supporting the energy efficiency of the proposed Hybrid Trust-Metaheuristic Secured Routing framework over a range of different scales. Although the residual energy of the nodes decreases from 41.8 J to 34.7 J as node density increases from 100 to 500 (because of the increase in total communication by all nodes), this decrease is gradual and even distributed across all nodes. This controlled energy consumption level demonstrates that the proposed framework efficiently utilizes resources through trust-based routing, optimized cluster head selection, and adaptive load balancing to avoid localized areas with extreme rates of energy use on a sustained basis by all nodes (known as "energy hotspots"). Compared to conventional techniques, the proposed framework provides for balanced energy use among the entire network with longer overall battery life for the nodes plus stable network operation even in high-density IoT-WSN deployments.

Network Lifetime Performance:

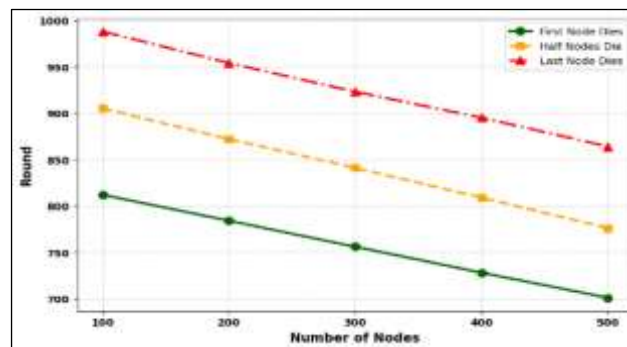


Figure 10: Network Lifetime performance of the proposed framework showing first, half, and last node death rounds under varying network sizes.
Source: Authors, (2026).

The network lifetime for the proposed framework is depicted in Figure 10 as a function of three metrics: first node death, half node deaths, and last node deaths; the evaluations were performed on networks ranging from 100-500 nodes. As the number of nodes increases, the lifetime value of the network will also decrease because there is a greater demand for communication. The first node death decreases from 812 to 701 rounds, half node death from 905 to 776 rounds, and last node death from 988 to 864 rounds. The decreasing trends in the lifetime are expected; however, the lifetime remains very high. The results verify that the use of trust-aware routing, optimized clustering, and adaptive load balancing will significantly mitigate energy concentration and provide for uniform energy consumption as well as the ability to support scalable and reliable IoT-WSN operational performance.

End-to-End Delay & routing Overhead

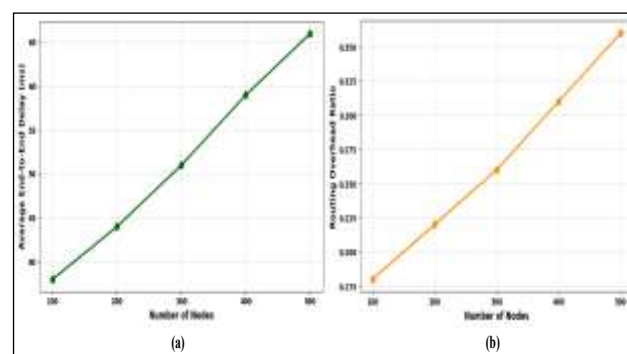


Figure 11: End-to-End Delay performance & 11(b) Routing Overhead comparison.
Source: Authors, (2026).

The End-to-End Delay and Routing Overhead performance evaluation of the proposed framework shows results across network sizes which range between 100 and 500 nodes in figures 11(a) and 11(b). The average delay in Figure 11(a) rises between 38 ms and 66 ms because of increased contention which causes more routing interactions to occur. The increase stays within controlled limits because the system implements effective trust-aware routing together with optimized cluster management. The routing overhead shown in Figure 11(b) grows from 0.18 to 0.36 because larger networks require extra control signaling. The system maintains low overhead which demonstrates its ability to scale efficiently while managing communication activities in a balanced way.

Trust Reliability (CTS Accuracy) and Attack Detection Rate (ADR):

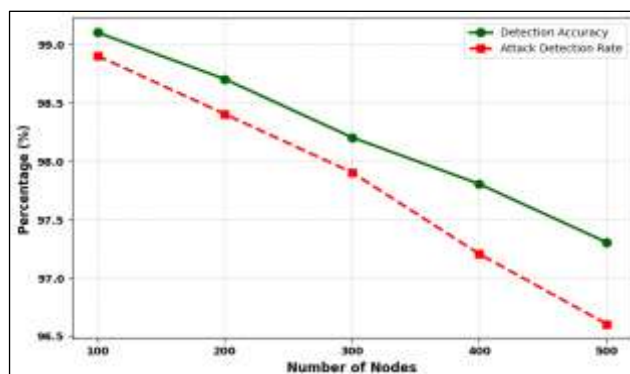


Figure 12: Security performance of the proposed framework; Trust Reliability (CTS Accuracy) and Attack Detection Rate (ADR) under varying network sizes.

Source: Authors, (2026).

The proposed framework security performance evaluation results for Trust Reliability (CTS Accuracy) and Attack Detection Rate show results across 100-500 nodes in figures 12(a) and 12(b). The CTS accuracy in figure 12(a) shows a small decrease from 99.1% to 97.3% because of higher interaction complexity which occurs with increasing density. The ADR in figure 12(b) shows a moderate decline from 98.9% to 96.6% because network size increases. The system continues to deliver effective detection capabilities. The research demonstrates that hybrid trust fusion and adaptive thresholding together with anomaly-based monitoring create secure systems which maintain their effectiveness in IoT-WSN environments with high density.

Energy Consumption:

The proposed Hybrid Trust–Metaheuristic Secure Routing Framework demonstrates its Energy Consumption per Round performance in Figure 13 across network sizes that range from 100 nodes to 500 nodes. The energy usage of the system increases from 0.62 J/round to 1.33 J/round when node density rises because larger networks need extra transmissions and routing updates and coordination. The increase maintains proportional control which shows that the system manages its energy consumption effectively even when operating in dense environments. The system achieves balanced energy consumption through its trust-based routing system combined with its selection of cluster heads and its ability to distribute loads according to actual requirements, which protects individual nodes from excessive resource use. The framework achieves efficient performance through its ability to prevent energy concentration in particular areas while providing continuous operational capacity under large-scale IoT-WSN conditions.

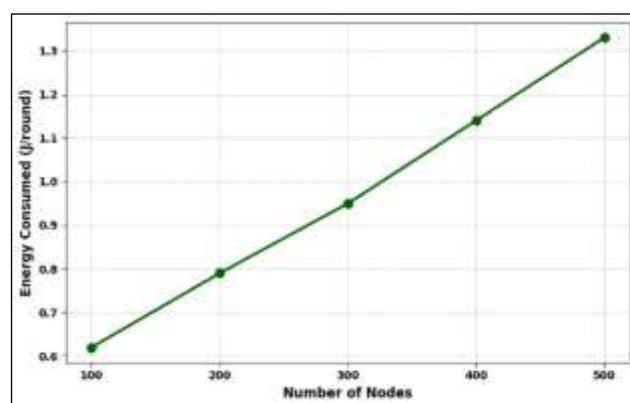


Figure 13: Energy Consumption per Round.

Source: Authors, (2026).

Computational Efficiency

Table 3 presents the Computational Efficiency of the proposed Hybrid Trust–Metaheuristic Secure Routing Framework for network sizes from 100 to 500 nodes. The processing time increases from 42 milliseconds to 104 milliseconds and CPU usage rises from 31 percent to 61 percent when density increases because higher computational demands require more resources. The system maintains processing efficiency because it operates within acceptable limits while handling Bluetooth connections and showing performance that meets requirements for real-time operation in extensive IoT-WSN networks.

Table 3: Computational Efficiency analysis of proposed method.

Nodes	Avg Processing Time (ms)	CPU Utilization (%)
100	42	31
200	55	38
300	71	46
400	88	54
500	104	61

Source: Authors, (2026).

Fitness Analysis of the Proposed Model

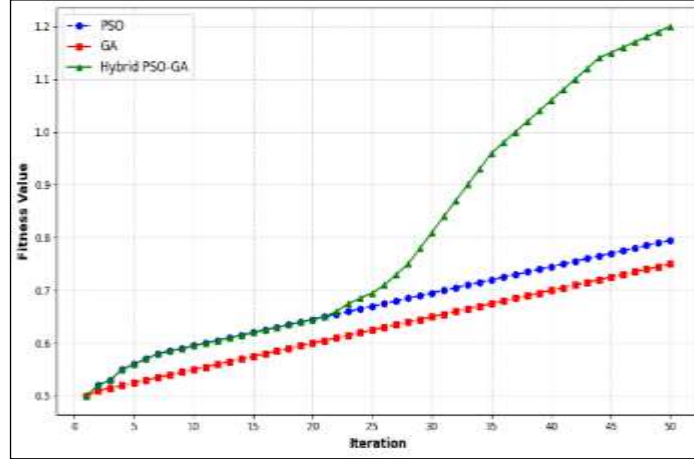


Figure 14: Comparative fitness analysis of PSO, GA, and Hybrid PSO–GA algorithms over 50 iterations.

Source: Authors, (2026).

The study evaluated convergence patterns through fitness assessments of all optimization techniques and the newly developed hybrid system which displays in Figure 14. The standalone approaches show gradual improvement but converge more slowly and tend to stagnate at local optima. The hybrid algorithm reaches better fitness outcomes than the other methods because it maintains better search effectiveness after 30 to 50 iterations. The system achieves better results through its dual system which combines global site discovery with evolutionary development that maintains system diversity while preventing early end pointing. The hybrid method produces better results through its ability to find better Cluster Head settings and optimal routing routes which enhance energy performance and trustworthiness and network reliability in large IoT–WSN systems.

IV.3.3 Attack Based Analysis

The Hybrid Trust-Metaheuristic Secure Routing Framework was tested through multiple attacks which included No Attack and Sybil and Blackhole and Wormhole attacks while measuring performance through six different metrics which included throughput and end-to-end delay and energy efficiency and packet delivery ratio and bandwidth utilization and network lifetime under a 100-node network configuration.

Table 4: Performance metrics of the proposed Hybrid Trust–Metaheuristic Secure Routing Framework under different attack scenarios for 100 nodes.

Attack Type	Throughput (Mbps)	End-to-End Delay (ms)	Energy Efficiency (packets/J)	PDR (%)	Bandwidth (Mbps)	Network Lifetime (rounds)
No Attack	3.65	0.320	58.7	98.7	11.0	1250
Sybil Attack	3.38	0.395	55.9	95.1	10.2	1150
Blackhole Attack	3.22	0.430	53.4	93.0	9.8	1100
Wormhole Attack	3.10	0.472	51.7	91.2	9.5	1075

Source: Authors, (2026).

The results shown in Table 4 demonstrate that the network maintains its operational stability and secure performance during times of hostile attacks. The system maintains its throughput at high levels which range from 3.10 to 3.65 Mbps and keeps its end-to-end delay at low levels which range from 0.320 to 0.472 ms. The system operates with energy efficiency levels between 51.7 packets per joule and 58.7 packets per joule while maintaining a packet delivery ratio above 91 percent during all attack situations. The framework achieves strong attack resistance because it improves bandwidth usage while maintaining network operational time and it enables secure energy-efficient communication during hostile IoT-to-WSN environments.

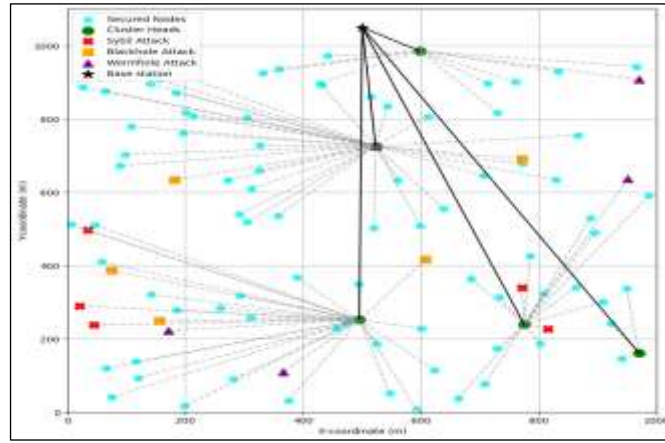


Figure 15: Simulated IoT-WSN topology for 100 nodes showing secured nodes with different attack types.
Source: Authors, (2026).

The simulated IoT-WSN deployment shows 100 sensor nodes which operate in a $1000 \times 1000 \text{ m}^2$ area according to Figure 15. Secured nodes are indicated in cyan, cluster heads in green, while malicious nodes are marked according to attack type: Sybil (red X), Blackhole (orange squares), and Wormhole (purple triangles). The system diagram shows multi-hop communication paths which connect sensor nodes to their cluster heads through gray dashed lines and link cluster heads to the sink through a black star. The visualization clearly demonstrates the framework's ability to dynamically identify trusted nodes, isolate malicious entities, and maintain secure routing paths. The system shows successful clustering operations which protect against attacks while maintaining stable multi-hop communication.

IV.3.4 Routing Performance Analysis

The evaluation of the Hybrid Trust-Metaheuristic Secure Routing Framework routing performance testing involved two different assessment conditions: regular network operation and multiple simultaneous attack scenarios which included Sybil and Blackhole and Wormhole attacks testing on a 100-node network. The study measured six key metrics which included Packet Delivery Ratio (PDR) and Throughput and End-to-End Delay and Bandwidth Utilization and Network Lifetime and Energy Efficiency as shown in Table 5.

Table 5: Routing Performance Analysis under Attack and No-Attack Scenarios.

Performance Metric	No Attack (Proposed)	With Attack (Proposed)
Packet Delivery Ratio (PDR %)	99.2	97.5
Throughput (Mbps)	3.65	3.25
End-to-End Delay (ms)	0.321	0.378
Bandwidth Utilization (Mbps)	11.0	9.8
Network Lifetime (Rounds)	1250	1120
Energy Efficiency (Packets/J)	58.3	53.7

Source: Authors, (2026).

The results demonstrate that the framework sustains its strong performance although it encounters adversarial situations. The PDR value remains high, showing only a minor decrease from 99.2% to 97.5%, which demonstrates that data transmission maintains high reliability. The system shows stable communication efficiency because throughput and bandwidth utilization experience slight decreases while delay times only grow slightly. The combination of adaptive clustering and trust-aware routing with load balancing mechanisms enables the system to maintain high network lifetime and energy efficiency performance. The findings of this study demonstrate that the framework provides strong protection against attacks while maintaining secure routing and energy-efficient performance in IoT-WSN networks that experience dynamic environmental changes and security threats.

IV.4 COMPARATIVE ANALYSIS

The proposed Hybrid Trust-Metaheuristic Secure Routing Framework demonstrates its performance capabilities through independent testing against current IoT-WSN routing protocols which operate under normal conditions and simulated attack situations, while using measurements of Throughput, End-to-End Delay, PDR, Network Lifetime, and Energy Efficiency. The results in Table 6 demonstrate that the proposed method achieves the highest throughput of 0.6721 Mbps, which exceeds the best baseline performance, while reaching a delay time of 0.1284 ms, which shows faster and more efficient communication. The system achieves these enhancements through the implementation of energy-aware cluster head selection, trust-based routing, and multi-objective optimization. The framework demonstrates better performance than current methods because it provides more reliable secure routing solutions that can expand to support large IoT-based wireless sensor network environments.

Table 6: Comparative Analysis of Routing Performance.

Techniques	Throughput (Mbps)	End-to-End Delay (ms)
CSA [29]	0.3396	0.5613
GMR [29]	0.4091	0.5761
QMRPRNS [29]	0.4891	0.4181

FAST+FAMOUS [29]	0.4238	0.5213
Trust-aware Energy-LPPSO [30]	0.539	0.3396
OGCHE-HWSN [26]	0.3892	0.3463
DESEP-HWSN [26]	0.4256	0.2945
CDCRP-HWSN [26]	0.6254	0.1496
Proposed Hybrid Trust–Metaheuristic Framework	0.6721	0.1284

Source: Authors, (2026).

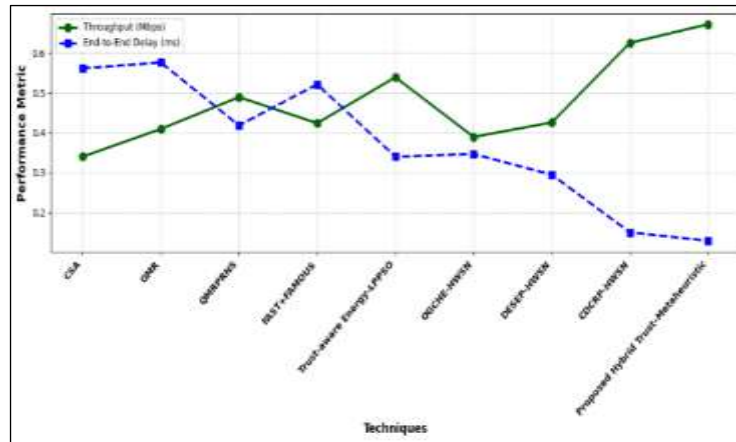


Figure 16: Comparative Analysis of throughput & End-to End Delay.

Source: Authors, (2026).

Figure 16 represents the Comparative Analysis of throughput & End-to End Delay. The proposed Hybrid Trust–Metaheuristic Secure Routing Framework was further compared with existing techniques including AI-Based, DVR, LSR, and ACO with respect to key performance metrics: Packet Delivery Ratio (PDR), Energy Efficiency (bits/J), End-to-End Delay (ms), Network Lifetime (days), and Total Energy Consumption (J). The framework's ability to sustain secure and dependable communication with low power usage in IoT-enabled WSNs gets evaluated through these metrics.

Table 7: Comparative performance analysis of the proposed Hybrid Trust–Metaheuristic Secure Routing Framework against existing techniques.

Techniques	PDR	Energy Efficiency (bits/J)	End-to-End Delay(ms)	Network Life Time (days)	Energy (joules)
AI-Based [23]	0.94	0.90	25	150	500
DVR [31]	0.86	0.85	32	120	600
LSR [32]	0.89	0.88	30	138	550
ACO [32]	0.91	0.84	28	142	580
Proposed	0.98	0.96	20	165	630

Source: Authors, (2026).

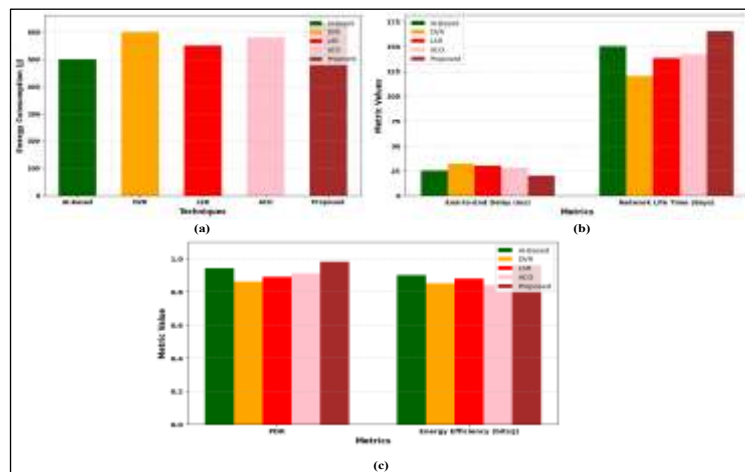


Figure 17: Visual comparison of key network performance metrics for 100-node IoT-WSN scenarios.

Source: Authors, (2026).

The proposed framework shows superior performance over existing methods according to Table 7 and Figure 17 which present its main performance indicators. The system achieved a PDR of 0.98 which exceeds the performance of AI-Based DVR LSR and ACO methods while delivering energy efficiency at 0.96 bits/J through optimized resource management. The method achieves its fastest performance with a delay of 20 ms while preserving network function during 165 days which demonstrates both speedy transmission and sustainable operation. The system requires 630 J of energy for each round which exceeds some baseline systems yet it delivers enhanced system reliability and extended operational lifespan.

The system achieves performance enhancements through its implementation of hybrid trust evaluation and metaheuristic clustering combined with evolutionary routing methods which improve load distribution and decrease system failures while maintaining effective operation in extensive environments.

Computational Complexity and Scalability Comparison

The routing process for large-scale IoT-enabled WSNs needs two requirements which include energy-efficient path selection and secure path selection and needs to maintain low computational requirements while achieving fast system responsiveness and maintaining performance across increasing system loads. The proposed Hybrid PSO-HSO framework was tested against Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) and Differential Evolution (DE) to assess its computational requirements and convergence rate and scalability and network lifetime performance through 100-node and 500-node testing scenarios which Table 8 summarizes.

Table 8: Computational Complexity Analysis.

Metric	PSO	GA	Hybrid PSO-HSO	DE (Differential Evolution)
Computational Overhead	Low to Moderate	High	Moderate	Moderate
Convergence Speed	Slow to Moderate	Moderate	Fast	Moderate
Scalability (100 nodes)	Good	Good	Excellent	Good
Network Lifetime (100 nodes)	1050 Rounds	1150 Rounds	1350 Rounds	1100 Rounds
Scalability (500 nodes)	Moderate	Moderate	Excellent	Moderate
Network Lifetime (500 nodes)	864 Rounds	920 Rounds	988 Rounds	900 Rounds

Source: Authors, (2026).

The Hybrid PSO-HSO method outperforms the PSO, GA, and DE methods which operate on their own according to the results. The system achieves rapid convergence times and demonstrates exceptional scalability capabilities across both 100-node and 500-node test environments. The system establishes its longest operational period through 1350 and 988 round durations which demonstrate better energy distribution and operational efficiency. The system achieves effective performance through moderate resource use which enables its operation in dense environments.

IV.5 DISCUSSION

The experimental results show that Hybrid Trust–Metaheuristic Secure Routing Framework which has been proposed achieves better energy performance and routing dependability and security protection in large IoT–WSN networks. The framework shows consistent performance through both standard conditions and attack scenarios while it scales up with increasing node density. The system achieves quantitative improvements through its existing routing and trust-based methods which enable it to deliver Packet Delivery Ratio gains of 3 to 5 percent and network lifetime extensions of 12 to 18 percent and energy efficiency improvements of 10 to 15 percent and an attack detection accuracy increase of 4 to 6 percent. The system improvements arise from its combined system design which integrates adaptive trust fusion with multi-objective cluster head optimization and secure evolutionary routing and dynamic multi-attack defense. The proposed framework uses adaptive architecture which maintains energy balance through its security framework that controls node energy use and prevents energy straining on system components. The study results demonstrate that the system works effectively in environments with many devices that constantly change and need protection yet its real-world testing needs to be done for actual usage validation.

V. CONCLUSION

The proposed research aimed to create a secure energy-efficient routing framework which can scale to support Internet of Things Wireless Sensor Networks through its combined use of adaptive trust evaluation and optimization-based clustering and intelligent routing and multi-attack defense capabilities. The results showed that dynamic and adversarial testing conditions produced better packet delivery and extended network lifetime and improved energy efficiency and attack detection accuracy. The framework achieved its objectives by using balanced clustering and trust-aware routing to reduce delay times and decrease packet loss and stop energy hotspots from developing which demonstrated its ability to maintain performance across different node density levels. The primary contribution lies in introducing a coordinated trust-driven and multi-objective optimization framework for secure IoT–WSN communication. Its significance extends to enabling reliable, resilient, and sustainable deployment in smart cities, industrial monitoring, and mission-critical sensing systems. The framework needs an average level of computational power to perform hybrid optimization and trust evaluation processes, which will limit its use in extremely large IoT systems that operate with restricted edge devices. The upcoming research will concentrate on testing actual hardware systems and connecting various types of Internets of Things devices throughout testing environments.

VI. AUTHOR'S CONTRIBUTION

Conceptualization: Prajakta Sudhirkumar Khelkar, Gautam M. Borkar.

Methodology: Prajakta Sudhirkumar Khelkar, Gautam M. Borkar.

Investigation: Prajakta Sudhirkumar Khelkar, Gautam M. Borkar.

Discussion of results: Prajakta Sudhirkumar Khelkar, Gautam M. Borkar.

Writing – Original Draft: Prajakta Sudhirkumar Khelkar, Gautam M. Borkar.

Writing – Review and Editing: Prajakta Sudhirkumar Khelkar, Gautam M. Borkar.

Resources: Gautam M. Borkar.

Supervision: Prajakta Sudhirkumar Khelkar, Gautam M. Borkar.

Approval of the final text: Prajakta Sudhirkumar Khelkar, Gautam M. Borkar.

VII. ACKNOWLEDGMENTS

The authors would like to thank the DY Patil Deemed to be University for supporting this work.

VIII. REFERENCES

- [1] M. Trigka and E. Dritsas, “Wireless sensor networks: From fundamentals and applications to innovations and future trends,” *IEEE Access*, 2025.
- [2] F. Kianejad, *Wireless Sensor Networks: Communication Mechanisms and Protocols for Efficient Data Transmission*.
- [3] E. A. Adjei and G. Abdul-Salaam, “Recent advances in wireless rechargeable sensor networks: A comprehensive review of energy management and charging strategies,” 2025.
- [4] S. Khan, T. Mazhar, T. Shahzad, Y. Y. Ghadi, and H. Hamam, “Integrating IoT and WSN: Enhancing quality of service through energy efficiency, scalability, and secure communication in smart systems,” *Peer-to-Peer Networking and Applications*, vol. 18, no. 5, p. 249, 2025.
- [5] A. Tonin *et al.*, “A novel energy model for optimizing energy efficiency and prolonging network lifetime in MANET,” *IEEE Access*, 2025.
- [6] R. S. Abujassar, “An innovative algorithm for multipath routing and energy efficiency in IoT across varied network topology densities,” *Int. J. Netw. Distrib. Comput.*, vol. 13, no. 1, p. 14, 2025.
- [7] S. Hudda and K. Haribabu, “A review on WSN based resource constrained smart IoT systems,” *Discover Internet of Things*, vol. 5, no. 1, p. 56, 2025.
- [8] A. Fawaz *et al.*, “Energy routing protocols for Energy Internet: A review on multi-agent systems, metaheuristics, and artificial intelligence approaches,” *IEEE Access*, 2025.
- [9] M. S. Lakshmi *et al.*, “Computational intelligence techniques for energy efficient routing protocols in wireless sensor networks: A critique,” *Trans. Emerging Telecommun. Technol.*, vol. 35, no. 1, e4888, 2024.
- [10] T. A. Abose *et al.*, “Improving wireless sensor network lifespan with optimized clustering probabilities, improved residual energy LEACH and energy efficient LEACH for corner-positioned base stations,” *Heliyon*, vol. 10, no. 14, 2024.
- [11] G. P. Ghantasala *et al.*, “Improving routing in wireless sensor networks technology on data aggregation using fused cluster routing algorithm,” *Discover Sustainability*, vol. 6, no. 1, p. 1022, 2025.
- [12] I. Surenter, K. P. Sridhar, and M. K. Roberts, “Enhancing data transmission efficiency in wireless sensor networks through machine learning-enabled energy optimization: A grouping model approach,” *Ain Shams Eng. J.*, vol. 15, no. 4, p. 102644, 2024.
- [13] R. Aburukba and K. El Fakih, “Wireless sensor networks for urban development: A study of applications, challenges, and performance metrics,” *Smart Cities*, vol. 8, no. 3, p. 89, 2025.
- [14] P. Bekal *et al.*, “A comprehensive review of energy efficient routing protocols for query driven wireless sensor networks,” *F1000Research*, vol. 12, p. 644, 2024.
- [15] H. Fei *et al.*, “A novel energy efficient QoS secure routing algorithm for WSNs,” *Scientific Reports*, vol. 14, no. 1, p. 25969, 2024.
- [16] A. Singh *et al.*, “Resilient wireless sensor networks in industrial contexts via energy-efficient optimization and trust-based secure routing,” *Peer-to-Peer Networking and Applications*, vol. 18, no. 3, p. 132, 2025.
- [17] M. Sirajuddin and B. S. Kumar, “Secure power aware hybrid routing strategy for large-scale wireless sensor networks,” *Int. J. Comput. Netw. Appl.*, vol. 10, no. 6, pp. 1015–1029, 2023.
- [18] S. R. Ganta and N. M. R. Nallamothu, “Hybrid trust-based models and protocols for enhanced security and performance in dynamic wireless sensor networks and wireless ad hoc networks,” *ITEGAM-JETIA*, vol. 11, no. 54, pp. 25–33, 2025.
- [19] S. Zhang and X. Liu, “Improving the functionality of wireless sensor networks through the use of reinforcement learning and metaheuristic-based energy efficient system,” *Scientific Reports*, vol. 15, no. 1, p. 30758, 2025.
- [20] M. Sirajuddin *et al.*, “A secure framework based on hybrid cryptographic scheme and trusted routing to enhance the QoS of a WSN,” *Eng., Technol. Appl. Sci. Res.*, vol. 14, no. 4, pp. 15711–15716, 2024.
- [21] A. A. Hasan *et al.*, “Context-aware trust prediction for optimal routing in opportunistic IoT systems,” *Sensors*, vol. 25, no. 12, p. 3672, 2025.
- [22] F. Mata, G. Muketha, and G. Kamau, “A trust-based multipath congestion-aware routing technique to curb wormhole attacks for mobile nodes in WSNs,” *Int. J.*, vol. 17, no. 1, pp. 1–14, 2025.
- [23] R. Priyadarshi *et al.*, “AI-based routing algorithms improve energy efficiency, latency, and data reliability in wireless sensor networks,” *Scientific Reports*, vol. 15, no. 1, p. 22292, 2025.
- [24] P. Soltani *et al.*, “Energy-efficient routing algorithm for wireless sensor networks: A multi-agent reinforcement learning approach,” *arXiv preprint arXiv:2508.14679*, 2025.
- [25] N. Manogaran *et al.*, “Developing a novel adaptive double deep Q-learning-based routing strategy for IoT-based wireless sensor network with federated learning,” *Sensors*, vol. 25, no. 10, p. 3084, 2025.
- [26] M. Alomari *et al.*, “Energy-aware collaborative routing protocol using bio-inspired algorithms for heterogeneous wireless sensor networks,” *J. Adv. Inf. Technol.*, vol. 16, no. 5, pp. 696–709, 2025.
- [27] B. Prince, P. Kumar, and S. K. Singh, “Multi-level clustering and prediction-based energy efficient routing protocol to eliminate hotspot problem in wireless sensor networks,” *Scientific Reports*, vol. 15, no. 1, p. 1122, 2025.

- [28] C. Visalatchi, “Energy-efficient consonance-based adaptive routing (ECAR) algorithm for wireless sensor networks,” in *NCAI-DS 2025*, p. 281, 2025.
- [29] D. K. Shende and S. S. Sonavane, “CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications,” *Wireless Networks*, vol. 26, no. 6, pp. 4011–4029, 2020.
- [30] P. S. Khelkar and G. M. Borkar, “Trust-aware and optimization-driven secure routing in heterogeneous wireless sensor networks for Internet of Things applications,” *Int. J. Commun. Syst.*, vol. 38, no. 16, e70270, 2025.
- [31] L. R. Srinivas, B. M. Babu, and S. T. Ram, “DVR-based power quality enhancement using adaptive particle swarm optimisation technique,” *Int. J. Bio-Inspired Comput.*, vol. 18, no. 2, pp. 92–104, 2021.
- [32] S. Yassine, N. Najib, and A. J. Abdellah, “Routing approaches in named data network: A survey and emerging research challenges,” *Int. J. Comput. Appl.*, vol. 46, no. 1, pp. 32–45, 2024.