Tech Science Press

An Optimized Novel Trust-Based Security Mechanism Using Elephant Herd Optimization

Saranya Veerapaulraj[1,*], M. Karthikeyan[1], S. Sasipriya[2] and A. S. Shanthi[1]

[1]Tamilnadu College of Engineering, Coimbatore, India
[2]Krishna College of Engineering, Coimbatore, India
*Corresponding Author: Saranya Veerapaulraj. Emails: catchsaro@gmail.com, vsaranya-it@tnce.in

Abstract: Routing strategies and security issues are the greatest challenges in Wireless Sensor Network (WSN). Cluster-based routing Low Energy adaptive Clustering Hierarchy (LEACH) decreases power consumption and increases network lifetime considerably. Securing WSN is a challenging issue faced by researchers. Trust systems are very helpful in detecting interfering nodes in WSN. Researchers have successfully applied Nature-inspired Metaheuristics Optimization Algorithms as a decision-making factor to derive an improved and effective solution for a real-time optimization problem. The metaheuristic Elephant Herding Optimizations (EHO) algorithm is formulated based on elephant herding in their clans. EHO considers two herding behaviors to solve and enhance optimization problem. Based on Elephant Herd Optimization, a trust-based security method is built in this work. The proposed routing selects routes to destination based on the trust values, thus, finding optimal secure routes for transmitting data. Experimental results have demonstrated the effectiveness of the proposed EHO based routing. The Average Packet Loss Rate of the proposed Trust Elephant Herd Optimization performs better by 35.42%, by 1.45%, and by 31.94% than LEACH, Elephant Herd Optimization, and Trust LEACH, respectively at Number of Nodes 3000. As the proposed routing is efficient in selecting secure routes, the average packet loss rate is significantly reduced, improving the network's performance. It is also observed that the lifetime of the network is enhanced with the proposed Trust Elephant Herd Optimization.

Keywords: Wireless sensor network; low energy adaptive clustering hierarchy; trust systems; elephant herding optimizations algorithm; trust-based elephant herd optimization

1 Introduction

Wireless Sensor Network (WSN) [1] can leverage multiple features in data communication. WSN is generally accepted and performed in multiple ventures created by humans, and it draws the attention of researchers from various fields. Series of small-sized, disposable, and independent sensors are used to build a network in WSN. The sensor nodes sense the data in the environment collect and transmit it

through a wireless link [2]; the data is transferred to the network. Military, space, national, and surveillance use WSN applications extensively.

Now, researchers are shifting their interest towards WSN, whereas, in a WSN network, multiple sensor nodes create a sensor field to collect and transfer the data to the sink. However, several sensor nodes in the WSN network, low power rating, and short-distance communication are the major disadvantages. Sensor nodes in WSN are used to monitor, track, and transmit information, create suitable wireless sensors to monitor natural calamities and environmental changes, traffic management, security monitoring, and military operations. But all the applications discussed earlier need highly reliable sensor networks, so recent studies on WSN are focused on heterogeneous WSNs.

WSNs are related to mission-critical tasks; it is regarded as the most important issue. Because the deployment of nodes is typically in an open environment, security must be considered the most important element. Cryptography techniques are used to ensure integrity, confidentiality, and authentication factors. Internal and external attackers have to be controlled in the WSN network. Various safety techniques, such as authentication, message integrity, and confidentiality, are suggested. This approach is effective in defending against outsider attacks, not network insider attacks.

Trusted [3] communicating nodes are required to assure safe data transfers and initialize secure communication. Routing is a famous alternative to prevent attacks and enhance the probability of successful routes. A trust value [4] guarantees for every node based primarily on the node's forwarding behavior. Nodes with higher trust values are chosen for participating in the route. Essential factors of the present study of WSNs are trust management factors. Insecurity management is utilized while choosing safe cluster heads, data aggregation, routing, and other applications.

Various kinds of protocols are designed for WSN, but the hierarchical-based routing protocols are more advantageous than flat-based ones. The former is highly flexible with higher scalability. It is an effective method to ensure lesser power usage in a cluster, and it improves the network's performance considerably. A two-layer routing procedure is used for Hierarchical-based routing. The first layer is utilized to choose cluster heads, and the second is for routing. Many clusters are formed in a single network. All clusters comprise cluster heads and normal nodes, and normal nodes collect data, and cluster heads transfer those data to the base station for data management. Better network performance with lifetime extension is performed because of the self-organizing feature of hierarchical-based routing.

For WSNs, Low Energy Adaptive Clustering Hierarchy (LEACH) [5,6] is better than direct communication protocol, minimum transmission energy protocol, and static clustering protocol. The nodes of the LEACH cluster together, and a single node behaves as the cluster head. LEACH uses randomization for distributing the energy load in an even manner amongst network sensors. Therefore, the extension of the useful system lifetime is achieved.

Developing and designing intelligent and interactive multi-agent systems that work cooperatively to achieve a particular aim is called swarm intelligence. In 2015, Wang proposed Elephant Herding Optimization (EHO) [7] as an intelligent swarm-based meta-heuristics search technique. The herding behavior of real elephants in nature is used to develop the algorithm, and optimization problems are solved using this habitation. Clan updating operators, as well as separating operators, are admired for the behavior of elephant herding in nature. The elephant in EHO implements a clan updating operator to update the current position, and the matriarch is updated in the responding clan. The separating operator replaces the worst elephant.

The motivation of this work is based on the energy conservation of the WSN network, as the sensor nodes are powered by batteries. An essential factor in the WSN is the efficiency of energy for prolonging the network time and balancing energy consumption. Another key challenge is the security of the data. There are several types of research to design and implement either the energy or security issue. Energy

conservation is required to improve the lifetime of the network. Security mechanisms to improve the reliability of the network. As the EHO metaheuristic performs better than standard algorithms like GA, DE, in this work, it is used for optimizing the performance of the WSN network.

The contributions of this work are improving the clustering process to enhance scalability in the sensor network and to improve security using a trust mechanism. The proposed hybrid Trust-based Elephant Herding Optimization (EHO) incorporates the high searching efficiency of EHO integrated with dynamic updating for efficient cluster head selection for prolonging lifetime. The proposed EHO is used to optimize the trust-based security mechanism in this work.

The rest of the paper is organized into four sections. Techniques used in the investigation are explained in Section 2. Experimental results are discussed in Section 3, and work is concluded in Section 4.

2 Related Works

Beheshtiasl et al. [8] presents a comprehensive survey of major congestion control mechanisms used in WSNs and analyzes the available techniques into four categories, i.e., traffic control protocols, resource control, queue assisted protocols, and priority-aware protocols. This examines the important techniques in congestion detection, congestion notification, and congestion mitigation and directions for future investigation and works.

Dibaei et al. [9] proposed a Trust-Based Scheme for Increasing Security (TSIS) model for WSNs. The proposed trust-based scheme divides the network into several clusters. A special node named the supervisor node is reliable for evaluating the trusted values of other nodes. When supervisor nodes calculate the trust value of other nodes within a cluster, they do not distribute them. The receiver node requests the sender node authentication from its supervisor node. The proposed method uses the NS-2 environment. The simulation results show that the proposed method has increased energy efficiency and packet delivery rate. Hence, it has better performance than the earlier works concerning the parameters mentioned above.

In Khabiri et al. [10], using a cuckoo optimization algorithm, an energy-aware clustering-based routing protocol was proposed in WSNs, which can cluster the network and select optimal cluster heads. The proposed method considered four criteria for choosing cluster heads in the targeted cuckoo algorithm, particularly the remaining energy of nodes, distance to the base station, within-cluster distances, and between cluster distances. The results of simulating the proposed method in a Matlab environment showed it is better than other algorithms such as LEACH, application-specific low power routing, LEACH-EP, and LEACH with distance-based threshold wherein the first node die on average and packet delivery rate for six scenarios.

Various low power and cost network sensors are the assembly present in WSNs for sensing environment, collecting & processing data. Through cluster heads (CH), collected data is transmitted to a base station (BS). For analysis purposes, CH gathers the sensed and processed data from the sensors and forwards them to the base station. The significant problem of WSN is an energy hole, which results in energy depletion in nodes near BS. When retaining the original method's basic functionality, Song et al. [11] suggested a trust-based LEACH for providing safe routing. The decision trust is the base of the decision-making method, and by the basic situational, Trust is assessed separately and dynamically for different decisions. Trust management module integrated with trust-based routine module maintains the situational Trust. It has a novel technique in the trust update model as well as cluster-head-assisted monitoring control.

Clustering was the focus in Rajaram et al. [12] for balancing the network load to improve the sensor nodes' power usage. There is ongoing research on efficiency improvement in the critical WSN technique of clustering. The proposed work had gathered all sensor nodes for the formation of multiple groups referred to as clusters. An efficient satin bowerbird optimization algorithm, wherein the node's weight

was taken into account as a parameter, was employed for the cluster heads' election. Out of all these numerous cluster heads, the crow search optimization was used to design the highly powered cluster heads, referred to as the chief cluster heads. With a Multi-hop manner, the sensor nodes sensed the collected data towards the cluster heads, which later delivered the aggregated data towards the chief cluster heads. The central server node received the collected data from every chosen chief cluster head. Simulations did on the MATLAB R2020a, and the proposed heuristic-based clustering's performance compared against that of other clustering protocols regarding delivery ratio, throughput, and energy efficiency. The better outcomes of the proposed protocol were verified.

Strumberger et al. [13] had improved the tree growth algorithm's basic variants and applied them to the wireless sensor networks localization problem's resolution. Empirical experiments were carried out on diverse sensor networks, ranging from 25 to 150 target nodes. The Gaussian noise corrupted the distance measurements. Nevertheless, it was demonstrated from the simulation outcomes that, in comparison to the literature's other approaches, these proposed algorithms could attain more consistent and accurate locations of the wireless sensor networks' topology's unknown target nodes. For secure routing, suggestions are offered for numerous trust-based protocols.

In wireless sensor networks, Correia et al. [14] had addressed the problem of energy-based source localization via direct utilization of metaheuristics. It contrasted convex relaxations and approximations for circumvention of the maximum likelihood (ML) problem. Reportedly, this was the first application of the metaheuristics for this problem type. To be more specific, there was the application of the EHO algorithm. Comprehensive simulations were conducted to optimize the EHO algorithm's critical parameters to match the energy decay model between the two sensor nodes. Finally, there was the presentation of the computational complexity's detailed analysis.

Moreover, a performance comparison did between the proposed algorithm and the existing non-metaheuristic algorithms. Simulation outcomes demonstrated that the proposed algorithm greatly surpassed the existing solutions' performance in noisy environments and encouraged further improvement and testing of the metaheuristic methods. For the network lifespan's extension, a proposal for a hybrid elephant herding optimization and cultural algorithm for optimal cluster head selection (HEHO-CA-OCHS) scheme was given in Murugadass et al. [15]. The proposed scheme utilized the belief space's merits, framed by the cultural algorithm for defining a separating operator that was potent for constructing new local optimal solutions within the search space. Moreover, the belief space's inclusion aided the balance between optimal exploitation and exploration procedures with enhanced search abilities under optimal cluster head selection. The proposed HEHO-CA-OCHS scheme also boosted the algorithm's characteristic properties by incorporating the separating and clan updating operators for effective cluster head selection to maximize the network lifespan. In comparison to the benchmarked cluster head selection schemes, the proposed HEHO-CA-OCHS scheme's simulation outcomes were assessed to be superior with regards to the percentage of alive nodes by 11.21%, percentage of dead nodes by 13.84%, residual energy by 16.38%, throughput by 13.94%, and network lifespan by 19.42%.

To overcome issues of fast unjustified convergence towards the basic EHO's origin, Ismaeel et al. [16] had proposed three value-based enhanced variants of the EHO known as EEHO15, EEHO20, and EEHO25. The two operators (clan and separation operator) updated the EHO algorithms' exploration/exploitation capabilities. Generally, for inspection of the evolutionary algorithms' biased convergence, a constant function was utilized as a benchmark. In addition to that, the CEC'17 test suite benchmark functions utilized for the performance assessments of the three proposed EEHO variants in comparison with the EHO, the particle swarm optimization (PSO), the bird's swarm algorithm (BSA), and the ant lion optimizer (ALO) algorithms. In the end, it was revealed from the experimental outcomes that the proposed EEHO algorithms had achieved better results in comparison with other competitive algorithms.

Sharad et al. [17] had devised and simulated a novel performance-aware approach known as the Elephant Herd Optimisation -based Cluster Head Selection for the optimization level's accomplishment. During energy optimization, nature-inspired soft computing approaches were always beneficial for optimizing and reducing numerous problems. This research work has given the key focus on these approaches. Simulations of cluster head shuffling are the vital fundamental concept through EHO and other prominent exchange methods. These were done on an open-source simulator for wireless sensor networks known as Contiki-Cooja.

A review of the EHO algorithm is presented by Almufti et al. [18]. Based on previous work results, a comparison of the result of EHO compared to another optimization algorithm is presented. In solving Traveling Salesman Problem (TSP), the result of EHO is compared with the U-Turning Ant Colony, based on the Ant Colony Optimization (ACO). Stumberger et al. [19] focused on reaching greater success in resolving the WSN localization issue by employing swarm intelligence. The fundamental versions of the tree growth algorithm and EHO have been enhanced and applied. Experiments have been conducted on various network sizes (between 5 and 150 nodes) to determine whether the improvement is present, where the distance metrics are corrupted by Gaussian noise. The suggested method is comparatively analyzed with other swarm intelligence algorithms like the butterfly optimization algorithm, PSO, and FA, which have evaluated the same issue. Simulation results of the suggested method show greater consistency and accuracy in unknown node locations in the WSN topology than other existing methods. To solve optimization tasks, Wang et al. [20] proposed a novel kind of swarm-based meta-heuristic search mechanism termed EHO. The herding behavior of elephant groups inspires the EHO method. In EHO [21], elephants' current position and matriarch in all clans are kept up to date through a clan updating operator. Then the separating operator follows it, which enhances the population diversity at a later search stage. EHO shows its efficacy in 15 test cases and comparison with BBO, DE, and GA. When compared with those three metaheuristic algorithms, EHO results show improved performance in most benchmark problems.

Based on the survey, it is observed that optimization is widely used in WSN. In this work, the EHO algorithm is used as it has better performance when compared to ACO, PSO, FA, BBO, DE, and GA. Trust mechanism is popular in providing security, as seen from the reviews. Thus, in this work, the objective is to optimize the trust mechanism using EHO.

3 Methodology

LEACH, Trust LEACH, and proposed Trust-based Elephant Herding Optimization are detailed in this section. The popular LEACH routing forms the basis of the investigation and acts as the benchmark for evaluating the proposed EHO routing.

3.1 Energy Consumption

The energy consumed is given by:

The total non-rechargeable primary energy ε_0, λ is the average sensor broadcasting rate defined as the number of data assemblies for each unit time and $E[Er]$ is the predictable broadcasting energy consumed by all sensors in a data collection in a random way. The average broadcasting energy consumed in the i-th data collection is represented as in Eq. (1):

$$E[E_i] - \lim_{M \to \infty} \frac{\sum_{m=1}^{M} E_i^{(m)} \chi_m^{(i)}}{D_i}, 1 \leq i \leq T \tag{1}$$

where $\chi_m^{(i)} = 1$ for $1 \leq i \leq N^{(m)}$ and 0 otherwise, $D_i = \sum_{m=1}^{M} \chi_m^{(i)}$ characterizes the total number of the existence of the i-th data collection between the M trials, and $T = \max_m \{N^{(m)}\}$ specifies the maximum

number of data collections for the period of the network lifetime. The feasibility of randomly selected data collection happens to be the i-th data collection is provided by Eq. (2):

$$\rho_i = \lim_{M \to \infty} \frac{D_i}{\sum_{m=1}^{M} N^{(m)}}, 1 \leq i \leq T \tag{2}$$

The expected broadcasting energy consumed is achieved in a random process of data collection.

3.2 Low Energy Adaptation Cluster Hierarchy (LEACH)

In WSNs, the LEACH [22] is one of the first noteworthy enhancements to the regular grouping approaches. LEACH is based on ground-based techniques, and it is a self-arranging clustering convention [23]. LEACH anticipates that BS is settled and arranged far from all homogeneous sensors with a confined energy source. At an altered rate, sensors can sense earth and grant among each other, and it can also specifically compare with BS. For ensuring scalability as well as robustness for dynamic networks, LEACH uses localized coordination. For reducing the quantity of data forwarded to the base station, LEACH incorporates data fusion. The network's cluster is rearranged dynamically and periodically by LEACH. It makes it difficult to create a secure protocol by relying on only node-to-node trust relationships. By transmitting with sufficiently high power, LEACH estimate every node can directly contact the base station, and this protocol provides a concept of the round.

LEACH protocol runs with many rounds. Each round contains two stages. The first is the setup wherein the cluster setup happens apart from the advertisement and schedule creation. In the start of this phase, each node chooses an arbitrary number around 0 and 1 and then determines an edge condition [24]. If the chosen number is lesser than the threshold number T(n), the node, fortunately, becomes a cluster head for that round. The threshold number is given in formula (3):

$$T(n) = \begin{cases} \frac{P}{1 - P^* \left(r \bmod \frac{1}{p} \right)} & \text{if } n \in G \\ 0 & \text{Otherwise} \end{cases} \tag{3}$$

wherein the CH's desired percentage is P; the current round is r, the competing nodes are G, which were not selected to be the CH in the previous 1/P rounds. If the number is lesser than limit T(n), the node is the CH for that round. If a node is selected to be CH, it cannot be a CH again until all the other group nodes have been a CH at least once. It is important for adjusting energy usage. The second phase is the steady phase; Where non-CH gets the CH request and sends join demand to the CH, informing them that they are part of the group under that CH. In the perspective of the TDMA schedule, every sensor node collates and forwards data to its CH during the steady-state phase. LEACH protocol uses TDMA/CDMA MAC. Before sending the data to BS, CHs receives and aggregates each one of the data. After a while, the framework initiates one more round by reverting to the setup, and the next state arranges once more.

3.3 Trust-based LEACH (TLEACH) Protocol

To enhance the security of the LEACH protocol, a Trust-based LEACH (TLEACH) [25] protocol is proposed for preserving the basic functionality of the original method like the cluster head-election algorithm and the working phases. Through direct observation or via second-hand information, with a new trust updation model and a second-hand information exchange method, a trust management module is included in the proposed method for maintaining the basic neighbours' situational Trust. Providing better support for trust evaluation, a Trust-based routing mechanism is employed, adding trust slots. When decisions are made by the decision trust, basic situational Trust evaluates different decisions separately and dynamically.

The subjective evaluation of A to B is the Trust of node A on node B, i.e., in A's belief on whether and how well B will finish task A has assigned to B. Trust is of 2 types: Direct Trust and Indirect Trust. The calculation of Direct Trust depends on the history of past collaborations of A and B, whereas the calculation of Indirect Trust depends on other nodes' recommendations for B. In this article, Trust is a combination of Direct as well as Indirect Trust. 0 to 1 is the range, where 0 is unreliability, and absolute reliability is 1.

If a node is chosen as a CH based on the LEACH CH algorithm [26], a notice is broadcasted to nodes within its communication scope. Node ID, as well as the remaining energy items, is included in the notice. After the non-cluster head receives these notices, it includes the node ID into the set of standby CHs, while a CH table is constructed by cluster-head. The table is utilized during route establishment as well.

Periodical trust updates can be taken advantage of by high-level malicious nodes to perform time-domain inconsistent behaviours. It also breaks the functioning of trust management systems.

One of the largest mammals on earth is Elephants. Two traditionally recognized species are African and Asian elephants. Their representative characteristic is their trunk used for several purposes like breathing, taking in water, and holding objects. [27] In nature, social animals like elephants have complex social systems for their adult females as well as calves. Elephant groups comprise a matriarch, the leader, often the oldest elephant, and several clans. Clans comprise a single female and her calves or a few related females. Male elephants tend to stay in isolation, so they leave the family when they grow up. However, females choose to live in familial groups [28]. While living far away from family, male elephants contact their family elephants through low-frequency.

3.4 Proposed Trust-based Elephant Herding Optimization

The Elephant population is level-headed into clans and sets the number of elephants in every clan. In every generation, a set quantity of male elephants will move out of their family group and the far way in solitarily. The leader of the clan is the matriarch, and each elephant lives together under the clan.

Clan updating operator: As mentioned earlier, the elephants live together in all the clans under a matriarch's leadership. Hence, for every elephant in a clan ci, the subsequent position is affected by the matriarch ci. For an elephant in clan ci, it is given by the following formula (4):

$$x_{new,ci,j} = x_{ci,j} + \alpha \times (x_{best,ci} - x_{ci,j}) \times r \tag{4}$$

wherein $x_{new,ci,j}$ and $x_{ci,j}$ are the freshly updated position and the previous position for elephant j in the clan ci. To determine the effect of the matriarch ci on $x_{ci,j}$ $\alpha \in [0, 1]$ is a scale factor

$x_{best,ci}$ denotes the matriarch ci, the fittest elephant in the 0 clan $ci.r[0, 1]$. Here, the uniform distribution is utilized. The elephant with the greatest fitness in all the clans is not updated through (1), i.e., $x_{ci,j} = x_{best,ci}$. Rather, the elephant with the greatest fitness is updated through Eq. (5):

$$x_{new,ci,j} = \beta \times x_{center,ci} \tag{5}$$

wherein $\beta \in [0, 1]$ denotes a factor that influences the effect of $x_{center,ci}$ on $x_{new,ci,j}$. The new individual $x_{new,ci,j}$ can be seen as Eq. (5), which is produced via the data got by every elephant in the clan $x_{center,ci}$, ci denotes the centre for clan ci, as for the d-th dimension, it may be computed through Eq. (6):

$$x_{center,ci,d} = \frac{1}{n_{ci}} \times \sum_{j=1}^{n_{ci}} x_{ci,j,d} \tag{6}$$

wherein 1≤d≤D denotes the d-th dimension while D refers to the total dimension. n_{ci} This refers to the number of elephants in the clan ci and $x_{ci,j,d}$ is the d-th of the elephant $x_{ci,j}$. The centre of the clan ci $x_{center,ci}$ may be computed via Eq. (6).

Separating operator: In an elephant clan, when male elephants reach puberty, they will leave their family. When solving optimization issues, the elephant separating process may be modeled as a separating operator. For improving the searching capability of EHO, it is assumed that the elephants with the poorest fitness employ the separating operator in every generation as given by Eq. (7).

$$x_{worst,ci} = xminmax_{min} \tag{7}$$

wherein x_{max} and x_{min} are the upper as well as lower bounds of the location of the elephant. $x_{worst,ci}$ Denotes the poorest elephant of clan ci. $rand \in [0, 1]$ Denotes a type of stochastic distribution and uniform distribution within [0,1].

Step 1: Initialization.

Establish a generation counter as t = 1 to set up the population and the maximum generation MaxGen.

Step 2: While t<MaxGen do

Rank the elephants as per their fitness. Deploy the clan updating operator.

Deploy the separating operator.

Assess the population through the freshly updated positions (t = t + 1).

Step 3: end while

The trust level of each node is evaluated in the trust model. Data packet modifications, loss as well as misreporting are noted due to malicious nodes. By assuming all nodes are trustworthy, each node is assigned as 1 to start with the trust level. Later based on the node's malicious behaviour, the trust level of a node modifies from 1 to 0. If a trust level is lesser than a predefined threshold value, it is treated as a malicious node. Such nodes are detected and separated from the network. In the sink node, nodes' trust values are stored and evaluated. Each node also retains a copy of the trust level. The trust value of each node is dynamically stored locally by the sink node through an acknowledgment.

The proposed Trust Elephant Herding Optimization optimizes the routes to destination based on the trust values of the nodes in the route. When a source node initializes the requirement to send data packets, the proposed method considers various routes to the destination based on trust value and energy levels. Optimal routes with the highest trust values and lowest energy requirements are chosen for transmitting data.

4 Results and Discussion

The simulations were carried out using the Matlab and Weka tools. The LEACH, Elephant Herd Optimization, Trust LEACH, and Trust Elephant Herd Optimization are evaluated. The various routing was evaluated in varying network sizes (500 to 3000 nodes). Tab. 1 shows the simulation parameter. The graphical depiction of the number of clusters, the average end-to-end delay (sec), average packet loss rate, and the percentage of nodes alive achieved for the various methods is shown in Figs. 1 to 4.

Table 1: Simulation parameters

| Parameters	Values
Pop size	80
Network sizes	500 to 3000 nodes
Max Gen	100
Initial energy	2J
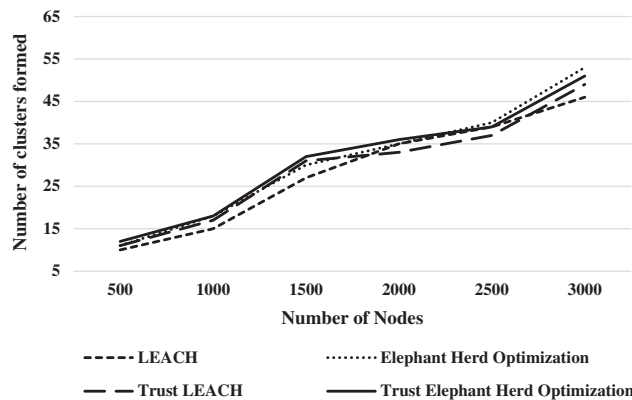
Figure 1: Number of clusters formed for trust elephant herd optimization
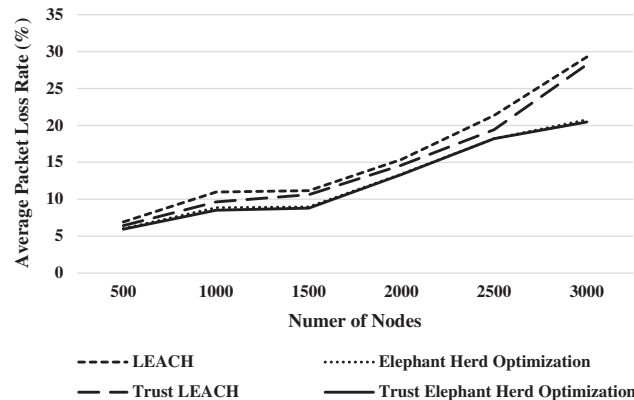
Fig. 1 reveals that the Number of Clusters Formed of Trust Elephant Herd Optimization performs better by 18.2%, no change, and by 5.71% than LEACH, Elephant Herd Optimization, and Trust LEACH respectively at Number of Nodes 1000. The Number of Clusters Formed of Trust Elephant Herd Optimization performs better by 2.82%, by 2.82%, and by 8.7% than LEACH, Elephant Herd Optimization, and Trust LEACH, respectively at Number of Nodes 2000. The Number of Clusters Formed of Trust Elephant Herd Optimization performs better by 10.31%, by 3.85%, and by 4% than LEACH, Elephant Herd Optimization, and Trust LEACH respectively at Number of Nodes 3000.

Fig. 2 reveals that the Average End to End Delay (sec) of Trust Elephant Herd Optimization performs better by 4.18%, by 7.31%, and by 23.1% than LEACH Elephant Herd Optimization, and Trust LEACH, respectively at Number of Nodes 1000. It is observed that the delay is slightly higher for the proposed Trust Elephant Herd Optimization compared to LEACH and Trust LEACH as the network size increases.
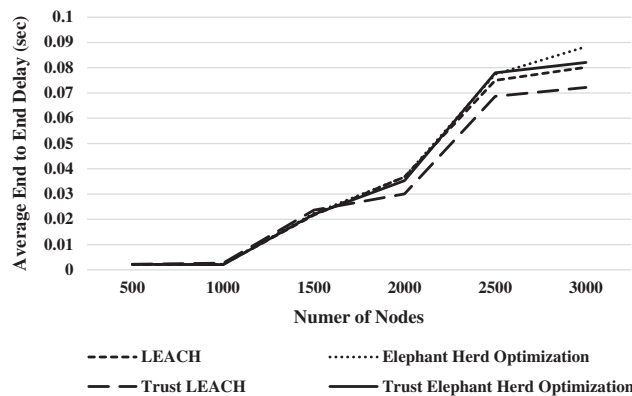

Figure 2: Average end to end delay (sec) for trust elephant herd optimization

Fig. 3 reveals that the Average Packet Loss Rate (%) of Trust Elephant Herd Optimization performs better by 25.26%, by 4.03%, and by 12.5% than LEACH Elephant Herd Optimization, and Trust LEACH, respectively at Number of Nodes 1000. The Average Packet Loss Rate (%) of Trust Elephant Herd Optimization performs better by 14.2%, by 0.37%, and by 8.94% than LEACH, Elephant Herd Optimization, and Trust LEACH, respectively at Number of Nodes 2000. The Average Packet Loss Rate (%) of Trust Elephant Herd Optimization performs better by 35.42%, by 1.45%, and by 31.94% than LEACH, Elephant Herd Optimization, and Trust LEACH, respectively at Number of Nodes 3000.

Figure 3: Average packet loss rate (%) for trust elephant herd optimization

The lifetime of the network is estimated based on the percentage of nodes alive after specific number of rounds. Fig. 4 reveals that the Percentage of Nodes Alive of Trust Elephant Herd Optimization performs better by 9.42%, by 6.19%, and by 6.19% than LEACH, Elephant Herd Optimization, and Trust LEACH, respectively, at Number of Rounds 200. The Percentage of Nodes Alive of Trust Elephant Herd Optimization performs better by 60.32%, by 7.59%, and by 11.61% than LEACH, Elephant Herd Optimization, and Trust LEACH, respectively at Number of Rounds 400. The Percentage of Nodes Alive of Trust Elephant Herd Optimization performs better by 124.14%, by 72.5%, and by 8.9% than LEACH, Elephant Herd Optimization, and Trust LEACH, respectively at Number of Rounds 600.
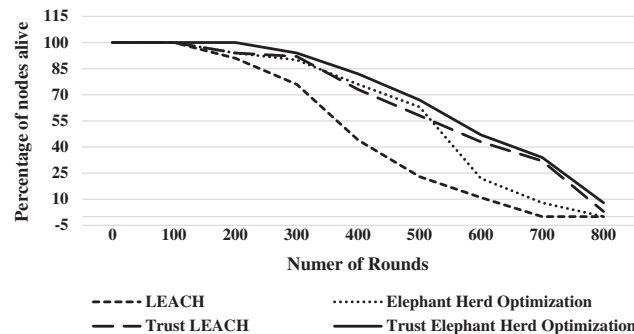
Figure 4: Lifetime for trust elephant herd optimization

5 Conclusion

Wireless Sensor Networks (WSNs) are self-structured wireless networks that comprise several cheap and resource-limited sensors. For distributing the energy load in an even manner amongst the sensor nodes, LEACH uses randomization in the networks, so the lifetime of the useful system is increased. In a 1000 node network, the outcomes reveal that the number of clusters formed of Trust Elephant Herd Optimization performs better by 18.2%, no change, and by 5.71% than LEACH, Elephant Herd Optimization, and Trust LEACH, respectively. Though the end-to-end delay is of the Trust Elephant Herd Optimization is higher than the LEACH and Trust LEACH, it is considered an acceptable trade-off as both the average packet loss ratio and the network lifetime improve. In the future, the proposed method can be evaluated for heterogeneous networks. Though EHO improves the performance, investigations on hybrid EHO can be carried out. Similarly, evaluations on a heterogeneous network can be carried out to check the efficacy of the proposed method.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi and A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks," *Wireless Personal Communications*, vol. 110, no. 4, pp. 1637–1658, 2020.

[2] S. R. Ahmed, M. A. Kadhim and T. Abdulkarim, "Wireless sensor networks improvement using leach algorithm," *IOP Conference Series: Materials Science and Engineering*, vol. 518, no. 5, pp. 1–7, 2019.

[3] C. Konstantopoulos, B. Mamalis and G. Pantziou, "Secure and trust-aware routing in wireless sensor networks," in *Proc. of the 22nd Pan-Hellenic Conf. on Informatics*, Athens, Greece, pp. 312–317, 2018.

[4] J. He and F. Xu, "Research on trust-based secure routing in wireless sensor networks," *Journal of Physics: Conference Series*, vol. 1486, no. 2, pp. 1–9, 2020.

[5] W. Wang, F. Du and Q. Xu, "An improvement of leach routing protocol based on trust for wireless sensor networks," in *5th Int. Conf. on Wireless Communications, Networking and Mobile Computing*, Beijing, China, pp. 1–4, 2009.

[6] I. A. Ezenugu, "Low-energy adaptive clustering hierarchy (leach) algorithm for selection of cluster head in wireless sensor nodes," *Journal of Multidisciplinary Engineering Science and Technology*, vol. 7, no. 1, pp. 12327–12335, 2020.

[7] J. Li, L. Guo, Y. Li and C. Liu, "Enhancing elephant herding optimization with novel individual updating strategies for large-scale optimization problems," *Mathematics*, vol. 7, no. 5, pp. 395–403, 2019.

[8] A. Beheshtiasl and A. Ghaffari, "Secure and trust-aware routing scheme in wireless sensor networks," *Wireless Personal Communications*, vol. 107, no. 4, pp. 1799–1814, 2019.

[9] M. Dibaei and A. Ghaffari, "TSIS: A trust-based scheme for increasing security in wireless sensor networks," *Majlesi Journal of Electrical Engineering*, vol. 11, no. 4, pp. 45–52, 2017.

[10] M. Khabiri and A. Ghaffari, "Energy-aware clustering-based routing in wireless sensor networks using cuckoo optimization algorithm," *Wireless Personal Communications*, vol. 98, no. 3, pp. 2473–2495, 2018.

[11] F. Song and B. Zhao, "Trust-based leach protocol for wireless sensor networks," *2008 Second International Conference on Future Generation Communication and Networking*, vol. 1, pp. 202–207, 2008.

[12] V. Rajaram and N. Kumaratharan, "An optimized clustering using hybrid meta-heuristic approach for wireless sensor," *International Journal of Communication System*, vol. 33, no. 18, pp. 1–12, 2020.

[13] I. Strumberger, M. Minovic, M. Tuba and N. Bacanin, "Performance of Elephant herding optimization and tree growth algorithm adapted for node localization in wireless sensor networks," *Sensors*, vol. 19, no. 11, pp. 2515–2523, 2019.

[14] S. D. Correia, M. Beko, L. A. da Silva Cruz and S. Tomic, "Elephant herding optimization for energy-based localization," *Sensors*, vol. 18, no. 9, pp. 1–14, 2018.

[15] G. Murugadass and P. Sivakumar, "A hybrid Elephant herding optimization and cultural algorithm for energy-balanced cluster head selection scheme to extend the lifetime in WSNs," *International Journal of Communication Systems*, vol. 33, no. 15, pp. 1–12, 2020.

[16] A. A. Ismaeel, I. A. Elshaarawy, E. H. Houssein, F. H. Ismail and A. E. Hassanien, "Enhanced Elephant herding optimization for global optimization," *IEEE Access 7*, vol. 7, pp. 34738–34752, 2019.

[17] K. Sharad and Deepshikha, "Cluster based techniques leach and modified leach using optimized technique eho in wsn," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 9S, pp. 1–7, 2019.

[18] S. Almufti, R. Asaad and B. Salim, "Review on elephant herding optimization algorithm performance in solving optimization problems," *International Journal of Engineering & Technology*, vol. 7, no. 1, pp. 6109–6114, 2018.

[19] I. Strumberger, M. Minovic, M. Tuba and N. Bacanin, "Performance of elephant herding optimization and tree growth algorithm adapted for node localization in wireless sensor networks," *Sensors*, vol. 19, no. 11, pp. 2515–2523, 2019.

[20] G. G. Wang, S. Deb and L. D. S. Coelho, "Elephant herding optimization," in *2015 3rd Int. Sym. on Computational and Business Intelligence*, Bali, Indonesia, pp. 1–5, 2015.

[21] K. Kaur and R. Randhawa, "Energy efficient approach for underwater sensor network using elephant herd optimization," *Research Cell: An International Journal of Engineering Sciences*, vol. 30, pp. 148–160, 2018.

[22] W. Abushiba, P. Johnson, S. Alharthi and C. Wright, "An energy efficient and adaptive clustering for wireless sensor network (ch-leach) using leach protocol," in *13th Int. Computer Engineering Conf.*, Giza, Egypt, pp. 50–54, 2017.

[23] C. Fu, Z. Jiang, W. Wei and A. Wei, "An energy balanced algorithm of leach protocol in wsn," *International Journal Computing Science*, vol. 10, no. 1, pp. 354–359, 2013.

[24] A. Al-Baz and A. El-Sayed, "A new algorithm for cluster head selection in leach protocol for wireless sensor networks," *International Journal of Communication Systems*, vol. 31, no. 1, pp. 1–13, 2018.

[25] K. S. Gautam and T. Senthil Kumar, Video analytics-based intelligent surveillance system for smart buildings. Springer Soft computing, Bali, Indonesia, pp. 2813–2837, 2019.

[26] A. Vishnu Priya and Ashish kumar srivastava, "Hybrid optimal energy management for clustering in wireless sensor network," *in Computers and Electrical Engineering*, vol. 86, pp. 379–387, 2020.

[27] R. Sharma, V. Vashisht and U. Singh, "Analytical modeling of trust based protocols for cluster head selection in wireless sensor networks," in *2020 8th Int. Conf. on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, Noida, India, pp. 643–647, 2020.

[28] M. Mishra, G. S. Gupta and X. Gui, "Trust-based cluster head selection using the k-means algorithm for wireless sensor networks," in *Int. Conf. on Smart Systems and Inventive Technology*, Tirunelveli, India, pp. 819–825, 2019.