Eximia Journal

(ISSN 2784-0735)

Vol. 13

2024

Eximia Journal
Vol. 13, 729-739, January, 2024
ISSN: 2784-0735
www.eximiajournal.com

Optimizing Cluster Head Selection through improved Memetic Algorithm and Blockchain Technology for Securing WSN

Huda H. Ali[1] , Ruwaida M. Yas[2] , Maysaa H. Abdulameer[3]

[1]Department of computer engneering techneques, Imam Al-Kadhum University College, Baghdad, Iraq, [2,3]Informatics Institute for Post-Graduation Studie, Iraqi Commission for Computer & Informatic, Baghdad, Iraq

burdenmay2018@gmail.com

Abstract. Wireless Sensor Networks (WSNs) contain numerous wireless sensor nodes positioned around the geographical positions. The WSN used in several applications necessity to be efficient and secured, Hence the organization of trustworthy nodes and links in WSN offers more secure data transmission in Secured Wireless Sensor Networks (SWSNs) , Therefore, construction of secure and efficient WSN is acritical and challenged task. In this paper, for efficiently choose of cluster head (which is work to have data from the S.Ns and deliver it to the B.S) Improved Memetic Algorithms is proposed to used. Moreover, to ensure cluster head (CH) authenticity in order to identify malicious nodes and avoid attacks, Blockchain technique is implemented, in the proposed method; mischievous nodes would be found and removed from the WSN. Finally choosing the best route based on two parameters, residual energy and the distance from next CH and Basie station (BS). The proposed methodology proved its efficiency and security through simulation implementation results, which compared with similar study results.

Keywords. WSN, Memetic algorithm, blockchain, authentication, nods, cluster head

1. INTRODUCTION

A WSN is made up of huge number of randomly spread sensor nodes, which sense and pass on data such as temperature, pressure, humidity, light, and sound [1]. That mean WSNs play a serious role in various applications, and correct localization of sensor nodes is vital for their effective operation. In recent years, optimization algorithms have garnered significant attention as a means of enhancing the WSN node localization [2]. WSNs must deal with two substantial challenges, security and energy consumption, continuously enhancing each other. As the level of security of WNS increases or decreases, the system's energy requirements also increase accordingly [3]. The challenges expert in WSNs configuration, are commonly associated to its stringent limitations, which integrate energy, transmission measurements, memory, computational capabilities and on the way to the necessities of the specific application. Due to the high-energy utilization and data processing requirements, the use of outdated algorithms

Eximia Journal
Vol. 13, 729-739, January, 2024
ISSN: 2784-0735
www.eximiajournal.com

has frequently been corrupted. In this sense, current researchers have begun using optimization approaches in the field of wireless sensor networks. However, efforts for overcrowding control technique in sensor networks using optimization model has not yet been finished to any excessive extent in the nonfiction [4]. In other hand, the problem of computer network data and information security has become one of the problems that must be seriously faced and urgently solved [5]. Security and energy effectiveness are mutually gotten as critical characteristics in WSN-based IoT that are disturbed with extending network lifetime. Researchers used a variety of approaches to create a smart security system to address the aforementioned issues. A variety of performance indicators is used to validate the generated systems in their study [6]. Many network edge devices and real-world items are combined with wireless sensors to display and gather real-time data from the observing area. Subsequently, this construction has reformed with the creation of the Internet of Thing (IoT) [7]. In latest years, optimization algorithms have bring in important thoughtfulness as a resources of improving the WSN node localization, Optimization algorithms offer a influential methodology to develop the localization manner in WSNs by leveraging mathematical optimization procedures to gain ideal solutions . These algorithms intention to adjust localization accurateness, scalability, computational complexity, and strength. By articulating the localization challenging as an optimization mission, these algorithms can efficiently achievement the existing amounts and constraints to accurately guesstimate the locations of the sensor nodes [2].

Memetic computing is a topic in computer science, which reflects intricate constructions such as the grouping of simple agents, and memes, whose evolutionary interfaces principal to intelligent complexes accomplished of problem solving. The establishing foundation of this subject has been the concept of memetic algorithms, that is a class of optimization algorithms whose structure is characterized by an evolutionary framework and a list of local search components [8]. The blockchain offers a secure way to communicate across networked devices. Nevertheless, malicious interferences and cyber-attacks attitude a danger to IoT network systems .A blockchain is devoted to as the chain of blocks in a digital layout. It is also stated to as the dispersed ledger that annals all transactions. The blockchain has even now been subjugated for organization of individual distinctiveness by a number of researchers in the field of research community [9].

In this paper, Memetic algorithm and blockchain technique is employee to made efficient and secure WSN. In this paper, memetic algorithms and blockchain technique are used to improve WSN efficiency and security.

2. CONTRIBUTIONS

This paper presents an improved memetic Secure Clustering Routing Technique accurately custom made for WSNs a blockchain based. Our contributions are as follows.

• More secure and energy-efficient, clustering routing solution is provided to statement many security hazards challenged by Wireless Sensor Networks., Blockchain technology into the clustering routing technique of WSNs was proposed to use.

• Based on a developed Memetic Algorithm, An enhanced CH selection technique in WSNs clustering routing was proposed, where efficiently refining the value of clustering results of routing protocol.

• An enhanced route choice technique in WSNs routing algorithm was proposed, which

Eximia Journal
Vol. 13, 729-739, January, 2024
ISSN: 2784-0735
www.eximiajournal.com

successfully improves the quality of routing outcomes.
• An improved route maintenance technique in WSNs routing algorithm was proposed which successfully expands the NW lifetime.

3. LITERATURE REVIEW

The researchers throughout last year's still in suggested solution for efficiency and security of WSNs as its shown in the next section where:
A blockchain based multi-hop routing protocol and clustering model for Wireless Sensor Networks (WSNs) has been suggested in 2023 by Muhammad Faisal and Ghassan Husnain. The model reveals three restrictions for cluster head select residual energy, distance from base station, and packet transfer ratio. The protocol usages Energy-Efficient Adhoc On-demand Distance Vector for data transmission, the simulation outcomes show that the suggested I-LEACH protocol implements well than the standard ALEACH. [10].
Radha Raman, et al, 2023, a blockchain based modal, Transaction Confirmation Starved of struggle with fake node, (TVDCSN) approach, was offered in this study designed for wireless communication machineries to distinguish malicious nodes and avoid attacks. In the offered mode, mischievous nodes are found and removed from the MWCN and intrusion is forbidden before transmission of the sensitive information to the intended recipient. The performance of the method was evaluated using the following metrics: accuracy of recognition, security, prevention of attack, network overhead, and computation time. Various performance measures are used to assess the method's efficacy, and it is compared with more traditional methods [11].
In 2023 Maytham S. Jabor , et al, , the further struggle of addition BC in WSNs is repaid over and done with an energy minimization methodology, which basically be determined by minimizing the processing load of producing the blockchain hash value, and encrypting and constricting the data that transferable from the cluster-heads to the base station to reduction the overall traffic, principal to condensed energy per node. A explicit (dedicated) circuit is considered to implement the compression procedure, create the blockchain hash values and data encryption. The compression algorithm is proven on chaotic theory. A guesstimate of the power spent by a WSN with a blockchain carrying out with and without the devoted circuit, demonstrates that the hardware design contributes significantly to decrease the consumption of power. When simulating both approaches, the energy consumed when replacing functions by hardware decreases up to 63%. [12].
Ghada Sultan Aljumaie and Wajdi Alhakami, 2022, to protection WSNs a novel irregular of the LEACH-PRO protocol via supposing the blockchain security procedure. The suggested protocol (SLEACH-PRO) does a decentralized authentication means by put on a blockchain to multiple base stations to escape system and performance shortage in the case of a station failure. The security analysis of the SLEACH-PRO is accomplished using Burrows Abadi–Needham (BAN) logic and Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. As well, the SLEACH-PRO is evaluated and corresponding to attendant protocols in terms of computational cost and security level based on its resistance against several attacks. The assessment results exposed that SLEACH-PRO protocol corresponding to other associated protocols is more secure and have less computational cost [13].
A new Secure Clustering Routing Scheme stranded on Blockchain and Swarm Intelligence (BS-SCRM) by Jing Xiao et al in 2024, which used for Wireless Sensor Networks (WSNs), which offerings as a basis in the Internet of Things (IoT) building. Noticing the limitations of standing clustering routing techniques in addressing security threats, simulation results in divergent

Eximia Journal
Vol. 13, 729-739, January, 2024
ISSN: 2784-0735
www.eximiajournal.com

scenarios produce that BS-SCRM increases network period by 24–73% matched with other clustering processes when facing attacks [14].
Four deep learning procedures and a real time message satisfied endorsement (RMCV) scheme based on blockchain introduced by Zahoor etal 2023 ,are used for the recognition of malicious nodes, to overwhelmed the single point of disappointment issue, a decentralized blockchain is prearranged on Cluster Heads and Base Station. Besides, malicious nodes are separate from the network using RMCV and Deep Learning procedures. Likewise, reliable nodes are established in the blockchain network by means of proof of authority agreement protocol; the analysis indicate that blockchain network is robust in contrast to vulnerabilities [15].

4. The Proposed Methodology

The proposed method in this paper consist of multistep, which illustrated in figure 1 and the next sections:

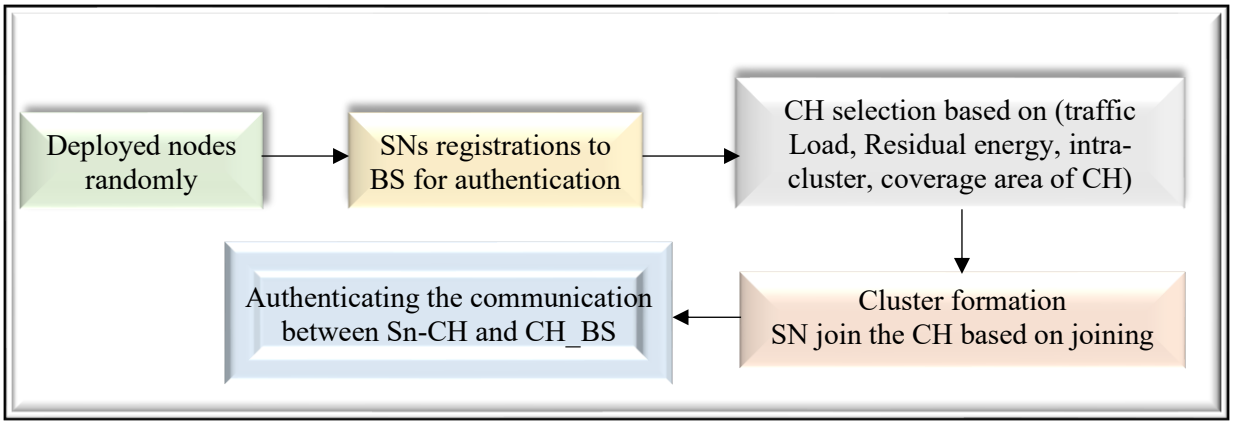

Figure 1 Proposed Methodology Block Diagram

4.1 Nodes' Registration

When all nodes have been deployed in the field, they must first be registered by a base station. Every node send their MAC address to base station for that. Each node is MAC address hashed by the base station through SHA-3 to give each a unique id. It assigns this unique id to the node in question.

4.2 Cluster Head Selection Using Improved Memetic Algorithm

The cluster head (CH), is responsible for receiving the distinguished data from the sensor nodes (SNs) in WSN and then delivered to the (B.S). This procedure makes the energy of the CH rapidly depleted and leads to a network crash. To solve the above problem we recommended an improved memetic algorithm for selecting the CHs.
The memetic algorithm in general consists of five phases, which are population initialization, evaluation, solution selection, solution crossover, mutation, and local search.

4.2.1 Initialization

for inhabitant's initialization, a set of solutions are randomly chosen, which denote the CHs in the network, The length of these results is equivalent to 10% of the total number of sensors deployed within WSN.

Eximia Journal
Vol. 13, 729-739, January, 2024
ISSN: 2784-0735
www.eximiajournal.com

4.2.2 Evaluation

Each solution will be assessed using the fitness function, and it is derived to find the optimal CHs. The optimal CH selection be determined by multiple factors which are: residual energy, average distance from SNs to their CH (intra-cluster distance), data traffic of each CH (Traffic Load), and coverage area of each CH.

The fitness function contingent on the above factors for selecting CHs, and it can be expressed as follows:

$$Minimize\ F = \sum_{i=1}^{m} \left(w_1 * \frac{1}{E_i} + w_2 * \frac{1}{D_i} - w_3 * \frac{1}{L_i} + w_4 * C_i \right) \quad (1)$$

Where:

- m is the number of CH
- i is the ith CH
- $w_1, w_2, w_3, and\ w_4$ are weight factors and their value between (0,1)

a) Energy consumption (E): Represents the total Energy consumed by each sensor node that belong to cluster i (cluster memberCM) to transmit data for its cluster head. This includes both transmission and reception energy. Lowering E_i means our network can run for longer periods without needing battery replacements.

b) Intra Cluster Distance (D): represents the average distance between CM and their respective CHs. the SN is selected as a CH such that the average distance between (CM) and the CH is minimized.

$$D = \frac{1}{n_i} \sum_{j=1}^{n_i} dis(x_{i.j}, y_{i,j}, x_{h,i}, y_{h,i}) \quad (2)$$

Where dis is the Euclidean distance between a sensor x_i, y_i and its cluster head x_h, y_h, and $n_i$is the number of CM of the cluster i.

c) Traffic Load (L): represents the load or data traffic handled by cluster head. Balancing Traffic Load ensures fair distribution of data traffic.

$$L_i = P_i * S_i \quad (3)$$

Where L_i represent the traffic load of cluster head i, P_i represent the number of packets that received by CH_i from its *CM*, S_i is the size of the transmitted packet from *CM* to CH_i.

d) Network coverage (C): represent the area covered by each cluster head. We want to maximize coverage to ensure that our network has good connectivity and no areas are left unmonitored.

$$C_i = \pi * R_i^2 \quad (4)$$

Where C_i is the area that covered by CH_i, R_i is the radius of circular area that covered by CH_i and its computed as follows:

$$R_i = \sqrt{\frac{S\_R_i}{\pi}} \quad (5)$$

S_R_i is the sensing range of the sensor nodes associated with CH_i

4.2.3 Improved Memetic Algorithm

Figure 2 show decryption for the main steps of memetic algorithm.

Eximia Journal
Vol. 13, 729-739, January, 2024
ISSN: 2784-0735
www.eximiajournal.com

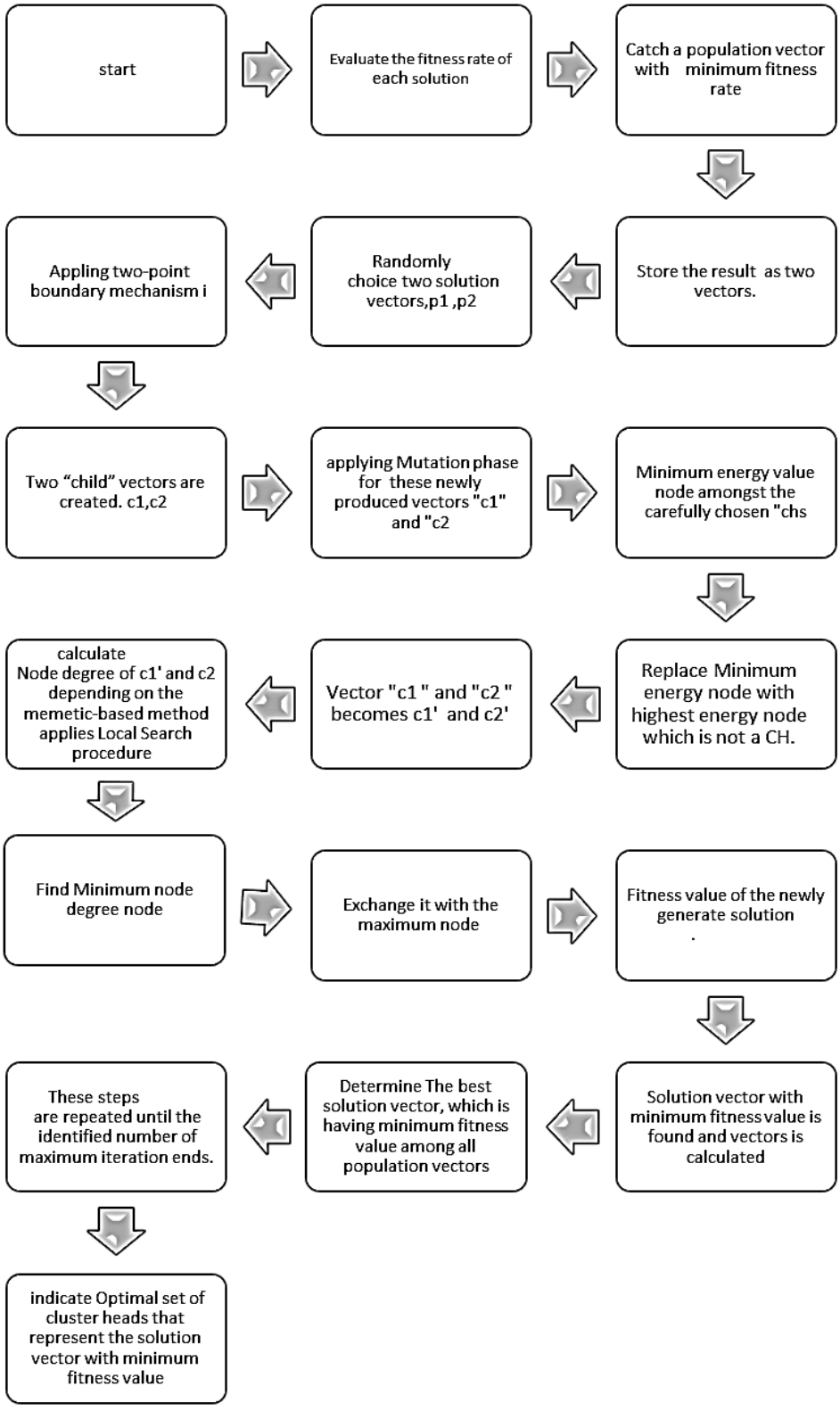

Figure 2. Memetic algorithm main steps

4.3 Block Chain Technique Implementation

Eximia Journal
Vol. 13, 729-739, January, 2024
ISSN: 2784-0735
www.eximiajournal.com

These steps is for formation the cluster then ensuring and verifying the authentication for nodes in clusters depending the principles of blockchain technique:

4.3.1 Cluster formation

After a set of best CHs are selected using Memetic-based Algorithm, the cluster formation process will begin. In this step, each selected CHs broadcast their location in the NW, the CMs may have several neighboring CHs to join. So. for making load-balanced clusters, a formula known as Cluster_Joining_Cost is proposed for creating load balanced clusters which id expressed in Eq.. (6). Cluster_Joining_Cost is based on three parameters which are the residual energy of "CH", node degree of the CH, and the distance between CH and CMs.

The following steps shows how CM joins CH

1. If a j[th] node (CM_j) wants to join an i[th] CH (CH_i).
2. CM_j needs to calculate the Cluster_Joining_Cos as given in Equation (6) for all CHs, then find the minimize cost value.
3. After that, the CM_j will join the CH_i with minimizing cost value.

$$Cluster_{joining_{Cost}}(C_{i,j}) = a * D_{i,j} + b * \left(\frac{1}{E_i}\right) + c * ND_i \quad (6)$$

Where a, b, and c are weighting factors and their values range between (0,1), $D_{i,j}$ is the distance between CH_i and CM_j, E_i is the remaining energy ofCH_i , and ND_i is the node degree of CH_i , as given in eq.7.

$$ND_i = \sum_{j=1}^{n} e^{-\alpha||CH_i - CM_j||^2} \quad (7)$$

Where n is the number of CM, e=2.718, $\alpha = \frac{4}{r^2}$ and $||CH_i - CM_{i,j}||^2$ is the Euclidian distance between i[th] CH and its CMs.

4.3.2 Nodes Authentication

The verification of SNs is a significant factor. It authenticated first before two SNs communicated. Multi steps applied when there are two communicated SNs A and B (SN_a , SN_b) which are:

1- The SN_a sends its identifications to their CH.
2- The identifications are the id of SN_a, the id of the CH to which it fits, and the id of the SN_b which it's want to communicate.
3- The CH's authenticity confirmation is delivered to the BS.
4- The BS matches the confirmation with the data stored on the isolated block-chain.
5- If the confirmation is not equal, an error will appear, and other verifications will also be confirmed.
6- If both identifications are equal then the BS performs the smart agreement and sends a verification message by the CH to the concerned node.
7- At SN_b similar process is repeated.
8- This authentication process is doing only when both SNs be in different cluster.
9- If they belong to the equivalent CH, they directly start to communicate.

4.4 Routing

The sensed data is transmitted towards BS through CH, there are several routes starting the source CH to BS, selecting the best route can give hand in the improvement of the existence of the network.

Eximia Journal
Vol. 13, 729-739, January, 2024
ISSN: 2784-0735
www.eximiajournal.com

4.4.1 Route selection

In this paper , data is sent towards the BS using a multi-hop model of routing, choosing the best route based on two parameters, residual energy and the distance from next CH and BS. so that next hop CH is selected by adopting Equation, eq.8.

$$CH_j = b_1\left(\frac{E_{res}(j)}{E_{ini}}\right) + b_2\left(1 - \frac{D_{(CH_j,BS)}}{D_{max}}\right) + b_3\left(1 - \frac{D_{(CH_i,CH_j)}}{D_{max-next\ CH}}\right) \quad (8)$$

Regarding to the above Equation, the function CH_j of the next CH node j; $E_{res}(j)$ represents the residual energy of the next cluster head node, E_{ini} represent the initial energy, $D_{(CH_j,BS)}$ represents the distance from the next CH node to the BS, D_{max} represents the maximum distance from the CH nodes to the BS, $D_{(CH_i,CH_j)}$ represents the distance between the current CH(i) and the next CH(j), and $D_{max-next\ CH}$ represents the maximum distance from the current CH to the next CHs. Whereas, the coefficients b1, b2, b3 are constants and their values are chosen within the interval [0, 1].

4.4.2 Route maintenance

In order to avoid premature death of CHs besides to restructure the network topology, the residual energy of each cluster head is checked after each round against an adaptive threshold of energy. The energy threshold for each epoch (i.e., for a variable number of rounds where the topology of the network nodes is not changed so that the threshold value of energy remains the same) can be determined using the following Equation (9). Therefore, after each round, if the residual energy of any cluster head becomes less than the energy threshold, the procedure of re-clustering sub-phase will be implemented again; otherwise, the phase of data transmission continues working.

$$threshold = \frac{1}{\alpha * m}\sum_{i=1}^{m} E_{res}(i) \quad (9)$$

Where:

- $E_{res}(i)$ represents the CH's residual energy.
- m represent the number of CHs.
- α is constant value and its between [1,3].

4.5 Simulation results and analysis

Suggested algorithm was tested using python with the following parameters and their values. where , The Area of NW (Dx, Dy) was100 * 100, Sink node's Location was (0,0), Communication range was 20m, Iterations number was 500, initial energy of each node was 2J, CHs number was 8,Population's number was 100, and Data bit length was 4000.

The imitation outcomes in Figure 3 occur that the proposed-model is accomplished to survive the network for a larger No. of loops as matched with the founding of clustering protocol. Four parameters are used for the selection of C.H.s. i.e., residual-energy, average distance from SNs to their CH (intra-cluster distance), data traffic of each CH (Traffic Load), and coverage area of each CH. In I-LEACH clustering protocol, they used three parameters for CH selection (residual energy, distance from BS, and packet delivery ratio). In BS-SCRM clustering algorithm, they used two parameters (the energy of the CH, and the distance between the CH and BS). Our proposed protocol outperforms I-LEACH because we consider four parameters for new CH selection, I-LEACH considers only three, and BS-SCRM consider only two parameters.

Eximia Journal
Vol. 13, 729-739, January, 2024
ISSN: 2784-0735
www.eximiajournal.com

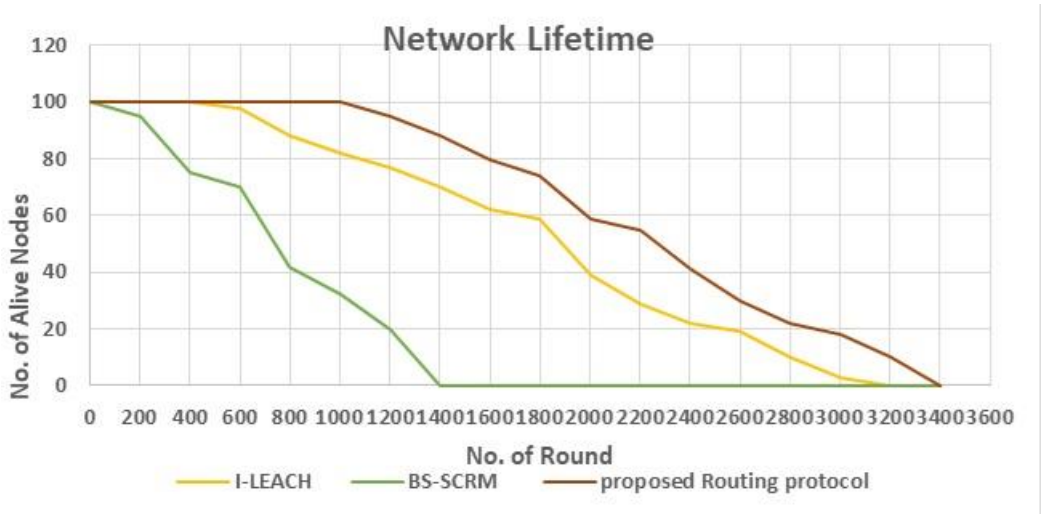

Figure 3. Comparison of NW Lifetime

Figure 4 displays the evaluation the comparison among the PDR value of the suggested model with I-LEACH and BS-SCRM. The recital of the suggested model is better than the two other routing protocols. The caution of the other tech. is the Ns die quickly because of ineffective energy consumption outstanding to C.H selection, which be determined by few parameters. On the other hand, in our suggested model the route is designated based on residual energy and the distance from next CH and BS of the next hop. Hence, the suggested model has a great PDR matched to the other procedures.

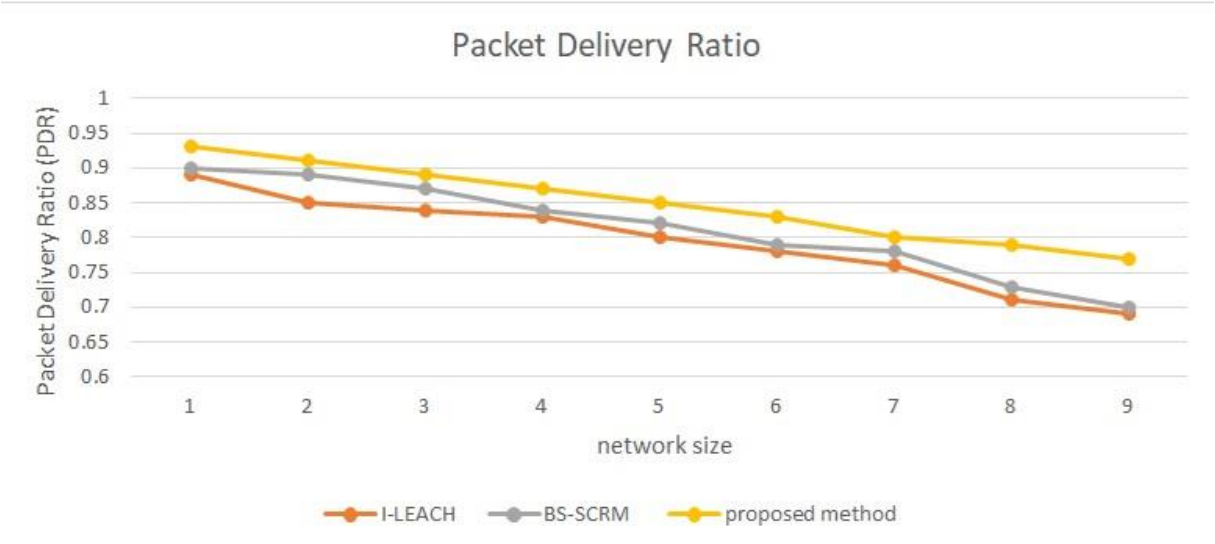

Figure 4. Comparison of PDR

Figure 5 displays the comparisons when a certain number of died nodes arises. It can be found that the suggested method is in general well than that of the other three contrast algorithms. This is due to the route maintenance technique.

Eximia Journal
Vol. 13, 729-739, January, 2024
ISSN: 2784-0735
www.eximiajournal.com

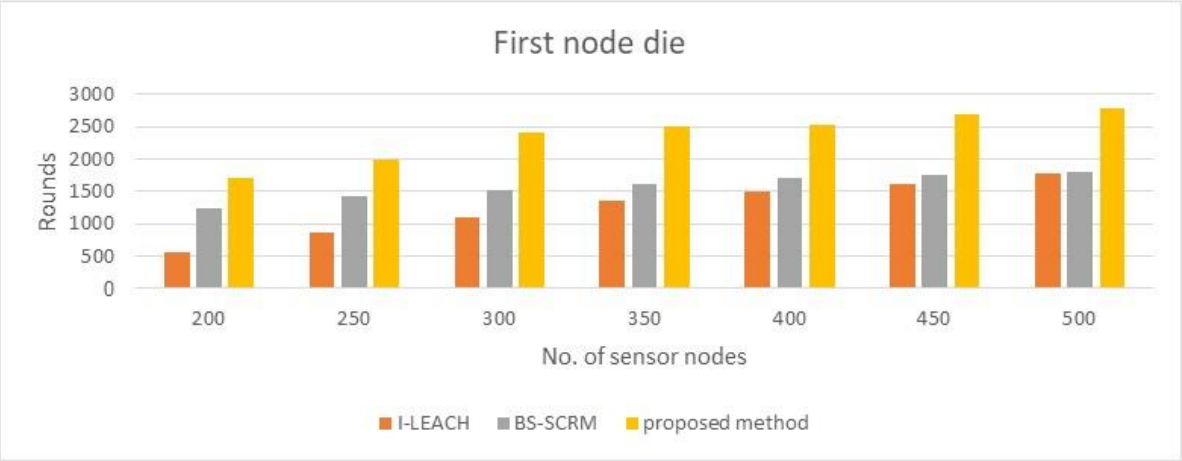

Figure 5. Comparison when numbers of dead nodes occur

5. Conclusion

offering an energy efficient mechanism and cost effective storage solutions for secure Wireless Sensor Networks (WSNs) was the objectives of the proposed methodology .where facilitates a secure clustering routing process through the design of cluster formation and a data-chaining phase depending on block chain technique principles. Additionally, introduced an enhanced Cluster Head (CH) selection algorithm grounded in an improved memetic based meta-heuristic approach. Where This algorithm considers several factors in its objective function, including the residual energy of nodes, the average distance from sensor nodes to their respective CHs (intra cluster distance), the data traffic associated with each CH (Traffic Load), and the coverage area of each CH. Furthermore, blockchain technology is employed during the data-chaining phase to encrypt and authenticate the data generated by nodes within the cluster, in this manner ensuring data integrity and resistance to tampering. Experimental results show that the proposed method shows significant advantages in terms of energy efficiency and Packet Delivery Ratio (PDR). Research offers an effective solution for enhancing the security of clustering routing in WSNs and provides valuable control and insights for the application and advancement of these networks. Future research endeavors may further explore and optimize the proposed methodology and discover its application across a wider array of real-world scenarios.

Refrenceses

[1] Tumula, Sridevi, et al. "An opportunistic energy-efficient dynamic self-configuration clustering algorithm in WSN-based IoT networks." *International Journal of Communication Systems* 37.1 (2024): e5633.

[2] Ahmad, Rami, et al. "Optimization Algorithms for Wireless Sensor Networks Node Localization: An Overview." *IEEE Access* (2024).

[3] Ghadi, Yazeed Yasin, et al. "Machine learning solution for the security of wireless sensor network." *IEEE Access* (2024).

[4] Pandey, Divya, And Vandana Kushwaha. "An Exploratory Study of Optimization Techniques for Congestion Control in Wireless Sensor Networks." Adhoc & Sensor Wireless Networks 58 (2024)

[5] R. Ren, M. Ma and W. Liu, "Design of Network Information Security Optimal Defense System Based on SM2 Algorithm and Blockchain Technology," 2023 2nd International Conference on Artificial Intelligence and Autonomous Robot Systems (AIARS), Bristol, United Kingdom, 2023, pp. 223-227, doi: 10.1109/AIARS59518.2023.00052]

[6] V. V. Bhandiwad and L. K. Ragha, "A Research Survey on Security Enhancement in WSN-based IoT Applications," 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 169-174.

[7] A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad and Z. Mushtaq, "An Energy-Efficient Data Aggregation Mechanism for IoT Secured by Blockchain," in IEEE Access, vol. 10, pp. 11404-11419, 2022, doi: 10.1109/ACCESS.2022.3146295.]

[8] Neri, Ferrante, and Carlos Cotta. "Memetic algorithms and memetic computing optimization: A literature review." Swarm and Evolutionary Computation 2 (2012): 1-14

[9] Darbandi, Mehdi, et al. "Blockchain systems in embedded internet of things: Systematic literature review, challenges analysis, and future direction suggestions." Electronics 11.23 (2022): 4020.

[10] Faisal, Muhammad, and Ghassan Husnain. "Blockchain Based Multi-hop Routing and Cost-Effective Decentralized Storage System for Wireless Sensor Networks." *Wireless Personal Communications* 131.4 (2023): 3009-3025.

[11] Chandan, Radha Raman, et al. "Secure modern wireless communication network based on blockchain technology." *Electronics* 12.5 (2023): 1095.

[12] Jabor, Maytham S., et al. "New approach to improve power consumption associated with blockchain in WSNs." *Plos one* 18.5 (2023): e0285924.

[13] Aljumaie, Ghada Sultan, and Wajdi Alhakami. "A secure LEACH-PRO protocol based on blockchain." *Sensors* 22.21 (2022): 8431.
[14] Xiao, Jing, et al. "BS-SCRM: a novel approach to secure wireless sensor networks via blockchain and swarm intelligence techniques." *Scientific Reports* 14.1 (2024): 9709.

[15] Khan, Zahoor Ali, et al. "A blockchain-based deep-learning-driven architecture for quality routing in wireless sensor networks." *IEEE Access* 11 (2023): 31036-31051.