National Journal of Antennas and Propagation
Research Article

National Journal of Antennas and Propagation, ISSN: 2582-2659 Vol. 7, No. 1, 2025 (pp. 342-358)
WWW.ANTENNAJOURNAL.COM

A Hybrid DAMFO-IWQPSO-HS Framework for Optimal Path Selection and Secure, Energy-Efficient Multipath Routing in Wireless Sensor Networks

C. Visalatchi[1*], K.S. Mohanasathiya[2]

[1]Research Scholar, Department of Computer Science, VET Institute of Arts and Science (Co-education) College, Thindal, Erode, Tamil Nadu, India.

[2]Assistant Professor and Research Supervisor, Department of Computer Science, VET Institute of Arts and Science (Co-education) College, Thindal, Erode.

KEYWORDS:

Wireless Sensor Networks;
Optimal Path Selection;
Data Aggregation;
Secure Multipath Routing;
Dynamic Adaptive Multifactor Optimization;
Cluster- Based Networks;
Improved Weighed Quantum Particle Swarm Optimization;
Harmony Search

ARTICLE HISTORY:

Received	27.06.2025
Revised	15.08.2025
Accepted	03.09.2025

DOI:
https://doi.org/10.31838/NJAP/07.01.38

Abstract

Routing protocols continue to be an active research area in wireless sensor networks (WSNs), as they determine security and the lifetime of the communications system, particularly in limited environments. This paper introduces the IWPSO-HS approach, application of the DAMFO method, and design of the IRSA algorithm for efficient multipath routing for cluster-based WSNs. The primary issues addressed are those of energy conservation, enhanced sensing quality, longer network lifetime, and information transmission protection against attack. The latest methods are marred with the limitations of excessive power usage, reduced sensing efficiency, and compromise on security, thereby limiting WSNs in terms of increases and sustainability. Therefore, the algorithm employeduses DAMFO for path optimization to reduce redundant data transmission and enhance network operation. Parallelly, the suggested IWQPSO-HS approach also considers safe data transmission and energy usage distribution among sensor nodes. Implementation of the improved RSA (IRSA) algorithm enhances data encryption to ensure secure existence with enhanced security against security attacks, such as eavesdropping and Man in the middle attacks prevalent in WSNs. The hybrid DAMFO-IWQPSO-HS method, with the inclusion of IRSA, gets rid of premature convergence and enhances overall robustness in the optimization process, along with additional security in transmitting data. The results are knownto demonstrate outstanding improvements, such as a 28% rise in energy conservation, a 35% rise in network life expectancy, an improvement of 92% in network coverage, and outstanding improvement in sensor data security, and thus the hybrid DAMFO-IWQPSO-HS-IRSA system is a better solution for future WSNs. Combining these optimization methods with more robust security measures offers proper solutions to today's WSNs problems, such as network management and optimization and resistance to security threats.

Authors' e-mail ID: visalatchic09@gmail.com; sathyaanandh08@gmail.com

Authors' ORCID ID: 0009-0002-5232-1714; 0009-0004-5897-602X

How to cite this article: Visalatchi, C. and Mohanasathiya, K.S., A Hybrid DAMFO-IWQPSO-HS Framework for Optimal Path Selection and Secure, Energy-Efficient Multipath Routing in Wireless Sensor Networks, National Journal of Antennas and Propagation, Vol. 7, No. 1, 2025 (pp. 342-358).

Introduction

Wireless sensor networks (WSNs) are power-hungry networks made up of numerous compact, portable sensor nodes used to sense various conditions in the environment.

As very well explained above,Wes research is highly desirable asit may be used in almost all social and industrial environments. In today's fast world, quick communication is unavoidable, and WSNs facilitate it using real-time data transmission.[1] Sensor networks are either wired or wireless, as shown in Figure 1. Wired sensor networks comprise nodes that cannot be moved but are firmly fixed at a point. These sensors are accurate in most cases because they are permanently wired to the equipment capturing data. Integrated sensors are also likely to be long-lasting and hence cheaper for replacement.[2] Wired networks, however, has its cost in wires making it relatively expensive compared to wireless networks. Wired systems, on the other hand, are more complex to manage and take up a significant amount of physical space.[3]

On the other hand, WSN utilizes the radio channels for transmission between nodes and they do not need physical cables. This provides the feasibility of locating the sensors in geographical positions in an attempt to sense other physical conditions like weather, humidity and fire, wildlife, etc. In WSNs, there are two available methods with which the sensor nodes can communicate; either direct or indirect.[10] In direct transmission, the sensor node sends information to some other node or base station, while in indirect transmission, information is forwarded through reference node or the base station. Therefore, every sensor node of the network senses the environment, gathers data, processes data, stores data, and transfers data.[5] In such networks, the base station is the high-energy central data processing node and all sensor nodes relay their sensed data to this node for further processing and resultant action.[6]

A sensor node setup is shown in Figure 2. The system includes transceivers, memories, microprocessors, sensors, and the analog to digital converter (ADC). The next section provides description of these units' specifications.[7]

As it has been proven, clustering of WSNs is very advantageous. A well-established advantage is the fact that the routing table size also gets reduced because route management only happens between clusters and therefore reduces traffic load.[8] Deployment of a cluster with multinodes minimizes communication between CH's and nodes and therefore saves the limited transmission resources.[9] It also minimizes the impact of network failures at the inter-CH level because one sensor node only communicates directly with one such CH. This makes backbone design simpler and avoids flooding, collision, and expensive experiments.[10] This paper contributes to insight into the performance of the CH toward the forecasted integrated healthcare network.

In order to manage individual lifetime of senor nodes as well as network lifetime, it can perform effective management procedures. In the same manner, CHs can schedule sensor activity and inactive them at low power level frequently and thereby reduce energy consumption,[7,40] Prescheduling of the medium can be done on a round-robin basis through scheduling tables while communication timings are used to avoid conflicts in the media access and overlap of sensor coverage. CHs can also reduce packets being transmitted, at least 10,[12] by aggregating data from cluster nodes.

Clustering and CH selection are the pillars of WSNs' efficiency. Ideal clustering will terminate the sharing of information with other base stations because it will reduce wastage of energy. Clustering also enhances capacity management within WSNs, most particularly in large applications.[13,37] In clustering, then, some of the key problems that must be expedited include identifying the optimal number of clusters, how to re-elect and elect the CH, and how to operate clusters. These

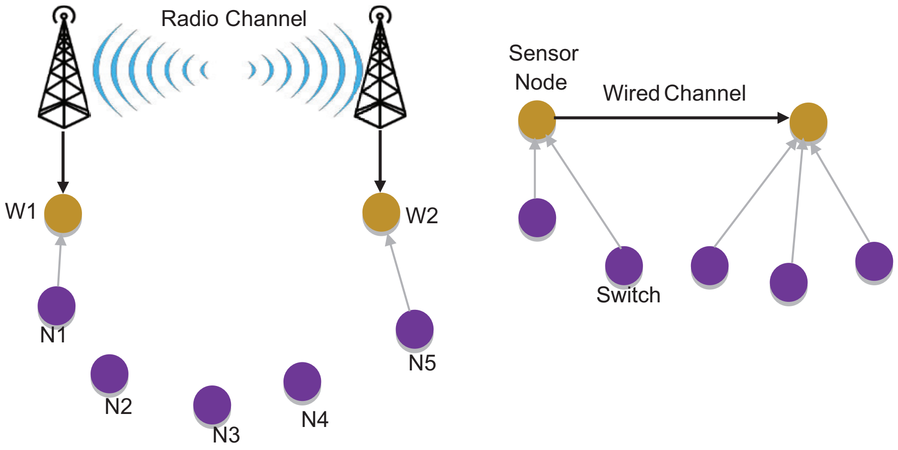

Fig. 1: Wireless and wired sensor network model.

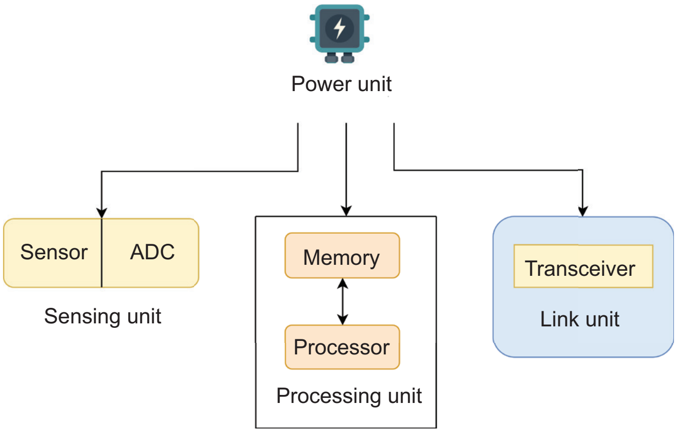

Fig. 2: Sensor node architecture.

parameters need to be optimized to use the energy efficiently and there's no requirement for several sensor nodes to gather the same information.[14,39] Care needs to be taken to select the clustering methodology to the efficiency of the way in which the information gathering is executed later. There is also a routing protocol taxonomy in WSNs that is to be flat, centralized, or location-based, and it can be differentiated based on QoS, query-based networking, and multipath routing.[15,36]

The metaheuristic approaches therefore give guaranteed solutions to problems that impede WSNs, particularly when the information given might be incomplete or imprecise. These techniques provide a broad variety of potential solutions and in the main, motivated by natural phenomena to obtain solutions for some of the WSN parameters such as navigation, energy usage, and WSN duration.[16,38] Among all the metaheuristic strategies, the swarm intelligence strategies are particularly beneficial for WSN problems. These behaviors allow a search space to be explored efficiently by successfully balancing the exploitation of promising areas by fusing the behaviors of both dragonflies and moth groups. But, there is a need to discuss the security aspects of WSN, mainly key management for clustering and optimization. The key can be managed in four steps. The first is the management of key distribution where secret keys are given to sensor nodes to provide data confidentiality, integrity, and authorization.[17] Security keys are distributed in insecure channels in large-scale WSNs, which may be hard; so, centralized "key setup" beforehand is required. The second phase, shared-key discovery, is after network initialization when neighboring nodes identify their neighbors and form shared keys. Nodes in the third phase of key setup establish secure communication channels directly or secure paths through the use of private keys and ensure secure key exchange as well as network security at large.[18]

Problem Statement

In applications like medicine, military reconnaissance, and environmental monitoring, where data acquisition is critical to network survivability, cost-effectiveness, and the security of data communication, wireless sensor networks, or WSNs, are a vital tool. WSNs face significant challenges in the guise of limited energy resources, poor path selection for data communication, insecure data communications, and balancing maintaining the quality of sensing while maximizing network life. Under dynamic conditions, conventional routing methods sacrifice energy efficiency, safety, and optimal data aggregation. To enhance the lifespan and reliability of cluster-based WSNs, there is a need to select optimal routes for information transmission, effectively aggregate data, and ensure safe multipath routing. The current systems are not strong enough to accommodate the problems of energy saving, secure routing, and optimal sensing protection together. Thus, to ensure efficient sensing and longer lifetime of the network in optimal path selection, enhancing data acquisition, and providing secure and power-saving routing in WSNs, a better approach is required. The Hybrid DAMFO-IWQPSO-HS was developed in this research to improve the information gathered and multipath routing for safety and environmental preservation in cluster-based WSNs.

Motivation

The increasing need for efficient, effective, and secure communication in WSNs in smart cities, healthcare services, environmental monitoring, and for military uses is themotivationfor this research. Most WSNs operate in hostile environments or with limited access to a power source where network security is an issue and WSN lifespan as well as information fear rates need to be attained most of the time.Dynamic routing methods most of the times are unable to strike a balance between information gathering, safeguarding, as well as saving the WSN environment and therefore WSN nodes experience frequent failure and short lifespan and the gathered information is most of the times inaccurate. Moreover, it is difficult to provide good coverage and guarantee high-quality monitoring because WSN are reputed to possess dynamic topology. Because of all these difficulties, there is a need for high-order optimization techniques that can cope with the energy expenditure, network security of connections, and safe transmission of data simultaneously. This paper aims to address the world-wide inefficiencies and nonsustainability of WSNs by integrating safe multipath navigation and energy-conscious path selection and information fusion.

Related Works

Lei, C.[19] considers energy-efficient routing in IoT settings through a fuzzy clustering and particle swarm optimization (PSO)-based hybrid solution. The method first clusters geographically close-by sensor nodes based on fuzzy logic and subsequently optimizes the development of clusters and routing through a PSO fitness function maximizing energy usage against communication distance. Simulation results show considerable enhancements in network lifetime and energy utilization compared to conventional approaches.

Prasad, V. & Roopashree, H.R.[20] present an energy-aware and secure routing (EASR) protocol for hierarchical cluster-based WSNs. Expanding on LEACH, they incorporate trust evaluation (TE) parameters to identify and prevent faulty or untrustworthy nodes, along with dynamic cluster thresholding for energy conservation. Their hybrid approach improves network lifetime and security stance.

Meenakshi, N., et al.[21] introduce an enhanced "Engroove LEACH" cluster head protocol for improved energy efficiency in WSN communication. With optimized cluster head selection and routing paths, their scheme is environment-aware, reduces energy consumption, reduces packet loss, and prolongs network operation time.

Goud, B.H., et al.[22] solve high energy consumption and latency in random-path WSNs via route optimization using machine learning. The system identifies low-power and high-throughput routes with higher packet delivery ratios and minimum delay. Simulation demonstrates significant improvements in energy efficiency and transmission reliability.

Jalalinejad, H., et al.[23] introduce a novel hybrid multihop clustering protocol for WSNs with ambient energy-harvesting. Decentralized and centralized clustering are merged on the basis of node energy levels and harvest capabilities, modifying routing for ambient energy-dependent nodes. The outcome is improved network efficiency, stability, and sustainability.

Krishnamoorthy, R., et al.[24] propose an enhanced cluster-assisted routing protocol with node position optimization from a Gaussian network model. Their framework combines grid-based clustering and shortest-path routing for improved energy distribution. NS2 simulation results demonstrate enhanced energy usage and communication reliability.

Hu, H., et al.[25] propose QPSOFL a fuzzy logic and clustering-based routing protocol with quantum PSO (QPSO).

Table 1: Comparison table on quality monitoring in wireless sensor network.

Authors & Year	Technique(s)	Objective(s)	Results
Jiao et al.[28]	KNN-based sink position prediction + improved RDA	Minimize energy while meeting delay constraints for mobile sink WSNs	Fewer hops, lower energy use, timely packet delivery
Kiran Kumar et al.[29]	Metaheuristic clustering + security layer	Secure and energy-efficient cluster-based routing	Noted improved network lifetime and resilience
Kaviarasan & Srinivasan[30]	Adaptive Remora Optimization	Energy-efficient CH selection and route optimization	Better energy usage versus standard protocols
Prakash et al.[31]	Modified-PSO (M-PSO) + genetic algorithms (GA)	Optimize route and CH selection for energy savings	Extended network lifespan and balanced energy
Saemi & Goodarzian[32]	Hybrid metaheuristic for underwater networks	Minimize energy use and prolong underwater WSN lifetime	Significant energy reduction and connectivity gains
Sharma & Kansal[33]	Enhanced CH selection + routing improvements	Simplify routing while improving energy efficiency	Improved packet delivery and reduced energy
Roopa Devi[34]	Hybrid gravitational search + PSO	Secure multipath routing with energy awareness	Achieved better throughput and lower drop rate
Teja & Srinivasan[35]	Multiobjective trust-aware dynamic weight pelican optimization algorithm (M-TDWPOA)	Optimize secure CH and routing in WSNs with trust, energy, delay, and distance	Minimal energy ~0.46-0.49 J; improved throughput & alive nodes

It uses innovations such as Sobol sequence initialization, Lévy flights, and Gaussian perturbations to escape local optima, and fuzzy decision-making to choose the next-hop cluster heads based on residual energy and distance. In contrast to HHO, GWO, PSO, and QPSO, QPSOFL exhibits better network lifetime and throughput.

Ramalingam, S., et al.[26] enhance a robust clustering and routing mechanism through a more effective elephant herd optimization (EHO) algorithm. The enhanced EHO enhances cluster head selection and data routing. MATLAB simulations demonstrate significant improvements in energy efficiency, network lifespan, and overall communication efficiency in comparison with previous metaheuristic-based approaches.

Vellela, S.S., & Balamanigandan, R.[27] The primary problem of energy-efficient routing in WSNs underpinning mobile cloud platforms is tackled by Vellela and Balamanigandan. A Chimp-based clustering flat routing protocol (CbCFRP) is presented by them, wherein cluster organization and routes for routing are optimized with a chimp-inspired metaheuristic. This method tries to reduce energy and latency at the same time. Deployed and verified with MATLAB simulations, their design performed better than other designs in terms of larger throughput, less delay, less packet loss, and better delivery ratios

Materials and Methods

Three robust techniques are employed in this hybrid approach. They are the harmony search (HS) algorithm, improved weighted QPSO (IWQPSO), and the dynamic adaptive multifactor optimization (DAMFO) illustrated in Figure 3. By offering increased network lifetime, protection of information transmission, and control of energy consumption, their combination ensures maximum network efficiency. Through a search for optimal cluster organization and optimal information paths, DAMFO increases information aggregation reliability and quality between clusters. Through the promotion of improved convergence rates to optimum values and minimizing computationally expensive routing decisions, IWQPSO optimizes path choice. For achieving peak energy frugality and ensuring safe multipath routing methods, the HS approach incorporates a refining layer. This is used to avoid possible security violations without maintaining excessive power consumption. This hybrid design fits well in dynamic and resource-constrained WSN applications as well as where safety is a concern and power savings is of utmost importance. Using diverse optimization methods, the software tries to optimize network

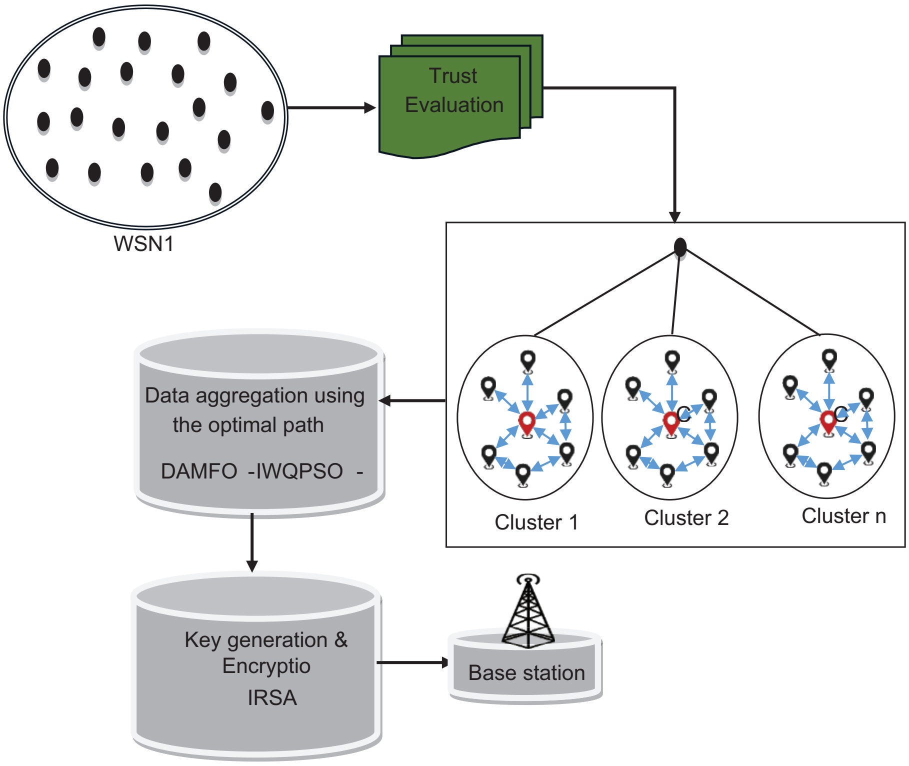

Fig. 3: Proposed architecture of DAMFO-IWQPSO-HS.

stability, data exchange, and sensor node longevity to make it suitable for applications like smart city, industrial Internet of Things, and environment monitoring among others.

Recovery of sensor nodes from hard-to-reach locations enables collection of environment information. The two considerations that made Sensor Nodes energy efficient (EE) in Wireless Sensor Networks (WSN) are how much energy they use in data transmission and how much they use in data reception.. Sensor networks consist of a greater node density; greater than one node will sense the same information, which results in redundancies. When DA is used for relaying messages from SNs to the base station, redundancies can be eliminated from the problem. For maintaining the consistency of the interactions, the TE process is used first. In case of safety and identification of malicious nodes (MN), TE is a suitable choice. To select the most profitable route among SNs, the DAMFO-IWQPSO-HS algorithm is advised. By encrypting and transmitting the gathered data to the BS, the IRSA methodology increases the Security Level (SL), and this assists in avoiding unwanted information manipulation.

Dataset Description

Table 1 merges the most significant parameters and characteristics relevant to the dataset used for WSN training, including traffic patterns, power levels, network parameters, and efficiency measures for measuring the efficiency of the hybrid algorithm. The configurations can be modified based on requirements for a particular experiment or dataset. This is an example of a WSN table utilized that entails information aggregation, secure energy-efficient multipaths routing, and best path selection and sample data shown in Table 2.

IWQPSO and HS

After choosing, cluster heads aredeployed.IWQPSO is combined with HS-based meta-heuristic approaches to and low discovery, maintenance, and administration overhead of routes. IWQPSO has been used along with HS-based meta-heuristic methods to find the most eco-friendly and secure method. The HS optimization method can yield solutions according to parameters HMCR and PAR. This takes away from the locally discovered solution but at the same time facilitates enhancing the global solution. The efficiency of the

Table 2: Dataset description.

Attribute	Description
Dataset Name	Wireless sensor network simulation dataset
Number of Nodes	500
Number of Clusters	25
Sensing Area	1000m × 1000m
Transmission Range	100 m
Node Energy Capacity	2 Joules
Data Packet Size	512 Bytes
Initial Node Energy	Uniform distribution between 0.5 and2 Joules
Mobility Model	Random waypoint
Routing Protocol	Cluster-based multipath routing (Hybrid DAMFO-IWQPSO-HS)
Simulation Time	1000 seconds
Traffic Pattern	Constant bit rate (CBR)
Network Lifetime	Total time before the first node dies
Data Aggregation Model	Threshold-based data aggregation with dynamic path selection
Security Parameters	End-to-end encryption authentication via hybrid optimization multipath routing for fault tolerance
Performance Metrics	Energy consumption packet delivery ratio (PDR). throughput path reliability and data aggregation efficiency

Table 3: Energy evaluation of sensor nodes in WSN[20] (Sample data).

Node ID	Timestamp	Temperature	Humidity	Signal Strength (dBm)	Battery Level (%)	Data Aggregated (KB)	Optimal Path Selected	Energy Consumed (J)
N1	2024-09-23 11:30:00	22.6	56	−81	86	121	Yes	0.6
N2	2024-09-23 11:30:00	23.2	53	−79	83	116	No	0.7
N3	2024-09-23 11:30:00	21.9	58	−76	89	131	Yes	0.5
N4	2024-09-23 11:30:00	22.3	55	−78	81	141	Yes	0.4
N5	2024-09-23 11:30:00	23.2	51	−77	80	136	No	0.6

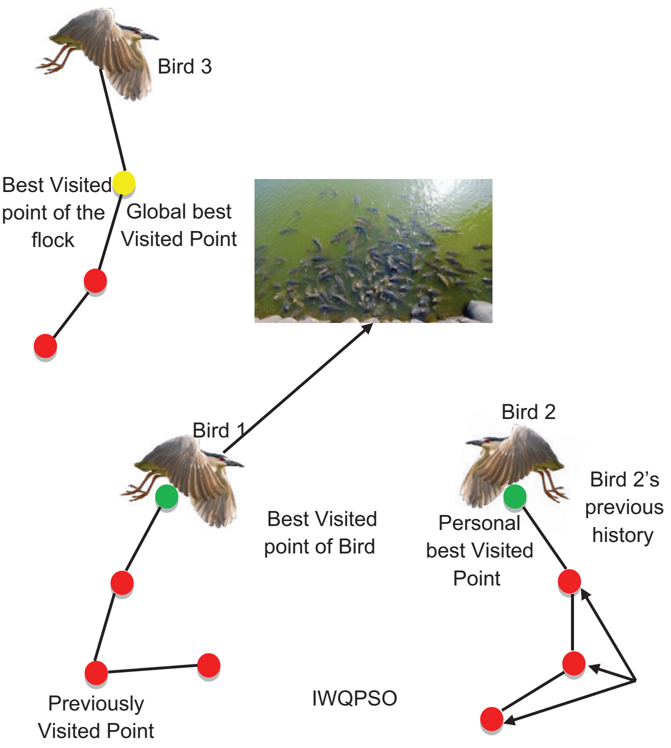

Fig. 4: Architecture of IWQPSO.

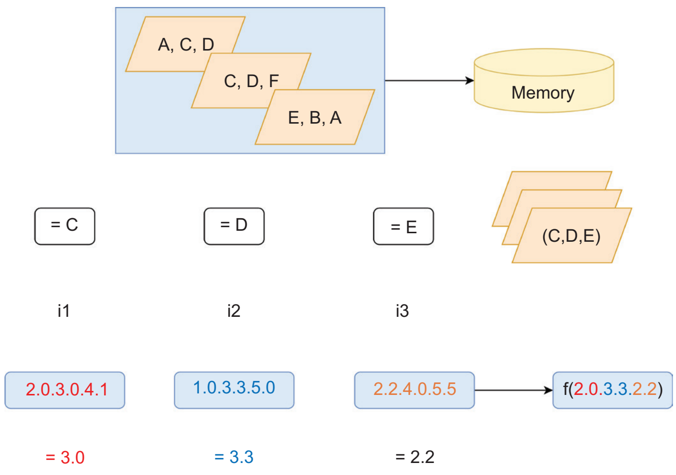

Fig.5: HS correlation between music progression and optimization.

investigate the most dependable and environmentally friendly optimum routing path.

The IWQPSO-HS meta-heuristics method recognizes that the safest andquickestpower-conscious path encompasses distance and confidence requirements. It possesses a prespecified number (Np) of particles. In IWQPSO, a particle or bird represents a solution in the search space. An iteration equals the generation, and each particle calculates its personal best, referred to as ps_b, and global best, referred to as gl_b. For acquiring anoptimal world-wide response, the individual and global best values are utilized to update the velocity Vi,d and position xi,d. The conceptual model of IWQPSO for the selection of the best visited location is illustrated in Figure 4.

The HS replicates the activity of music playing in which an artist attempts to achieve harmony. In composing music, an artist selects and obtains melodic notes from some source. In trying to achieve the best harmony, the artist then typically plays the notes on his instrument. The optimum solution to optimization problems is realizable in an optimum design approach that is exactly the same as this sort of activity. Similar to how it is possible to multiply the value of a fitness function at every step, aesthetic acoustic efficiency can also be achieved time and again. If one desires to improvise, he has three options. Play any familiar tune from memory as a starting point. The second way is doing little pitch manipulations to reproduce notes of a familiar piece of music. Creating new or random notes is the third option. A well-defined quantitative optimizing process was established for these three options. Harmony memory (HM) is the major consideration, and then there is harmony memory consideration rate (HMCR). To determine whether the potential solution for another harmony is a random selection from the range space of the feasible space pitch adjustment rate (PAR) or the relative value of any harmony in the HM, the improvising process uses HMCR. Applying the HS method to optimization problems is easy and requires less mathematics.

It provides superior space searching. The connection between optimization problem and musical improvising is illustrated in Figure 5. Each musician has some favored pitches, i.e., “A, C, D” for the saxophone, “C, D, F” for the cello, and “E, B, A” for the guitar. These plucks of the saxophone, cello, and guitar are provided by the variables x1 as 3.0, 2.2, 4.0; x2 as 1.0, 3.3, 5.0; and x3 as 2.2, 4.1, and 5.6. When the guitarist picks the note “E” out of “E, B, A”, the cellist picks the note “D” out of “C, D, F”, and the saxophonist picks the note “C” haphazardly out of “A, C, D”, a new harmony of “C, D, E” is formed. This repeats until there is total harmony. The aim function checks this solution, and the target values for the new solution vector are (3.0, 3.3, 2.2). If the goal functional is improved from the worst harmony of the HM, it is preserved.

A good routing technique should have fast convergence; high success ratio in finding the optimal route;

search of HS is better. As opposed to being stuck in one zone as in HS, exploration in IWQPSO is facilitated as particles have the ability to cross areas by varying their position and speed at the solutions in search of a globally optimal solution. To aid the problem of mining and exploration in high dimensions, IWQPSO is thus associated with HS. This yields precise, convergent optimal solution. The hybrid technique regulates the workload safety ratio of energy consumption among sensor nodes as well as chooses safe network channels. In order to acquire the optimal trajectory of the WSN, the IWQPSO-HS algorithm combines the fast convergence and dynamic nature of IWQPSO with the high search ability of HS. The primary goal of the PSO-HS approach is to drastically increase the number of valid solutions within iterations.

Improved RSA (IRSA) Algorithm to Provide Security

The IRSAalgorithm enhances the existing RSA encryption scheme by incorporating additional security measures and optimizations.

Step 1: Using the Chinese Remainder Theorem (CRT) for Decryption
Step 1.1: To speed up decryption, precompute

$$d_p = d \ mod \ (p - 1) \tag{1}$$

$$d_p = d \ mod \ (q - 1) \tag{2}$$

Step 1.2: Compute C_1 and C_2 as

$$C_1 = \mathrm{C}^{d_p} \ ) \ mod \ p \tag{3}$$

$$C_1 = \mathrm{C}^{d_q} \ ) \ mod \ q \tag{4}$$

Step 1.3: Combine the results using the CRT

$$M = C_2 + q.\left(\frac{C_1 - C_2}{q} mod \, p \right) mod \, n \tag{5}$$

Step 2: Hybrid Encryption Approach
Use RSA to encrypt a symmetric key (for example, AES key). Encrypt the actual message using the symmetric encryption algorithm.

Step 3: Padding Schemes
Step 3.1: Implement padding schemes (e.g., optimal asymmetric encryption padding (OAEP)) to prevent attacks:

$$M' = Padding(M) \tag{6}$$

Step 3.2: Encrypt the padded message:

$$C = \mathrm{M}'^{e} \ \text{ mode n} \tag{7}$$

The IRSA algorithm incorporates optimizations such as the CRT for efficient decryption, hybrid encryption methods, and enhanced security through padding schemes. These modifications make it more secure and efficient compared to the existing RSA algorithm while maintaining its foundational principles.

TE with Node Characteristics and Recommendations

TE is a useful tool in WSN to detect malicious activities as well as ensuring safety. Based on its behavior with regard to others, it allocates TV to every node,employing a continuous variable within an interval. From (−1 to +1). A node in the network immediately starts calculating the TV of the requested node as soon as it receives a node (on receiving information request messages by the neighboring node) automatically compares the trustworthiness of the requesting node. This provides secure communication by taking into account direct and indirect trust. Some believe that combined trust is

$$T_N = \sum(T_D + \mathrm{T}_1) \tag{8}$$

Here, ‘T_N’ denotes the TE, ‘T_D’ denotes direct trust, and ‘T_1’ denotes indirect trust. When nodes communicate directly with each other, direct TV is formed. The node’s trust is confirmed and scanned to see if it’s dropping packets or forwarding them. Node ‘T_N’ trusts node ‘T_A’ as a precaution to see if packets that were sent through it were actually delivered by the node. As can be derived from the value ‘LT〛_((N,A))^’, node ‘T_N’’s trust in node ‘T_A’ with time stamp ‘t’ is:

$$LT^t_{(N,A)} = \left(\tilde{w}_1 * C^t_{pac} \right) + \tilde{w}_2 * D^t_{pac} \tag{9}$$

Here, C^t_{pac} and D^t_{pac} are control forwarding and data pac packet forwarding ratios, respectively, for the same time step ‘t’, and $\tilde{w}_1$ and $\tilde{w}_2$ are the weight values that were used in C^t_{pac} and D^t_{pac}, respectively.

The reliability of the path that has been utilized to transport the data packets is quantified via path TV computation. It is determined and calculated through the weighted average of TVs in every node along the path.

$$HT^t_{(NA)} = \prod LT^t_{(NA)} \mid T_N . T_A \, and \, T_N \rightarrow T_A \tag{10}$$

In this case, ‘T_A’ is ‘T_N’’s next hop. The direct trust is evaluated in the following manner.

$$T_{D_{(N,A)}} = \sum\left(LT_{(N,A)} + HT_{(N,A)}\right) \tag{11}$$

Indirect trust among nodes that do not directly communicate leads to indirect trust. Neighbor nodes’ indirect TV is not evaluated without the evaluating node. Finding the common neighbors of node T_N and T_A and the indirect trust of node T_i are important in order to make the TV more trustworthy. The following are the parameters for measuring indirect TV from neighbor node T_i to node:

$$T^{(T)}_{X(N,4)} = T_{D(N,I)} * T_{D(I,A)} \tag{12}$$

Algorithm 1: CH Selection and Switching

Step 1: Initialization
Define the network parameters:Number of nodes N; Sensing area dimensions (e.g., L W); Maximum allowable distance D_{max}

Step 2: Cluster Formation
Each node x randomly chooses a cluster ID from a predefined set of IDs C.
Nodes within a defined range (e.g., within D_{max}) become neighbors.

Step 3: Leader Election
Each node calculates its energy level E_x.
The leader selection criterion can be based on energy level, distance to the center, or a combination:

$$Leader\ Score = \frac{E_x}{d_x} \tag{13}$$

Where:is the distance from node x to the center of its cluster.The node with the highest leader score is elected as the CH.

Step 4: CH Announcement: The elected leader broadcasts its ID to all members of the cluster.

Step 5: Leader Switching Condition: If the energy level of the current leader E_{leader} falls below a threshold T or after a predefined time T_{switch}, initiate leader switching.

Step 6: Leader Switching
All cluster members recalculate their leader score.
The node with the highest score takes over as the new CH.
The new leader broadcasts its ID to the cluster.

Step 7: Repeat
The process continues as long as the network operates.

Here, $T^{(T)}_{X(N,4)}$ is utilized for indirect TV of node ‘T_N’ and ‘T_A’ to $T_{D(N,I)}$ for direct trust of node ‘T_N’ to node ‘T_I’. $T_{D(I,A)}$ is utilized for direct trust of node ‘T_A’ to node ‘T_I’

The algorithm ensures that the most energy-efficient and centrally located node is chosen as the leader, enhancing the overall network performance.It is fully dependable and qualified to take on the position of CH. The CH stores the normalized amount of energy range of 0–1.By selecting a particularly energy-efficient and strategically positioned node as the leader, the method improves the efficiency of the whole network. The network’s switching architecture encourages robust and effective information transfer.An illustration of the DAMFO algorithmic flow is shown in Figure 6. The algorithm at issue is a mixed optimization method that combines the benefits of moth flame efficiency with the dragonfly method.

The Figure 6 is a process of the DAMFO algorithm for data collection optimization is shown in the flowchart.

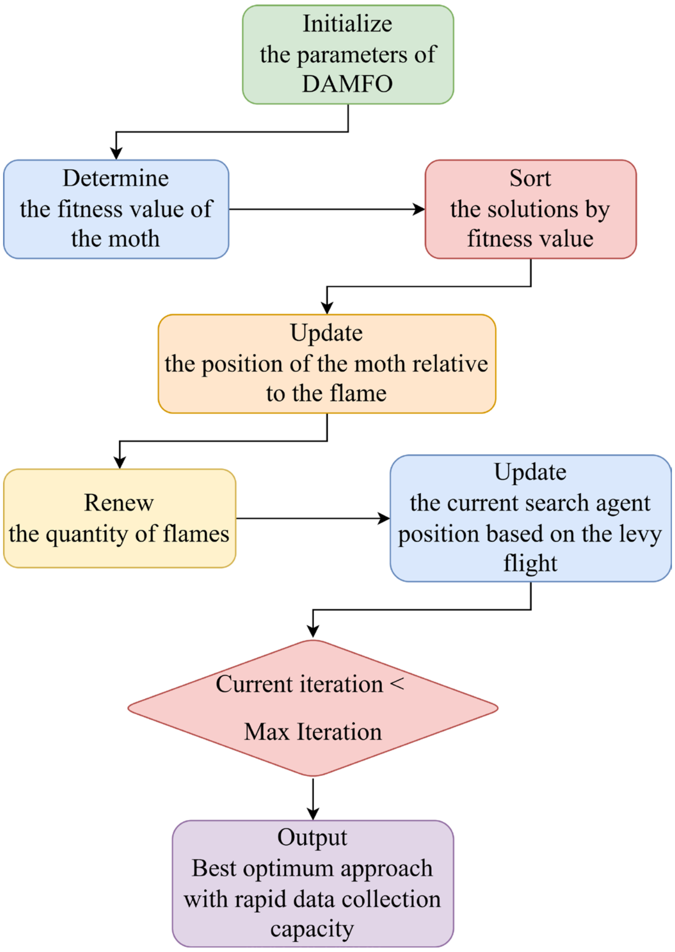

Fig. 6: Flowchart of the DAMFO algorithm.

Algorithm 2: DAMFO

Step 1: Initialization: Set the parameters for the algorithm, including the population size, initial positions of the moths, and the maximum number of iterations.

Step 2: Fitness Evaluation: Calculate the fitness value for each moth based on the objective function.

Step 3 Sorting: Sort the moths based on their fitness values in descending order.

Step 4 Position Update: Update the positions of the moths with respect to the flames using the moth flame optimization strategy.

Step 5 Levy Flight: Update the positions of the moths using the levy flight mechanism, which is a random walk with a power-law step-size distribution.

Step 6 Flame Renewal: Renew the number of flames based on their fitness values.

Step 7 Iteration Check: Check if the current iteration is less than the maximum number of iterations. If yes, go back to step 2. Otherwise, proceed to step 8.

Step 8 Output: Output the best optimal path obtained by the algorithm, along with its data gathering capacity.

It starts with parameter initialization and the calculation of the fitness of moths (solutions), which are sorted in the order of performance. The positions of the moths are updated in terms of flames (optimal solutions), and their flights are made faster using levy flight for exploration. There are adaptive flames, and iteration is performed until the final iteration with the result being an optimal strategy possessing fast data acquisition ability.

Overall, the DAMFO algorithm aims to find the optimal solution to a given problem by simulating the behavior of dragonflies and moths. The dragonfly algorithm is used to explore the search space, while the moth flame optimization strategy is used to exploit promising regions. The combination of these two techniques allows the DAMFO algorithm to effectively balance exploration and exploitation, leading to efficient and accurate solutions.

In cluster-based WSN, hybrid DAMFO-IWQPSO-HS algorithms optimize adaptively collected data, provide multiple routes security, and ensure energy utilization. It is a much safer and efficient scheme for transmitting longer network life span capable of leveraging changing

Algorithm 3: Hybrid DAMFO-IWQPSO-HS Algorithm

Step 1. Initialization: Define the WSN parameters including node positions, cluster formation, energy levels, sensing area, and transmission range.
Initialize DAMFO, IWQPSO, and HS parameters:
DAMFO: Parameters related to dynamic path factor (such as node energy, link reliability, and distance).
IWQPSO: Particle positions; velocities;inertia weight w; learning coefficients C1, C2;and quantum parameters.
HS: HM, HMCR, and PAR.

Step 2. Fitness Function Definition: The fitness function $F_{fitness}$ aims to minimize energy consumption, maximize networklifetime, and ensure security and reliable data aggregation.

$$F_{fitness} = \alpha_1.E_{residual} + \alpha_2.L_{lifetime} + \alpha_3.Q_{sensing} + \alpha_4.S_{security} \quad (14)$$

where $E_{residual}$: Residual energy of nodes. $L_{lifetime}$: Network lifetime. $Q_{sensing}$: Sensing quality based on data aggregation efficiency. $S_{security}$: SL of multipath routing. : α_1, α_2, α_3, and α_4: Weights assigned to different performance metrics.

Step 3. Dynamic Adaptive Multi-Factor Optimization (DAMFO)
Path selection based on dynamic factors: DAMFO evaluates paths dynamically based on node energy, distance, reliability, and link quality.Dynamic factor D_{factor} for path x is calculated as:

$$D_{factor}(x) = \frac{E_{node}(x)}{d(x,y)}.R_{link}(x,y) \quad (15)$$

Where $E_{node}(x)$: Energy of node x.$d(x,y)$: Distance between nodes x and y.$R_{link}(x,y)$: Link reliability between nodes x and y.Optimal path selection: Paths with higher D_{factor} values are selected for routing.

Step 4 IWQPSO
Particle Velocity and Position Update: The positions and velocities of particles are updated using standard PSO equations with quantum enhancements.

$$v_x(t+1) = w.v_x(t) + c_1.r_1.(Pbest - i_x(t)) + c_2.r_2.(g_{best} - i_x(t)) \quad (16)$$

$$i_x(t+1) = i_x(t) + v_x(t+1) \quad (17)$$

where: $v_x(t)$: Velocity of particle x at time t. $i_x(t)$: Position of particle x at time t. w: Inertia weight to balance exploration and exploitation. P_{best}: Best position of particle x. g_{best}: Global best position of the swarm.
Quantum Behavior: Quantum behavior is introduced to enhance exploration by updating positions probabilistically:

$$D_{factor}(x) = \frac{E_{node}(x)}{d(x,y)}.R_{link}(x,y) \quad (18)$$

variables of DAMFO, optimization through quantum of IWQPSO, and even through memory of HS.

Algorithm 3: Continued

where β is the quantum coefficient and is a random number between 0 and 1.

Step 5: Harmony Search (HS) Optimization
Memory Consideration: Select a solution from HM with a probability based on HMCR:

$$i_{new}(x) = \begin{cases} i_{HM}(x) \, if \, r < HMCR \\ random\,value\,otherwise \end{cases} \quad (19)$$

Pitch Adjustment: Fine-tune the solution by making slight adjustments based on the PAR:

$$i_{new}(x) = i_{new}(x) + PAR.\delta \quad (20)$$

where δ is a small value for adjusting the position.
HM Update: If the new solution is better than the worst solution in HM, update the memory by replacing the worst solution.

Step 6: Security and Data Aggregation
Multipath Routing: More than one path is chosen in accordance with DAMFO conditions and optimized using IWQPSO and HS for safe as well as energy-saving routing.

Data Aggregation: Threshold-based data aggregation is employed to reduce redundant data transmission and save energy.

Step 7: Termination Criteria
The algorithm continues until convergence or until a given number of iterations are attained.Convergence is indicated by no significant improvement in fitness function values within a given number of iterations.

Results and Discussions

This subsection describes the main experimental setup and most important parameters used in measuring the performance of the proposed DAMFO and IRSA scheme. Compared to this, EC, NLT, Throughput, PDR, and latency are used to gauge the running performance of the proposed task, as explained below. Most importantly, by identifying the best channel for data transmission, the solution in question guarantees the security and effectiveness of WSNs. It is achieved by combining the IRSA technique with the DAMFO approach into a system.

Simulation Parameters of DAMFO

The experiment site is discussed in this context and thus simple steps to determine the efficiency of the proposed DAMFO and IRSA techniques discussed in Table 4 are used. The above research is compared with another research to compare the efficiency of the proposed research which is discussed below with parameters like EC, NLT, Throughput, PDR and delay. The proposed method here offers a power-efficient, secure optimal path for data communication and hence enhances WSNs in efficiency and security terms. This is achieved by applying Dynamic Adaptive Multi-Factor Optimization (DAMFO) algorithm in conjunction with IRSA Scheme. P- and q-bit lengthsaretypically chosen to be 512 bits and higher to offer approximately 128-bit security. Therefore, the security of encryption relies purely on parameter, that is, key size, which is dependent on n. This new method includes optimizations over the vulnerabilities of classical RSA and hence making it more secure for secure communication.

DAMFO-IWQPSO-HS using IRSA is less energy-intensive and uses the safe shortest path, reducing network attacks. All SNs are of equal energy consumption as a

Table 4: Simulation parameters.

Parameter	Description	Value/Setting
Prime Number *P*	First large prime number	Example: 61
Prime Number *q*	Second large prime number	Example: 53
Modulus n	Products of *p* and *q*	$n = p \times q$
Euler's Totient ∅(*n*)	Totient function value	∅(*n*) = (*p* − 1)(*q* − 1)
Public Exponent e	Chosen public exponent	Example: 65537
Private Exponent d	Modular inverse of e modulo ∅(*n*)	Computed using extended euclidean algorithm
Bit Lengths of p and q	Size of prime numbers	512 bits or higher
Security Level	Desired level of security	High (e.g., 128-bit security)
Key Size	Size of public and private keys	Depends on n
Encryption Algorithm	Type of encryption algorithm used	RSA with improvements

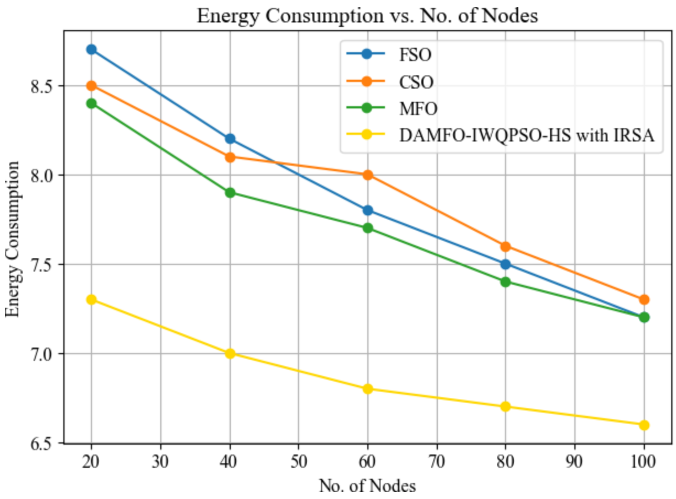

Fig. 7: The proposed DAMFO-IWQPSO-HS with IRSA comparative analysis with respect to EC.

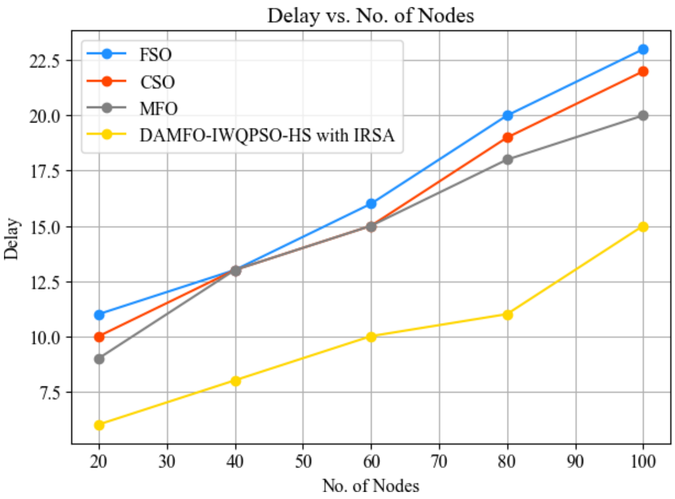

Fig. 9: Proposed DAMFO-IWQPSO-HS with IRSA comparative analysis with respect to delay.

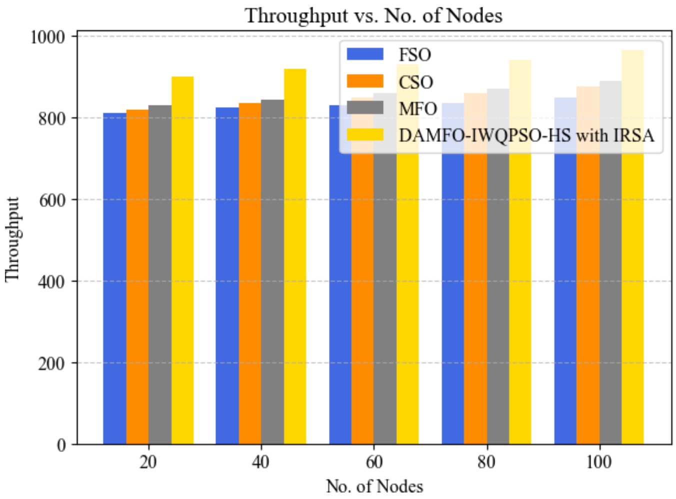

Fig. 8: The proposed DAMFO-IWQPSO-HS with IRSA analysis with respect to throughput.

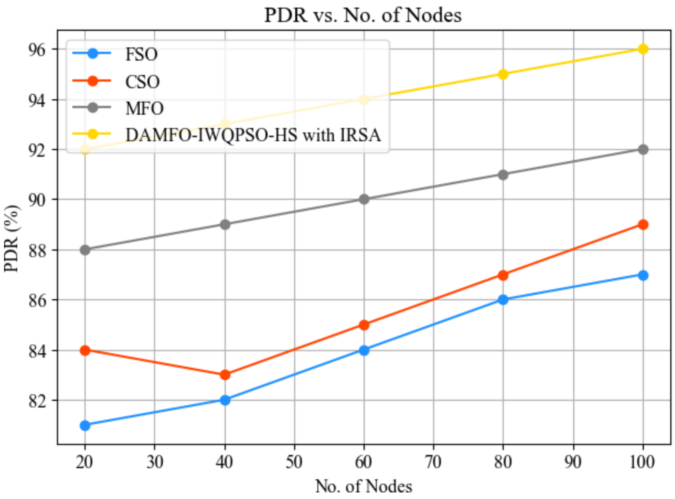

Fig. 10: The proposed DAMFO-IWQPSO-HS with IRSA comparative analysis with respect to PDR.

result, and unlike other research works, this model leaves the nodes with more residual energy. Figure 7 illustrates the results obtained using both the existing approaches and the one proposed by DAMFO-IWQPSO-HS using IRSA. To make a comparison with EC, the value of SN is adjusted from 20 to 100. The newDAMFO-IWQPSO-HS with IRSA offers 7.2-EC for 20 nodes, which is lower than other competing methods. For nodes ranging from 40 to 100, the newDAMFO-IWQPSO-HS with IRSA also offers the smallest EC rates.

Figure 8 shows the throughput performance of different optimization algorithms in relation to the network size in number of nodes. The proposed DAMFO-IWQPSO-HS with IRSA always has a high throughput in comparison to FSO, CSO, and MFO at all node numbers. The throughput of all algorithms is on the rise as the number of nodes grows, and the proposed approach has a better scalability and efficiency. This shows that DAMFO-IWQPSO-HS that is used with IRSA has the capability of optimizing network performance at varying network densities.

The deployment of the trust mechanism gives security to the SNs, and the trust management helps in identifying the MNs. The reliable CH is used for secure DA. Compared to existing techniques that currently exist, DAMFO-IWQPSO-HS with IRSA has a greater tendency of obtaining a better throughput and improving the accuracy of routes' validity. Throughput of the proposed DAMFO-IWQPSO-HS with IRSA versus current approaches is presented in Figure 9.To select an environment-friendly and energy-efficient solution, the proposed system also takes into account the maximum path trust and shortest distance path while computing the fitness. This enhances the ability to collect information quicker and accelerate the travel to the destination. Figure 9 showsthe results obtained using the existing methods and the suggested DAMFO-IWQPSO-HS with IRSA under delay.

Packet losses due to MN in the DAMFO are avoided in WSN secure data transmission because of a successful TE scheme and IRSA. IRSA encrypts information obtained prior to sending it to the BS with the aim of helping to avoid unauthorized use of the information. Figure 10 illustrates the packet delivery rate. Increased ability of the techniques in packet delivery from source to destination is indicated by their highest PDR rate.

Cluster establishment and cluster head election are most important factors to influence NLT improvement. Network NLT improves with the reduction of energy consumption. Trust system removes MNs and securely exchanges data among SNs through an extremely useful, trusted ideal channel utilizing DAMFO-IWQPSO-HS with the IRSAmethod in Figure 11.

The detection rates show the efficiency with which all systems are able to detect MN in a WSN.The proposed system performs better at all levels of MN insertion. Values are exemplary; results would be calculated using individual simulations and testing in a controlled environment presented in Table 5.

Figure 12 shows the detection rate comparison of different algorithms when the MN ratio is altered. The proposed system outperforms PSO, CSO, and MFO under all circumstances with a high and uniform detection rate even at 50% MN. Although all algorithms are bad for more MN, the proposed system is more reliable and stronger in unfriendly network environments.

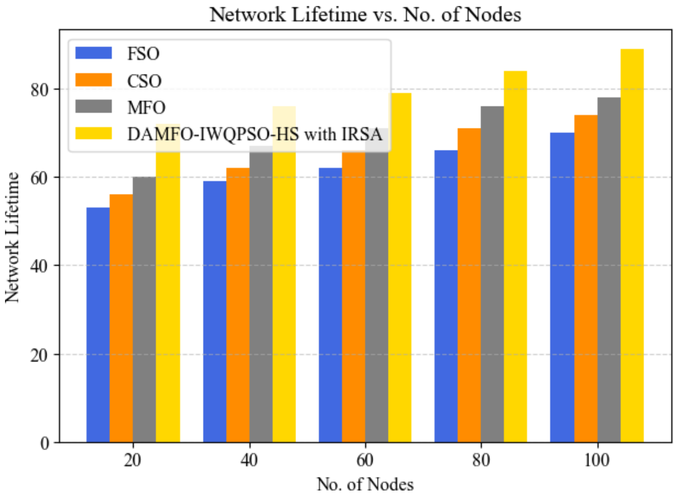

Fig. 11: The proposed DAMFO-IWQPSO-HS with IRSA comparative analysis with respect to network lifetime.

Time is in milliseconds (ms).The system under consideration exhibits improved performance in key generation time at all levels of MN over other systems in Table 6. Values are representative; actual performance would vary with implementations and trials. Key generation times are the durations that would be expended for the generation of the encryption key and decryption key. In the IRSA algorithm employed in the above combined method, generation of keys is made easier so that the cryptographic keys are produced as quickly and securely as possible to ensure that secure communication channels are established almost immediately. With this, the suggested system enhances the security and efficiency of the multipath routing in cluster-based WSN.

Figure 13 illustrates the time taken in key generation by various algorithms with MN on the rise. The proposed

Table 5: Comparison ofdetection rate.

Degree of Malicious Nodes (%)	Proposed System Detection Rate (%)	PSO Detection Rate (%)	CSO Detection Rate (%)	MFO Detection Rate (%)
0	99	96	91	93
10	99	91	86	89
20	96	86	81	85
30	93	81	76	81
40	89	76	71	77
50	86	71	66	73

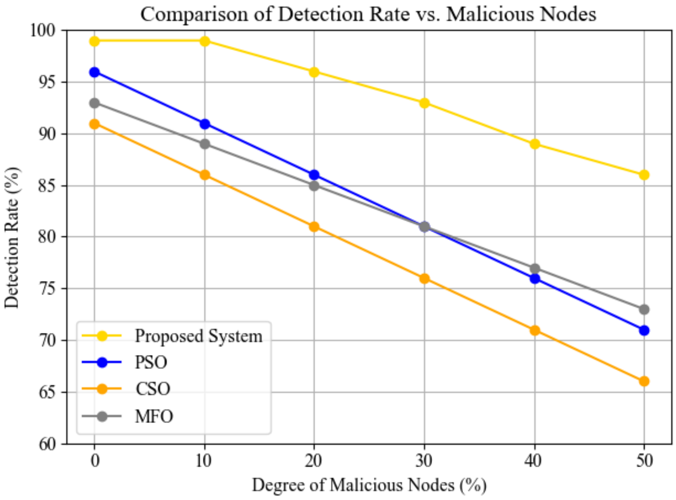

Fig. 12: Comparison chart ondetection rate.

system has the minimum time for key generation at all levels of malicious activity, followed by PSO, CSO, and MFO. With an increase in compromised network, all methods display extra generation time, with the proposed system being the most effective method with better scalability and resilience.

Encryption time is the time it takes to encrypt a message from plaintext to ciphertext using the assistance of a cipher. Hybrid DAMFO-IWQPSO-HS presumes that the encryption operation in search of exchanging safe information at a high rate improves and optimizes to effectively alleviate latency to the bits. The Hybrid DAMFO-IWQPSO-HS assumes that the encryption process of search of exchanging secure information at a high rate enhances and optimizes to actually reduce latency to the bits. This is particularly true for real-time operations where timely delivery of the data is essential, as indicated in Table 7.

Figure 14 plots the comparison of the encryption time of different techniques proposed in the system, namely, PSO, CSO, and MFO,when MN are increased from 0% to 50%. The proposed system shows minimum encryption time in all scenarios, which means greater efficiency and immunity from malicious operations. Conversely, MFO shows maximum encryption time, which represents lower performance for the same scenario. This shows the greater scalability and lightweight nature of the proposed system.

Decryption time is the time takenfor decrypting and transforming the encrypted data into normal readable form called the plaintext. In a friendly context, decryption time plays a vital role for efficient data reconstruction upon reception As it has been emphasized, in the networks where malicious sensor nodes are very dense, Table 8 shows the influence of security measures on overheads. Efforts toward maximizing decryption efficiency are on top of the recommended system in this study maintaining strict security controls to facilitate enhanced original fast response of the network.

Figure 15 illustrates the comparison of decryption time between various techniques in the proposed system,

Table 6: Comparison ofkey generation time.

Degree of Malicious Nodes (%)	Proposed System Key Generation Time (ms)	PSO Key Generation Time (ms)	CSO Key Generation Time (ms)	MFO Key Generation Time (ms)
0	6	7	8	9
10	7	8	9	11
20	8	9	11	12
30	9	11	12	13
40	11	12	13	14
50	12	13	14	15

Table 7: Comparison ofencryption time.

Degree of Malicious Nodes (%)	Proposed System Encryption Time(ms)	PSO Encryption Time (ms)	CSO Encryption Time (ms)	MFO Encryption Time (ms)
0	11	13	14	15
10	12	14	15	16
20	13	15	16	17
30	14	16	17	18
40	15	17	18	19
50	16	18	19	20

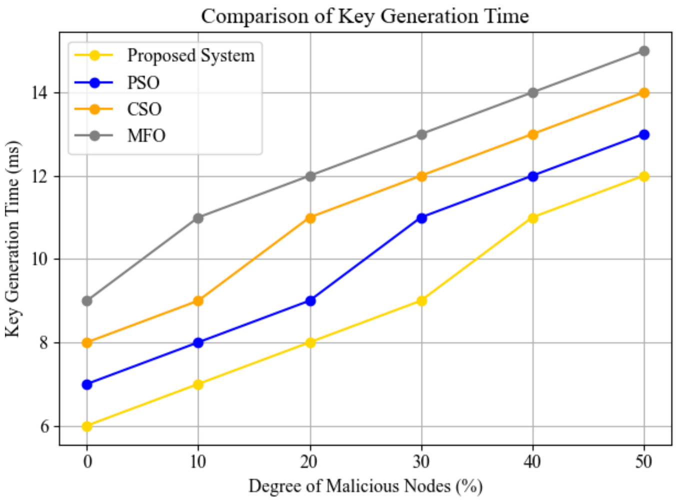

Fig. 13: Comparison chart ongeneration time.

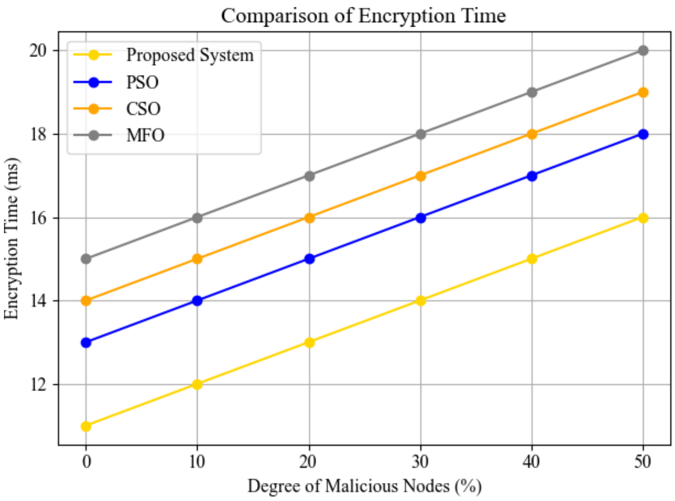

Fig. 14: Comparison chart onencryption time.

namely, PSO, CSO, and MFO, against various percentages of MN. The proposed system indicates the least decryption time for each percentage of MN, testifying forits computational efficiency. On the other hand, MFO indicates the maximum decryption time, signifying lesser applicability against adversarial environments. This verifies the dominance of the proposed system in fast recovery of data in the wake of increasing threats.

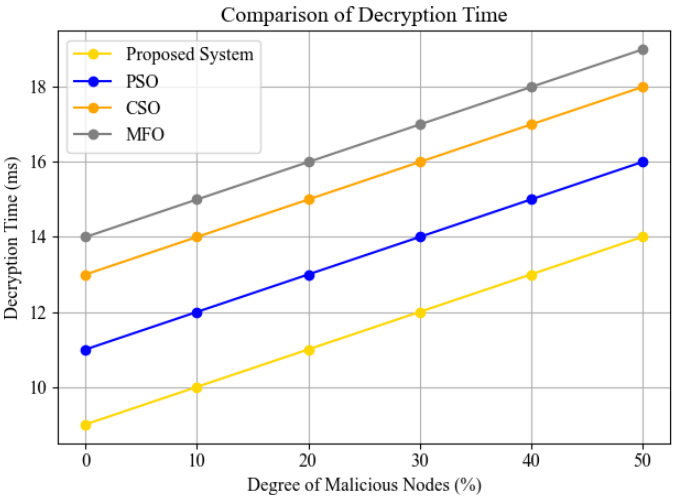

Fig. 15: Comparison chart ondecryption time.

Table 8: Comparison ofdecryption time.

Degree of Malicious Nodes (%)	Proposed System Decryption Time (ms)	PSO Decryption Time (ms)	CSO Decryption Time (ms)	MFO Decryption Time (ms)
0	9	11	13	14
10	10	12	14	15
20	11	13	15	16
30	12	14	16	17
40	13	15	17	18
50	14	16	18	19

Conclusions

The hybrid DAMFO-IWQPSO-HS algorithm shows improvement over the existing optimal path decision data aggregation and secure energy efficient multipath routing in cluster-based WSN. A novel hybrid method combining the benefits of the DAMFO algorithm, IWQPSO algorithm, and HS algorithm is presented in this paper with a target of solving the key energy management and security problems. Characteristics like load transport reliability with adjustable path choice has a tendency of ensuring the maximum lifespan of the network by optimizing energy conservation.Apart from all the above enhancements, IRSA algorithm within network security ensures the maximum security of the routing phase. IRSA possesses an elevated degree of security capacity that is apt to resist malicious attacks on sensor nodes and other threats to the security of information which must be transmitted securely by upholding its confidentiality and integrity. This secondary layer of security is of paramount importance in an endeavor to prevent vulnerabilities, such as eavesdropping, data modulation, and unauthenticated access, that are exceedingly prevalent in a resource-constrained environment such as WSN. The result proves hybrid DAMFO-IWQPSO-HS-IRSA to be excellent in the PDR, with fewer energy consumptions and fewer latencies compared to other routing protocols. The well-structured multipath characteristic of the routing with secure delivery through energy optimized routes and security through robust encryption processes proves useful utilization of this algorithm for constrained resource-deprived dynamic WSN scenario. Thus, the hybrid DAMFO-IWQPSO-HS-IRSA algorithm improves network performance and sets up a secure and efficient communication channel that proves to be an optimal method for future WSN applications.

References

1. Verma, V., &Jha, V.K. (2024). Secure and energy-aware data transmission for IoT-WSNs with the help of cluster-based secure optimal routing. Wireless Personal Communications, 134(3), 1665–1686.
2. Dan, F., Ma, Y., Yin, W., Yang, X., Zhou, F., Lu, S., & Ning, B. (2024). An accuracy-aware energy-efficient multipath routing algorithm for WSNs. Sensors, 24(1), 285.
3. Fatima, M., Krishnan, S., &Nayanam, K. (2024). Energy-efficient and secure routing protocols for WSN architectures, strategies, and performance. Energy, 4(1). Article 19536
4. Selvi, M., Kalaiarasi, G., Mana, S.C., Yogitha, R., & Padmavathy, R. (2024). Energy and security aware hybrid optimal cluster-based routing in wireless sensor network. Wireless Personal Communications, 1-28.
5. Rajaram, V., Pandimurugan, V., Rajasoundaran, S., Rodrigues, P., Kumar, S.S., Selvi, M., &Loganathan, V. (2024). Enriched energy optimized LEACH protocol for efficient data transmission in wireless sensor network. Wireless Networks, 1-16.
6. Abujassar, R.S. (2024). A novel algorithm for the development of a multipath protocol for routing and energy efficient in IoT with varying density. Telecommunication Systems, 1-15.
7. Fan, B., &Xin, Y. (2024). EBPT-CRA: A clustering and routing algorithm based on energy-balanced path tree for wireless sensor networks. Expert Systems with Applications, 125232.
8. He, S., Li, Q., Khishe, M., Salih Mohammed, A., Mohammadi, H., &Mohammadi, M. (2024). The optimization of nodes clustering and multi-hop routing protocol using hierarchical chimp optimization for

sustainable energy efficient underwater wireless sensor networks. Wireless networks, 30(1), 233–252.

9. Ali, A., Ali, A., Masud, F., Bashir, M.K., Zahid, A.H., Mustafa, G., & Ali, Z. (2024). Enhanced fuzzy logic zone stable election protocol for cluster head election (E-FLZSEPFCH) and multipath routing in wireless sensor networks. Ain Shams Engineering Journal 15(2), 102356.
10. Tumula, S., Ramadevi, Y., Padmalatha, E., Kiran Kumar, G., VenuGopalachari, M., Abualigah, L., ... & Kumar, M. (2024). An opportunistic energy-efficient dynamic self-configuration clustering algorithm in WSN-based IoT networks. International Journal of Communication Systems, 37(1), e5633.
11. Yang, L., Zhang, D., Li, L., & He, Q. (2024). Energy efficient cluster-based routing protocol for WSN using multi-strategy fusion snake optimizer and minimum spanning tree. Scientific Reports, 14(1), 16786.
12. DharmaTeja, M., & Srinivasan, R. (2024). Secure and energy efficient-based clustering and routing protocol of WSN using MCSA. Journal of Computational Analysis and Applications, 33(2), 206–219.
13. Chandrasekaran, S.K., &Rajasekaran, V.A. (2024). Energy-efficient cluster head using modified fuzzy logic with WOA and path selection using enhanced CSO in IoT-enabled smart agriculture systems. The Journal of Supercomputing, 80(8), 11149–11190.
14. Jamaesha, S.S., Kumar, R.S., &Gowtham, M.S. (2024). Cluster based hybrid optimization and kronecker gradient factored approximate optimum path curvature network for energy efficiency routing in WSN. Peer-to-Peer Networking and Applications, 1–22.
15. Qamar, M.S., ulHaq, I., Daraz, A., Alamri, A.M., AlQahtani, S.A., &FahadMunir, M. (2024). A novel approach to energy optimization: Efficient path selection in wireless sensor networks with hybrid ANN. Computers, Materials & Continua, 79(2). 2945–2970
16. Arunkumar, K. (2024). A HSEERP—Hierarchical secured energy efficient routing protocol for wireless sensor networks. Peer-to-Peer Networking and Applications, 17(1), 163–175.
17. Wang, H., Liu, K., Wang, C., & Hu, H. (2024). Energy-efficient, cluster-based routing protocol for wireless sensor networks using fuzzy logic and quantum annealing algorithm. (13), 4105.
18. El Khediri, S., Selmi, A., Khan, R.U., Moulahi, T., & Lorenz, P. (2024). Energy efficient cluster routing protocol for wireless sensor networks using hybrid metaheuristic approaches. Ad Hoc Networks, 158, 103473.
19. Lei, C. (2024). An energy-aware cluster-based routing in the Internet of things using particle swarm optimization algorithm and fuzzy clustering. Journal of Engineering and Applied Science, 71(1), 135.
20. Prasad, V., &Roopashree, H.R. (2024). Energy aware and secure routing for hierarchical cluster through trust evaluation. Measurement: Sensors, 33, 101132.
21. Meenakshi, N., Ahmad, S., Prabu, A.V., Rao, J.N., Othman, N.A., Abdeljaber, H.A., ... & Nazeer, J. (2024). Efficient communication in wireless sensor networks using optimized energy efficient engroove leach clustering protocol. Tsinghua Science and Technology, 29(4), 985–1001.
22. Goud, B.H., Shankar, T.N., Sah, B., & Aluvalu, R. (2024). Energy optimization in path arbitrary wireless sensor network. Expert Systems, 41(2), e13282.
23. Jalalinejad, H., Hajiabadi, M.R., Hosseinabadi, A.A.R., Mirkamali, S., Abraham, A., Weber, G.W., & Parikh, J. (2024). A hybrid multi-hop clustering and energy-aware routing protocol for efficient resource management in renewable energy harvesting wireless sensor networks. IEEE Access. Article 103479
24. Krishnamoorthy, R., Tanaka, K., & Begum, M.A. (2024, June). Enhanced cluster-assisted routing protocol for improved energy efficiency of wireless sensor network. In *2024 International Conference on Smart Systems for Electrical, Electronics, Communication and Computer Engineering (ICSSEECC)* (pp. 609–614). IEEE.
25. Hu, H., Fan, X., & Wang, C. (2024). Energy efficient clustering and routing protocol based on quantum particle swarm optimization and fuzzy logic for wireless sensor networks. Scientific Reports, 14(1), 18595.
26. Ramalingam, S., Dhanasekaran, S., Sinnasamy, S.S., Salau, A.O., & Alagarsamy, M. (2024). Performance enhancement of efficient clustering and routing protocol for wireless sensor networks using improved elephant herd optimization algorithm. Wireless Networks, 30(3), 1773–1789.
27. Vellela, S.S., & Balamanigandan, R. (2024). Optimized clustering routing framework to maintain the optimal energy status in the WSN mobile cloud environment. *Multimedia Tools and Applications*, *83*(3), 7919-7938.
28. Jiao, W., Tang, R., & Zhou, W. (2024). Delay-sensitive energy-efficient routing scheme for the wireless sensor network with path-constrained mobile sink. Ad Hoc Networks, 158, 103479.
29. Kiran Kumar, G., K Prashanth, S., Padmalatha, E., Venkata Krishna Reddy, M., Rama Devi, N., Abualigah, L., ... & Kumar, M. (2024). An optimized meta-heuristic clustering-based routing scheme for secured wireless sensor networks. International Journal of Communication Systems, e5791.
30. Kaviarasan, S., & Srinivasan, R. (2024). Developing a novel energy efficient routing protocol in WSN using adaptive remora optimization algorithm. Expert Systems with Applications, 244, 122873.
31. Prakash, V., Singh, D., Pandey, S., Singh, S., & Singh, P.K. (2024). Energy-optimization route and cluster head selection using M-PSO and GA in wireless sensor networks. Wireless Personal Communications, 1–26.
32. Saemi, B., &Goodarzian, F. (2024). Energy-efficient routing protocol for underwater wireless sensor networks using a hybrid metaheuristic algorithm. Engineering Applications of Artificial Intelligence, 133, 108132.
33. Sharma, A., &Kansal, A. (2024). Enhanced CH selection and energy efficient routing algorithm for WSN. Microsystem Technologies, 1–13.
34. Roopa Devi, E.M., Hemalatha, T., Usha, D., & Nanda, A.K. (2024). An optimal multipath routing protocol using hybrid gravitational search particle swarm optimization for secure communication. International Journal of Communication Systems, 37(7), e5731.
35. Teja, M.D., & Srinivasan, R. (2024). Multi-objective trust-aware dynamic weight pelican optimization algorithm for secure cluster head and routing selection in WSN. Journal of Electrical Systems, 20(3s), 89–102.
36. Flammini, F., & Trasnea, G. (2025). Battery-powered embedded systems in IoT applications: Low power design techniques. SCCTS Journal of Embedded Systems Design and Applications, 2(2), 39–46.

37. James, A., Elizabeth, C., Henry, W., & Rose, I. (2025). Energy-efficient communication protocols for long-range IoT sensor networks. Journal of Wireless Sensor Networks and IoT, 2(1), 62–68.

38. Karthika, J. (2025). Sparse signal recovery via reinforcement-learned basis selection in wireless sensor networks. National Journal of Signal and Image Processing, 1(1), 44–51.

39. Sadulla, S. (2024). Development of a wireless power transfer system for low-power biomedical implants using resonant RF coupling. National Journal of RF Circuits and Wireless Systems, 1(2), 27–36.

40. Uvarajan, K.P. (2024). Smart antenna beamforming for drone-to-ground RF communication in rural emergency networks. National Journal of RF Circuits and Wireless Systems, 1(2), 37–46.