EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

# A Trust Based Energy Efficient Routing Design Based on Hybrid Particle Swarm Optimization (HPSO) for Wireless Sensor Networks

S.Gnana Selvan[1], G.Gifta Jerith[2], C.Mahesh[3], S.Ravikumar[4], S.Samsudeen Shaffi[4], S.Jagadeesh[4,*]

[1]Department of Electronics and Communication Engineering, Jayaraj Annapackiam CSI College of Engineering, Tuticorin, Tamilnadu, India.
[2]Dept. of CSE(Artificial Intelligence and Machine Learning), School of Engineering, Malla Reddy University, Hyderabad, India.
[3]Department of Computer Science and Engineering Emerging Technologies, SRM Institute of Science and Technology Vadapalani Campus, Tamilnadu, India.
[4] Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu, India.

## Abstract

Congestion in wireless sensor networks (WSNs) reduces resource availability, often leading to sensor node failures and misbehavior. Additionally, high energy consumption decreases the overall lifespan and performance of the network. To address these limitations, this paper presents a trust-based and congestion-aware optimization method for WSNs. The proposed strategy consists of two main stages. In the first stage, congestion levels and node trust values are evaluated to derive an optimal congestion metric. In the second stage, a Hybrid Particle Swarm Optimization (HPSO) algorithm is applied to determine optimal data routing paths from Sensor Nodes (SNs) to the Base Station (BS), considering both distance and trust-congestion parameters. The proposed HPSO combines the immigration and emigration processes of the Biogeography-Based Optimization (BBO) algorithm with the mutation process of Particle Swarm Optimization (PSO) to achieve efficient data distribution. Experimental comparisons with existing methods demonstrate that the proposed approach significantly improves performance in terms of energy consumption, latency, packet delivery ratio (PDR), and network lifetime.

**Keywords:** Trust congestion, HPSO, congestion index, Transmission, latency, Packet Delivery Ratio (PDR)

Received on 29 May 2025, accepted on 12 August 2025, published on 16 September 2025



doi: 10.4108/eetiot.9427

## 1. Introduction

WSN consist of small device referred as sensor nodes that has low power battery, restricted storage and the least computational capacities employed in a biological area for sensing, communicating and collecting the data. WSN is utilized for determining the pressure and temperature, military surveillance, health monitoring and more, but it has some limitations in computing power, energy, and security [1]. Because of certain limitation of source and power computation of the SN, trust, as well as the energy, is the two significant parameters of estimation. WSN consists of the base stations and various distributed sensor node via the sensing of definite physical factors that communicates with the environment. The nodes in the WSN depend upon their restricted, non-changeable, and non-rechargeable batteries. In addition to this nodes are restricted to memory, processing capacities, and storage [2].Through the relay nodes, the data collected by the sensor nodes reaches the sink node. Any time information has to be sent from a collection of wireless nodes to a central location, or "sink," the selection of the next

*Corresponding author. Email: jagadeesh15.sj@gmail.com

forwarder is a crucial step [3]. If there is a great distance between the SN and the BS, a wide-scale WSN will have a high number of nodes via which the data packet will be relayed. Effective forwarder selection through distributed decision making is crucial for efficient routing. So, the various nodes in the network must send the information they've collected to the sink node through multi-hop routing paths within their range. [4].

As part of multi-hop routing, all sensor nodes must be willing to share their data with one another and any intermediate nodes. The WSNs power optimization is a significant performance measure due to the accessibility of least power battery in the sensor node that depends on the configuration. The energy utilization is decreased by employing smart decision-making methods depends upon the rule and clustering of node for efficient routing [5]. The majority of the WSN's drawbacks are because of the resource limitation objects. The open range WSN sensors are constantly susceptible to harsh environmental issues with respect to humidity, dust, high temperature, snow, pressure, etc., that affect the WSN operation. Additionally, the issues in WSN composed of stability, restricted communication capacity, restricted constrained resources, mobility, availability, accountability, bandwidth, integration, precision, heterogeneity, technology, denial of service attack (DoS), trust, and unmanageable atmosphere [6]. The main issues in the WSN are the power consumption and in addition to this security are considered as the major important concern. Therefore, the majority of the researchers are working to decrease energy usage by using the routing algorithm. In order to acquire the battery energy usage in any uncontrolled scenarios, security is one of the major goals in WSN [7]. In spite of authentication and encryption for routing information provided by routing protocols, malevolent nodes nevertheless contribute to the network under the guise of a legitimate node, allowing them to overcome the flaws of a number of routing methods. Due to the need of proper network procedure, security is seen as severely susceptible to WSN, and the routing process is the target of attackers. WSNs are classified into unstructured as well as structured network types. The gatherings of dense sensor networks are employed in the ad-hoc nature are termed as unstructured WSN. When the entire nodes are employed based on the pre-planned way, and then the network is termed as structured WSN [8].

The robust trust aware routing structure is utilized to create the safe multi-hop routing in the active WSN against dangerous attacker utilizing the repeating the routing information. Securities as well as the energy-efficient displaced routing by the secret-sharing method randomly distributes through the entire network in the first two phases and then forwards to the sink node. WSN is an anxious environment because of the most critical attacks that are established on various node by the attacker [9]. Few attacks that are conceded out at the routing level are spoofing, Sybil, denial of service, black hole attacks. Considering all the above-stated attacks, DoS attack is a significant security issue. Hence, most of the researchers are creating a novel secure routing protocol for protecting the WSN. When a node in a WSN is compromised and used in an attack, the network as a whole experiences an increase in its energy usage. Thus, by ignoring the malicious attempts, the sensor nodes are able to save energy [10].

This study suggests a split into two major sections. First, we check the network's congestion and assess the reliability of its nodes. Therefore, the best possible congestion metric may be attained. Next, the Hybrid Particle Swarm Optimization (HPSO) algorithm is used to regulate the finest path for each packet as it travels from the source node to BS, taking into account both distance and trust congestion parameters. The following is the paper's main result, which shows the contribution of the paper.

- Evaluating trust value and congestion state among various nodes to obtain optimal congestion metric.
- Proposing a hybrid particle swarm optimization algorithm to obtain an optimal data routing protocol.
- Testing the efficacy of the system by comparing it to similar methods already in use.

Here's how you can get your hands on the rest of the paper: We will look at the previous literature assessments of the WSN's trust-based energy-efficient routing protocol in Section 2. In Section 3, we see the suggested method in action over two distinct time periods. The comparison analysis and discussion of simulation outcome are presented in Section 4. Part 5 is where the article wraps up.

## 2. Literature Survey

As a means of ensuring the dependability, response time consistency, and security of WSNs, Bashar A. devised a multi-tier sustainable secure routing protocol. This strategy improves safety and reduces the shortfall that results from lost data. Throughput, packet delivery ratio, energy use, latency and network lifetime were among the metrics we examined in the performance evaluation [11]. Qabouche H introduced a new hybrid energy-efficient static routing protocol (HEESR) that combines the multi-hop and clustering methodologies to build a network that can accept and route data while using as little energy as feasible. The simulation results were shown via the usage of throughput, stability, network residual energy and lifespan. The network's lifetime is extended while power consumption is decreased [12].

Dhand G. et al. developed a secure multi-tier energy-effective routing protocol that employs a Miscegenation of Ant Lion optimizer within K-means for clustering and a Spherical grid-based multi-curve Elliptic curves cryptography routing to minimise power consumption and improve data security. parameters such End-to-End latency, PDR, throughput, reliability and power consumption were employed during testing. This method was used to increase the security and reliability of the wireless communication system [13]. For networks to last longer while using less power, Srikanth N. and Prasad MS. proposed a trusted-node based routing protocol. The experimental results were proven

across a number of metrics, including throughput, network loss, network longevity, and energy usage. Lowered energy usage is one of the many benefits of this approach [14].
Uddin MA, et al. introduced a novel way to selecting cluster heads and a mechanism for generating routing paths to create an adequate and secure cluster-based routing protocol (ESCRP) for WSN. Network uptime, dependability, power consumption, and throughput were used in the performance evaluation. Assuring appropriate privacy and security in WSN [15] is achieved by the discovery of this approach of measuring dependability and trust. As a means of bolstering WSN security and maximising energy efficiency, Kalidoss T. et al. proposed a Secured Quality of Service (QoS) aware Power Optimization Routing Protocol. Energy use, packet delivery ratio, security, throughput and detection precision were all proved as a consequence of the simulations. An inability to easily control uncertainty was a major drawback of this approach [16].

In order to decrease packet loss in large-scale wireless sensor networks, Khalid NA et al. introduced an adaptive trust-based routing system. Packet loss, energy consumption and latency were among the metrics used to show the experimental findings. This method reduces energy waste and lengthens the useful life of the network [17]. To identify the trustworthy sensor nodes and distinguish them from the malicious ones, Zahedi A. et al. suggested the Energy-aware Trust-based Gravitational Search Approach (ETGSA). For this study, they used the measures of energy consumption, throughput, normalised routing load and latency. There is less of a computational burden with this strategy, and it's more secure against network intrusions [18].To achieve maximum network security while minimising energy consumption, Sun Z et al. suggested a Secure Routing Protocol based on Multi-objective Ant-colony-optimization (SRPMA). Routing workload, packet loss rate, and energy usage were analysed for performance. There are downsides to this method, such as a shorter lifespan and higher failure rate for networks [19]. Cuckoo search optimization technique with fuzzy type-2 logic based clustering scheme was introduced by Mittal N et al. to increase network reliability and longevity. The simulation results were analysed using the performance metrics of interest (i.e., network lifespan, energy consumption, packet delivery ratio and residual energy) [20].

A multi-objective particle swarm optimisation with Levy distribution (MOPSO-L) algorithm-based dynamic clustering and process protocol. [21] Multi-objective parameters should be used in the cluster head selection and routing processes since WSN parameters are related to one another. For organising the clusters and CH selected by merging consolidated and shared models, the proposed MOPSO-L technique is provided. To avoid being caught in local optimums, the MOPSO-L method combines the advantages of the PSO algorithm and the Levy distribution.
Designed a changing evolution that depends on a routing algorithm with more than 1000 forwarding nodes and has more energy-preserving nodes that should be reduced in terms of energy consumption. [22] There are some types of irregular clustering that could produce severely inefficient relay nodes. Particle swarm optimisation (PSO) is inspired by the behaviour of fish schools, flocks of birds, and evolutionary algorithms' random search methods. Nature demonstrates that animals, particularly fish and birds, always move in groups to avoid collisions. This is because each member is followed by a group that modifies each member's position and velocity using group information. As a result, less effort will be required on the part of the individual to look for food, shelter, etc. [23] used PSO for CH election between common sensors without taking into account cluster design difficulties.

In order to save time and fix the threshold value, CH in each cluster completes the information aggregation. The CH is then committed to broadcasting the estimated cumulative information for the CH utilising single hop communication when the communication distance between the CH nodes and the BS is less than the threshold value. Otherwise, CH would use the least expensive neighbouring relay node to find the next hop [24]. Additionally, the choice of this node would rely on its distance and remaining energy.

## 3. Proposed Methodology

This tactic consists of two primary elements. First, we check the network's congestion and assess the reliability of its nodes. As a result, it's feasible to achieve the optimal congestion indicator. In the second phase, data packets are optimally routed from the SN to BS based on two metrics: distance and trust congestion, using the HPSO algorithm. The next paragraphs will provide an in-depth examination of each phase.

### 3.1. Phase-I

In initial phase, the trust hypothesis is employed in detecting the sensor node misbehavior. The nodes containing trust values above the pre-determined threshold level are referred to as trust nodes. Such types of nodes are determined and accordingly, the computation statuses are evaluated. In addition to this, the trust-based congestion metrics are formed for the trusted nodes that are described as valid nodes. The nodes containing trust values below the pre-determined threshold level are ignored for the routing of data packet. In such a case, the congestion metrics are not evaluated for these types of nodes that further lead to reducing the computational overhead and maximizing the lifetime of the battery. The following section describes three major strategies namely: Trust node threshold, node congestion estimation as well as trust estimation [25].

### 3.2 Trust node threshold

Here, the trust value is based on three various measures: leftover nodal energy, packet latency ratio, and packet delivery ratio. All these measures are standardized

with a boundary limit that ranges from 0 to 1. The definitions and mathematical expressions for the above-mentioned parameters are described in the subsequent section.

### Packet transmission ratio

To put it simply, the PDR is the percentage of data that arrived at its destination from the mth to the nth node, relative to the total number of data packets transferred between the two nodes.

### Packet Latency ratio

Each node's latency is expressed as a fraction of the average network delay while sending a data packet to another node.

### Packet nodal energy

The packet nodal energy is the average energy of the mth node and the nth node. Let us assume the existing energy of both the mth and the nth node is $e(m) and e(n)$ respectively. The existing energy of the mth node and nth node represents $e(m) and e(n)$.

$$n(e) = \frac{e(m)+e(n)}{2} \quad (1)$$

Further, sensor node energies are above or near the threshold levels for efficient data packet transmission. The following formula may be used to calculate the mth trust node on the nth trust node.

$$T_{mn} = \frac{W_1 * n(e) + W_2 * p(t) + W_3 * p(l)}{W_1 + W_2 + W_3} \quad (2)$$

From equation (2), the weights employed for packet transmission ratio, packet latency ratio, packet nodal energy are represented by $W_1, W_2 and W_3$; where $W_1, W_2, W_3 \in (0,1)$. $n(e), p(t) and p(l)$ signifies the nodal energy, packet transmission ratio, packet latency ratio respectively.

$$\begin{cases} If T_{mn} > T_t; trust - worthy link \\ If T_{mn} < T_t; untrusted link \end{cases} \quad (3)$$

If a node doesn't have at least one trusted incoming link, we call it malicious, and if it does, we call it genuine.

## 3.3 Node estimation

In this section, the congestion index is employed in estimating the congestion level of the trusted nodes. Here, every individual node is capable of maintaining a queue to store the data packet. The buffer spaces are cleared after the transmission of a particular node to the subsequent nodes. The congestion level and the queue node are increased if the obtained packet rate transmission is lesser than the packet received. In addition to this, the node waits for a pre-determined cycle if the nodes are unable to clear the data packet. The following mathematical expressions derive the evaluation of congestion index with respect to the ith node [26].

Here are some key considerations for evaluating a congestion index in wireless sensor networks:

The mathematical expression for the congestion index with respect to the ith node is derived in equation (4),

$$C_I = \frac{R_{IN}^I + E^I(x-1) - R_{OUT}^I}{R_{IN}^I + E^I(x-1)} \quad (4)$$

From the above equation, the remaining empty space in the queue with respect to the ith node is represented by $E^I(x-1)$. The parameters $R_{IN}^I$ and $R_{OUT}^I$ are explained in the following equation.

$$R_{IN}^I = \frac{\sum_{m=1}^{x-1}(n_{m,I}^q)}{x-1} \quad (5)$$

$$R_{OUT}^I = \frac{\sum_{m=1}^{x-1}(n_{m,I}^r)}{x-1} \quad (6)$$

From equations (5) and (6), $n_{m,I}^q$ and $n_{m,I}^r$ signifies the total number of data packets forwarded to the Ith node in the mth cycle and the various other nodes in the mth cycle.

Congestion in WSNs is represented by the value of the congestion index, which is provided in equation (4) for all reliable nodes. The frequency with which these congestion indices are measured is dynamic and is determined by the specific needs of each networking application.

### Trust Estimation

This section provides the determination of every valid node or trusted nodes.

$$T_{C(mn)} = \beta * C_n + (1-\beta) * T_{mn} \quad (7)$$

From equation (7), the congestion index and the trusted node value with respect to the nth and the mth node is represented by $C_n$ and $T_{C(mn)}$ respectively. $\beta$ signifies the trust coefficient that ranges from [0,1].

## 3.4. Phase-II

This is where a PSO algorithm variant is used to build the data routing protocol (HPSO). In the next section, we will discuss the HPSO, which is an amalgamation of the PSO method and the biogeography based optimization algorithm [27].

### Particle Swarm Optimization Algorithm (PSO)

In the PSO algorithm [28], the searching techniques imitate the swarm behavior in which each individual is described as a particle. The PSO comprises two different vectors namely the position vector and velocity vector. The mathematical expression in terms of both position and particle is represented in the following equations.

$$Velocity: P_M^{T+1} = P_M^T + \gamma_1 R_1^T (B_M^T - Q_M^T) + \gamma_2 R_2^T (B_M^T - Q_M^T) \quad (8)$$

$$Position: Q_M^{T+1} = Q_M^T + P_M^{T+1} \quad (9)$$

From equations (8) and (9), the update equation of position and velocity are represented as $P_M^{T+1}$ and $Q_M^{T+1}$ respectively. $R_1^T$ and $R_2^T$ signifies the diagonal matrix and the parameters

of the acceleration coefficient is denoted as $\gamma_1$ and $\gamma_2$ respectively.

### Bio-geographical Based Optimization Algorithm (BBO)

The BBO algorithm [29] was initiated by Simon in 2008 that employs the bio-geographical concept. Let us consider the rate of immigration and emigration with respect to the total number of species, then

$$I = m\left(1 - \frac{s}{N}\right) \quad (10)$$

$$E = n\left(\frac{s}{N}\right) \quad (11)$$

From equation (10) and (11), the immigration and emigration of the BBO algorithm are represented as I and E respectively. m and n signify the rate of immigration and emigration. s represents the total number of species and $N = s_{\max}$. Soon after the determination of emigration $E$, the immigration value can be calculated by,

$$I = 1 - E \quad (12)$$

Here, every solution is modified at all phases during the lack of elitism. Here the modified solution is selected by the probability rate. The suitability index variables $S_I$ during the transferring of one solution to the subsequent solutions are represented in equation (13).

$$S_{I(m,n)}(new) = S_{I(m,o)} + \beta\left(S_{I(n,o)} - S_{I(m,o)}\right) \quad (13)$$

From equation (13), $\beta$ signifies the parameter value that ranges from 0 to 1. The variation in habitat condition to inadequate from adequate of the mth solution analogous to the mutation processes of genetic algorithm.

## 3.5 Hybrid PSO

Hybrid Particle Swarm Optimization (PSO) is an optimization technique that combines the basic principles of PSO with elements from other optimization methods or problem-solving approaches to enhance its performance and overcome specific limitations. PSO itself is a population-based optimization algorithm inspired by the social behavior of birds or fish in flocks and schools, where particles (representing potential solutions) move through a solution space to find the optimal solution.

The term "Hybrid PSO" typically implies that additional strategies or techniques are integrated into the standard PSO algorithm to improve its efficiency, accuracy, or convergence speed while addressing the limitations it might have in finding global optima, especially in complex or multimodal optimization problems.

This section introduces two new operators—the BBO algorithm's mutation process and the emigration and immigration processes—to explain a unique HPSO method. The optimization problems that the hybrid PSO method can handle are vast. In addition, the complexity rate is lowered, leading to the best possible outcome. The procedure used by HPSO to arrive at the best possible data-routing protocol is shown in Fig.1.

Fig.1. comprises three different phases namely the initialization phase, local best phase, and global best phase respectively. During initialization processes, the respective control parameters of the particle swarm optimization algorithms are defined followed by the generation of a random population. In the local best phase, new swarms are generated to evaluate the FF. Following that, the particle's speed is adjusted. There is little difference between the global best phase and the local best phase. In the global best step, however, the particle locations are assessed. At the same time that the FF is being calcuated and the update process is being put into motion in both the local and global best phases of the BBO algorithm, two new operators—emigration and immigration—are added. When the condition criteria is satisfied, the iterative procedure is terminated until an optimum solution is found.

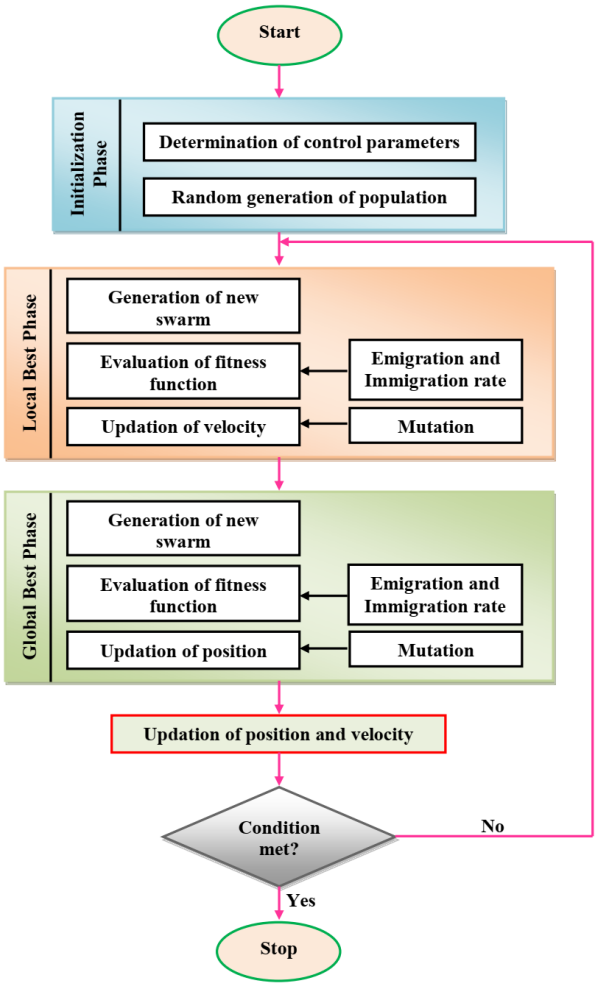


**Figure 1**. HPSO for the optimal data routing protocol

## 4. Experimental Evaluation

The experimentation of the proposed method have been explored via the MATLAB platform. Let us assume that the random network consists of 100 nodes employed arbitrarily to the area of the dimension of 1000 x 1000 sq. m. In this analysis, we assume that the nodes' separation from the hub is constant. Within the network, the nodes are assumed to be connected at different levels using first order radio method [30]. Each node's trust congestion measurements are used to determine the optimum path for transferring data. Using MATLAB simulations, we evaluate how well the suggested method performs. In this case, the node is travelling at a speed of 20 metres per second. Using a 75-meter node spacing, a simulation of the technique is performed in the Physical Layer of IEEE 802.11. The simulation of the network takes just three minutes. Methods like TA-ACO [31], TEFCSRP [20], and QEBSR [32] are compared to the proposed approaches for the trust aware energy-efficient routing protocols in WSN using performance metrics like detection network lifetime, accuracy, end-to-end delay, EC, PDR and percentage of dead nodes.

### 4.1 Simulation measures

The following shows the performance metrics that will be used to assess the suggested method.

**a) Energy consumption (EC)**: Power consumption in a network is measured as the total amount of energy used by the nodes to complete the three tasks of data reception, distribution, and transmission. Every node was given a certain amount of energy to start with, and the simulation constantly updates its measurements to account for changes in those energies.

**b) Detection accuracy**: The effectiveness of a detection system is measured by how many potential threats in a network can actually be discovered.

**c) Network lifetime**: Ultimately, a network's useful life span extends with time, although in a roundabout way. A long operational lifespan for a network is contingent on its ability to operate with less power. This indicates that towards the conclusion of the simulation time, there will be more functioning nodes in the network.

**d) Packet delivery ratio (PDR)**: It is the amount of data packets that are generated divided by the number of packets that are successfully sent.

**e) End-to-end delay**: At receiver node, we measure how long it takes on average between when a packet is created at the creator node and when it is successfully broadcast. Including queue time, packet transmission, distribution, and retransmission at the MAC layer, it predicts every conceivable delay that might occur throughout the whole source and all intermediary nodes.

### 4.2 Performance evaluation

Multiple metrics, including network lifespan, energy usage, end-to-end latency, packet delivery ratio, detection accuracy are used to assess the efficacy of the proposed method. TA-ACO, TEFCSRP, and QEBSR are some of the current methodologies compared to the suggested solution for the trust aware energy-efficient routing protocol in WSN performance. When compared to competing methods, the one that was presented performed better.

#### Detection Accuracy

In Fig.2, we see how the suggested technique fares in comparison to several other methods in terms of performance. As the no. of malevolent nodes in a network grows, the detection accuracies of the methods will always decrease. Since the suggested method precisely calculates the node's reliability, it boasts the highest detection accuracy of any method so far. Higher accuracy in identifying malicious nodes is achieved due to the detection rate's role in forming the opinion that separates benign from harmful nodes. Because of this, the other methods' false malicious ratio rises, and their ability to identify malicious content decreases. In comparison to existing methods, the one described here performs better.

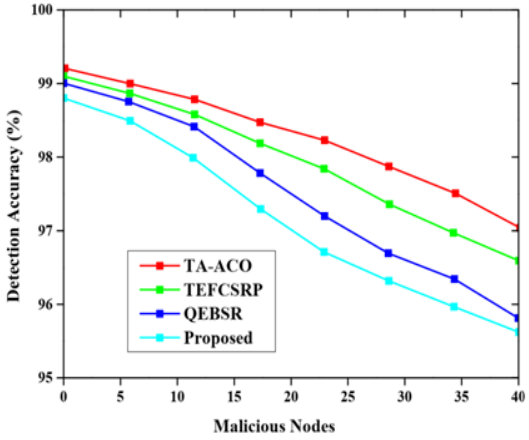


**Figure 2**. Analysis based on detection accuracy

#### Energy consumption

Figure 3 displays the results of a comparison of the suggested method's energy usage with those of existing state-of-the-art methods. The x-axis mean the number of cycles, while the y-axis mean the corresponding shift in energy usage. As can be seen in the figure, the suggested method requires far less energy than any alternative when it comes to ensuring reliable transmission of data packets.

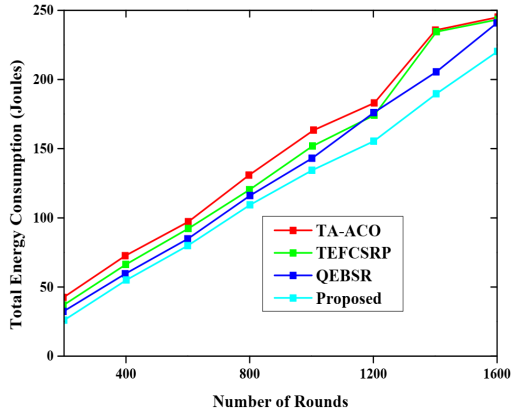


**Figure 3.** Comparative analysis for energy consumption

## Average delay

Fig.4 shows a comparison of the performance metrics for end-to-end latency when packets are queued before transmission. In contrast to existing technologies, the proposed solution decreases latency all the way through a packet's transmission. Occasionally, the node becomes overloaded due to network traffic limitation, which lengthens the time it takes to send packets and therefore causes a significant amount of lost energy. When compared to other methods, the suggested method reduces the amount of time it takes to send data packets.

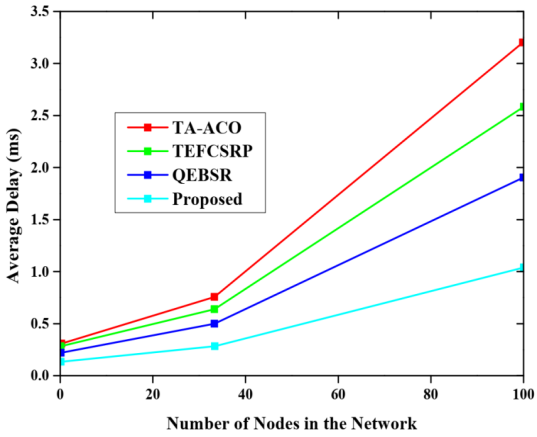


**Figure 4.** Comparative analysis for average delay

## Network lifetime

Figure 5 displays a comparison between the proposed method's and other ways' effects on the network's lifetime. On the x-axis, you can adjust the number of nodes, and on the y-axis, you may alter the expected lifetime of the network. The graph demonstrates that the proposed approach, which takes use of long-lasting power, significantly extends the network's lifetime in contrast to the status quo.

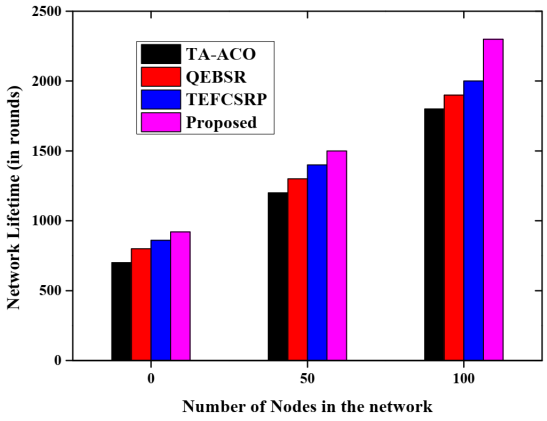


**Figure 5.** Comparative analysis for network lifetime

## Packet delivery rate (PDR)

The suggested method's PDR is shown in comparison to other approaches in Fig. 6. Successfully received packets as reported by the receiver to the sender constitute the packet delivery ratio. When data packets are sent effectively over a network, this measure characterises the network's dependability. As a result of reliable route finding, the suggested method is able to achieve a higher packet delivery ratio than competing methods.

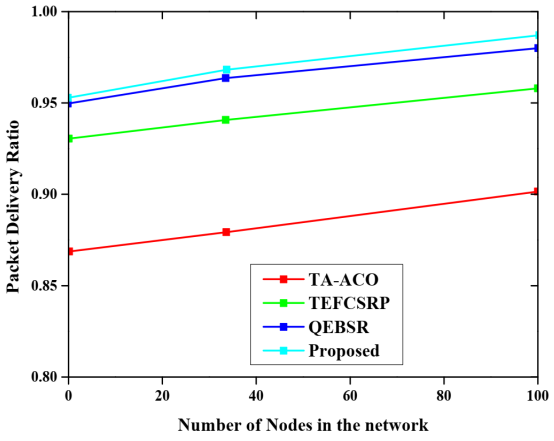


**Figure 6.** Comparative analysis for packet delivery rate

## Percentage of dead nodes

Using the metric of no. of rounds vs percentage of dead nodes with initial energy of 1.0 Joule/node, Fig.7 compares the proposed method to other methods. The experimental findings reveal that the suggested method provides longer network lifetimes than competing methods, making it the superior choice.

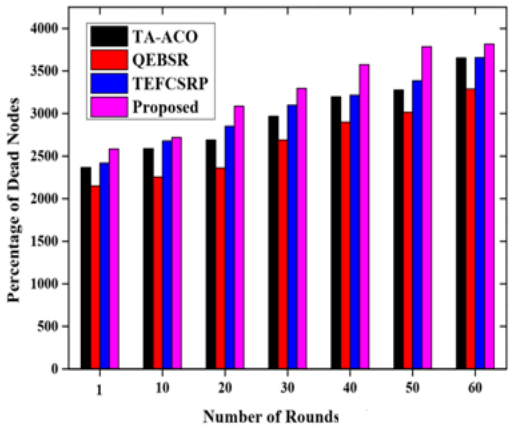


**Figure 7.** Comparative analysis for the percentage of dead nodes

The outcomes derived from MATLAB simulations confirm the superiority of the proposed HPSO-based trust-congestion-aware routing methodology compared to existing protocols.

**Detection Accuracy:** Figure 2 illustrates that the proposed technique attains above 95% accuracy in identifying malicious nodes, even with an increasing number of hostile nodes, while alternative methods like TA-ACO and TEFCSRP exhibit a significant reduction in performance. This enhancement results from the precise trust assessment mechanism integrated into the routing process.

**Energy Consumption:** Figure 3 demonstrates that the proposed method utilises 20–30% less energy than baseline methods during several simulation cycles. This illustrates the efficacy of integrating trust-congestion awareness to minimise redundant transmissions.

**End-to-End latency:** As illustrated in Figure 4, the proposed methodology regularly diminishes latency by an average of 15–20% in comparison to current techniques. The decrease is mainly due to the congestion-aware measure that reduces queue delays.

**Network Lifetime:** As illustrated in Figure 5, the suggested methodology enhances network longevity by 25–40%, contingent upon network size, due to energy-balanced routing strategies.

**The Packet Delivery Ratio (PDR):** illustrated in Figure 6 indicates that the suggested technique attains a PDR above 98%, markedly surpassing rival methods. This underscores the method's reliability in guaranteeing successful data transmission.

**Dead Node Ratio:** Figure 7 illustrates that the proposed method considerably postpones the emergence of dead nodes, thereby preserving elevated node availability across prolonged operational rounds.

The results validate that the suggested HPSO-based routing protocol optimises routing efficiency, security, scalability, and overall network sustainability.

## 5. Conclusion

Here, we provide a trust-based congestion-aware routing strategy for WSN that makes use of a unique combination of particle swarm optimization and trust-based approaches. Based on criteria including network stability, hop count, and traffic volume, the proposed technique selects the optimal way for transmitting packets. If implemented, the proposed strategy may foresee the ripple impact of the errant node's behaviour on network congestion and mitigate it throughout data packet routing. The results of the tests demonstrate that our approach extends the life of the network much more than the other options. Testing results reveal that the proposed approach outrun existing methods in terms of latency, network lifetime, energy consumption and packet delivery ratio. The key benefits of the suggested trust aware power routing protocol are increased accuracy in detecting malicious nodes and improved routing performances. The advantages of our proposed appraoch include: Improved Convergence Speed, Enhanced Global Search, Robustness, Better Handling of Constraint Optimization, Versatility, Scalability, Effective Handling of Multi-Objective Problems. The advantages of proposed system from its ability to leverage the strengths of different optimization techniques, making it a versatile and powerful tool for solving complex optimization problems. Success of the routing algorithm in real-time WSN settings will be investigated in future study.

### Conflict of Interest

The writers have all denied any involvement in a potential conflict of interest. We would want to make it clear that we did not accept any kind of financial support or payment to conduct this study.

### Acknowledgements

SG, SJ and RJ drafted and edited the paper. The tables and graphs in the experimental findings section were contributed by CM, SS and SA, who also conducted the experiments.

## References

[1] Saini K, Ahlawat P. A trust-based secure hybrid framework for routing in WSN. InRecent Findings in Intelligent Computing Techniques 2019 (pp. 585-591). Springer, Singapore.

[2] Gilbert EP, Baskaran K, Rajsingh EB, Lydia M, Selvakumar AI. Trust aware nature inspired optimised routing in clustered wireless sensor networks. International Journal of Bio-Inspired Computation. 2019;14(2):103-13.

[3] Rajeswari AR, Kulothungan K, Ganapathy S, Kannan A. A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks. Peer-to-Peer Networking and Applications. 2019 Sep 13;12(5):1076-96.

[4] Anand JV. Trust-Value Based Wireless Sensor Network Using Compressed Sensing. Journal of Electronics. 2020;2(02):88-95.
[5] Anchari AA, Amin A, Ashraf S. Routing Problems in Mobile Ad hoc Networks (MANET). Int. Journal of Computer Science and Mobile Computing (IJCSMC). 2017 Jul;6(7):9-15.
[6] Ilyas M, Ullah Z, Khan FA, Chaudary MH, Malik MS, Zaheer Z, Durrani HU. Trust-based energy-efficient routing protocol for Internet of things–based sensor networks. International Journal of Distributed Sensor Networks. 2020 Oct;16(10):1550147720964358.
[7] Selvi M, Thangaramya K, Ganapathy S, Kulothungan K, Nehemiah HK, Kannan A. An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. Wireless Personal Communications. 2019 Apr 30;105(4):1475-90.
[8] Yu X, Li F, Li T, Wu N, Wang H, Zhou H. Trust-based secure directed diffusion routing protocol in WSN. Journal of Ambient Intelligence and Humanized Computing. 2020 Nov 10:1-3.
[9] Basha AR. Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network. IET Wireless Sensor Systems. 2020 Apr 17.
[10] Salari-Moghaddam S, Taheri H, Karimi A. Trust Based Routing Algorithm to Improve Quality of Service in DSR Protocol. Wireless Personal Communications. 2019 Nov 1;109(1):1-6.
[11] Bashar A. "Energy Efficient Multi-Tier Sustainable Secure Routing Protocol for Mobile Wireless Sensor Networks", J. Sustain. Wireless System, Vol.01/ No. 02, 2019, Pages: 87-102.
[12] Qabouche H, Sahel A, Badri A. Hybrid energy efficient static routing protocol for homogeneous and heterogeneous large scale WSN. Wireless Networks. 2020 Oct 6:1-3.
[13] Dhand G, Tyagi SS. SMEER: Secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks. Wireless Personal Communications. 2019 Mar 15;105(1):17-35.
[14] Srikanth N, Prasad MS. Energy efficient trust node based routing protocol (EETRP) to maximize the lifetime of wireless sensor networks in Plateaus. International Journal of Online and Biomedical Engineering (iJOE). 2019 Mar 29;15(06):113-30.
[15] Uddin MA, Islam MM, Khanom R, Mosaddek M. Efficient and Secure Cluster based Routing Protocol for Wireless Sensor Network, Jagannath University Journal Of Computer Science And Engineering,Volume 01, Number 01, March 2019, pp.25 – 36
[16] Kalidoss T, Rajasekaran L, Kanagasabai K, Sannasi G, Kannan A. QoS aware trust based routing algorithm for wireless sensor networks. Wireless Personal Communications. 2020 Feb;110(4):1637-58.
[17] Khalid NA, Bai Q, Al-Anbuky A. Adaptive trust-based routing protocol for large scale WSNs. IEEE Access. 2019 Sep 30; 7:143539-49.
[18] Zahedi A, Parma F. An energy-aware trust-based routing algorithm using gravitational search approach in wireless sensor networks. Peer-to-Peer Networking and Applications. 2019 Jan 1;12(1):167-76.
[19] Sun Z, Wei M, Zhang Z, Qu G. Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks. Applied Soft Computing. 2019 Apr 1;77:366-75.
[20] Mittal N, Singh S, Singh U, Salgotra R. Trust-aware energy-efficient stable clustering approach using fuzzy type-2 Cuckoo search optimization algorithm for wireless sensor networks. Wireless Networks. 2020 Aug 19:1-24.
[21] Jagadeesh S, Muthulakshmi I. "Dynamic Clustering and Routing using Multi-Objective Particle Swarm Optimization with Levy Distribution for Wireless Sensor Networks" International Journal of Communication Systems. 2021 June 18, 34, no.13.
[22] Chakraborty, U.K., et al., 2012. Energy-efficient routing in hierarchical wireless sensor networks using differential-evolution-based memetic algorithm. In: IEEE WCCI 2012, pp. 1–8.
[23] Singh, B., Lobiyal, D.K., 2012. Energy-aware cluster head selection using particle swarm optimization and analysis of packet retransmission in WSN. Procedia Technol. 4, 171–176.
[24] Vimalarani, C., Subramanian, R. and Sivanandam, S.N., 2016. An enhanced PSO-based clustering energy optimization algorithm for wireless sensor network. The Scientific World Journal, 2016.
[25] Sumalatha, M. S., and V. Nandalal. "An intelligent cross layer security based fuzzy trust calculation mechanism (CLS-FTCM) for securing wireless sensor network (WSN)." Journal of Ambient Intelligence and Humanized Computing (2020): 1-15.
[26] Srivastava, Vikas, Sachin Tripathi, and Karan Singh. "Energy efficient optimized rate based congestion control routing in wireless sensor network." Journal of Ambient Intelligence and Humanized Computing 11, no. 3 (2020): 1325-1338.
[27] Srivastava, Vikas, Sachin Tripathi, and Karan Singh. "Energy efficient optimized rate based congestion control routing in wireless sensor network." Journal of Ambient Intelligence and Humanized Computing 11, no. 3 (2020): 1325-1338.
[28] Cui, Zhihua, Jiangjiang Zhang, Di Wu, Xingjuan Cai, Hui Wang, Wensheng Zhang, and Jinjun Chen. "Hybrid many-objective particle swarm optimization algorithm for green coal production problem." Information Sciences 518 (2020): 256-271.
[29] Haddad, Omid Bozorg, Seyed-Mohammad Hosseini-Moghari, and Hugo A. Loáiciga. "Biogeography-based optimization algorithm for optimal operation of reservoir systems." Journal of Water Resources Planning and Management 142, no. 1 (2016): 04015034.
[30] W. R .Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy Efficient Communication Protocol for Wireless Microsensor Networks" , Proceedings of the 33 Hawaii International Conference on System Sciences 2000.
[31] Chakraborty A, Ganguly S, Karmakar A, Naskar MK. A trust based congestion aware hybrid Ant Colony Optimization algorithm for energy efficient routing in Wireless Sensor Networks (TC-ACO). In2013 Fifth International Conference on Advanced Computing (ICoAC) 2013 Dec 18 (pp. 137-142). IEEE.
[32] Rathee M, Kumar S, Gandomi AH, Dilip K, Balusamy B, Patan R. Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks. IEEE Transactions on Engineering Management. 2019 Nov 28.