

Secure clustering and routing – based adaptive – bald eagle search for wireless sensor networks

Asha Rani Mahadeva¹, Roopashree Hejjaji Ranganathasharma²,
Yogeesh Ambalagere Chandrashekaraiah³

¹Department of Computer Science Engineering, GSSS Institute of Engineering and Technology for Women, Mysuru, India, Affiliated to Visvesvaraya Technological University, Belagavi, India

²Department of Artificial Intelligence and Data Science, GSSS Institute of Engineering and Technology for Women, Mysuru, India, Affiliated to Visvesvaraya Technological University, Belagavi, India

³Department of Computer Science Engineering, Government Engineering College, Chamarajnagar, Badanaguppe, India, Affiliated to Visvesvaraya Technological University, Belagavi, India

Article Info

Article history:

Received Sep 9, 2024

Revised Mar 29, 2025

Accepted May 24, 2025

Keywords:

Adaptive – bald eagle search

Network lifetime

Secure cluster heads

Secure optimal route

Wireless sensor networks

ABSTRACT

Wireless sensor networks (WSNs) are self-regulating networks consisting of several tiny sensor nodes for monitoring and tracking applications over extensive areas. Energy consumption and security are the two significant challenges in these networks due to their limited resources and open nature. To address these challenges and optimize energy consumption while ensuring security, this research proposes an adaptive – bald eagle search (A-BES) optimization algorithm enabled secure clustering and routing for WSNs. The A-BES algorithm selects secure cluster heads (SCHs) through several fitness functions, thereby reducing energy consumption across the nodes. Next, secure and optimal routes are chosen using A-BES to prevent malicious nodes from interfering with the communication paths and to enhance the overall network lifetime. The proposed algorithm shows significantly lower energy consumption, with values of 0.27, 0.81, 1.38, 2.27, and 3.01 J as the number of nodes increases from 100 to 300. This demonstrates a clear improvement over the existing residual energy-based data availability approach (REDAA).

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Asha Rani Mahadeva

Department of Computer Science Engineering, GSSS Institute of Engineering and Technology for Women

Affiliated to Visvesvaraya Technological University

KRS Road, Metagalli, Hebbal Industrial Area, Mysuru, Karnataka 570016, India

Email: asharanim@gsss.edu.in

1. INTRODUCTION

Wireless sensor networks (WSNs) includes group of tiny sensor nodes (SNs) that gather data from the surrounding environment [1]. Collected information is transmitted to a base station (BS) through multi-hop communication using wireless radio communication for further processing [2]. Because of quick increase in the usage of sensing techniques, WSNs are made to be adaptable in harsh environments where human intervention is not welcomed [3]–[5]. Several researchers have developed several techniques to resolve a energy optimization issue in WSNs [6]–[8]. In WSNs, clustering is a major technique used to optimize energy consumption by grouping SNs into clusters of different sizes [9]. Each cluster in a WSN has a cluster head (CH) collects information from its cluster members (CMs) and transfers it to a BS for further processing [10], [11]. However, WSNs are vulnerable to malicious nodes from wide range of sources that include insecure management of keys, inadequate verification level, insider attacks, and attacks targeting the sensors

themselves [12]–[15]. Several security and routing techniques have been developed through researchers to maximize packet transmission range and identify optimal routes without compromising transmission reliability, which are the two critical challenges in WSNs [16], [17].

Roberts and Thangavel [18] implemented residual energy-enabled data availability algorithm (REDAA) on WSNs to increase network lifetime by electing route paths and cluster heads. Vinitha *et al.* [19] employed Taylor-enabled cat salp swarm approach (Taylor C-SSA) by integrating C-SSA with a Taylor series. Balachandra *et al.* [20] used multi-objective trust centric artificial algae algorithm (M-TCAAA) to secure transmission across WSNs. Kumar and Srimanchari [21] presented quantum behavior and gaussian mutation archimedes optimization algorithm (QGAA) to secured cluster head and route selection. Asiri *et al.* [22] developed an improved duck and traveller optimization (IDTO)-enabled cluster multi-hop routing (IDTOMHR) technique to a selection of a secure cluster head and route selection. Kalburgi and Manimozhi [23]–[25] introduced taylor-spotted hyena optimization (Taylor-SHO) technique to secure CH and path selection. Existing methods were seen to carry the limitations including the failure to consider appropriate fitness functions of energy, distance, cluster density, and node degree, in addition to the high packet loss. These limitations increase energy consumption and affect the effectiveness of clustering and routing performances. In this research, adaptive–bald eagle search (A-BES)-based clustering and routing algorithm is proposed to enhance the network lifetime of WSNs. By considering these fitness functions for secure clustering and routing, the network lifetime is improved while the energy consumption and packet loss ratio (PLR) are minimized. The essential contributions of the research are:

- The A-BES algorithm is proposed to for secure CH selection from a group of clusters using different fitness functions. A secure CH selection ensures integrity and confidentiality of data transfer, and also minimizes energy consumption.
- The potential function is used to cluster the chosen secure CHs for communication. Network clutsering is employed to minimize the energy consumption of nodes.
- The A-BES algorithm is employed for selecting an optimal and secured route path to transfer the data with different fitness functions. The selection of a secure route path prevents malicious nodes from interfering along the route, thereby improving the WSN's network lifetime.

This manuscript is arranged as: section 2 explains brief description of a developed methodology. section 3 presents a results, comparisons, and discussion of a developed methodology. Finally, section 5 gives a conclusion to this research.

2. RESEARCH METHOD

In this research, A-BES optimization approach is assigned for secure data transfer in WSNs. Proposed A-BES algorithm includes four main phases namely, sensor deployment, secure cluster head (SCH) selection, cluster generation, and secure route selection. By carefully selecting a secure CH and route, the algorithm efficiently avoids malicious nodes during data transmission, enhancing the overall structure. Figure 1 illustrates the functioning of A-BES-based secure clustering and routing.

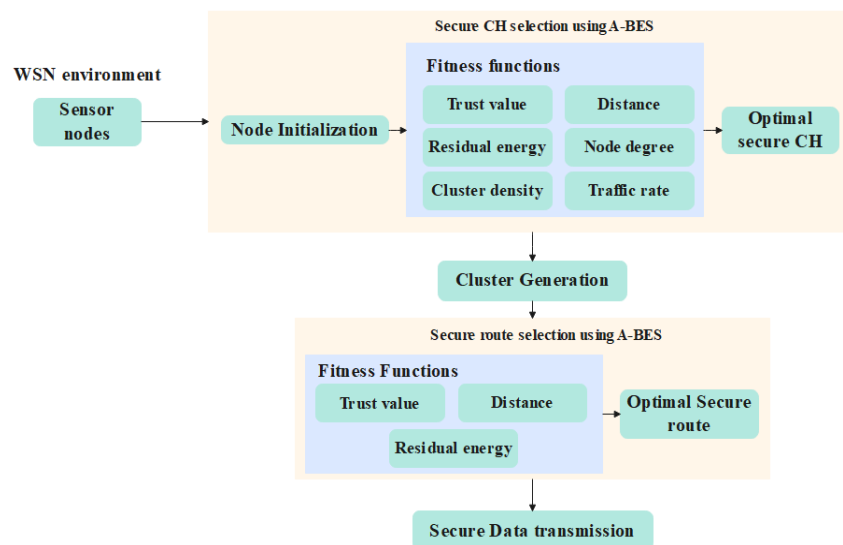


Figure 1. Process of A-BES-based secure clustering and routing

2.1. Sensor deployment and SCH selection using A-BES

The sensor nodes are randomly deployed in the network, and the optimal SCH and secure routes are determined using A-BES, which facilitates secure data transfer in the WSN. By leveraging various fitness functions, A-BES [26]–[28] selects the optimal CHs from a group of clusters, enabling secure data transmission over the WSN. The process of identifying the optimal CHs is briefly explained.

2.2. Representation and Initialization

In A-BES, the bald eagle represents a group of nodes that are selected as CH from the clusters. This group of nodes is referred to as the SCH during the solution initialization phase. Each dimension of the bald eagle corresponds to the number of CHs in the network. Every solution is initialized with a random sensor ID from 1 to the Number of Sensors (NS). Furthermore, the i th solution of A-BES is represented as $x_i = (x_{i,1}, x_{i,2}, \dots, x_{i,NC})$, wherein NC denotes the amount of CHs and $1 \leq d \leq NC$ denotes node ID from 1 to NS.

2.3. A-BES approach

BES is novel metaheuristic optimization algorithm inspired by bald eagle's hunting behavior. The A-BES algorithm mimics the condor's hunting behavior when targeting prey and is divided into three phases: selection, searching, and swooping phases. These three phases are explained in detail below, along with their corresponding mathematical expressions.

- a. Selection phase. In the selection phase, the search space is randomly chosen by the bald eagle when it is looking for its prey. The updated mathematical expression for the randomized parameter is provided in (1), and a position of a bald eagle during selection phase is described in (2). In (2), α_t represents the updated control parameter of a bald eagle's location, t denotes a present iteration number, and T represents a highest iteration number. Term L_{new}^i denotes a present location of a i^{th} bald eagle, L_{best} refers to a present best location, and L^i represents a position of a i^{th} bald eagle. Additionally, L_{mean} describes the average position of all the bald eagles, and $r \in (0,1)$ represents a random number.

$$\alpha_t = \exp\left(\frac{T-t}{T}\right) - 1 \quad (1)$$

$$L_{new}^i = L_{best} + \alpha_t \times r(L_{mean} - L^i) \quad (2)$$

- b. Searching phase. In this stage, a bald eagle flies in conical spiral within a chosen search space and searches to the prey. In a space of a conical spiral, bald eagle moves towards various courses for accelerating the search speed and identifying an optimal position. The mathematical expression for the position of a spiral flight of a bald eagle is given in (3)–(5).

$$L_{new}^i = L^i + x(i) \times (L^i - L_{mean}) + y(i) \times (L^i - L^{i+1}) \quad (3)$$

$$x(i) = \frac{x \times r(i)}{\max(|x \times r|)} \quad (4)$$

$$y(i) = \frac{y \times r(i)}{\max(|y \times r|)} a \quad (5)$$

In (3)–(5), L^{i+1} represents the following updated position of i th bald eagle, where $\theta(i)$ denotes a polar angle on a spiral equation, and $r(i)$ signifies a spiral equation diameter. Finally, $\beta \in (0, 5)$ and $\gamma \in (0.5, 2)$ represent a factors which control a spiral. The $x(i)$ and $y(i)$ describe a positions of bald eagles in polar coordinates with the values $(-1, 1)$.

- c. Swooping phase: Once bald eagle has locked onto its destination, that rapidly diverges from optimal location and heads towards a target. Swooping phase's movement state remains in effect, and the mathematical expressions for polar coordinates are outlined in (6) to (8). In (7) and (8), λ_1 and λ_2 represent the optimal and central positions of the bald eagles, respectively.

$$L_{new}^i = rand(0,1) \times L_{best} + \delta_x + \delta_y \quad (6)$$

$$\delta_x = x1(i) \times (L^i - \lambda_1 \times L_{mean}), \lambda_1 \in [1,2] \quad (7)$$

$$\delta_y = y1(i) \times (L^i - \lambda_2 \times L_{best}), \lambda_2 \in [1,2] \quad (8)$$

2.4. Fitness functions for identifying the optimal SCHs

The fitness functions considered to identify the optimal SCH using A-BES are, trust (ff_1), residual energy (ff_2), distance (ff_3), node degree (ff_4), traffic rate (ff_5), and cluster density (ff_6). The fitness functions are assigned to identify the optimal SCHs in the WSN, and a brief explanation of the fitness functions is explained below. In the (9), F represents the single fitness function, and $\alpha_1 - \alpha_6$ represents the weight metric employed for every fitness function. The weight values for all six fitness functions are set to 1 and normalized for further processing.

$$F = \alpha_1 \times ff_1 + \alpha_2 \times ff_2 + \alpha_3 \times ff_3 + \alpha_4 \times ff_4 + \alpha_5 \times ff_5 + \alpha_6 \times ff_6 \quad (9)$$

- a. Trust: the value of trust utilized in A-BES is a significant component that enhances security against malicious attacks. The value of trust (ff_1) defines the relation between the number of forwarded and received packets in the nodes. In (10), $PT_{s_{i,j}}$ and $PR_{s_{i,j}}$ signify the number of packets transferred and received among i and j sensors, respectively.

$$ff_1 = \frac{PT_{s_{i,j}}}{PR_{s_{i,j}}} \quad (10)$$

- b. Residual energy: the data is collected by CHs from their CMs and is transferred to the desired nodes. A large amount of residual energy is required for the CHs to process the tasks. The sensors with high energy are the best solutions to identify CHs and mathematical expression for residual energy (ff_2) is given in (11). In (11), E_{SCH_i} is the residual energy of the SCH candidate.

$$ff_2 = \sum_{i=1}^q \frac{1}{E_{SCH_i}} \quad (11)$$

- c. Distance: the mean distance between the nodes of CMs and their CHs is considered as the next fitness function. Node energy distribution is primarily influenced by the path distance. The sensor's energy degradation is lesser when the routing path is shorter and the mathematical expression for distance (ff_3) is given in (12). In the below (12), $dis(s_i, CH_j)$ is the distance among i th and j th CHs' sensors, and cm_j is the amount of nodes in the cluster.

$$ff_3 = \sum_{j=1}^q \left(\sum_{i=1}^{cm_j} dis(s_i, CH_j) / cm_j \right) \quad (12)$$

- d. Node degree: the next fitness function is a node degree that is determined as number of CMs for the corresponding CH. Mathematical expression for node degree is given in (13). In the (13), ff_4 represents the result of node degree fitness function, and cm_j represents the corresponding CM for the j th sensor.

$$ff_4 = \sum_{i=1}^q cm_j \quad (13)$$

- e. Traffic rate: the traffic rate is influenced by buffer utilization, packet drop, and network channel conditions. It is evaluated by taking the mean of these three parameters. For an effective network, the traffic rate should be minimized, and its mathematical expression is provided in (14). In (14), $B_{utilization}$ represents buffer utilization, P_{drop} denotes packet drop, and C_{load} refers to the channel load.

$$ff_5 = \frac{1}{3} [B_{utilization} + P_{drop} + C_{load}] \quad (14)$$

- f. Cluster density: the cluster density of the node enhances node communication by minimizing the interactions among nodes. When the density increases, it results in high packet drop and congestion. Every node in a cluster is integrated into all other nodes in the network and its mathematical expression is given in (15).

$$ff_6 = \frac{1}{M} \sum_{i=1}^M |Y_i| \quad (15)$$

In the (15), $|Y_i|$ represents the i th cluster node, M represents the whole nodes in the network, and A represents the whole CHs. By considering these six fitness functions to identify the SCHs using A-BES, the malicious nodes are effectively avoided. This approach leads to reduced energy degradation and packet loss during communication.

2.1. Cluster generation

In the cluster generation process, the ordinary sensor nodes are employed for SCHs. The residual energy and distance are considered as potential solutions for employing ordinary sensor nodes to the chosen SCHs. The mathematical expression for cluster generation is given in (16).

$$PotentialSolution(N_i) = \frac{E_{SCH}}{dis(N_i, SCH)} \quad (16)$$

2.2. Secure routing using A-BES

After cluster generation, the secure routing discovery is performed using A-BES algorithm with various fitness functions. Secure routing using A-BES enhances the security and efficiency of data broadcasting in a network. The process of secure route discovery is explained.

- Initialization: Every bald eagle in the route discovery process is initialized to the possible transfer path between the source node and the BS. Dimension of every bald eagle corresponds to a number of CHs present in a respective transfer route. For the i^{th} bald eagle in A-BES during route discovery, it is denoted as $x_i = (x_{i,1}, x_{i,2}, \dots, x_{i,q})$, where $1 \leq k \leq q$ denotes the subsequent SCH.
- Route discovery process: The probable routes from the selected CHs to a BS are chosen as a main solutions for path identification. The fitness functions considered for route discovery include trust, residual energy, and distance, which are used to update the location of the solution. The mathematical expression for computing the fitness function is provided in (17).

$$RF = \alpha_1 \times \frac{PT_{s_{i,j}}}{PR_{s_{i,j}}} + \alpha_2 \times \sum_{j=1}^q (\sum_{i=1}^{cm_j} dis(s_i, CH_j)/cm_j) + \alpha_3 \times \sum_{i=1}^q \frac{1}{E_{SCH_i}} \quad (17)$$

In (17), α_1, α_2 and α_3 are the weight parameters employed for fitness functions of the route discovery process. By considering these six fitness functions to identify the SCHs by using A-BES, the malicious nodes are effectively avoided. Therefore, the optimal secured paths are chosen to improve the network security while also increasing data delivery.

3. RESULTS AND DISCUSSION

The proposed A-BES-based secure clustering and routing is simulated through network simulator 2 (NS2) with a system configuration of 16 GR RAM, an i5 processor, and Windows 11 OS. The performance metrics considered to evaluate the proposed algorithm are: packet delivery ratio (PDR), PLR, energy consumption, delay, throughput, and residual energy. Table 1 represents a simulation parameters of a proposed algorithm.

Table 1. Simulation parameters	
Parameter	Value
Algorithm	A-BES
No. of Nodes	100, 150, 200, 250 and 300
Area	1000×1000 m
Initial energy	0.55 J
Packet size	4000 bytes
Simulation time	100 s

In Figure 2, the evaluated PDR of the proposed A-BES-based clustering and routing algorithm is compared with the evaluated PDRs of different existing algorithms namely, cat swarm optimization (CSO), rsemora optimization algorithm (ROA), reptile search algorithm (RSA), and sine cosine RSA (SCRSA). Figure 3 illustrates the PLR, while Figure 4 represents the results of energy consumption, and Figure 5 provides the results of delay. Figure 6 represents the analysis of throughput, while Figure 7 illustrates the residual energy of the proposed A-BES-based clustering and routing algorithm by varying the nodes from 100, 150, 200, 250 and 300.

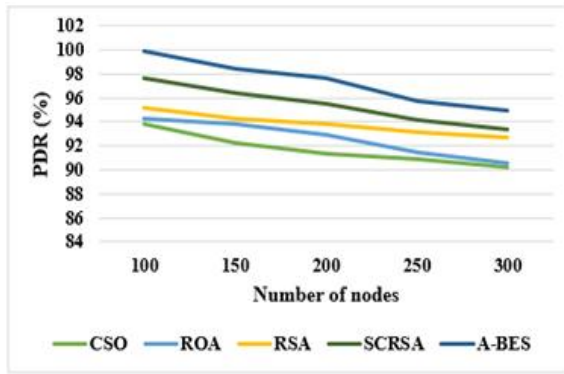


Figure 2. PDR analysis

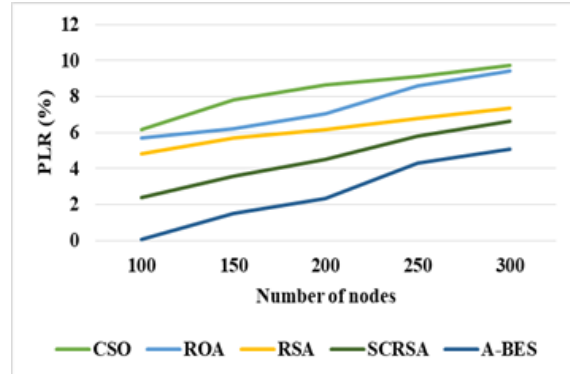


Figure 3. PLR analysis

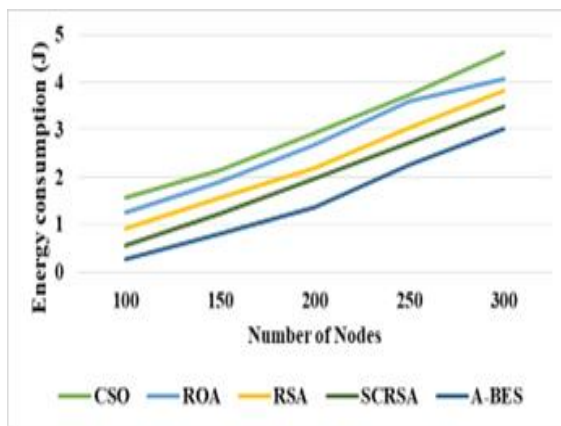


Figure 4. Energy consumption analysis

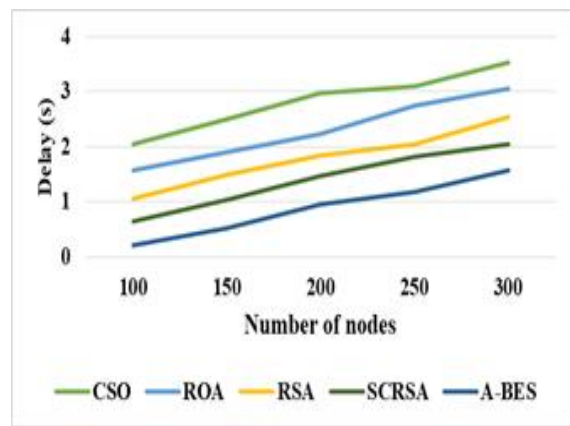


Figure 5. Delay analysis

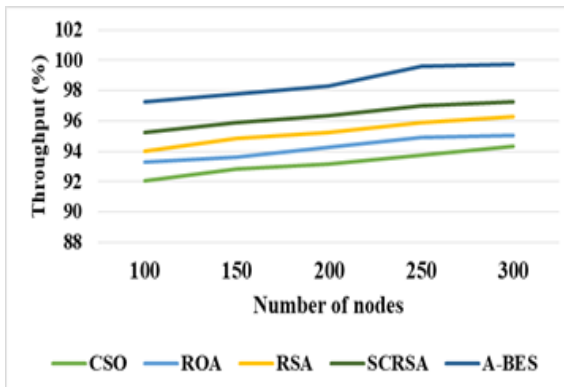


Figure 6. Throughput analysis

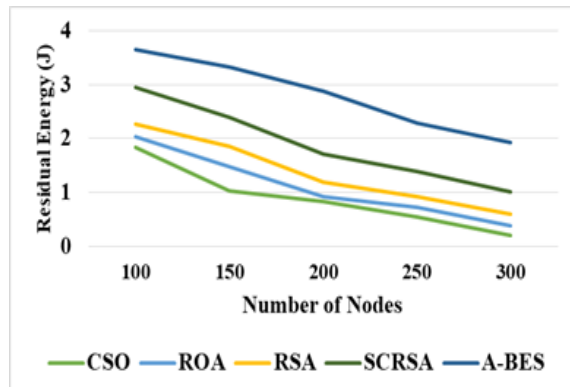


Figure 7. Residual energy analysis

3.1. Comparative analysis

Performance of a developed algorithm is comparing to following previous algorithms, as shown in Table 2: i) the REDAA [18] method, simulated in a 1300×1300 m area with 250 nodes, ii) the Taylor C-SSA [19] method, simulated in a 100×100 m area with the number of nodes varying from 50 to 100, 2000 simulation rounds, and an initial energy 0.5 J, iii) the M-TCAAA [20] method, simulated in a 200×200 m area with the number of nodes varying from 20, 40, 60, 80, and 100, and an initial energy 5 J, iv) the QGAOA [21] method, simulated in a 1500×1500 m area with 100 nodes, an initial energy 1 J, and a simulation time 500 s, and finally v) the IDTOMHR [22] method, simulated for 100 and 250 nodes.

Table 2. Comparative analysis

Performance metrics	Methods	No. of nodes	
		100	250
PDR (%)	REDAA [18]	-	79
	M-TCAAA [20]	99.87	-
	QGAOA [21]	94.5	-
	A-BES	99.93	95.71
Delay (sec)	REDAA [18]	-	8.3
	Taylor C-SSA [19]	0.456	-
	A-BES	0.207	1.179
Energy consumption (J)	M-TCAAA [20]	0.41	-
	IDTOMHR [22]	3.34	8.70
	A-BES	0.27	2.27
	QGAOA [21]	96	-
Throughput (%)	A-BES	97.24	99.59
	Taylor C-SSA [19]	0.129	-
Residual energy (J)	IDTOMHR [22]	2.97	2.98
	A-BES	3.64	2.29

3.2. Discussion

This section discusses limitations of previous algorithms and the benefits of the proposed algorithm. REDAA [18], Taylor C-SSA [19], M-TCAAA [20], QGAOA [21], and IDTOMHR [22] methods have limitations, such as not considering appropriate fitness functions for energy, distance, cluster density, and node degree, as well as leading to high packet loss. These limitations increase energy consumption and negatively impact the performance of clustering and routing. Existing methods were seen to carry the limitations including the failure to consider appropriate fitness functions of energy, distance, cluster density, and node degree, in addition to the high packet loss. These limitations increase energy consumption and affect the effectiveness of clustering and routing performances. In this research, an A-BES-based clustering and routing algorithm is proposed to enhance the network lifetime of WSNs. The fitness functions considered for secure CH selection include trust score, residual energy, distance, node degree, cluster density, and traffic rate. By incorporating these fitness functions into the secure clustering and routing process, energy consumption and PLR are minimized, while network lifetime is significantly improved.

4. CONCLUSION

The A-BES algorithm is proposed to select the SCHs based on fitness functions that evaluate trust score, residual energy, distance, node degree, cluster density, and traffic rate. These selected SCHs reduce a energy consumption of nodes in every round, which extends a network's lifetime. After SCH selection, clusters are formed and secure optimal routes are determined using fitness functions that evaluate residual energy, distance, and energy. By choosing secure optimal routes, the algorithm effectively avoids malicious nodes, improving the network's overall lifetime. The proposed algorithm demands decreased energy consumption of 0.27, 0.81, 1.38, 2.27, and 3.01 J, respectively for varying nodes of 100, 150, 200, 250, and 300, thereby proving to be more effective and robust than the conventional algorithms. In the future, the computation time of the network can be reduced to further enhance the network lifetime.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Asha Rani Mahadeva	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Roopashree Hejjaji		✓				✓		✓	✓	✓	✓	✓		
Ranganathasharma														
Yogeesha Ambalagere	✓		✓	✓			✓			✓	✓		✓	✓
Chandrashekaraiah														

C : Conceptualization	I : Investigation	Vi : Visualization
M : Methodology	R : Resources	Su : Supervision
So : Software	D : Data Curation	P : Project administration
Va : Validation	O : Writing - Original Draft	Fu : Funding acquisition
Fo : Formal analysis	E : Writing - Review & Editing	

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.




REFERENCES

- [1] V. Prasad B.S and H. R. Roopashree, "Energy aware and secure routing for hierarchical cluster through trust evaluation," *Measurement: Sensors*, vol. 33, p. 101132, Jun. 2024, doi: 10.1016/j.measen.2024.101132.
- [2] A. Janarthanan and V. Srinivasan, "Multi-objective cluster head-based energy aware routing using optimized auto-metric graph neural network for secured data aggregation in wireless sensor network," *International Journal of Communication Systems*, vol. 37, no. 3, Feb. 2024, doi: 10.1002/dac.5664.
- [3] S. El Khediri, A. Selmi, R. U. Khan, T. Moulahi, and P. Lorenz, "Energy efficient cluster routing protocol for wireless sensor networks using hybrid metaheuristic approach's," *Ad Hoc Networks*, vol. 158, p. 103473, May 2024, doi: 10.1016/j.adhoc.2024.103473.
- [4] A. Ali *et al.*, "Enhanced fuzzy logic zone stable election protocol for cluster head election (E-FLZSEPFCH) and multipath routing in wireless sensor networks," *Ain Shams Engineering Journal*, vol. 15, no. 2, p. 102356, Feb. 2024, doi: 10.1016/j.asej.2023.102356.
- [5] Y. Liu, H. Huang, and J. Zhou, "A dual cluster head hierarchical routing protocol for wireless sensor networks based on hybrid swarm intelligence optimization," *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 16710–16721, May 2024, doi: 10.1109/JIOT.2024.3355993.
- [6] J.-D. Abdulai, K. S. Adu-Manu, F. A. Katsriku, and F. Engmann, "A modified distance-based energy-aware (mDBEA) routing protocol in wireless sensor networks (WSNs)," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 8, pp. 10195–10217, Aug. 2023, doi: 10.1007/s12652-021-03683-y.
- [7] S. M. P. and G. Satyavathy, "Energy-aware optimal clustering and secure routing protocol for heterogeneous wireless sensor network," *International Journal of Computer Networks and Applications*, vol. 9, no. 1, p. 12, Feb. 2022, doi: 10.22247/ijcna/2022/211594.
- [8] R. I. Sajan, V. B. Christopher, M. J. Kavitha, and T. S. Akhila, "An energy aware secure three-level weighted trust evaluation and grey wolf optimization based routing in wireless ad hoc sensor network," *Wireless Networks*, vol. 28, no. 4, pp. 1439–1455, May 2022, doi: 10.1007/s11276-022-02917-x.
- [9] R. F. Mansour *et al.*, "Energy aware fault tolerant clustering with routing protocol for improved survivability in wireless sensor networks," *Computer Networks*, vol. 212, p. 109049, Jul. 2022, doi: 10.1016/j.comnet.2022.109049.
- [10] D. Bhanu and R. Santhosh, "Fuzzy enhanced location aware secure multicast routing protocol for balancing energy and security in wireless sensor network," *Wireless Networks*, vol. 30, no. 7, pp. 6569–6588, Oct. 2024, doi: 10.1007/s11276-023-03461-y.
- [11] M. K. Roberts and P. Ramasamy, "An improved high performance clustering based routing protocol for wireless sensor networks in IoT," *Telecommunication Systems*, vol. 82, no. 1, pp. 45–59, Jan. 2023, doi: 10.1007/s11235-022-00968-1.
- [12] G. Mahalakshmi, S. Ramalingam, and A. Manikandan, "An energy efficient data fault prediction based clustering and routing protocol using hybrid ASSO with MERNN in wireless sensor network," *Telecommunication Systems*, vol. 86, no. 1, pp. 61–82, May 2024, doi: 10.1007/s11235-024-01109-6.
- [13] D. Sivakumar, S. S. Devi, and T. Nalini, "Energy aware clustering protocol using chaotic gorilla troops optimization algorithm for wireless sensor networks," *Multimedia Tools and Applications*, vol. 83, no. 8, pp. 23853–23871, Aug. 2023, doi: 10.1007/s11042-023-16487-3.
- [14] S. D. Mishra and D. Verma, "Energy-efficient and reliable clustering with optimized scheduling and routing for wireless sensor networks," *Multimedia Tools and Applications*, vol. 83, no. 26, pp. 68107–68133, Mar. 2024, doi: 10.1007/s11042-024-18623-z.
- [15] V. Verma and V. K. Jha, "Secure and energy-aware data transmission for IoT-WSNs with the help of cluster-based secure optimal routing," *Wireless Personal Communications*, vol. 134, no. 3, pp. 1665–1686, Feb. 2024, doi: 10.1007/s11277-024-10983-x.
- [16] S. Yadawad and S. M. Joshi, "Efficient energy consumption and fault tolerant method for clustering and reliable routing in wireless sensor network," *Peer-to-Peer Networking and Applications*, vol. 17, no. 3, pp. 1552–1568, May 2024, doi: 10.1007/s12083-024-01664-4.
- [17] G. S. Karthick, "Energy-aware reliable medium access control protocol for energy-efficient and reliable data communication in wireless sensor networks," *SN Computer Science*, vol. 4, no. 5, p. 449, Jun. 2023, doi: 10.1007/s42979-023-01869-z.
- [18] M. Kingston Roberts and J. Thangavel, "An improved optimal energy aware data availability approach for secure clustering and routing in wireless sensor networks," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 3, Mar. 2023, doi: 10.1002/ett.4711.
- [19] A. Vinitha, M. S. S. Rukmini, and Dhirajsunehra, "Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 5, pp. 1857–1868, May 2022, doi: 10.1016/j.jksuci.2019.11.009.
- [20] D. Habbanakuppe Balachandra, P. Chaluve Gowda, and N. P. Kanakapura Shivaprasad, "Secure cluster-based routing using multi objective-trust centric artificial algae algorithm for wireless sensor network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, p. 1618, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1618-1628.




- [21] R. N. Kumar and P. Srimanchari, "A trust and optimal energy efficient data aggregation scheme for wireless sensor networks using QGAOA," *International Journal of System Assurance Engineering and Management*, vol. 15, no. 3, pp. 1057–1069, Mar. 2024, doi: 10.1007/s13198-023-02189-4.
- [22] M. M. Asiri *et al.*, "Metaheuristics enabled clustering with routing scheme for wireless sensor networks," *Computers, Materials & Continua*, vol. 73, no. 3, pp. 5491–5507, 2022, doi: 10.32604/cmc.2022.031345.
- [23] S. S. Kalburgi and M. Manimozhi, "Taylor-spotted hyena optimization algorithm for reliable and energy-efficient cluster head selection based secure data routing and failure tolerance in WSN," *Multimedia Tools and Applications*, vol. 81, no. 11, pp. 15815–15839, May 2022, doi: 10.1007/s11042-022-12302-7.
- [24] A. A. Khan *et al.*, "GAN-IoTVS: a novel internet of multimedia things-enabled video streaming compression model using GAN and fuzzy logic," *IEEE Sensors Journal*, vol. 23, no. 23, pp. 29434–29441, Dec. 2023, doi: 10.1109/JSEN.2023.3316088.
- [25] F. Mehmood, A. A. Khan, H. Wang, S. Karim, U. Khalid, and F. Zhao, "BLPCA-ledger: a lightweight plenum consensus protocols for consortium blockchain based on the hyperledger indy," *Computer Standards & Interfaces*, vol. 91, p. 103876, Jan. 2025, doi: 10.1016/j.csi.2024.103876.
- [26] A. Chhabra, A. G. Hussien, and F. A. Hashim, "Improved bald eagle search algorithm for global optimization and feature selection," *Alexandria Engineering Journal*, vol. 68, pp. 141–180, Apr. 2023, doi: 10.1016/j.aej.2022.12.045.
- [27] H. Youssef, S. Kamel, M. H. Hassan, L. Nasrat, and F. Jurado, "An improved bald eagle search optimization algorithm for optimal home energy management systems," *Soft Computing*, vol. 28, no. 2, pp. 1367–1390, Jan. 2024, doi: 10.1007/s00500-023-08328-0.
- [28] A. Ayub Khan, S. Dhahi, J. Yang, W. Alhakami, S. Bourouis, and P. L. Yee, "B-LPoET: a middleware lightweight Proof-of-elapsed time (PoET) for efficient distributed transaction execution and security on blockchain using multithreading technology," *Computers and Electrical Engineering*, vol. 118, p. 109343, Aug. 2024, doi: 10.1016/j.compeleceng.2024.109343.

BIOGRAPHIES OF AUTHORS



Asha Rani Mahadeva    has completed B.E in information science and engineering and M.Tech in computer network engineering and research scholar from VTU, Belagavi, and Karnataka, India. She has 15 years of teaching experience in engineering college. Currently working as an assistant professor in GSSSIETW, Mysuru, India. She can be contacted at email: asharanim@gsss.edu.in.



Roopashree Hejjaji Ranganathasharma    has completed B.E (E&C) in M.Tech (CS&E) from VTU, Belagavi, Karnataka, India, and Ph.D. from CHRIST (Deemed to be University) Bengaluru, Karnataka, India. She has around 13 years of industrial experience and three years of teaching experience. she is presently working as a professor and HOD in dept of AI&DS at GSSSIETW, Mysuru, India. She can be contacted at email: roopashreehr@gsss.edu.in.



Yogeesh Ambalagere Chandrashekaraiah    has completed B.E, M.Tech, and Ph.D. from Visvesvaraya Technological University Belagavi, Karnataka, India. Currently working as an assistant professor in CS&E, Government Engineering College, Chamarajnagar, Karnataka, India. His area of interest is wireless sensor network, IOT, and machine learning. He can be contacted at email: yogeesh13@gmail.com.