

A Novel Optimization based Energy Efficient and Secured Routing Scheme using SRFIS-CWOSRR for Wireless Sensor Networks

S. Srinivasa Rao¹, K. Chenna Keshava Reddy², S. Ravi Chand³

¹Research Scholar, Department of Electronics and Communication Engineering, Jawaharlal Nehru Technological University, Hyderabad, Telangana-500085, India, Email: srinivasaraoece2022@gmail.com

²Professor & Principal, Department of Electronics and Communication Engineering, Jyothishmathi College of Engineering and Technology, Sharmirpet, Telangana-500078, India. E-mail: kesavary@hotmail.com

³Professor & Head, Department of Electronics and Communication Engineering, Nalla Narasimha Reddy Education Society's Group of Institutions- Integrated Campus, Hyderabad-500088, Telangana, India. Email: ravichandsankuru1@gmail.com

*Correspondence: S.Srinivasa Rao; Email: srinivasaraoece2022@gmail.com

ABSTRACT- Ensuring the reliable and energy efficient data routing in Wireless Sensor Networks (WSNs) is still remains one of the challenging and demanding tasks due to its dynamic architecture. For this purpose, the different types of routing methodologies and security schemes have been developed in the conventional works. However, it faced the problems related to increased network overhead, high cost consumption, reduced Quality of Service (QoS), and inefficient bandwidth utilization. The main contribution of this work is to implement an optimization based secured routing methodology for establishing an energy efficient data communication in WSNs. For clustering the nodes, the parameters such as residual energy, trust score, and mobility have been considered, which also helps to simplify the networking operations. Moreover, the outliers in the network are detected with the help of Spatial Temporal Fuzzy Inference System technique, which generates the set of inference rules based on the distance, energy, and mobility measures. Also, the Crow-Whale Optimized Secured Robin Routing (CWOSRR) is used to enable the data transmission in the network through the optimized path, which avoids the loss of information. During the simulation analysis, the results of the proposed technique is validated and compared by using various performance measures.

Keywords: Wireless Sensor Networks (WSNs), Clustering, Spatial Temporal Fuzzy Inference System (SRFIS), Crow-Whale Optimized Secured Robin Routing (CWOSRR), Outlier Detection, and Energy Efficient Data Transmission.

ARTICLE INFORMATION

Author(s): S. Srinivasa Rao, K. Chenna Keshava Reddy and S. Ravi Chand;

Received: 22/06/2022; **Accepted:** 10/08/2022; **Published:** 18/09/2022;

e-ISSN: 2347-470X;

Paper Id: IJEER220628;

Citation: 10.37391/IJEER.100338;

Webpage-link:

<https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100338.html>



Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) [1, 2] have gained significant attention in the present days, due to their benefits of ubiquitous devices, topology, scalability, and controlling sensors. Also, the WSN has been increasingly used in different types of applications systems such as surveillance of monitoring, military applications, medical applications, agriculture, and etc [3-5]. But, ensuring the reliable and energy efficient data routing in WSN is still remains one of the complex and challenging tasks. Here, the routing protocols play an essential role in determining the performance of network, because which helps to transmit the packets from the source to the desired destination. The different types of routing protocols used in WSNs are as follows: the protocols based on the

network structure, path establishment, protocol operation, and next hop selection.

Also, an energy is one of the most important and essential factor need to be satisfied in the network. Normally, the sensor nodes consume more energy for performing the networking operations like transmission, reception, forwarding, sensing, and etc. The increased energy consumption reduces the lifetime of both sensor nodes and network, hence it must be improved for guaranteeing the improved performance of network. Moreover, the WSN is highly susceptible to outliers or malicious nodes, which objects to interrupt the normal operations of network by performing the attacking activities. So, an establishment of optimal routing with ensured security is one of the challenging and demanding task, because which determines the entire performance of networking system. For this purpose, there are many research works [6-8] have been carried out with the focus on optimal path selection and secured routing in WSN. Still, it faces the major challenges of high network overhead, increased loss of packets, reduced reliability in routing, and lack of security [9-11]. In order to solve these problems, the proposed research work intends to develop the novel mechanisms for establishing an optimal and secured routing in the network. The major objectives of this work are as follows:

- To simplify the networking operations with increased Quality of Service (QoS) performance, the node clustering is

performed by grouping the nodes based on the residual energy, distance, mobility, and trust score measures.

- To detect the outliers for enabling the reliable and secured data transmission in the network, the Spatial Temporal Fuzzy Inference System (SRFIS) technique is deployed.
- To select the optimal routing paths based on the factors of energy, trust score, and authentication score, an integrated Crow-Whale Optimized Secured Robin Routing (CWOSRR) technique is implemented.
- To ensure the successful and valid data communication in the network by developing a secured optimization based routing scheme.
- To simulate and compare the results of proposed SRFIS-CWOSRR technique, various evaluation measures such as delay, residual energy, packet loss rate, delivery ratio, number of alive nodes, and network lifetime are considered during performance analysis.

2. RELATED WORKS

This section discusses about some of the recent state-of-the-art energy efficient routing algorithms, protocols, and optimization methodologies used for improving the QoS of WSN. Vinitha and Rukmini [12] deployed a Taylor based hybrid optimization technique for enabling a secure data routing in WSNs. The main purpose of this work was to perform the multi-hop routing in the network by using an energy efficient clustering technique. The optimization technique was used for optimally selecting the hops based on the parameters of direct trust, indirect trust, forwarding rate, and integrity factor. Here, the standard LEACH protocol was also used to increase the energy efficiency of network. The multi-hop routing methodology was used to establish an efficient data transmission by grouping the nodes in the form of clusters. Yet, this work limits with the major problems increased loss of data packets, traffic rate, and minimal count of alive nodes. Wohme, *et al* [13] investigated about the performance and effectiveness of various optimized clustering algorithms used for increasing the security of WSNs. Similarly, it includes the optimized clustering techniques based on the concepts of fuzzy logic, Genetic Algorithm (GA), Neural Network (NN), reinforcement learning, and swarm intelligence methodologies. Vijayalakshmi, *et al* [14] deployed a Tabu Particle Swarm Optimization (TPSO) technique for selecting the CHs to improve the energy efficiency of WSNs. The main purpose of this work was to minimize the average packet loss and delay of networks by using the meta-heuristic optimization technique. However, it requires increased time consumption for data transmission and, requires more cost for processing, which degrades the performance of entire network. Singh, *et al* [15] employed a Genetic Algorithm (GA) based mobile sinking technique for determining the optimal paths to enable the data transmission. The different types of QoS parameters highly concentrated on this work were network lifetime, residual energy, throughput, and delay. It mainly objects to minimize the time complexity and, increase the lifetime of network. Qureshi, *et al* [16] introduced a Gateway Clustering Energy Efficient Centroid (GCEEC) based routing protocol to avoid the data transmission failure by optimally selecting the CH. In addition to that, it utilizes an efficient communication channel for enabling the reliable and valid data transmission.

Elhabyan, *et al* [17] used a Pareto optimization methodology incorporated with the Multi-Objective

Evolutionary Algorithms (MOEA) for enabling the reliable, scalable, and energy efficient routing in WSN. In addition to that, the sleep scheduling mechanism was utilized to ensure the increased data delivery and reliability in WSN. Yet, it has the problems of increased loss of data packets, reduced life span, and high time consumption. Reddy, *et al* [18] deployed a Merged Glowworm Optimization technique incorporated with ACO for improving the energy efficiency of networks. The key benefit of using this integrated technique is minimized time complexity and better convergent rate. Visu, *et al* [19] utilized a bio-inspired optimization algorithm, named as, Dual Cluster Head - Krill Herd Optimization (DC-KHO) technique for randomly selecting the path for ensuring the reliable data transmission. The main purpose of this work was to minimize the communication cost and ensuring the energy efficiency of network.

Singh, *et al* [20] investigated about the performance of various multi-objective optimization techniques used in WSNs. Here, it was indicated that the multi-objective optimization techniques [21-23] have been used to increase the network lifetime, coverage, reduce the transmission delay, and packet loss rate. Prashanth, *et al* [24] utilized a novel multi-objective optimization methodology for increasing the QoS of WSN-IoT networks. Here, the optimal solution was used to cover the target objects with reduced energy consumption. Raychaudari, *et al* [25] examined the different types of bio-inspired optimization techniques used for improving the performance of WSNs. From the literature review, it is analyzed that the existing works limit with the following problems: Reduced delivery rate, minimal network lifespan and low count of alive nodes, routing overhead, increased time consumption, and count of dead nodes, and lack of security. Hence, it is more essential to develop an efficient and secured routing methodology for improving the QoS of WSNs. For this purpose, the proposed work objects to implement a new clustering based optimization system for enabling the trusted and reliable data transmission.

3. RESEARCH METHODOLOGY

This section presents the complete description about the proposed methodology used for ensuring the data security, optimal routing and reliable packet transmission of networks. The novel contribution of this work is to develop a clustering based hybrid optimization methodology for optimally selecting the path to enable the data transmission in WSN. In this system, the networking environment is constructed with the set of sensor nodes with the properties of speed, energy level, bandwidth, and etc. After that, the nodes are grouped into the form of clusters, where the Cluster Head (CH) is selected from group of cluster for avoiding the loss of information. Also, the Spatial Temporal Fuzzy Inference System (SR-FIS) is designed for decision management, which also used to detect the malicious nodes in the network based on the behavior analysis model. Here, the Crow-Whale Optimized Secured Robin Routing (CWO-SRR) scheme is developed for optimally selecting the routing paths.

3.1 Cluster Formation

After constructing the network, the nodes having minimum distance value are grouped to form the clusters, which

comprises the modules of cluster formation, CH selection, and maintenance. Here, the clustering is mainly used to group the nodes into the form of clusters, which helps to save the energy during data transmission. Also, the clustering improves the QoS of network with reduced loss of information and energy consumption. For this purpose, an energy efficient clustering mechanism is implemented in the proposed work. In this environment, each and every node participated in the communication is assigned with the unique node number, which is used to identify the nodes for the sub-sequential data communications and transmissions. During the cluster formation, the Euclidean distance between the nodes is estimated for identifying the minimum distance nodes. Here, the main purpose of clustering is to simplify the networking operations with ensured QoS performance. The performance of entire networking system is highly depends on the cluster formation and CH selection.

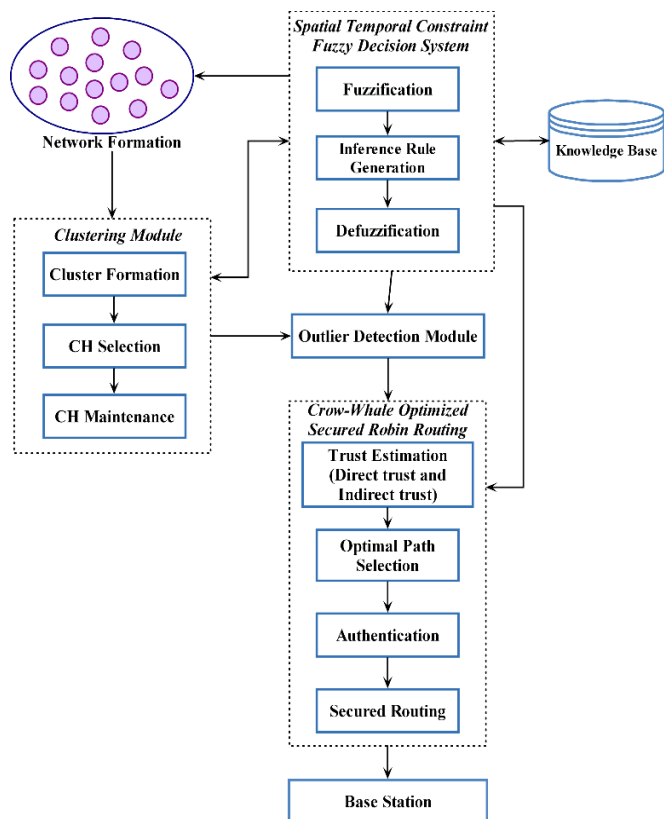


Fig 1. Working flow of the proposed optimized secure routing system

3.2 Spatial Temporal Fuzzy Inference System (SR-FIS)

Here, the main purpose of implementing the SRFIS technique is protect the network against the outliers, which helps to ensure the security by detecting the outliers before enabling the data transmission. The improved performance and QoS of network are entirely depends on its security, because the lack or loss of data packets can degrade the overall system. Also, ensuring the security of network is also one of the important concern in recent days, due to the rapid growth of information technologies. Therefore, the proposed work intends to deploy a SRFIS technique for detecting outliers in the network. Typically, the outliers are considered as the kind of malicious

nodes that targets to degrade the normal operations of network by interrupting the communication. Hence, this kind of nodes should be identified and removed from the network for ensuring the reliable and valid data transmission and communication. Moreover, the outliers are detected from the network based on the properties of energy, packet drop, and delay. The proposed intends to deploy a new algorithm for accurately identifying the outliers from the network before establishing the data transmission. For this purpose, the Spatial Temporal Fuzzy Inference System (SR-FIS) technique is implemented, where the weight values are assigned based on the level of security and distance value. During this process, the euclidean distance is computed between the communicating nodes. The re-clustering is performed after forming the clusters for listing the outlier nodes, where the not-trusted and not-authenticated nodes are properly located based on the fuzzy rules.

In this stage, the weight value is assigned to each node in the cluster based on the parameters of initial distance D , Energy Consumption E_C , and Mobility M_O . Then, the trust value is computed for determining the security level of nodes, where the authentication score is also computed according to the trust level. Here, the fit factor is used to compute the fit factor for choosing the trusted/secured nodes to enable the communication. The main purpose of trust computation is to ensure the data integrity, confidentiality, and validness by selecting the trusted to establish the reliable transmission. Typically, the fit factor is considered as one of the most essential parameter mainly used to compute the energy and trust of nodes exist in the network, where the nodes having maximum trust score and energy level are treated as the secured nodes. The fit factor F_F is calculated as follows:

$$F_F = \frac{1}{2} \times \left[EL_N + \frac{1}{N} \times \sum_{i \in j}^N Tr_{ij} \right] \quad (1)$$

Where, EL_N indicates the energy level of node, N is the total number of nodes exist in the network, and Tr_{ij} denotes the trust value of node. Consequently, the trust and energy level of nodes are estimated by using the following model:

$$NT_{ij} = NT_{i,j}^{di} + NT_{i,j}^{id} + NT_{i,j}^r + NT_{i,j}^b \quad (2)$$

Where, NT_{ij} is the node trust, di indicates the direct trust value, id denotes the indirect trust value, r is the recent trust value, and b indicates the transmitted bytes. The direct trust is estimated for improving the nodal trust, and its value is highly depends on the definite and expected time of computation. It is computed as follows:

$$NT_{i,j}^{di}(time) = \frac{1}{3} \left[NT_{i,j}^{di}(time - 1) - \left[\frac{A_k - Ex_k}{A_k} \right] + \varphi \right] \quad (3)$$

Where, A_k is the approximate time for transmitting the key, E_k denotes the expected amount of time for obtaining the key, and φ indicates the witness factor? Similarly. The indirect trust is also estimated as shown in below:

$$NT_{i,j}^{id}(time) = \frac{1}{N} \sum_{i=1}^N NT_{i,s}^{id}(s)$$

The indirect trust is mainly estimated to validate the trust worthiness of the nodes, where the node receives the key for authentication. Consequently, the recent trust is estimated according to the regression rate of both direct and indirect trust of nodes in the network. The authenticity of node is also computed based on the function of time as shown in below:

$$NT_{i,j}^r(time) = \rho \times NT_{i,j}^{di}(time) + (1 - \rho) \times NT_{i,j}^{in}(time) \quad (4)$$

Where, ρ indicates the constant value. In addition to that, the trust is estimated according to the total number of data bytes transmitted from the source to destination as represented below:

$$NT_{i,j}^\delta = \frac{1}{2} \times \left[\frac{\delta_{i,j}^i}{DP_L} + \frac{\delta_{i,j}^j}{DP_L} \right] \quad (5)$$

Where, $\delta_{i,j}^i$ indicates the amount of data bytes transmitted from the source to desired destination, $\delta_{i,j}^j$ denotes the actual amount of data bytes received by the destination from the source, and DP_L is the data packet limit. After computing the trust, the energy level of all nodes is computed for extending the lifespan of network. Typically, the entire lifetime and performance of network is highly depends on the energy of nodes, hence it must be properly controlled for ensuring the reliability of network. Let, consider that the energy level of node is Eg_0 at the initial data transmission/communication. Once the destination node receives the data sent by the source, there may be an energy loss, because which is highly depends on the distance between the nodes. Here, the energy dissipation factor is estimated for determining the energy level of node after data transmission/reception as shown in below:

$$\varepsilon_s(1, d_x) = \begin{cases} 1\varepsilon_{el} + 1\varepsilon_{af}d_x^2 & \text{for } d_x < d_{x0} \\ 1\varepsilon_{el} + 1\varepsilon_{am}d_x^4 & \text{for } d_x > d_{x0} \end{cases} \quad (6)$$

$$d_{x0} = \sqrt{\varepsilon_{af}/\varepsilon_{am}} \quad (7)$$

Where, ε_{el} indicates the electrical energy, ε_{af} denotes the amplifier energy in free space, and ε_{am} is the amplifier energy in multipath. After evaluating the trust and energy level of node, the authentication is performed for determining that whether the node can be participated in the communication or not. Here, the authentication is verified based on the identity of node as shown in below:

$$Id_N(i) = \text{Node } Id_N(i) || IP \text{ address}(i) || \text{Cluster member } Id_N(i) \quad (8)$$

Where, Id_N indicates the identity of node. Based on the level of energy, and trust, the secured nodes are selected for enabling the data transmission.

3.3 Crow-Whale Optimized Secured Robin Routing (CWO-SRR)

After authenticating the nodes, the optimized routing path is selected for establishing the communication between the source and destination nodes with ensured reliability. In this work, the optimized paths are selected based on the best fitness function estimated by using an integrated Crow-Whale Optimization (CWO) mechanism. Here, the randomly generated routings are optimized for according to the objective function estimated by using the fit factor of sensor nodes in the network. In a multicast

routing environment, there are multiple destinations can receive the data from the single source through some intermediate communication nodes. The solution vector is estimated to enable the multicast routing in the network based on the fit factor. In this model, the objective function is computed based on the level of energy and trust as shown in below:

$$Obj = \sum_{i=1}^{ND_S} \sum_{j=1}^{ND_{Sij}} F_{ij} \quad (9)$$

Where, ND_S indicates the dimension, ND_{Sij} denotes the number of intermediate nodes between the source and destination, and F_{ij} indicates the fitness function. In this work, the main purpose of using the CWO technique is to enable the multicast routing by optimally selecting the routes. Also, the CWO technique has an increased ability to balance the properties of intensification and diversification by determining the awareness probability. The CWO technique has an increased ability to balance the properties of intensification and diversification by determining the awareness probability. Moreover, this technique incorporates the benefits of both Crow Search (CS) and Whale Optimization (WO) methods for enabling the data transmission with reduced computational cost. In this technique, P number of crows are initialized in the searching space with its appropriate positions represented as H^k , where $(1 \leq k \leq P)$. Then, its solution matrix is constructed as follows:

$$H = \begin{bmatrix} H_1^1 & H_2^1 & \dots & H_x^1 \\ H_1^2 & H_2^2 & \dots & H_x^2 \\ \vdots & \vdots & \vdots & \vdots \\ H_1^k & H_2^k & \dots & H_x^k \end{bmatrix} \quad (10)$$

Then, the crows are update their positions on the memory as represented below:

$$V = \begin{bmatrix} V_1^1 & V_2^1 & \dots & V_x^1 \\ V_1^2 & V_2^2 & \dots & V_x^2 \\ \vdots & \vdots & \vdots & \vdots \\ V_1^k & V_2^k & \dots & V_x^k \end{bmatrix} \quad (11)$$

Consequently, the update function is estimated to identify the crow in the searching space as shown in below:

$$H^{k,\vartheta+1} = H^{k,\vartheta} + RN \times FL^{k,\vartheta} \times (V^{c,\vartheta} - |H^{k,\vartheta}|) \quad (12)$$

Where, $H^{k,\vartheta+1}$ represents the position of crow k at time $\vartheta + 1$, RN denotes the random number ranging from 0 to 1, $FL^{k,\vartheta}$ is the flight of length, and $V^{c,\vartheta}$ indicates the position of crow. Here, the CS algorithm is modified with the WO as represented below:

$$H^{k,\vartheta+1} = V^{c,\vartheta} - \overrightarrow{CV} \cdot \overrightarrow{CM} ; \alpha < 0.5 \quad (13)$$

Where, α is the random probability, \overrightarrow{CV} and \overrightarrow{CM} are the coefficient vectors.

$$H^{k,\vartheta+1} = \frac{\overrightarrow{CV}}{\overrightarrow{CV} - r1 \times S^{k,\vartheta}} \{r1 \times S^{k,\vartheta} \times V^{k,\vartheta}\} + \frac{(1-r1 \times S^{k,\vartheta})}{\overrightarrow{CV}} [\overrightarrow{CV} \cdot \overrightarrow{CM} \cdot V^{c,\vartheta} - V^{c,\vartheta}] \quad (14)$$

According to the feasibility of crow, the objective function is estimated as shown in below:

$$V^{c,\vartheta+1} = \begin{cases} H^{k,\vartheta+1} & \text{fit}(H^{k,\vartheta+1}) > \text{fit}(V^{k,\vartheta}) \\ V^{k,\vartheta} & \text{Otherwise} \end{cases} \quad (15)$$

Where, $\text{fit}(H^{k,\vartheta+1})$ indicates the fitness of solution at time $\vartheta + 1$. The obtained solutions are repeated until reaching the maximum number of iterations. Based on this process, the best optimal solution is obtained for enabling the data routing in WSN with ensured reliability and scalability. After estimating the best optimal solution, the routing path between the source and destination nodes is constructed to enable the data transmission. The primary advantages of using CWO-SRR technique are increased convergence rate, optimized performance, reaches the best solution with reduced number of iterations, and minimal processing time.

4. RESULTS AND DISCUSSION

This section presents the simulation and comparative analysis of conventional and proposed optimization based routing methods, where the results are evaluated and compared by using various performance measures. *Figure 2* compares the existing and proposed routing techniques based on the number of alive nodes in the network with respect to the simulation round. For this analysis, the conventional SeLeach, and tree based logic routing methodologies are considered.

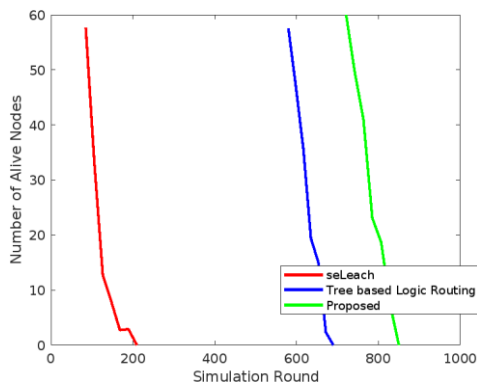


Fig 2. Number of alive nodes Vs Simulation round

Typically, the lifetime of network is highly depends on the number of alive nodes, which are defined as the sensor nodes that could be active after executing the maximum number of simulation rounds. The increased number of alive nodes ensure the improved system performance and network lifespan. According to this evaluation, it is identified that the proposed SRFIS- CWOSRR technique outperforms the other approaches with increased number of alive nodes. Due to optimized routing process, the energy efficiency of the sensor nodes could be highly increased, hence the count of alive nodes of proposed system are greater than the existing techniques [26]. *Figure 3* validates the number of alive nodes exist in the network for both existing [27] and proposed routing strategies with respect to varying number of rounds. For this analysis, some other recent state-of-the-art approaches are considered to validate the effectiveness and performance of the proposed routing methodology. Consequently, the average energy consumption of the conventional and proposed routing methodologies are validated and compared in *figure 4*. The energy consumption of

network is defined based on the amount of energy consumed by the communicating nodes, and increased level of energy consumption reduces the lifetime of both nodes and network. Hence, it should be minimized by enabling the proper routing for data transmission and communication. Based on the obtained results, it is stated that the average energy consumption of the proposed SRFIS- CWOSRR approach is efficiently reduced, when compared to the other techniques.

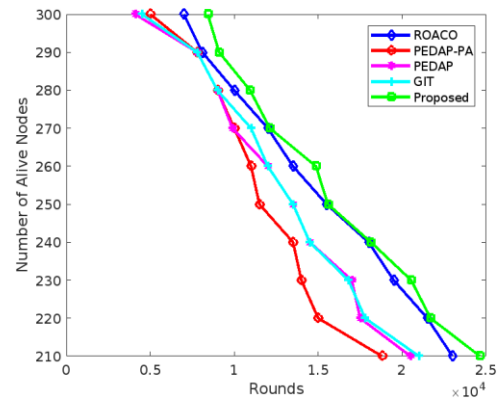


Fig 3. Number of alive nodes

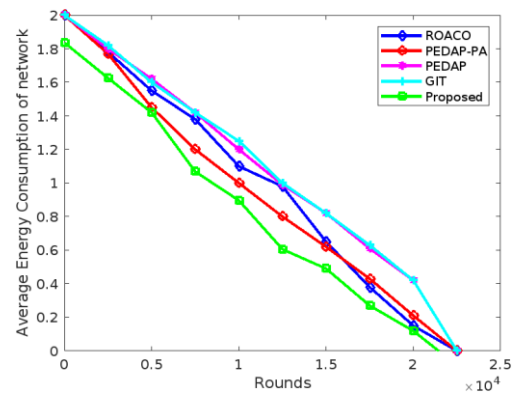


Fig 4. Average energy consumption

Figure 5 validates the network delay of existing [28] and proposed routing methodologies with respect to varying number of nodes in the network. It is also defined as the latency of network, which is estimated based on the amount of time taken by a data packet to reach the destination from the source. The SRFIS- CWOSRR technique provides the reduced network delay, when compared to the other existing approaches. *Figure 6* compares the packet drop ratio of existing and proposed routing methodologies with respect to varying rounds of operations.

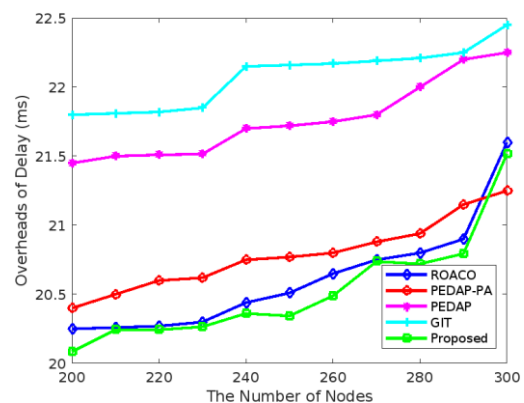


Fig 5. Network delay

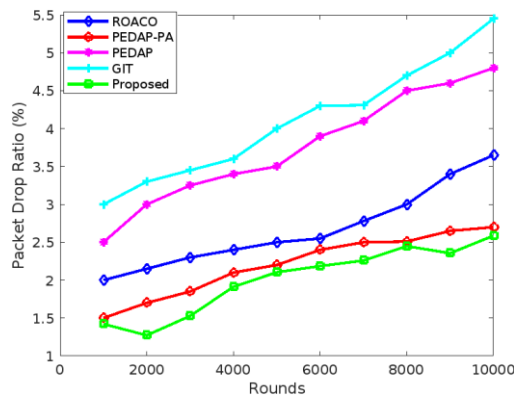


Fig 7. Packet drop ratio

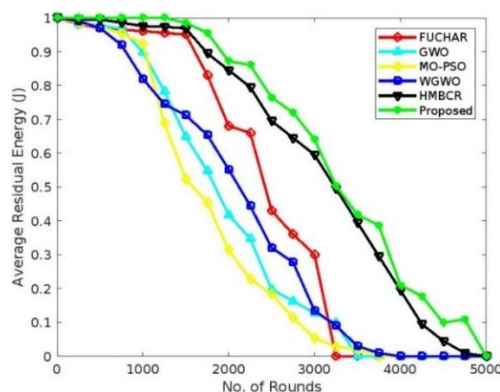


Fig 8. Average residual energy analysis

This analysis also depicts that the proposed SRFIS- CWOSRR technique could efficiently reduce the packet drop ratio by enabling the reliable and successful data transmission in the network. Consequently, *figure 7* validates the average residual analysis of both existing [29] and proposed techniques with respect to varying rounds of operations. The average delay is also estimated for both existing and proposed routing methods with respect to different number of nodes. These evaluations indicate that the proposed SRFIS- CWOSRR outperforms the other approaches with increased average residual energy and reduced delay of network. By using the optimal solution, the an energy efficeint data routing is established in the network, which supports to reduce the packet drop ratio as well as average residual energy.

5. CONCLUSION

The main purpose of this work is to develop an energy efficient and secured optimization based routing scheme for ensuring the reliable and valid data transmission in WSNs. For this purpose, an advanced and integrated soft-computing methodologies are implemented in this work. Here, the main purpose of clustering is to simplify the networking operations with ensured QoS performance. Then, the SRFIS technique is implemented protect the network against the outliers, which helps to ensure the security by detecting the outliers before enabling the data transmission. During optimization, the weight values are estimated corresponding to the factors of security and distance value. Moreover, the euclidean distance is computed between the communicating nodes, where the set of fuzzy inference rules are generated for detecting outliers based on the parameters of distance, energy, and mobility. Then, the optimized routings paths are selected based on the best fitness function estimated

by using an integrated Crow-Whale Optimization (CWO) mechanism. It is used for establishing the communication between the source and destination nodes with ensured reliability. During evaluation, the simulation and comparative analysis have been performed for validating the performance and effectiveness of the proposed scheme. Based on the evaluation, it is analyzed that the SRFIS- CWOSRR technique outperforms the other approaches with increased number of alive nodes, residual energy, packet delivery ratio, reduced latency, packet loss rate, and minimized network lifetime. In future, this work can be extended by implementing a new optimization and machine learning methodologies for ensuring the security of an integrated WSN-IoT systems. In addition, a new protocol can be developed for establishing the reliable and secured data transmission in an integrated network.

6. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template.

REFERENCES

- [1] S. M. Chowdhury and A. Hossain, "Different energy saving schemes in wireless sensor networks: A survey," *Wireless Personal Communications*, vol. 114, pp. 2043-2062, 2020.
- [2] R. E. Mohamed, A. I. Saleh, M. Abdelrazzak, and A. S. Samra, "Survey on wireless sensor network applications and energy efficient routing protocols," *Wireless Personal Communications*, vol. 101, pp. 1019-1055, 2018.
- [3] C. Nakas, D. Kandris, and G. Visvardis, "Energy efficient routing in wireless sensor networks: A comprehensive survey," *Algorithms*, vol. 13, p. 72, 2020.
- [4] T. A. Alghamdi, "Energy efficient protocol in wireless sensor network: optimized cluster head selection model," *Telecommunication Systems*, vol. 74, pp. 331-345, 2020.
- [5] R. Priyadarshi, S. K. Soni, and V. Nath, "Energy efficient cluster head formation in wireless sensor network," *Microsystem Technologies*, vol. 24, pp. 4775-4784, 2018.
- [6] J. Bhola, S. Soni, and G. K. Cheema, "Genetic algorithm based optimized leach protocol for energy efficient wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 1281-1288, 2020.
- [7] R. Wan and N. Xiong, "An energy-efficient sleep scheduling mechanism with similarity measure for wireless sensor networks," *Human-centric Computing and Information Sciences*, vol. 8, pp. 1-22, 2018.
- [8] N. Ramluckun and V. Bassoo, "Energy-efficient chain-cluster based intelligent routing technique for Wireless Sensor Networks," *Applied Computing and Informatics*, 2018.
- [9] Đ. Bandur, B. Jakšić, M. Bandur, and S. Jović, "An analysis of energy efficiency in Wireless Sensor Networks (WSNs) applied in smart agriculture," *Computers and Electronics in Agriculture*, vol. 156, pp. 500-507, 2019.
- [10] C. S. Abella, S. Bonina, A. Cucuccio, S. D'Angelo, G. Giustolisi, A. D. Grasso, et al., "Autonomous energy-efficient wireless sensor network platform for home/office automation," *IEEE Sensors Journal*, vol. 19, pp. 3501-3512, 2019.
- [11] A. Hamzah, M. Shurman, O. Al-Jarrah, and E. Taqieddin, "Energy-efficient fuzzy-logic-based clustering technique for hierarchical routing protocols in wireless sensor networks," *Sensors*, vol. 19, p. 561, 2019.
- [12] A. Vinitha and M. Rukmini, "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*, 2019.
- [13] D. Wohwe Sambo, B. O. Yenke, A. Förster, and P. Dayang, "Optimized clustering algorithms for large wireless sensor networks: A review," *Sensors*, vol. 19, p. 322, 2019.

- [14] K. Vijayalakshmi and P. Anandan, "A multi objective Tabu particle swarm optimization for effective cluster head selection in WSN," Cluster computing, vol. 22, pp. 12275-12282, 2019.
- [15] M. K. Singh, S. I. Amin, and A. Choudhary, "Genetic algorithm based sink mobility for energy efficient data routing in wireless sensor networks," AEU-International Journal of Electronics and Communications, vol. 131, p. 153605, 2021.
- [16] K. N. Qureshi, M. U. Bashir, J. Lloret, and A. Leon, "Optimized cluster-based dynamic energy-aware routing protocol for wireless sensor networks in agriculture precision," Journal of sensors, vol. 2020, 2020.
- [17] R. Elhabyan, W. Shi, and M. St-Hilaire, "A Pareto optimization-based approach to clustering and routing in Wireless Sensor Networks," Journal of Network and Computer Applications, vol. 114, pp. 57-69, 2018.
- [18] D. L. Reddy, C. Puttamadappa, and H. Suresh, "Merged glowworm swarm with ant colony optimization for energy efficient clustering and routing in Wireless Sensor Network," Pervasive and Mobile Computing, vol. 71, p. 101338, 2021.
- [19] P. Visu, T. S. Praba, N. Sivakumar, R. Srinivasan, and T. Sethukarasi, "Bio-inspired dual cluster heads optimized routing algorithm for wireless sensor networks," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 3753-3761, 2021.
- [20] O. Singh, V. Rishiwal, R. Chaudhry, and M. Yadav, "Multi-objective optimization in WSN: Opportunities and challenges," Wireless Personal Communications, vol. 121, pp. 127-152, 2021.
- [21] M. Malakar, "TLBO based cluster-head selection for multi-objective optimization in wireless sensor networks," in Nature inspired computing for wireless sensor networks, ed: Springer, 2020, pp. 303-319.
- [22] K. Singh, K. Singh, and A. Aziz, "Congestion control in wireless sensor networks by hybrid multi-objective optimization algorithm," Computer Networks, vol. 138, pp. 90-107, 2018.
- [23] J. Lou, "Location-based multi-objective optimization routing algorithm for WSN," in Recent Developments in Intelligent Computing, Communication and Devices, ed: Springer, 2019, pp. 523-529.
- [24] A. Prasanth and S. Jayachitra, "A novel multi-objective optimization strategy for enhancing quality of service in IoT-enabled WSN applications," Peer-to-Peer Networking and Applications, vol. 13, pp. 1905-1920, 2020.
- [25] A. Raychaudhuri and D. De, "Bio-inspired algorithm for multi-objective optimization in wireless sensor network," in Nature inspired computing for wireless sensor networks, ed: Springer, 2020, pp. 279-301.
- [26] M. Mathapati, T. S. Kumaran, A. Muruganandham, and M. Mathivanan, "Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 6047-6055, 2021.
- [27] S. Sathya and K. Umadevi, "An optimized distributed secure routing protocol using dynamic rate aware classified key for improving network security in wireless sensor network," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 7165-7171, 2021.
- [28] Z. Zhang, J. Li, and N. Xu, "Robust optimization based on ant colony optimization in the data transmission path selection of WSNs," Neural Computing and Applications, vol. 33, pp. 17119-17130, 2021.
- [29] S. Al-Otaibi, A. Al-Rasheed, R. F. Mansour, E. Yang, G. P. Joshi, and W. Cho, "Hybridization of Metaheuristic Algorithm for Dynamic Cluster-Based Routing Protocol in Wireless Sensor Networks," IEEE Access, vol. 9, pp. 83751-83761, 2021.
- [30] L. Jenila and R. Aroul Canessane (2022), Cross Layer Based Dynamic Traffic Scheduling Algorithm for Wireless Multimedia Sensor Network. IJEER 10(2), 399-404. DOI: 10.37391/IJEER.100256.



© 2022 by S. Srinivasa Rao, K. Chenna Keshava Reddy and S. Ravi Chand. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).