MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4919-4927

A HYBRID TRUST-STABILIZED META-HEURISTIC ROUTING FRAMEWORK USING MFO–JFS FOR SECURE AND ENERGY-EFFICIENT IOT–WSNs

Aswin Vignesh Ramesh
Research Scholar, Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India.
achuaswinvigneshr@gmail.com
Dr. E. J. Thomson Fredrik
Professor, Department of Information Technology,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India.
thomson.ej@kahedu.edu.in

ABSTRACT

Wireless Sensor Networks (WSNs) are the core building block of the modern Internet-of-Things (IoT) applications, which require routing protocols that are both energy-efficient and security-aware, in addition to being resilient in response to the dynamism of the network environment. Trust-based protocols are often not stable to attack by malicious entities or quickly evolving topologies. The current paper presents an Optimized Hybrid Trust Stabilized Routing (TSR) Framework that combines both Moth-Flame Optimization (MFO) and Jelly-Fish Search (JFS) algorithms to find the best multi-hop routes without compromising the integrity of trust in the network. The proposed MFO-JFS framework utilizes the high global exploration attributes of MFO to avoid local optima, and JFS offers adaptive local exploitation so that route selection is improved by real-time Sensor Node (SN) behavior. SNs are repeatedly tested in terms of forwarding reliability, residual energy, aberrant patterns, and inter-SN reliability, which allow dynamically recalibrating a trust score and preventing the malicious impact. The framework can be used to attain robust routing with low energy consumption, low computational/processing, as well as high resilience to SN failures and adversarial behavior through global and local meta-heuristic strategies. The framework is proven to be efficient over dense and heterogeneous scenarios of the IoTs, specifically: IoT-WSN. The performance measurement uses four key measures: Security Ratio, Energy-Consumption Ratio, Computation Time, and a new measurement, Trust-based Connectivity rate, which measures the rate of SNs that can withstand reliable and trustworthy paths over the network topology. The findings reveal that the hybrid MFO-JFS system is far better than the traditional trust-based routing schemes since it provides a scalable, secure, and energy-aware solution to the next-generation IoT-enabled WSN applications.

Keywords: *Wireless Sensor Networks, Internet-of-Things, Energy-Efficient, Trust-Stabilized Routing, Moth–Flame Optimization, Jellyfish Search*

1. INTRODUCTION

The fast growth of the IoT has significantly changed the implementation of distributed sensing systems in various spheres of application, such as environmental monitoring, industrial automation, healthcare systems, and smart cities [1]. At the heart of this paradigm lies the WSN, which is a network of spatially distributed low-powered SNs that jointly monitor physical or environmental changes and communicate the information to the Sink Node (SiN) or Base Station (BS). Though IoT-enabled WSNs offer unprecedented possibilities of processing real-time data and automating it, they pose significant challenges, in particular, concerning secure and energy-efficient routing, resource limitations, changing network properties, and susceptibility to malicious activity [2]. WSNs are collective SNs that have limited computational resources, energy sources, and communication services. Such constraints make the traditional routing algorithms that are developed in the context of high-powered networks inappropriate in the settings of the WSN, which subsequently require the development of specialized routing methods that can be both energy-saving and security-aware [3]. In addition, the spread of IoT applications exponentially raises the network traffic and overheads of communication, which further complicates even more the maintenance of a reliable and secure communication path. Wireless channels are inherently broadcast as well, which implies that SNs are prone to a host of security risks such as eavesdropping, spoofing, Denial-of-Service (DoS) attacks, and the existence of rogue or compromised SNs, which intentionally modify or drop data packets [4].

To handle both of these issues, trust-based routing protocols have received a lot of attention. To measure the reliability and conduct of SNs, trust metrics are used, which allow the network to make preferential choices on data routing through trustworthy SNs and avoid malicious SNs. Determining trust is generally considered to use factors including packet forwarding history, residual energy status, interaction history, and neighbor recommendations, and so they keep on varying the trust scores. Although trust-based approaches can enhance routing security, they have to strike a balance between computational overheads, energy usage, and routing performance, which is still the subject of research [5]. At the same time, meta-heuristic optimization methods have proven to be effective in addressing complex optimization issues in WSN routing and especially when multiple optimization objectives (e.g., energy efficiency, security, and latency) have to be fulfilled simultaneously. Meta-heuristic methods leverage the principles of natural phenomena, swarm behavior, evolutionary biology, and physics-based motion techniques to search large spaces of solutions quickly [6]. These methods are well adapted to optimization of routing decisions in the IoT-WSN setting, where deterministic approaches frequently do not immerse because of the dynamism and uncertainty of the network environment.

Recently, meta-heuristics, such as the MFO and the JFS, have been identified to have complementary advantages; MFO demonstrates strong global exploration through the behavior of moth navigation, and JFS Search provides a strong local exploitation by the behavior of marine organisms [7]. The combination of such algorithms has produced better optimization abilities than individual heuristics, especially when there is a complicated optimization task on a network. However, the combination of trust assessment and hybrid meta-heuristic optimization in IoT-WSNs has not been fully investigated yet, and it has the potential to improve both security and energy efficiency [8]. The latest developments in the field of trust-based and meta-heuristic routing consist of blockchain-enhanced trust systems that enhance the authenticity of routing and decentralized security and minimize the usage of centralized trust authorities [9]. Moreover, new studies examine the multi-level trust models and adaptive attacker detection models to enhance routing security in more complex WSN settings [10]. These advancements indicate that an integration of trust evaluation and intelligent route optimization through hybrid meta-heuristics like MFO and JFS would result in high-quality results in secure IoT-WSN routing. To conclude, trust modeling-meta-heuristic optimization-secure energy-aware routing are essential areas of research in the design of IoT-WSN. Handling the dynamic nature of SNs as well as malicious threats through a single routing system can significantly improve network resiliency, lifespan, and Quality of Service (QoS).

Problem Statement: The issue of secure and energy-saving routing in IoT-based WSNs is still a problematic issue due to the nature of resource limitations of SNs, dynamic network behaviors, and malicious attacks. Current trust-based approaches address security problems, but in many cases, they are characterized by excessive computational complexity, a lack of support for multi-objective optimization, and a lack of adaptability to network topology changes. There is a need to have a unified routing architecture that effectively integrates the concept of trust assessment with adaptive optimization to improve the stability of routes, reducing energy use, and offering resilience to malicious or erroneous SNs in real-time IoT-WSN settings.

Paper Contribution: This paper proposes a new hybrid TSR topology of the IoT-WSNs that combines the MFO along with JFS algorithms to choose the intelligent multi-objective paths. The suggested MFO-JFS model keeps assessing SN credibility in terms of behavioral and performance indicators, which allows adapting the route recalibration to changing circumstances. This method can be used to enhance global

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4919-4927

exploration and local exploitation by using the complementary capabilities of both meta-heuristic algorithms, without compromising on energy efficiency or addressing malicious routing behavior. The framework shows considerable performance improvement in various measures of evaluation, such as Security Ratio, Energy-Consumption Ratio, Computation Time, and Trust-based Connectivity Rate. These works contribute to the state-of-the-art of secure and energy-aware IoT-WSN routing.

Paper Organization: The rest of the article is structured as follows. Section 2 is a review of the existing literature on TSR and hybrid optimization methods. Section 3 provides the methodologies of the proposed hybrid TSR framework. Section 4, performance evaluation results are given, and the findings are discussed. Lastly, Section 5 provides the conclusion of the paper and identifies possible future research directions.

2. RELATED WORKS

In [11], the authors suggest a Multi-Level TSR routing scheme that incorporates Blockchain technology to increase the QoS in the WSNs. The model assesses trust locally and globally by analyzing the SN transmission properties, frequency of retransmission, energy use, successful rate, and frequency of the signals, thus providing the ability to select secure routes. The strategy provides data transmission security by introducing an adaptive blockchain security algorithm and enhances malicious activity mitigation in dynamic IoT settings, hence, enhancing the routing reliability and energy-overhead. Simulation findings indicate lower overhead of energy consumption and an increase in secure routing performance at a broad SN population, which can provide a viable approach to blockchain-aided secure IoT-WSN communications.

In [12], the authors present the Levy Chaos Adaptive Snake Optimisation-Based Multi-Trust Routing Method (LCASO-MTRM), which is a heuristic and multi-objective trust routing algorithm that is tailored to the QoS-constrained WSN setting. This algorithm combines chaotic and adaptive operators in a heuristic model to increase the diversity of the populations and the exploration of the search-space as well as the strength of convergence. It also includes a link-trust mechanism to compute the trust levels more accurately with both direct and indirect trust calculations. The comparisons of simulations demonstrate considerable cuts in energy usage, latency, and packet loss, as well as enhanced bandwidth as compared to other heuristic schemes.

In [13], the authors introduce BS-SCRM, a Secure Clustering Routing Methodology, which combines swarm intelligence with blockchain technology for WSNs. Its methodology uses an improved version of the Whale Optimisation Algorithm (WOA) to select Cluster Head (CH) using SN energy with proximity measurements, and blockchain to perform a safe on-chain validation of data. It surpasses classical clustering methods by significantly improving energy efficiency and network lifetime through tampering attack reduction and improved quality of cluster-formation. The methodology shows significant improvements in the duration of the network and resilience during an attack.

In [14], the authors formulate a cohesive, secure routing and trust-management system that integrates reinforcement meta-learning with temporal trust evaluation using blockchain. The framework makes use of a Meta-Router to update rules dynamically, TGAT-Trust Chain to score trust dynamically with graph-attention, and a Generative Adversarial Network to identify malicious behaviour. It has very high packet-delivery ratios and low energy usage, false trust positives are greatly minimized, routing-convergence time is drastically reduced compared to traditional protocols, and it is shown to be effective in dynamically and adversarially operated IoT network scenarios.

In [15], the authors design safe and energy-efficient IoT-linked WSNs routing to support smart-city infrastructure. The method reduces unnecessary transmissions and allows energy-aware clustering by using Smart Contracts and a Distributed Ledger to enhance spectrum utilisation through cognitive-radio methods. The framework improves the security of a network with energy efficiency, minimizes communication expenses, and facilitates sustainable WSN systems in large-scale IoT deployments such as smart-city sensor deployments.

Research Gap: Although recent innovation has been made in the field of trust-based and secure routing in WSN and IoT settings, some gaps are still critical. Firstly, the main issue with the existing models is that most of them focus on either blockchain or trust metrics, and not fully combine dynamic trust management with adaptive routing optimisation. Second, most heuristic-based schemes do not focus on achieving security and routing stability together but on the individual goals (e.g., energy, latency). Third, blockchain-based mechanisms can bring substantial energy and computing burdens that are inadequately mitigated in sensor networks that have resource constraints. Finally, temporal and multi-objective trust-adaptation schemes that enable a dynamic adjustment of routing decisions to new attack conditions and network variations are not well developed, which highlights the necessity of hybrid, adaptive, and trust-stabilised optimisation models. The gaps indicate the need to conduct additional studies on the possibility of applying cohesive secure routing schemes to balance energy efficiency, trust accuracy, and stability in large-scale IoT-WSNs.

3. METHODOLOGIES

The paper presents a Hybrid TSR model combining the MFO algorithm with the JFS algorithm to find secure, energy-saving, and trust-sensitive forwarding paths in wireless multi-hop networks. The methodology is designed in such a way that: (i) it defines the operational network setting, (ii) it models the adversarial behaviors and trust differences, (iii) it stipulates the base routing strategies, (iv) it combines the hybrid MFO-JFS optimization procedure, and (v) it validates the routing choices through algorithmic and flow-based implementation. The next subsections describe modeling assumptions, formulation of the algorithm, and the computation of trust used in the proposed method.

3.1 Network Model :

It assumes a heterogeneous wireless multi-hop network "G (V, E)", where "V = {n_1, n_2, …, n_N}" is the set of SNs and 'E' is the set of communication links between SNs. The SNs have limited storage, processing, and energy capacity, and also act as a source of data and as an intermediate relay. There are omnidirectional links in SNs where the path loss depends on distance, and packets are delivered probabilistically. The multi-hop routing problem aims at finding an optimal route "P = {$n_s \rightarrow \ldots \rightarrow n_d$}" between a source SN "$n_s$" and a destination SN "$n_d$" with the aim of maximizing the stability of trust and minimizing the use of resources. Transmission energy has a standard radio dissipation model, mathematically expressed in Equation (1):

$$E_{tx}(k,d) = kE_{elec} + k \in_d d^{\alpha} \quad (1)$$

In which 'k' is the packet size, 'd' is the distance to the hop, "E_{elec}" is the energy of the electronic circuitry and "$\in_d$" is the amplifier coefficient with "$\alpha \in [2,4]$" being the path-loss exponent. The residual energy in each SN is updated as in Equation (2):

$$E_{res}(t+1) = E_{res}(t) - E_{tx} - E_{rx} \quad (2)$$

Where "$E_{rx} = kE_{elec}$". SNs are periodically transmitting control beacons with energy "E_{res}", forwarding potential and consistency of behaviour. Routing choices aim at a decentralised setting with no global topology information. Local inferences on link reliability and trust parameters are based on observation and joint assessment.

3.2 Threat & Trust Model :

It is assumed that the network is subject to adversarial behaviours such as selective forwarding, packet dropping, falsified trust updates, and energy-drain manipulation. Malicious SNs strive to reduce routing stability by either making them more appealing to route selection or by compromising forwarding after selection. Trust estimation is modeled as a composite function of "forwarding reliability (T_f)", "residual energy (T_e)", and "anomaly detection (T_a)". All the trust components are normalised within [0,1], and aggregated over weighted fusion as defined in Equation (3):

$$T(n_i) = w_f T_f(n_i) + w_e T_e(n_i) + w_a T_a(n_i) \quad (3)$$

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4919-4927

Where "$w_f + w_e + w_a$=1", and the weights are network preference. The exponentially decaying feedback is used to update forwarding trust on the basis of the successful packet forwarding ratio, and the anomaly trust is applied on the basis of deviations in the traffic or control report behaviour. Energy trust is associated with minimum energy limits to control unstable relays. Attackers are classified based on their type of strategic attack (selective dropping), opportunistic attack (burst misbehaviour), and energy subversion attack (selfish SNs do not forward to save energy). The local observation and neighbour consensus rescales trust scores to ensure that none of the singles dominate the trust propagation. Candidates that have a trust level less than a system-defined threshold are not members of optimisation routing pools.

3.3 Baseline Methods : To put into perspective the work of the suggested MFO-JFS framework, two recent baseline procedures are taken into account: (i) Logistic-Regression Trust (LRT) protocol, and (ii) Optimised Chimpanzee-based Secure Clustering (OCSC) approach. These baselines are two different trust-stabilisation methods, like statistical behavioural learning and meta-heuristic secure clustering, which offer some contrast in the way trust, security, and routing reliability are attained when dynamic adversarial environments are dealt with.

(a) LRT Protocol : The LRT protocol uses logistic regression to estimate the credibility of SNs according to behavioural characteristics in the form of direct encounters and global recommendations [16]. The trust assessment combines Direct Trust (DT), Experience Trust (ET), and Reputation Score (RS) into an Integrated Trust (IT) metric, which allows categorizing SNs as either reliable or malicious. Logistic regression modelling is as follows, according to Equation (4):

$$IT = \sigma(\beta_0 + \beta_1 DT + \beta_2 ET + \beta_3 RS) \quad (4)$$

In this case, the sigmoid activation, which limits the range of "IT ϵ [0,1]", is denoted by 'σ'. The classifier, after adequate behavioural training, identifies malicious SNs and assists in the filtering of such SNs in intra-network communications. LRT mainly works on identifying the black hole threat, such as forwarding attacks, as compromised SNs seek to interfere with communication streams. Its ability to make decisions is, however, restricted to intra-group entities, and the propagation of trust is consistent, which cannot withstand transient misbehaviour, collusion, or cross-boundary adversaries. Furthermore, the concept of energy-awareness is not present in LRT, and therefore, it cannot be deployed in a limited multi-hop wireless network that needs both security and resource stability.

(b) OCSC : The OCSC uses a swarm-based clustering mechanism that is based on chimpanzee foraging dynamics to create safe communication groups and select credible CHs [17]. Optimisation includes security constraints and resource descriptors like residual energy, connectivity, and trust score. The formulation of CH selection is created as an optimization objective and presented in Equation (5):

$$max_{CH} F = \alpha_1 T + \alpha_2 C + \alpha_3 E \quad (5)$$

In which 'T' is SN trust, 'C' is cluster connectivity, 'E' is the remaining energy, and "$\alpha_1 + \alpha_2 + \alpha_3 = 1$". The meta-heuristic balances the use of the resources and minimizes the exposure to the compromised SNs in the areas. Although clustering improves control and intrusion containment, OCSC does not specifically optimise multi-hop route discovery once CHs have been selected, nor does it adapt to SN trust variations in short-term time frames. Its computational cost reduces with the size of the population, and there are no hybrid exploration-exploitation strategies, so it is more vulnerable to local optima in optimization.

Baseline Summary: Both base approaches offer valuable insights into the concept of trust stabilisation, with LRT using statistical classification and OCSC relying on a meta-heuristic secure clustering technique. However, none of the baselines deal with joint needs in terms of energy stability, recalibration of trust, adversarial resilience, and optimisation of multi-hop routes. Their shortcomings are the motivation for a hybridized optimization-driven routing system that is able to handle both global search and local refinement under adversarial environments.

3.4 Proposed MFO–JFS Framework: A hybrid MFO-JFS framework proposed in the current work is aimed at stabilizing trust-based routing in dynamic IoT-WSN systems. The design goal is to achieve a balanced exploration of global paths, refining local trust, and forwarding with energy efficiency and reducing adversarial disruptions. MFO carries out coarse-grain global exploration to determine good candidates of routes along various paths, and JFS carries out fine-grain exploitation that continuously re-allocates SN weights based on environmental feedback and changes in trust states. The fusion mechanism ensures that the chosen paths are not only the most cost-efficient structurally (hop count, route delay, and energy consumption), but also, at the same time, maintain high trust consistency in the presence of malicious or compromised SNs. Figure 1 shows the proposed MFO-JFS framework in a conceptual way.

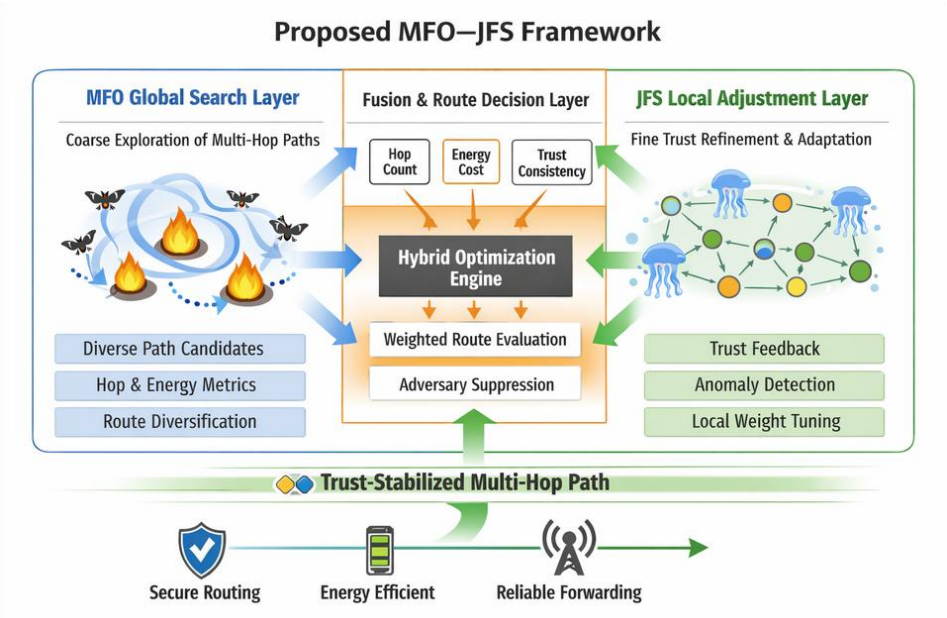

Figure 1: Proposed MFO-JFS Framework Architecture

3.4.1 MFO Global Search Layer

The MFO component carries out global exploration to uncover high-potential multi-hop routing paths throughout the network. Its mechanism has been organized into three stages:

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4919-4927

(i) Initialization: & Flame Encoding: The network is used to create several initial route paths in which the SNs are represented as moths and candidate forwarding chains as flames. The encodings of the hop structure, cumulative energy load, and preliminary trust attributes are carried in each flame. The initial positions are varied to prevent bias in the initial routing decisions and provide a higher coverage of searches globally.

(ii) Spiral Search & Diversification: In the process of exploration, moths orbit flames along a logarithmic spiral path to increase global diversification. The rule of update is mathematically defined as in Equation (6):

$$M_{t+1} = F_t + S.e^{bD}.\cos(2\pi D) \quad (6)$$

Here "M_{t+1}" is the new moth, "F_t" is the flame, 'S' is the orientation control, 'b' is the spiral tightness control, and "D = $\|F_t - M_t\|$". This diversified search avoids premature convergence and helps in avoiding the pitfalls of misguided trust, which are formed due to malicious SN behaviour.

(iii) Flame Reduction & Route Candidate Selection: With each iteration, the population of flames decreases until more selective pressure is attained, thus biasing the swarm to more competent routing chains. Optimal flames generate a set of candidate solution which is trusted and multi-hop. MFO is then a coarse global sampler that pushes structurally robust path candidates through to the refinement process.

3.4.2 JFS Local Adjustment Layer

JFS is the local exploitation unit that refines paths discovered in MFO along real-time SN behaviour and trust fluctuation. Its mechanism is made up of three steps:

(i) Environmental Feedback Sensing: JFS estimates the local environmental characteristics such as local trust variation, residual energy depleting rates, neighbour anomaly cues, and history of interaction. Such contextual sensing helps JFS to identify SN misbehaviour before it becomes problematic and adaptively reconfigures the forwarding chain based on environmental responses instead of using heuristic weights.

(ii) Mode Switching & Fine-Grain Adjustment: SNs switch between two modes of operation, Ocean Drift and Active Foraging, based on the intensity of feedback. The position update rule is as per Equation (7):

$$X_{t+1} = \begin{cases} X_t + \gamma.Current(X), & (drift) \\ X_t + \eta.Forage(X), & (foraging) \end{cases} \quad (7)$$

Where 'γ' and 'η' are adaptive coefficients. In drift mode, candidate chains are matched to candidate energy-trust currents, and in foraging mode, candidate exploitation is optimized about local optimum sequences.

(iii) Local Penalisation & Trust Refinement: The routes containing suspicious SNs are penalised either through local attenuation of trust or local path withdrawal. On the other hand, stable SNs are reinforced to participate and thus converge easily to trust-based forwarding behavior. This refinement mechanism is used to guarantee the finalised route is viable as well as threat-resilient without causing global recomputation of the entire network.

3.4.3 Fusion & Route Decision Layer

The last phase incorporates the complementary behaviours between MFO and JFS into a combined routing decision mechanism that can support the stability of trust, overcome the effect of adversarial behaviours, and ensure the forwarding efficiency across the IoT-WSN infrastructure. The fusion logic is aimed at balancing out global structural exploration and localised behaviour refinement.

(i) Multi-Criterion Cost Aggregation: The paths found in MFO are refined using a multi-criterion cost function, which takes structural hop continuity, cumulative residual energy distribution, and aggregated trust reliability into account. The path of the candidates denoted by "R_i" is represented by a tuple "R_i=<H_i, E_i, T_i>", whereby the former is the hop complexity, the latter is the expected energy burden, and the latter is the trust alignment calculated using JFS. This aggregation eliminates weak routes in MFO before exploitation and has the benefit of cutting computational cost.

(ii) Hybrid Scoring & Decision Surface Formulation: JFS-refined weights on trust get combined with structural MFO scores to create a hybrid decision surface. The best path is selected through a weighted optimisation criterion that is mathematically determined in Equation (8):

$$R^* = argmin_{R_i}(\alpha H_i + \beta E_i + \gamma T_i) \quad (8)$$

Where "α, β, γ>0" represent preference coefficients. The negative sign assigned to "T_i" makes sure that highly trusted paths are given higher preference, as well as allowing controlled trade-off with structural complexity and energy costs.

(iii) Final Route Stabilisation & Malicious SN Suppression: A stabilisation phase is taken to make sure that the chosen route is not nullified under evolving threat conditions. SNs with slow trust decays, behaviour inconsistency, or anomaly-caused deviations are removed, and quick re-election is activated to prevent cascading failures. The resulting path represents a multi-hop chain stabilised by trust, which balances the exploration-exploitation requirements and provides a resilient forwarding of packets in both dynamic and possibly hostile IoT-WSN systems.

3.5 MFO–JFS Algorithm

The proposed MFO-JFS has three broad stages of operations: (1) Initialisation, (2) Trust-guided Joint Optimisation, and (3) Final Selection and Ordering.

Algorithm: MFO–JFS

Input:

- Network Graph 'G', Traffic Data 'T', Feature Set 'F', Filter Set 'B', Trust Scores 'τ'

Output:

- Optimized Feature Subset "F*", Final Filter Order "Π*"

Steps:

Initialize:

- Set initial feature pool (F_0 = F)
- Assign initial filter sequence (Π_0)
- Compute baseline performance using existing filters

Trust Mapping:

- Estimate the trust of SNs based on observed traffic
- Use the trust score to adjust filter priority

Feature Screening:

- Rank features using Mutual Information (MI)
- Keep only the top-ranked candidates

Optimization (MFO Loop):

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4919-4927

- Evaluate joint filtering cost using candidate features
- Update features + filter order using MFO
- Retain the best combination across iterations

Finalization:

- Output optimal feature subset (F*)
- Output trust-aware filter order (Π*)

3.6 Military IoT Contextual Hybrid MFO-JFS Routing

The conceptual framework of the proposed MFO-JFS is formed by three areas of operation, namely, situational battlefield sensing, trust-based behavioral reasoning, and hybrid optimization-based routing to simulate the achievement of resilience in the forwarding of packets under contested conditions.

(i) Battlefield Sensing & SN Deployment Layer:

- Data sensing is triggered by combatants, wearable IoTs, and on-field tactical sensors.
- SNs subscribe to position awareness, squad-based association, and scope of communication.
- The initial trust is drawn upon previous interactions and group cohesion indicators.

(ii) Threat Recognition & Trust Evolution Layer:

- SNs observe hostile behaviours such as spoofing, packet loss, slow forwarding, or fraudulent reporting.
- The direct-trust and reputation cues are updated, and anomaly impulses cause an increased level of scrutiny.
- Betrayed or hacked SNs undermine trust and signal propagation within squads.

(iii) MFO-Based Global Path Exploration Layer:

- The global exploration finds alternative multi-hop battlefield relays in the heterogeneous SN groups.
- Flames represent forward viability, energy feasibility, and interconnectivity at the inter-squad level.
- In the presence of tactical ambiguity, MFO generates candidate strategic communication chains.

(iv) JFS-Based Local Trust Refinement Layer:

- Local refinement measures the trustworthiness of squad-specific forwarding agents.
- Drift and foraging modes vary the weights of the paths depending on changing trust gradients on the battlefield.
- SNs that are malicious or behave abnormally are either suppressed or bypassed.

(v) Hybrid Fusion & Decision Layer:

- Multi-criterion analysis is a combination of global path structure and local trust reasoning.
- Final route selection is guaranteed to provide forward integrity, squad-cohesive trust, and adversarial suppression.

(vi) Stabilized Multi-hop Forwarding Layer:

- Situational information (status, vitals, geolocation, commands) is provided by the finalized route.
- Tactical updates are used to make it resilient against SN mobility, capture, or compromise.
- Recalibration is adaptive to ensure a secure connection with teams undergoing reorganisation.

4. RESULTS AND DISCUSSIONS

4.1 Simulation Environment and Parameters

All simulations had been run on the NS -2.35 discrete-event network simulator, which had been extensively used to assess trust-sensitive routing in IoT-WSN settings because of its customizable MAC/PHY modules and the ability to customize protocols. The SNs were evenly distributed in a 1000 m x 1000 m sensing field, and the SNs interacted with a single sink data-collection model. Scalability at various operational loads was examined using three SN densities (100 SNs, 150 SNs, and 200 SNs). Propagation and radio model were based on the first-order WSN energy dissipation model and used a path-loss exponent "(α = 3)" to model multipath and obstacle-rich communication environments, which are characteristic of urban or battlefield IoT applications. The different attack vectors were injected to simulate the real-world adversarial conditions, including Blackhole Forwarding, Selective Packet Dropping, Trust Inconsistency, and False Recommendation Reporting, as coordinated and stealthy adversarial behaviours. The intensity of attacks was varied between 10% and 40% of SNs to enable the testing of resilience under low and high adversarial contamination. Periodic updates of trust and interaction between neighbours were put into consideration in order to simulate dynamic multi-hop collaborative sensing. Mean results were averaged across 30 runs of the simulation with different random seeds to reduce stochastic bias. Baseline protocols were LRT and OCSC, and the proposed MFO-JFS routing was the target protocol to analyze.

Table 1. NS-2 Simulation Configuration

Parameter	Value / Setting
Simulator	NS-2.35
Field Size	1000 m × 1000 m
Number of SNs	100, 150, 200
Sink Position	Fixed (center)
Propagation Model	Radio energy + (α = 3) path-loss
MAC Layer	IEEE 802.15.4
Routing	LRT / OCSC / MFO–JFS
Traffic Pattern	CBR (UDP)
Packet Size	64 bytes
Simulation Time	250 s
Attack Types	Blackhole + Selective Forwarding + Trust Inconsistency + False Reporting
Malicious Intensity	10–40%
Energy Model	First-order (Tx/Rx)
Deployment	Uniform static
Repetitions	30 runs (avg.)

4.2 Evaluation Metrics

4.2.1 Security Ratio (SR): SR is calculated as the ratio of the number of verified and trust-approved data forwarding operations to the total number of forwarding operations that occur due to malicious interference. The mathematical model of the SR is shown in Equation (9):

$$SR = \frac{F_{succ}}{F_{tot}} * 100 \quad (9)$$

Where:

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4919-4927

- F_{succ} = Number of forwarding events passing trust validation
- F_{tot} = Total forwarding attempts

In this work, SR is used to measure the efficiency of routing in the maintenance of secure packet forwarding under conditions of malicious or compromised SNs. In the MFO-JFS model, SR represents the ability of trust recalibration and meta-heuristic optimisation to inhibit malicious forwarding and avoid adversarial path infiltration.

4.2.2 Energy-Consumption Ratio (ECR): ECR is the normalised average energy that is dissipated on a successful multi-hop transmission compared to the malicious density against baseline consumption levels. ECR can be mathematically modeled as below in Equation (10):

$$ECR = \frac{E_{used}}{P_{succ}} \quad (10)$$

Where:

- E_{used} = Total energy consumed during routing
- P_{succ} = Number of successfully delivered packets

In this work, a lower ECR implies an improved energy-aware routing performance. The proposed MFO-JFS has a reduced ECR since it focuses on reducing route re-discovery, inhibiting retransmission caused by malicious behaviour, and also optimising hop selection based on trust and remaining energy. This feature is critical when using military IoT in deployment, where SNs are powered by limited battery resources.

4.2.3 Computation Time (CT): CT refers to the latency involved in making route establishment and route update decisions within a particular network state. The CT mathematical form is given in Equation (11):

$$CT = t_{end} - t_{start} \quad (11)$$

Otherwise, it can be normalised following Equation (12):

$$CT_{norm} = \frac{CT}{N} \quad (12)$$

Where:

- t_{start}, t_{end} = Timestamps for route computation
- N = Number of participating SNs

A lower CT in this work implies a quicker routing adaptation. In both tactical and military IoT environments, quick recalculation will be necessary in keeping operational impetus and countering the adversarial disruptions. MFO has faster convergence of the global search, whereas JFS is a narrowed-down local exploitation, which minimizes the redundant overhead of search.

4.2.4 Trust-Based Connectivity Rate (TCR): TCR is used to measure the fraction of SNs that are connected through the trust-validated multi-hop paths despite the adversarial behavior. TCR is mathematically modeled in Equation (13):

$$TCR = \frac{N_{conn}^{trust}}{N_{tot}} * 100 \quad (13)$$

Where:

- N_{conn}^{trust} = SNs maintaining valid trust-approved paths
- N_{tot} = Total SNs in network

In this work, an increase in the TCR implies increased resilience to partitioning by malicious SNs. The suggested MFO-JFS boosts TCR by stabilising trust spread, penalizing anomaly sets, and ensuring dependable inter-SN cooperation, which is an essential aspect of mission-driven military IoT networks where the lack of connectivity has operational implications.

4.3 Comparative Results

4.3.1 SR Performance: SR analyzes secure forwarding in the case of malicious interference. With the increase in the adversarial density, each of the methods suffers a security performance deterioration as the manipulation of packets and disruption of trust increase. However, the proposed MFO-JFS is more resilient due to (i) Meta-Heuristic Trust Stabilisation, (ii) Malicious SN Suppression, and (iii) Adaptive Multi-Hop Path Refinement.

Table 2. SR across Malicious Intensities

Method	10% Malicious	25% Malicious	40% Malicious
LRT	78.2%	63.9%	47.5%
OCSC	86.5%	74.1%	59.4%
MFO–JFS (Proposed)	**93.7%**	**86.2%**	**71.0%**

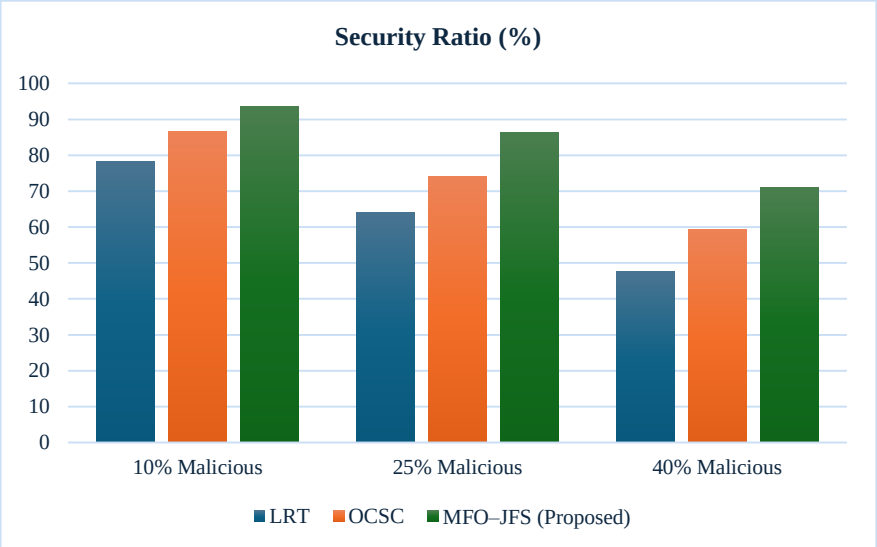

Figure 2. SR across Malicious Intensities

With a malicious density of 10%, the forwarding is maintained at a high rate with trust-preservation in the proposed MFO-JFS framework through early anomaly rejection and low optimisation cost. With increasing adversarial influence up to 25% malicious SNs, the base

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4919-4927

schemes degrade, and MFO-JFS averts above 85% SR, which indicates successful fraudulent path contribution rejection and consistent trust propagation. MFO-JFS maintains the 71% SR, even at a critical threat of 40% malicious SNs, when all the assessed methods suffer, ensuring the absence of topological collapse on a large scale and reducing the interference with mission-layer communications. This is consistent with the operations requirement of any IoT system with military-grade requirements because the security will degrade with cumulative adversarial pressure, but needs to satisfy reasonable mission throughput requirements. The stability margin of MFO-JFS over time implies that recalibration of adaptive trust limits the extent of malicious intrusion, optimisation-based route selection minimises the effective attack surface, and that multi-hop continuity mechanisms inhibit topological partitioning. Altogether, these features support the relevance of hybrid meta-heuristic routing to situations of tactical communication with the need to sustain situational awareness and information integrity under the conditions of compromised SNs.

4.3.2 ECR Performance: ECR indicates the normalised operational energy utilised by routing decisions, retransmissions, and overheads caused by trust assessment. Malignant SNs cause large increases in route failures and packet losses, compelling re-selection of multi-hop paths and re-evaluation of trust; this has the effect of increasing both LRT and OCSC energy consumption. In comparison, the proposed MFO-JFS eliminates redundancies by optimising forwarding and trust-stabilised selection, thereby regulating consumption.

Table 3. ECR under Malicious Intensities

Method	10% Malicious	25% Malicious	40% Malicious
LRT	104.8J	121.6J	147.5J
OCSC	98.3J	112.4J	134.1J
MFO–JFS (Proposed)	**91.7J**	**103.8J**	**118.9J**

Note: J (Joules) is normalised consumption per simulation cycle (1000 rounds).

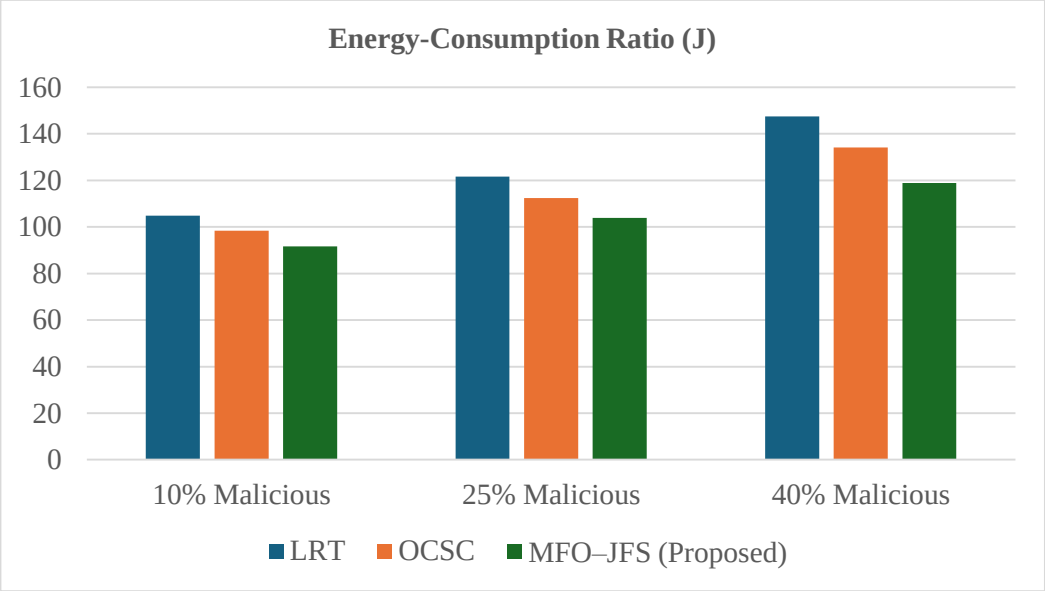

Figure 3. ECR under Malicious Intensities

The proposed MFO-JFS framework, at a rather low adversarial density of 10% malicious SNs, cuts network-wide ECR by about 12.5% compared to LRT and 6.7% compared to OCSC, mainly because of fewer route recalculations and prevented detours of packets. As the density of the malicious-set grows to 25%, adversarial interference increases the computation overhead of trust and path verification at all schemes, but MFO-JFS does manage to curb the energy explosion by favouring fewer sequences with greater energy density. In a threat level of 40% malicious SNs, all techniques inflate their energy costs exponentially, as a consequence of cumulative re-routing and attacker-induced disruption; however, the proposed technique exhibits a steadily lower ECR curve due to trust-optimised connectivity and not re-trial or path finding. Operationally, energy is a limited and mission-critical asset in a battlefield IoT implementation, especially in tactical SNs that run on a battery, wearable devices, or vehicles, and perimeter units. The MFO-JFS framework significantly enhances energy endurance by avoiding packet loops that incur energy costs in the deterministic evaluation of the trustworthiness by meta-heuristic scheduling and suppression of malicious packet loops. This contributes to improved sustainability, which helps maintain a long period of situational awareness and a long-term mission duration without battery replacement or reinforcement, even in active field deployment, which is a feature crucial to modern defence-grade IoBT and distributed sensor infrastructures.

4.3.3 CT Performance: CT records the sum of routing overheads spent to make reliable multi-hop paths that are under trust constraints. It has trust evaluation, meta-heuristic optimisation delay, re-routing when forwarding SNs fail, and adversarial interference. Indeed, where the adversarial environment is dynamic, the increased density of malicious SNs results in increased recomputation cycles. LRT is affected by repetitive LR-based trust inference, and OCSC by re-clustering processes. The suggested MFO-JFS reduces the convergence time by using adaptive exploration-exploitation scheduling to reduce the re-computation time in subsequent rounds.

Table 4. CT under Malicious Intensities

Method	10% Malicious	25% Malicious	40% Malicious
LRT	19.4 ms	26.8 ms	33.6 ms
OCSC	16.2 ms	22.7 ms	29.1 ms
MFO–JFS (Proposed)	**15.7 ms**	**20.1 ms**	**23.4 ms**

Note: ms represents per routing round convergence latency.

The overhead of trust computation is relatively low in all of the schemes studied at a low adversarial density of 10% malicious SNs, but the proposed MFO-JFS framework reduces the overall CT by an approximation of 19% compared to LRT and by 3% compared to OCSC, due to the reduction in re-routing attempts and earlier stabilization of trust paths. As the fraction of malicious SNs rises to 25%, attack-induced disruptions balloon re-routing and replenishment of trust in all the protocols, but MFO-JFS significantly mitigates the recompensation penalty by maintaining optimization of the forwarding path in a hybrid exploration-exploitation dynamic. The adversarial fragmentation increases the re-routing latency under harsh threat situations with 40% malicious SNs, but the hybrid framework of MFO-JFS remains computationally resilient

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4919-4927

to offer a 30% CT reduction compared to LRT and 19.6% compared to OCSC. Such results suggest that optimization-based trust calibration is a definitive parameter in the reduction of routing volatility when SN behaviour turns unpredictable or malicious. In tactical IoT applications, the fidelity of situational awareness is determined by routing latency because failure, capture, or spoofing of SNs adds uncertainty over time, which may adversely affect battlefield signalling. The suggested MFO-JFS framework achieves convergence due to coordinated and meta-heuristic scheduling, reduces unnecessary re-routing that is caused by malicious perturbation, and stabilizes forwarding decisions under evolving trust fluctuations. These features are reflected as shorter CT to quicker threat intelligence dissemination and troop telemetry, greater reaction agility by war fighters, and greater integrity of communication in unstable mission conditions.

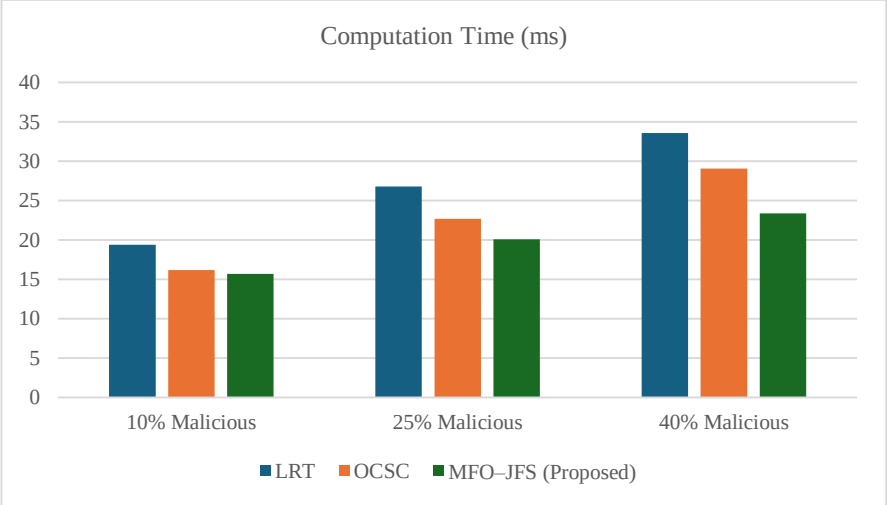

Figure 4. CT under Malicious Intensities

4.3.4 TCR Performance: TCR measures the number of SNs that are connected by reliable and trustworthy paths in the topology of the network. In malicious infiltration mode, untrusted SNs are eliminated in forwarding decisions, and this can break the topology and cause operational disconnectivity. LRT has a negative effect in the form of delayed isolation because of its inference latency due to logistic regression, and OCSC has more favourable stabilization of trust but suffers cluster fragmentation in adversarial churn. The suggested MFO-JFS boosts trust-preserving connectivity by dynamically balancing the SN selection and path refinement, which progressively allows the multi-hop continuity despite the aggressive pruning.

Table 5. TCR across Malicious Intensities

Method	10% Malicious	25% Malicious	40% Malicious
LRT	82.6%	68.3%	51.4%
OCSC	89.2%	79.5%	63.8%
MFO–JFS (Proposed)	**94.9%**	**88.6%**	**72.4%**

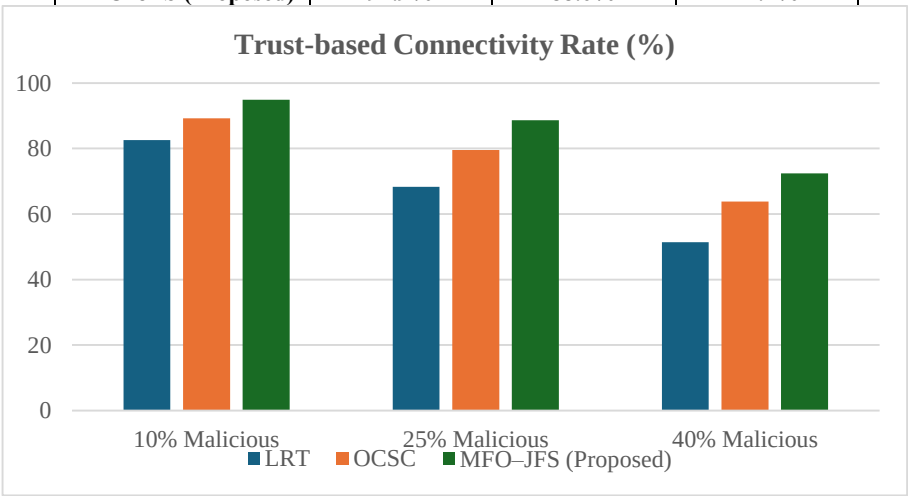

Figure 5. TCR across Malicious Intensities

When adversarial conditions are light (10% malicious SNs), the proposed MFO-JFS has over 94% connectivity, which is a strong feature in the propagation of trust with the least interference in the topology. In the medium threat environment (25% malicious SNs), the OCSC connection fails because of cluster-level partitioning, whilst MFO-JFS maintains the adaptive multi-hop relaying with continuous trust recalibration. When the adversarial load is really high (40% malicious SNs), both LRT and OCSC partially disconnect, whereas MFOJFS is at least 70% connected, avoiding isolation of the operations and significantly exceeding baseline protocols by this ratio. Constant network connectivity is imperative in tactical IoT settings where real-time distribution of geospatial intelligence, telemetry, and threat indications is necessary, especially when SN seizures, equipment failures, and spoofing occurrences are involved. The MFO-JFS framework is resistant to trust fragmentation in the presence of constant SN churn, supports secure multi-hop continuity in dispersed combat units, and re-bridges broken up topologies by an adaptive global-local route refinement mechanism. TCR performance is boosted by these combined behaviours, which allow the communication to be robust across the battlefield, and the execution of the mission to continue in changing adversarial conditions.

4.4 Discussion

- The comparative analysis shows clearly that adversarial intensity is a prevailing issue that affects trust-controlled routing behaviour within IoT-WSN settings. The two baselines (LRT and OCSC) are progressively degraded in all four performance dimensions as the

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4919-4927

malicious SN density goes higher, highlighting the challenge of being able to maintain consistent trust, insistent routes, and efficiency of resources at the same time. The logistic-trust estimation facility of LRT performs adequately when faced with low-threat environments, but adds re-computation time and does not eliminate all the attackers as the adversarial SNs keep springing. Similarly, OCSC can be optimised by cluster-based optimisation in the case of benign conditions, but changing adversarial behaviours causes fragmentation of trust, dissolution of clusters, and reconstruction of paths, which only compound the energy and latency overhead.

- On the other hand, the suggested MFO-JFS framework exhibits consistent performance across the adversarial gradient due to the dual-stage optimisation synergy. MFO is used to provide diversity in global search, thereby avoiding convergence to small trust basins, whilst JFS is used to provide local refinement to stabilise sequences of forwarding in response to dynamic disruption. Such interaction reduces redundant trust recalculations, interference among adversaries, and maintains multi-hop continuity processes that have a collective positive effect on the SR and TCR. Moreover, reduced re-routing overhead and speed of convergence help to decrease the energy use and shorter CT, which supports the idea that hybrid meta-heuristics can offer an acceptable trade-off between the security and resource consumption.
- In addition to the numerical advantage, the outcomes have importance to a defence-grade IoT and tactical sensor architecture, where topological survivability, communication latency, and threat resilience are mutually dependent. The ability to maintain trust-maintained connectivity even with uncertainty makes hybrid meta-heuristic routing an attractive paradigm in next-generation distributed cyber-physical systems. Moreover, the scaling behaviour that is observed indicates that it applies to large-scale and heterogeneous IoT implementations, whereby threat dynamics, resource allocation, and trust diffusion have non-linear interactions.

5. CONCLUSION

In this work, a hybrid TSR framework is proposed, which is a combination of the MFO algorithm and the JFS scheme to achieve secure multi-hop routing in adversarial IoT-WSN networks. The architecture collaboratively maximises the inference of trust, the stability of routes, and energy sustainability through global exploration and local refinement. The packet-forwarding behaviour, the residual energy, and anomalous activity are continually used in recalibrating the trust scores in order to prevent malicious influence whilst maintaining high topological cohesion. The outcome of experimental tests at different adversarial densities proves that the hybrid strategy significantly enhances the SR and TCR, facilitating the delivery of situational intelligence with trust. At the same time, energy usage and CT are also reduced, which can facilitate more efficient convergence and reduced re-routing overhead. Through comparative analysis, the shortcomings of logistic-trust and cluster-based baselines in dynamic threat evolution are revealed, therefore supporting the applicability of hybrid optimisation when deploying mission-critical IoT. In general, the results prove that the use of trust-based hybrid meta-heuristics is an attractive path towards secure, resilient, and resource-conscious routing of IoT-WSN. The tools, such as the cross-layer trust fusion and online threat forecasting, can be introduced to the framework, which will also help to increase the flexibility. Extending the framework to the UAVs, relays, and multi-domain IoBT ecosystems is also a promising direction for the next-generation battlefield communications.

REFERENCES:

1. H. N. Vishwas and T. K. Ramesh, "Recent Trends in Localization, Routing, and Security for Wireless Sensor Networks," in IEEE Access, vol. 13, pp. 55290-55312, 2025, doi: 10.1109/ACCESS.2025.3555280.
2. S. Singh, V. Tyagi, A. Malik, R. Kumar, Ankur and N. Kumar, "Intelligent Energy-Aware Routing via Protozoa Behavior in IoT-Enabled WSNs," in IEEE Transactions on Network and Service Management, vol. 23, pp. 1960-1969, 2026, doi: 10.1109/TNSM.2025.3636202.
3. Fei, H., Jia, D., Zhang, B. et al. A novel energy efficient QoS secure routing algorithm for WSNs. Sci Rep 14, 25969 (2024). https://doi.org/10.1038/s41598-024-77686-y
4. Wang, L., Petrova, K., & Yang, M. L. (2025). Trust Models in Wireless Sensor Networks for Defending Against Denial-of-Service Attacks: A Literature Review. Applied Sciences, 15(6), 3075. https://doi.org/10.3390/app15063075
5. Chandrasekaran, S.K., Rajasekaran, V.A. Trust evaluation model in IoT environment: a review. Environ Dev Sustain (2024). https://doi.org/10.1007/s10668-024-05731-x
6. S. Pratap Singh, N. Kumar, G. Kumar, B. Balusamy, A. K. Bashir and M. M. A. Dabel, "Enhancing Quality of Service in IoT-WSN Through Edge-Enabled Multi-Objective Optimization," in IEEE Transactions on Consumer Electronics, vol. 71, no. 2, pp. 4110-4119, May 2025, doi: 10.1109/TCE.2025.3526992.
7. Hartono, R., Mustika, I. W., & Sulistyo, S. (2026). Metaheuristic Approaches for Energy Optimization in Wireless Sensor Networks: A Systematic Review of Trends, Challenges, and Future Directions. EAI Endorsed Transactions on Internet of Things, 11. https://doi.org/10.4108/eetiot.10328
8. R. Zhu, A. Boukerche, L. Long and Q. Yang, "Design Guidelines on Trust Management for Underwater Wireless Sensor Networks," in IEEE Communications Surveys & Tutorials, vol. 26, no. 4, pp. 2547-2576, Fourthquarter 2024, doi: 10.1109/COMST.2024.3389728.
9. Ramachandra, S., & Baskar, M. (2025). Real-time multi-level trust-based secure routing for improved QoS in WSN using blockchain. Results in Engineering, 26, 104732. https://doi.org/10.1016/j.rineng.2025.104732
10. Sharma, V., Beniwal, R. & Kumar, V. Multi-level trust-based secure and optimal IoT-WSN routing for environmental monitoring applications. J Supercomput 80, 11338–11381 (2024). https://doi.org/10.1007/s11227-023-05875-z
11. Ramachandra, S., & Baskar, M. (2025). Real-time multi-level trust-based secure routing for improved QoS in WSN using blockchain. Results in Engineering, 26, 104732. https://doi.org/10.1016/j.rineng.2025.104732
12. Fei, H., et al. (2024). A novel energy efficient QoS secure routing algorithm for WSNs. Scientific Reports, 14, Article 77686. https://doi.org/10.1038/s41598-024-77686-y
13. Xiao, J., Li, C., Li, Z., & Zhou, J. (2024). BS-SCRM: a novel approach to secure wireless sensor networks via blockchain and swarm intelligence techniques. Scientific Reports, 14, 9709. https://doi.org/10.1038/s41598-024-60338-6
14. Anuradha, N., Rani, Y.A., Marry, P., Salotagi, S., Babu, D.R., Devi, G.N.R., Naresh, P, Reddy, E.S.L. (2025). Secure and adaptive routing in Wireless Sensor Networks using Meta-Router and TGAT-TrustChain. Mathematical Modelling of Engineering Problems, Vol. 12, No. 11, pp. 4000-4006. https://doi.org/10.18280/mmep.121126
15. Aldawsari, H. (2025). A blockchain-based approach for secure energy-efficient IoT-based Wireless Sensor Networks for smart cities. Alexandria Engineering Journal, 126, 1-7. https://doi.org/10.1016/j.aej.2025.04.052
16. Kannimuthu, K. Prathapchandran & Janani, T. (2021). “A Trust-Based Security Model to Detect Misbehaving Nodes in Internet of Things (IoT) Environment using Logistic Regression,” Journal of Physics: Conference Series. 1850. 012031. 10.1088/1742-6596/1850/1/012031.
17. A. V. Ramesh and E. J. Thomson Fredrik, "A Fission–Fusion Oriented Secured Protocol for IoT-based WSN Framework with Energy-Efficiency," 2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), Coimbatore, India, 2025, pp. 1099-1106, doi: 10.1109/ICoICI65217.2025.11254653.