Peer-to-Peer Networking and Applications
https://doi.org/10.1007/s12083-024-01748-1

An optimized secure cluster-based routing protocol for IoT-based WSN structures in smart agriculture with blockchain-based integrity checking

Ashutosh Kumar Rao[1] · **Kapil Kumar Nagwanshi**[2] · **Manoj Kumar Shukla**[3]

Received: 3 July 2023 / Accepted: 3 June 2024

Abstract
In the context of Internet of Things (IoT)-based Wireless Sensor Networks (WSNs) for smart agriculture, ensuring efficient resource utilization, prolonged network lifespan and robust security mechanisms is paramount. This paper addresses these challenges by introducing an optimized secure cluster-based routing protocol with blockchain. The algorithm initiates with node ID assignment, followed by the use of Distributed Fuzzy Cognitive Maps (DFCM) to select Cluster Heads (CHs) based on energy, proximity to the Base Station (BS) and neighbor count. DFCM aims for balanced CH distribution to optimize energy usage. The secure routing protocol, employing Earthworm-based Deer Hunting Optimization Algorithm (EW-DHOA) and blockchain, ensures reliable data transmission. Through extensive comparative analyses with existing techniques, including GA-PSO, CI-ROA, ACI-GSO and P-WWO, our approach consistently outperforms in critical parameters. At varying node densities, the proposed method demonstrates a substantial improvement in network lifetime, achieving a 60% increase over GA-PSO and maintaining a superior average of 3200 rounds. Energy consumption is notably reduced, with a 33.3% improvement compared to GA-PSO at a density of 100 nodes. The packet delivery ratio reaches 98%, showcasing a 4% enhancement over the best-performing existing technique P-WWO. Throughput at a density of 500 nodes achieves an impressive 33.3% increase, reaching 0.8 Mbps. Notably, our methodology excels in preserving active nodes, sustaining a network lifetime of 66.7% more than competing techniques at the 3500th round. The proposed approach demonstrates a higher detection rate, ranging from 75% to 90% and exhibits a significantly higher convergence rate. Therefore, our Optimized Secure Cluster-Based Routing Protocol with Blockchain-Based Integrity Checking presents a comprehensive and superior solution for enhancing the efficiency, resilience and security of WSNs in smart agriculture.

Keywords WSN · Clustering · IoT · Security · Integrity · Optimization · Routing · Blockchain

1 Introduction

In recent years, the integration of WSN and smart agriculture has emerged as a transformative force, revolutionizing traditional farming practices. This integration holds immense potential for real-time monitoring, data-driven decision-making, and resource optimization [1–4]. As agriculture increasingly adopts IoT solutions, the role of WSNs becomes pivotal, offering the promise of enhanced crop yield, resource efficiency, and environmental sustainability. Motivated by these factors, this paper addresses the critical need for an advanced and secure cluster-based routing protocol within WSN structures, specifically tailored for the intricacies of smart agriculture. The applications of WSNs in smart agriculture are diverse and profound. From monitoring soil conditions and climate parameters to tracking livestock health, these networks provide a granular understanding of the agricultural landscape. Precision agriculture, enabled by WSNs, empowers farmers to make informed decisions, optimize resource allocation, and mitigate environmental impact [5–7]. Achieving an equitable distribution of CHs to ensure balanced energy usage and extended network longevity remains an ongoing

✉ Kapil Kumar Nagwanshi
dr.kapil@ieee.org

[1] Department of Computer Science & Engineering, Amity School of Engineering & Technology, Amity University, Rajasthan, India

[2] SoS E&T, Guru Ghasidas Vishwadiyalaya (A Central University), Bilaspur, India

[3] Department of Computer Science & Engineering, Amity School of Engineering & Technology, Amity University, Uttar Pradesh, India

Published online: 22 June 2024

challenge. Existing methods such as Power Efficient Gathering in Sensor Information Systems (PEGASIS), Distributed Energy Efficient Clustering (DEEC), and Distributed Routing for In-Network Aggregation (DRINA) [8–13] face significant challenges related to CH selection, energy consumption, and overall network lifespan.

Moreover, the integration of blockchain-based integrity checking, a promising avenue for enhancing security, demands specialized attention for seamless adoption in WSNs tailored for smart agriculture. The research domain thus presents a nuanced landscape, wherein the fusion of advanced routing protocols, energy efficiency considerations, and security mechanisms becomes imperative. Existing secure routing protocols, such as Secure Routing Protocol (SRP) [14], Security Protocol for Sensor Networks (SPINS) [15], and Secure Cluster-based Route Planning (SCRP) [16], have made strides in addressing security concerns in WSNs. However, their adaptation to the unique requirements of smart agriculture is an area that warrants exploration and enhancement.

This paper aims to tackle critical research challenges within the realm of smart agriculture and WSN. One of the key issues is the necessity for an efficient and secure routing protocol to manage data transmission in WSNs deployed for agricultural monitoring. In particular, optimizing cluster-based structures, notably in the selection of CHs, presents a significant challenge that requires solutions to balance energy consumption, enhance network lifespan, and ensure an even distribution of CHs. Moreover, maintaining data authenticity and security during the transmission process is imperative. The proposal of this work is motivated by the urgent need to overcome these identified critical research problems in smart agriculture and WSN. As we delve into the complexities of WSNs tailored for agricultural monitoring, the paper explores innovative solutions to address existing challenges in the efficient and secure transmission of data within these networks.

Our focus extends to the optimization of cluster-based routing protocols, leveraging the Earthworm-based Deer Hunting Optimization Algorithm (EW-DHOA) and incorporating Distributed Fuzzy Cognitive Maps (DFCM) for CH selection. The proposed protocol not only aims to rectify the limitations of current methods but also endeavors to provide a comprehensive solution that enhances the efficiency, security, and resilience of WSNs in smart agriculture contexts. Through this research, we aim to contribute to the evolving landscape of agricultural technology, fostering sustainable and data-driven practices for the benefit of farmers and ecosystems alike. The major contributions of this paper are as follows:

- The integration of the Enhanced Whale Optimization Algorithm with Differential Harmony Search and Crowding Mechanism (EW-DHOA) routing protocol significantly improves energy efficiency. This is achieved through intelligent routing decisions that minimize energy wastage and contribute to the extended longevity of the network.
- The incorporation of a blockchain-based integrity checking mechanism adds an extra layer of security to the WSN. This ensures the authenticity and integrity of transmitted packets, reducing the risk of packet loss or corruption caused by malicious attacks.
- The EW-DHOA algorithm optimizes routing decisions, resulting in reduced latency and maximized utilization of available network resources. As a result, the proposed method achieves higher throughput compared to existing techniques, contributing to more efficient data transmission and communication within the WSN.
- The Distributed Fuzzy C-Means (DFCM) method effectively distributes and balances energy usage among sensor nodes. This innovative approach reduces the risk of early energy depletion, sustaining a higher number of active sensor nodes over time and contributing to the resilience of the WSN.
- The proposed method demonstrates superior performance in terms of malicious node detection. The incorporation of advanced detection mechanisms contributes to the enhanced security and robustness of the WSN, ensuring the integrity and confidentiality of transmitted data.
- The integration of the DHOA and EWA methods in the EW-DHOA algorithm results in a significantly high convergence rate. This indicates that the proposed method converges to optimal solutions more efficiently than other techniques, benefiting from the strengths and characteristics of both optimization approaches.

The subsequent sections of this document are outlined as follows: Section 2 offers a comprehensive overview of the existing literature. Section 3 elucidates the proposed routing protocol. Section 4 presents the simulation results and a comparative analysis. Lastly, Section 5 presents the concluding remarks.

2 Related work

This section covers an in-depth analysis of the secure routing schemes that are currently in use for wireless sensor networks.

Yao et al. [17] introduced an energy-efficient routing protocol with multi-threshold segmentation (EERPMS), which aims to enhance the rationality of the formation of cluster and CH selection. It groups sensor nodes into clusters based on the node angle and number variance principles. The Otsu algorithm is utilized to cluster the nodes, leading

to improved load distribution among cluster heads and distribution homogeneity. Moreover, a CH selection algorithm is introduced, which optimizes the selection of CHs depending on their best location and residual energy of nodes to prolong network lifetime. Moreover, because of overhead problems and improper clustering allocation, which reduce the network lifetime, the CH selection method suffers. In order to overcome this, researchers focus on improving the CH selection procedure using machine learning and optimization strategies that emphasise the best possible outcome. To get the overall best solution, metaheuristic models were used. Both the sink movement data transfer and the CH selection are optimised using a hybrid strategy suggested by Sahoo et al. [18] that takes into account the genetic algorithm (GA) and particle swarm optimization (PSO) respectively.

The Butterfly Optimization Algorithm (BOA) was introduced by Maheshwari et al. [19] in order to enhance the overall packet transfer to BS while lowering the energy consumption of the sensor nodes. The residual energy of nodes, the proximity of the neighbours and BS, and the node degree and centralization all play a role in the CH selection. Ant Colony Optimization (ACO) determines the optimal pathfrom the BSto the CH. Yadav and Mahapatra [20] suggested a Cuckoo Insisted-Rider Optimization Algorithm (CI-ROA) for energy-aware CH selection. Moreover, the selection is based on parameters like energy stability, minimising the distance between nodes, and minimising transmission latency. By choosing the best CH, the lifespan is extended. For homogeneous and heterogeneous settings, respectively, Zachariah and Kuppusamy [21] presented HECK and HOCK - energy efficient clustering techniques that extend the network lifespan. Both of these methods were developed utilising the Cuckoo search and the Krill herd. Whereas the ideal cluster heads are chosen based on Cuckoo search and the coordinates of optimal cluster centroid are calculated by employing Krill herd method.

None of the methods mentioned above are capable of withstanding attacks, which can render many nodes that rely on security measures that are based on trust ineffective. As a result, Han et al. [22] introduced a WSN routing protocol, which is energy-efficient and based on trust using adaptive genetic algorithms (TAGA). This protocol integrates a trust security process and AGA to consider energy conservation and security when routing data. It improves security by creating an adaptive trust model that evaluates the overall trustworthiness of each sensor and can resist both common and specific trust attacks. The CH selection threshold is enhanced based on changes in trust and energy levels, ensuring that malicious nodes cannot act as CHs. Anand and Sharma [23] proposed an advanced and efficient cluster key management scheme (AgroKy) to address the difficulties of setting up and managing web interfaces for IoT sensor nodes and managing cryptographic keys for clusters. AgroKy utilizes deep learning techniques to identify and avoid unsafe interactions with potential attacks. In addition, a web interface is created to collect feedback from nodes and manage notifications after detecting signals from the sensors. Even though trust-based systems have improved their ability to handle a variety of problematic node behaviours, certain issues such as energy-draining nodes, communication bottlenecks, and attacks still remain. To solve these problems, Hu et al. [24] suggested the trust-based secure and energy-efficient routing (TBSEER) method. It can more quickly identify faulty nodes and efficiently recognise attacks like sinkholes, selective forwarding, hello floods, and black holes. Moreover, the nodes use a multi-path search mechanism based on the model to identify a secure and energy-efficient way, actively avoiding wormhole attacks.

In order to provide safe and effective routing, load balancing is a crucial technique since it helps avoid network congestion. Unfortunately, the current routing system always sends packets to the node with the greatest trust value, adding to CH workload. Thus, a secure and load-balanced routing (SLBR) strategy is presented by Thahniyath and Jayaprasad [25] for heterogeneous cluster-based WSNs. In addition to balancing load across CH, SLBR offers a superior trust-based security that solves the issue of sensors that repeatedly switch between positive and negative states. Hence, it helps to improve security, packet transport, and energy efficiency. Moreover, Singh and Singh [26] presented the hierarchical clustering and routing (HCR) method for clustering while considering scalability, dependability, and energy. In that Secondly, a hierarchically layered architecture is developed to divide the network into circular layers for effective hierarchical data transfer. The choice of CHs is then made using an ant lion optimizer to assure scalable, energy-balanced, and dependable cluster creation.

One of the network's primary duties is to strike a balance between energy efficiency and network integrity. These metrics are not balanced in the existing approaches. So, Gopinath et al. [27] implement Secure cluster based efficient energy routing (SCEER) in order to avoid these issues and increase network lifespan. The optimal packet transfer is initially initialised using network and routing constraints. The cluster's stability metric is then chosen to enhance energy efficiency. Lastly, the initialization of the ideal cluster design model balances energy efficiency and network integrity. The effectiveness of several optimization methods was demonstrated in terms of increased lifespan, reduced energy usage, and improved efficiency. Unfortunately, it suffers from the slow convergence speed and local optimal problems. Moreover, the overlap difficulties, stability, expanding node coverage, and efficiency of energy in such technologies are still need to be addressed. As a result, Reddy et al. [28] introduced a brand-new hybrid technique called ACO integrated Glowworm Swarm Optimization

(GSO) approach (ACI-GSO). As opposed to previous approaches, this technique shows the performance utilising the objective function's inclusion of physical layer measurements like energy, distance, and latency. Whereas only physical layer measurements are taken into account in the objective function, here the cross-layer performance through throughput is explored as well. To find the best way without compromising transmission reliability, Khot and Naik [29] presented the Particle-Water Wave Optimization (P-WWO) safe routing method. The routing path with the smallest distance and the least amount of delay is considered the best way in this method. The aspects like latency, trust, consistent, energy, and manageability are taken into account while calculating the fitness metric. Another one approach that uses three attributes to identify malicious node called Trust Based Secure Intelligent Opportunistic Routing Protocol (TBSIOP) is introduced by Bangotra et al. [30]. The attributes considered in this approach are forwarding data packets and acknowledgment sincerity, and depletion of energy.

To avoid complexity in existing approaches, Fang et al. [31] developed lightweight trust management scheme (LTMS) to protect against internal attack using binomial distribution. Blockchain technology is a secure, decentralized, and tamper-proof way of managing transactions and data in WSNs, making it a better choice than other optimization techniques for secure cluster-based routing. Hence, Lazrag et al. [32] used Blockchain to communicate network activity in real-time and improve the routing. This method enhances the routing phase's security while lowering interference levels and better balancing traffic load. However, the system becomes more challenging in terms of device efficiency when determining routes through complex computations, greatly raising the cost of the nodes. Revanesh and Sridhar [33] presented an effective and trustworthy inter-correlated routing strategy based on meta-heuristics, blockchain, and deep learning. The distributed routing data in the network is maintained utilising a block-chain method, and the Salp Swarm optimization is employed to enhance the routing process. The deep network technique is employed to optimize routing decisions, accounting for variations in routing data among the nodes. It provides a high level of security against malicious attacks. However, the use of multiple algorithms may require significant computational resources, which can be a challenge for wireless sensor networks with limited resources.

Tabatabaei et al. [34] presented an eco-friendly clustering approach for WSNs employing the Fuzzy Logic and Lion Pride Optimizer Algorithm (LPO). The technique grouped sensor nodes into clusters by assessing their remaining energy and proximity to the sink, thereby enhancing energy efficiency. LPO identified leaders within the clusters by evaluating battery power and proximity to the sink, while the remaining nodes connected to the nearest leader, resulting in the formation of optimized clusters. Tabatabaei [35] proposed, a novel clustering method for WSNs was introduced, known as the Social Spider Optimization (SSO) algorithm. This algorithm was inspired by the social cooperative behaviour observed in spider colonies. In the proposed method, sensor nodes imitated the interactions of a group of spiders, following biological rules that govern colony behaviour. This unique approach aimed to optimize fault tolerance and energy efficiency in WSNs through the emulation of natural cooperative strategies observed in spiders and also, Tabatabaei [36] introduced a novel routing protocol, targeting enhanced efficiency of energy within MANETs. The protocol incorporated both the TOPSIS multi-criteria algorithm and the Cuckoo Optimization Algorithm, with the primary goal of optimizing energy consumption in the network. The TOPSIS algorithm played a crucial role by effectively selecting relay groups based on multiple criteria, enhancing the proposed routing protocol's capability for energy optimization in MANETs.

Moreover, Akbari and Tabatabaei [37] presented a novel approach for determining highly reliable routes in the IoT using a combination of Reinforcement Learning and Fuzzy Logic. The main aim of their research was to enhance network lifetime by introducing an innovative energy-efficient mechanism. The suggested approach entailed the fusion of fuzzy logic and reinforcement learning, emphasizing considerations like remaining node energies, accessible bandwidth, and proximity to the sink. Gorgich and Tabatabaei [38] introduced a novel energy-aware routing protocol to tackle the challenge of optimal power utilization in WSNs. Their proposed method leveraged the Fish Swarm Optimization algorithm to optimize power consumption within WSNs. By utilizing this bio-inspired algorithm, the research aimed to bridge existing gaps in energy-efficient routing protocols for WSNs. Ebrahimi and Tabatabaei [39] presented a methodology aiming to optimize power consumption in hierarchical WSNs by employing the Soccer League Competition Algorithm. The process involved initializing the network and utilizing the algorithm to dynamically cluster sensor nodes based on competitive performances. This smart clustering method, characterized by its hierarchical arrangement, was leveraged to enhance power consumption efficiency within the WSN.

Therefore, Mamaghani et al. [40] presented an innovative clustering protocol for WSNs employing the Willow Butterfly Algorithm to improve data diffusion efficiency. The methodology involved initiating the Willow Butterfly Algorithm to intelligently cluster sensor nodes. Drawing inspiration from nature, this algorithm offered a unique approach to clustering, optimizing the distribution of data across the network. Tabatabaei and Rigi [41] introduced a dependable routing algorithm for WSNs, emphasizing clustering and a mobile sink to tackle challenges. Their strategy aimed at attaining load balance and consistent energy usage across

the network. This technique, labelled the distributed clustering reliable routing protocol, functioned in a decentralized fashion with the primary goal of minimizing reported delays within the network.

Furthermore, Tabatabaei [42] proposed an energy-conscious routing protocol for WSNs. The approach integrated both a mobile sink and the Bacterial Foraging Optimization Algorithm. A distinctive aspect of this strategy was the computation of sensor node quantities, hinging on two pivotal factors: the amount of energy still available on the battery surface and the proximity to the sink. Miri and Tabatabaei [43] introduced a novel methodology to address challenges in VANETs routing. An innovative approach leveraging Fuzzy Logic for adaptive and context-aware decision-making. This novel methodology aimed to contribute to more efficient routing in the dynamic and challenging environments of VANET. Tabatabaei [44] introduced an innovative routing method for MANETs by incorporating the Symbiont Organism Search (SOS) algorithm. The proposed methodology harnessed the adaptive and intelligent capabilities of the SOS algorithm to address the challenges of dynamic MANET environments.

3 Proposed secure and optimal routing protocol

Our proposed routing protocol consists of two stages: cluster formation and transmission of data. In the cluster formation phase, the network is divided into clusters, with a CH assigned to lead each cluster. The CHs are responsible of aggregating and transmitting the data collected by the cluster members to the sink. In the next phase, the data is forwarded from the CHs to the sink using a blockchain-based secure routing scheme. The blockchain guarantees that the data is transmitted securely and accurately, and that the integrity of the data is checked at every step of the routing process. The overall architecture of proposed optimized secure cluster based routing protocol for IoT-based WSN in Fig. 1.

3.1 Phase 1: Data sensing and initialization

In our proposed secure routing protocol, the effectiveness hinges on the accurate and timely acquisition of data from the agricultural environment. The sensing process is meticulously designed to capture pertinent information crucial for smart agriculture applications. Our system incorporates a

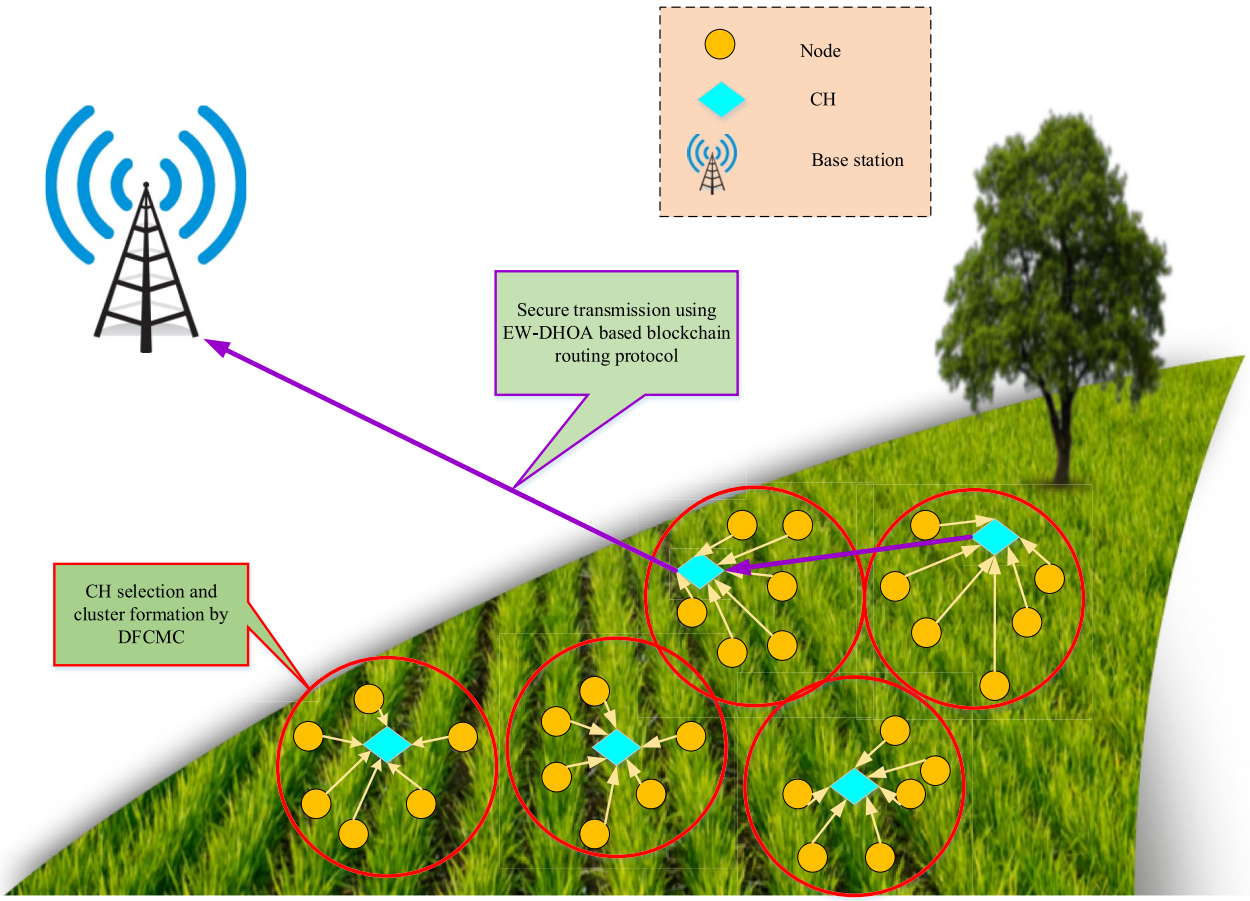


Fig. 1 Overall architecture of proposed optimized secure cluster-based routing protocol for IoT-based WSN

diverse array of sensors—soil moisture sensors, temperature sensors, and humidity sensors—strategically placed across the field, ensuring comprehensive coverage for holistic environmental monitoring. The data collection process involves sensors continuously gathering information on key environmental parameters. This collected data undergoes processing at the sensor nodes to generate meaningful datasets. Each sensor node is equipped with processing capabilities to perform initial analysis and aggregation, reducing the volume of transmitted data and optimizing energy usage. Our sensing strategy is event-driven, with sensors actively monitoring changes in environmental conditions. Upon detecting significant deviations or predefined thresholds, sensors trigger the data transmission process. To enhance energy efficiency, the sensing approach incorporates adaptive sensing intervals, dynamically adjusting sensing frequencies based on the urgency and criticality of observed environmental changes. When data transmission is deemed necessary, the sensor node initiates a secure communication process by sending a request to the nearest Cluster Head (CH). This request includes relevant information about the sensed data and the urgency of transmission. This meticulous approach ensures our routing protocol operates on high-quality, real-time data, enabling precise decision-making in smart agriculture applications.

In the initialization process, all nodes (IoT devices) in the network are initialized with a unique ID, a random value for their residual energy, and a pre-defined threshold value.

3.2 Phase 2: Cluster formation

The WSN nodes should be divided into clusters based on their proximity and energy level. A cluster head should be selected for each cluster based on its energy level and distance from the BS. The proposed Distributed Fuzzy Cognitive Maps based Clustering (DFCMC) algorithm is a distributed approach for cluster formation in WSNs that aims to address the problems of randomness, scalability, and single-hop communication in the existing clustering process.

In the first round, nodes with residual energy greater than the threshold value broadcast a message to their neighbours, indicating their willingness to become cluster heads. Nodes that receive multiple such messages choose the sensors with the highest residual energy as their CH. The selected nodes then broadcast a message to their neighbours to inform them of their selection. FCM approach uses optimal fuzzy sets and membership functions to select CHsbased on the input parameter. FCM can handle more complex and uncertain information and reduce the subjectivity in rule generation. The DFCMC algorithm aims to balance the energy usage and increase the lifespan of WSN by distributing the CHs evenly throughout the network.

Residual energy The residual energy refers to the remaining energy level of a sensor node. Nodes with higher residual energy are typically preferred as cluster heads since they can efficiently perform the additional communication and coordination tasks required by the clustering algorithm. The fuzzy cognitive approach takes into account the remaining energy of each sensor and assigns a weight or degree of membership to represent the node's energy level. Nodes with higher energy levels will have a higher membership value and are more likely to be selected as CHs.

$$E_{res} = E_{\text{int}\,ial} - E_{\cos\,um} \tag{1}$$

where$E_{\text{int}ial}$ represents the initial energy and $E_{\cos um}$ signifies the energy consumption.

Distance from the BS The distance of a SN from the BS plays a crucial role in determining its suitability as a cluster head. Typically, nodes closer to the BS are more likely to become cluster heads because they can directly communicate with the BS, thereby reducing the total energy consumed by the network. In the fuzzy cognitive-based approach, the distance from the BS is considered as a parameter, and a degree of membership is assigned based on this distance. Nodes with a shorter distance will have a higher membership value, indicating their potential to become CHs.

The distance between the BS$q$and the nodes $p$with location $(Y_p, Y_q)$and $(X_p, X_q)$is computed using Eq. (2).

$$d(p,q) = \sqrt{\left(X_p - Y_p\right)^2 + \left(X_q - Y_q\right)^2} \tag{2}$$

Number of neighbours The number of neighbours refers to the count of neighbouring sensor nodes within a specific range. In clustering algorithms, nodes with a higher number of neighbours are generally preferred as cluster heads because they can potentially provide better coverage and connectivity to the network. In the fuzzy cognitive-based approach, the number of neighbours is considered as a parameter, and its degree of membership is computed based on the specific clustering algorithm's requirements. Nodes with moreneighbours will have a higher membership value, increasing their chances of being selected as CHs.

By incorporating these factors and assigning appropriate degrees of membership, the fuzzy cognitive-based CH selection algorithm aims to identify the most suitable nodes to act as CHs in WSN. The weights or membership values assigned to each factor can be adjusted based on the specific requirements of the network and the desired trade-offs between energy efficiency, distance, and connectivity. The steps involved in the CH selection process is explained as follows:

3.2.1 Define input parameters and membership functions

In the model used for the implementation of nodes and Cluster Head (CH) selection, several critical input parameters, including residual energy, distance from the Base Station (BS), and the number of neighbors, are meticulously identified. Fuzzy logic is employed to address the inherent uncertainty and imprecision associated with these parameters, ensuring a nuanced and adaptive CH selection process within the Wireless Sensor Network (WSN). For residual energy, fuzzy sets such as "High," "Medium," and "Low" are defined, each with assigned triangular or trapezoidal membership functions. Similarly, for distance from the BS, fuzzy sets like "Near," "Intermediate," and "Far" are established with corresponding membership functions. The number of neighbors is characterized by fuzzy sets such as "Sparse," "Medium," and "Dense," each governed by triangular or trapezoidal membership functions. These functions determine the degree to which a node's characteristics belong to specific categories, enabling the model to effectively capture the nuanced relationships among input parameters. This fuzzy logic-based approach, combined with the chosen membership functions, facilitates an adaptive and comprehensive CH selection process in the WSN, demonstrating the model's efficacy in handling complex and imprecise information for enhanced network performance.

Identify the input parameters that will be used for CH selection. Here, the relevant input parameters are residual energy, distance from the BS, and the number of neighbours. Then the fuzzy sets for each input parameter are defined as given in Fig. 2. For example, fuzzy sets for residual energy is "high," "medium," and "low," while fuzzy sets for distance from the BS is "near," "intermediate," and "far". The fuzzy sets for number of neighbours is "sparse," "medium," and "dense". Assign membership functions to each fuzzy set. Membership functions determine how each input value belongs to each fuzzy set. They can be defined using various mathematical functions, such as triangular or trapezoidal membership functions.

3.2.2 Construct fuzzy cognitive maps

Build the FCM to model the relationships between the input parameters and the selection of CHs. Each FCM consists of a set of nodes, representing the input parameters and the selection of CHs, and directed edges, representing the relationships between the nodes. This approach enhances the selection process by considering three input parameters. The direction of the edges indicates the influence of one node on another. Positive edges indicate direct positive influence, while negative edges indicate direct negative influence. The weights assigned to the edges represent the strength of the influence.

FCMs play a crucial role in representing fuzzy sequential connections between concepts. Figure 3 presents an illustration of an FCM consisting of three nodes. FCMs, typically composed of P_1, P_2, …, P_n concepts. These concepts, also referred to as nodes, are commonly defined using fuzzy sets.

3.2.3 Train the FCM

In this step training data is used to determine the optimal weights for the edges in the FCM. Training data can be obtained from previous simulations, real-world deployments, or by using optimization algorithms. The training process aims to find the optimal weights that best represent the relationships between the input parameters and the CH selection.

The FCM model can be defined equivalently using a square matrix known as the connection matrix or weight matrix. This matrix stores the weight values assigned to the edges connecting concepts within the map. If the system consists of n nodes, the weights of the linkages between them can be represented in a $n \times n$weight matrix denoted as given in Eq. (3).

$$Q = \left[Q_{ij}\right],\ Q_{ij} \in [-1, 1],\ i, j = 1, 2, \cdots, n \tag{3}$$

Each element $Q_{ij}$of the weight matrix signifies the strength of the connection from the j^{th}concept to the i^{th}concept. These weights, which fall within the range of [−1, 1], quantify the level of association between the concepts.

3.2.4 Activation and propagation

Each node in the FCM are activated based on its input value and the weights of the incoming edges. Here, the activation level of each node is calculated by combining the input values and the weights using appropriate aggregation methods (e.g., max-min or max-product). Then propagate the activation level from the input nodes to the output nodes, considering the direction and weights of the edges. The activation and propagation process is repeated until a convergence criterion is met.

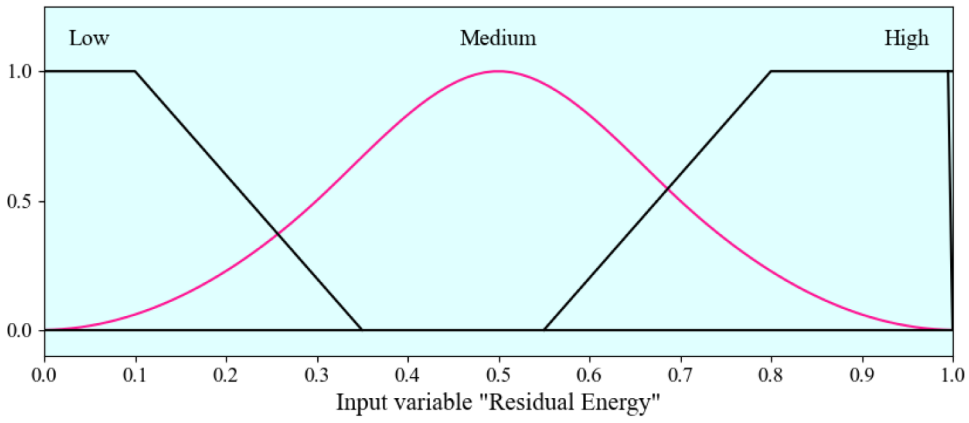
An FCM, where the activation at a specific discrete time moment is represented by a vector $y = [y_1, y_2, \ldots, y_n]^T$, with each y_i belonging to the interval [0, 1], produces a subsequent vector of concept activations at the next discrete time moment denoted as $z = [z_1, z_2, \ldots, z_n]^T$. Each z_i also belongs to the interval [0, 1].

A FCM responds to a current discrete time moment with an activation vector denoted as E. The FCM then produces a vector of concept activations in the next discrete time moment, represented as B which is expressed in Eq. (4).

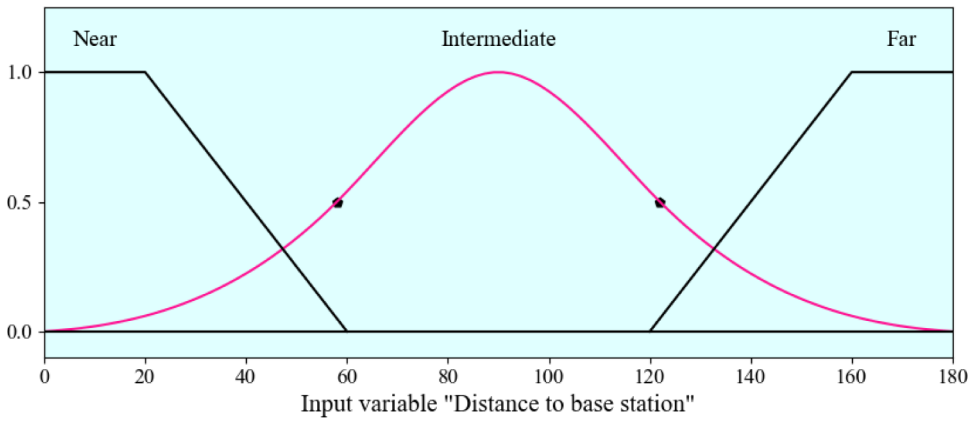
$$z = Q * y \tag{4}$$

The $*$ operation represents the multiplication of a matrix and a vector. It is common practice, both in literature and

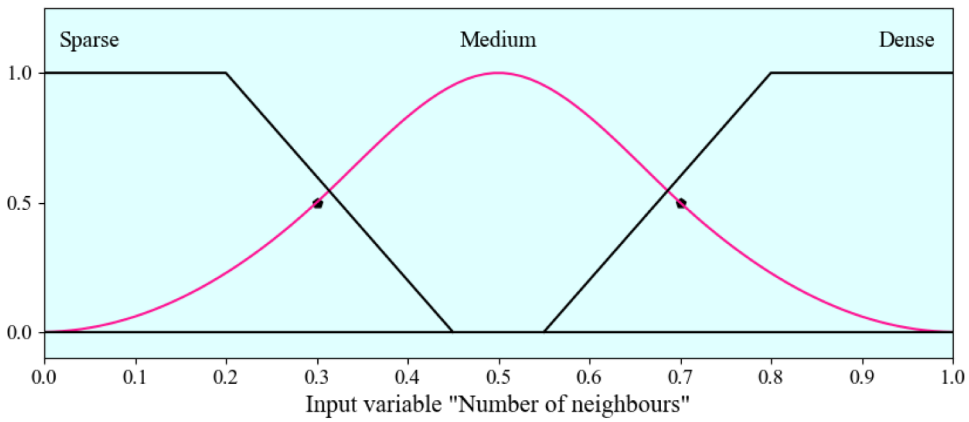
Fig. 2 Membership functions



(a) Residual energy



(b) Distance from the BS



(c) Number of neighbours

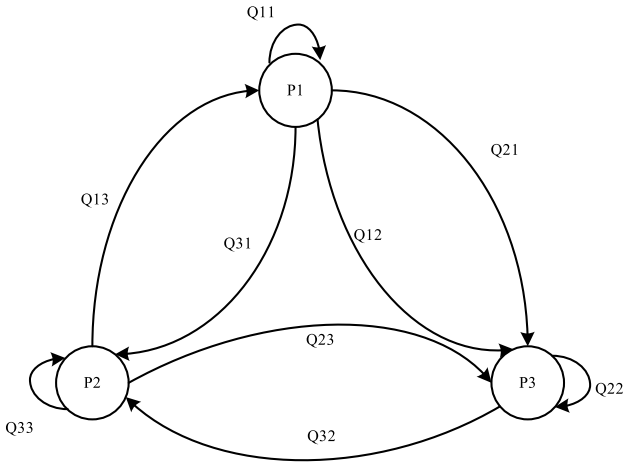


Fig. 3 Fuzzy Cognitive Map

in this study, to perform the matrix and vector product first, followed by the application of a squashing function that modifies all elements. Continuing with a more specific description regarding the activation of an individual node, the following is obtained for$i = 1, 2, \cdots, n$.

$$z_i = f\left(\sum_{j=1}^{n} Q_{ij} \cdot y_j\right) \tag{5}$$

The function f is responsible for squashing the product into the [0, 1] interval. In many cases, the sigmoid function is employed as $f$which includes a steepness parameter denoted as$\varepsilon > 0$. Therefore, the function can be expressed as the sigmoid function with the parameterε:

$$f(v) = \frac{1}{1 + e^{-\varepsilon v}} \tag{6}$$

The resemblance between the shape of function and the unit step function increases as the value of ε grows larger. The sensitivity to different activation strengths is determined by the value ofε.

Determine the CH selection on the basis of the activation levels of the output nodes. The sensors with higher activation levels are more likely to be selected as CHs. If multiple nodes have the same highest activation level, the node with the highest residual energy is chosen.

3.2.5 Update FCM and repeat

Update the FCM weights based on the selected CH and the actual performance of the network. For example, if the selected CHis efficient in terms of data transmission& energy efficiency, increase the weights of the edges leading to that node. Repeat the process for subsequent rounds or whenever it is necessary to select new CHs. The remaining nodes join the cluster of the nearest CH based on their distance from the CH.

After a certain number of rounds, each node updates its residual energy based on the energy consumed in transmitting and receiving data. Nodes with residual energy below the threshold value become part of the un-clustered nodes and can participate in the next round of CH selection. To address the problem of single-hop communication, DFCMC allows CHs to communicate with each other using multi-hop communication. This enables the sensors that are far away from the BS to relay data through intermediate cluster heads, which increases the network's scalability.

Algorithm 1 Algorithm 1 DFCMC based CH selection

Step 1: Initialize the FCM algorithm parameters:
- Set the number of sensors in the WSN.
- Set the maximum iteration to control the convergence of the algorithm.
- Set the learning rate to control the rate of updating the cognitive map.
- Set the threshold to determine convergence.

Step 2: Create a Fuzzy Cognitive Map (FCM) with P_n nodes, each representing a factor for CH selection. Initialize the FCM weights randomly or with predefined values.
Step 3: Repeat the following steps until the convergencecriteria is met:
Step 4: For each node in the FCM, calculate the activation level based on the inputs and weights.
Step 5: Update the state of each node in the FCM based on the activation levels and the current state of the nodes. Use a fuzzy logic function to determine the new state, considering the activation levels and the current states of the nodes.
Step 6: Calculate the difference between the previous and current states of the FCM nodes. If the difference is less than the threshold, stop the iteration and proceed to the next step.
Step 7: Update the weights of the FCM edges based on the current states of the nodes and the desired states. Use a learning rule, such as the Hebbian learning rule or the delta rule, to update the weights.
Step 8: Repeat from step 4.
Step 9: Choose the CHs based on the final state of the FCM. The node(s) with the highest activation level or the most significant influence on the CH selection can be chosen as the CHs.
Step 10: Return the selected CHs.

3.3 Phase 3: Data transmission

The proposed secure EW-DHOA based blockchainrouting protocol is employed to transmit the data packets from the sensor nodes to the BS via the CHs. In the EW-DHOA-based blockchain routing protocol, each sensor maintains a local blockchain that stores information about the network topology, node identity, and routing decisions. When a node wants to transfer data, it sends a request to the nearest CH, which then uses the EW-DHOA algorithm [45] to determine the optimal path for the data transmission. The CH then broadcasts the routing decision to the other nodes in the network, which update their local blockchains accordingly. By using blockchain to store and distribute routing information, the EW-DHOA algorithm can provide a secure and tamper-proof routing protocol that can protect against attacks such as node compromise or packet injection. Additionally, EW-DHOA's ability to adjust to varying network circumstances can help to improve the energy efficiency and scalability of the WSN.

3.3.1 Blockchain based security

Blockchain Implementation: A blockchain-based distributed ledger is used to store the hash values of the data packets. Each block in the blockchain contains a set of hash values and a reference to the previous block. This ensures that the data cannot be altered without detection.

Blockchain Authentication: The blockchain-based distributed ledger is used to authenticate the data packets during transmission. Each node in the network has a copy of the blockchain and can use it to validate the integrity of the data packets.

The data packets are checked for integrity during transmission to ensure that they have not been tampered with or modified in any way. This is done using hash functions. The WSN comprises CHs, sensor nodes (SNs), BS, and end users. Considering the limited storage capacity and computational power of the SNs, they gather data and transmit it to their respective CHs. The CHs then receive the data and transmits it to nearby BSs, which are equipped with ample resources including computational power, energy, and storage. To realize this model, a hybrid approach utilizing both public and private blockchains is employed. The public blockchain is implemented on the BS, while the private blockchain is implemented on the CHs.

The authentication scheme consists of several steps, including initialization, registration, and authentication. During the initialization phase, the BS initiates the initialization process for all the nodes within the network. The BS generates private and public keys for the SNs, CHs, and itself. These keys are utilized for secure communication and authentication within the network. Each node is assigned a distinctive Media Access Control (MAC) address, and the IDs of the BS, CHs, and the sensors are denoted as BSID, CHID, and SNID, respectively.

The registration process for CHs is carried out through the utilization of smart contracts implemented on the public blockchain. The public blockchain stores the identity information of the CHs. The smart contract validates the authenticity of the CH's MAC address as well as the accuracy of its identity. Upon successful completion of these verification steps, the CH's identity is recorded in the public blockchain. In case the identity verification fails, an error is returned.

Conversely, the registration of nodes occurs within the private blockchain. Upon registration, nodes are granted permission to join the blockchain network. The registration procedure for the nodes follows a similar approach to that of CHs. The identity of the sensors are stored within the private blockchain. Once deployed, the member nodes are paired with their corresponding CHs, establishing a binding relationship between them. WSNs face the risk of two types of attacks: external attacks from outside sources and internal attacks carried out by compromised nodes within the network. To counter external attacks, the registration and authentication process ensures that only authorized nodes are allowed into the network, preventing intrusion attempts.

However, internal nodes can still pose a threat by disseminating false or misleading information within the network. To address this, nodes must undergo registration before joining the network. When a SN interacts with a CH, the CH validates the identity of the SN by referring to the private blockchain. Similarly, when a CH communicates with the BS, the BS verifies the identity of the CH by consulting the public blockchain. Moreover, during communication between two CHs, a process of mutual authentication is conducted. Both CHs send authentication requests to the BS, ensuring the authenticity and integrity of the communication between them.

In the case of an internal attack, nodes may exhibit selfish or malicious behaviour within the network. It isvital to recognize and exclude these malicious sensors during the registration process. This is achieved through the computation of trust values for the nodes, which helps in identifying and removing the malicious ones. Algorithm 2 outline the process involved in evaluating the trust of the nodes.

Algorithm 2 Blockchain based integrity verification [46]

1. Initialization:
   - Initialize the WSN nodes with unique IDs and public keys.
   - Set up a private blockchain network with a designated trusted node acting as the blockchain administrator.
   - Establish a public blockchain network where all participating nodes can access the blockchain ledger.
2. Data Sensing and Encryption:
   - Sensor nodes collect data from the environment.
   - Encrypt the collected data using a hybrid homographic-blowfsh encryption algorithm [46].
   - Attach a digital signature to the encrypted data using the sender's private key.
3. Data Transmission:
   - Sensor nodes transmit the encrypted data to neighboring nodes.
   - Verify the authenticity of the receiving nodes using their public keys.

4. Data Aggregation and Blockchain Validation:
   - Aggregator nodes receive data from multiple sources and perform aggregation operations.
   - Aggregator nodes validate the integrity and authenticity of received data by verifying the digital signatures.
   - If any data is found to be tampered with or untrustworthy, mark it as suspicious.
5. Blockchain Logging and Consensus:
   - The aggregator nodes create a block containing the verified data.
   - The blockchain administrator validates the block and appends it to the private blockchain.
   - Consensus mechanisms like Proof of Stake is employed to ensure agreement on the validity of the block.
6. Public Blockchain Update:
   - The verified block is broadcasted to the public blockchain network.
   - Participating nodes in the public network validate and append the block to the public blockchain.
   - Consensus mechanisms, such as Proof of Work or Byzantine Fault Tolerance, are utilized to achieve agreement on the validity of the block.
7. Trust Evaluation:
   - Each sensor in the network maintains a trust evaluation mechanism based on the behavior and performance of other nodes.
   - Trust scores are updated based on successful validation and verification of data.
8. Data Retrieval and Integrity Verification:
   - Users or applications can retrieve data from the blockchain by querying specific blocks or transactions.
   - Data integrity can be verified by validating digital signatures and checking the consensus mechanism used for the block.

3.3.2 EWO-DHOA optimization algorithm

In the WSN routing context, the earthworms can be seen as the routes or paths that are explored to find optimal routing solutions. Each earthworm represents a potential routing solution in the population. Deer mimic the behavior of deer hunting for prey, which is analogous to exploiting promising routes in the WSN routing problem. The deer select the best routes or paths discovered by the earthworms and use them to refine the solutions further. The population is usually initialized with a set of randomly generated routing solutions.

(i) DHOA Algorithm

The conventional Deer-Hunting Optimization Algorithm(DHOA) is derived from the hunting behaviour of humans towards deer, drawing inspiration from specific characteristics of deer. These characteristics include their exceptional visual sense, superior sense of smell, and ability to perceive ultra-high-frequency sounds. The mathematical formulation of the conventional DHOA consists of four distinct steps.

The initial population of hunters in the conventional DHOA is established and represented by Eq. (7).

$$P = \left[P_1, P_2, \ldots, P_k\right];\ 1 < l \le m \tag{7}$$

where, the variable m represents the overall count of hunters, while P represents the population size of the hunters.

The Objective function, $f(\mathrm{x})$ is computed using Eq. (8).

$$f(x) = \frac{1}{3}\left[\alpha T_{tot} + \beta E_{res} + \gamma D\right] \tag{8}$$

where, α, β, and γindicates the weight values such that$\alpha+\beta+\gamma=1$.Higher weights are assigned to $E_{res}$and T_{tot}, while assigning a lower weight to the distance. Specifically, the weight are set as follows: $\gamma=0.05$, $\beta=0.45$, &$\alpha=0.5$. Using the fitness value computed through Eq. (4), the source node transmits the data packet to the next-hop neighbour with the optimal fitness value, ensuring the best possible choice.

To begin, set the initial values for the position and wind angle. The mathematical equation utilized to calculate the wind angle, which is derived from the circumference of a circle, is presented in Eq. (9).

$$\psi_t = 2\pi g \tag{9}$$

The wind angle is denoted by the symbolψ. The value of the random number h falls within the range of 0 to 1. The present iteration is represented by t. The mathematical formulation for the position angle is provided in Eq. (10), where the angle of position is represented by the symbolβ.

$$\beta_t = \psi + \pi \tag{10}$$

In Step 3, we focus on the propagation of position. We examine two positions: the leader position $P_{ld}$and the successor positionP_{suc}.

The propagation process involves the position of the leader. The updating of the hunters' positions begins, assuming an optimal position to search for the best solution. Here, the encircling behaviour is represented in Eq. (11).

$$P_{t+1} = P_{ld} - J \cdot a \cdot \left|R \times P_{ld} - P_t\right| \tag{11}$$

In the current iteration, the positions of the hunters is represented asP_t. The updated position is represented asP_{t+1}. $a$is a random variable in the range [0, 2] that is introduced to account for the speed of the wind. The coefficient vectors $J$and R, computed using the mathematical formulas provided in Eq. (12) and (13) respectively, are associated with the aforementioned notation.

$$J = {}^{1}/_{4}\log\left(t + \frac{1}{t_{\max}}\right)b \tag{12}$$

$$R = 2 \cdot c \tag{13}$$

The maximum number of iterations is represented by $t_{\max}$. The parameter$b$, employed in the equation for computing the coefficient vectors that takes values ranging from -1 to 1, and $c$is a random number that falls in the range [0, 1].

The propagation process entails the adjustment of the position angle by incorporating a novel parameter, denoted as e_t, which is calculated based on the disparity between the visualization angle and wind angle, as expressed in Eq. (14). The visualization angle, denoted as r_t, associated with the prey, can be computed using Eq. (15).

$$e_t = \psi_t + r_t \tag{14}$$

$$r_t = g \times \frac{\pi}{8} \tag{15}$$

The search agent's successor position is assigned as P_{ld}. The position angle updating process is accomplished using Eq. (16). Additionally, the hunter's position is updated according to the position angle, as described in Eq. (17).

$$\beta_{t+1} = \beta_t + e_t \tag{16}$$

$$P_{t+1} = P_{ld} - a \cdot \left|\cos(\omega) \times P_{ld} - P_t\right| \tag{17}$$

The propagation process involves determining the successor's position. In this approach, the encircling process concept is employed by adjusting the vector R during the exploration stage. Initially, a random search is performed, with the vector $R<1$. The hunter's position is subsequently updated according to the position of the successor, as outlined in Eq. (18).

$$P_{t+1} = P_{suc} - J \cdot a \cdot \left| R \times P_{suc} - P_t \right| \tag{18}$$

If $R<1$, the selection of the search agent will be stochastic. Conversely, if $R \geq 1$, the best solution is chosen to update the positionof the search agent.

During the final phase, the position update is performed for all iterations until the best position is attained.

(ii) EWO algorithm

The traditional EWO is derived from from the contributions of earthworms to nature. Within earthworms, two types of reproduction, namely Reproduction 1 and Reproduction 2, occur.

Reproduction 1 involves hermaphrodites, where one parent is capable of giving birth. The mathematical formulation for this reproductive process is presented in Eq. (19).

$$P_{o1,n} = P_{\max,n} + P_{\min,n} - \gamma P_{o,n} \tag{19}$$

where, the position of the earthworm with index o is denoted as $P_{o,\,n}$, while the new position of the o^{th} earthworm is denoted as $P_{o1,\,n}$. The lower and upper positions of the earthworm are denoted as $P_{\min,\,n}$and$P_{\max,\,n}$, respectively. The similarity factor is represented byγ.

When γ is small, it indicates a higher degree of local search. Conversely, if $\gamma = 0$, the distance between them is large, as illustrated in Eq. (20).

$$P_{o1,n} = P_{\max,n} + P_{\min,n} \tag{20}$$

An optimal-based learning method, which is referred to as a global search, is achieved when the similarity factor $\gamma = 1$, as derived in Eq. (21).

$$P_{o1,n} = P_{\max,n} + P_{\min,n} - P_{o,n} \tag{21}$$

To balance the exploration and exploitation stages in reproduction 1, adjustments are made to the value of γ. This ensures a harmonious interplay between the two phases.

Reproduction 2 involves the determination of P_{o2} using M offspring when$M = 1$, 2, *and* 3. This process is mathematically derived in Eq. (22).

$$P_{o2} = \sum_{n=1}^{M} \mu_n P_{M,n} \tag{22}$$

Within Eq. (23), the weight factor is represented by μ_n, and its derivation can be found in Eq. (24).

$$\mu_n = \frac{1}{M-1} \frac{\sum_{y=1, y \neq n}^{M} H_y}{\sum_{y=1}^{M} H_y} \tag{23}$$

$$\mu_n = \frac{1}{M-1} \frac{+H_{n+1} + \cdots + H_{M-1} + H_M}{H_1 + H_2 + \cdots + H_{n-1} + H_n + H_{n+1} + \cdots + H_{M-1} + H_M} \tag{24}$$

In Eq. (19), the fitness of the y^{th} offspring is denoted as H_y, δ represents the proportional factor that adjusts the value of $P_{o1}P_{o2}$. The position of o for the next generation is computed using Eq. (25) after the two stages of reproduction. The next iteration of δ, denoted as δ^{t+1} is determined by Eq. (26).

$$P'_{o,n} = P_{o,n} + Wt_n * y \tag{25}$$

$$\delta^{t+1} = \tau \delta^t \tag{26}$$

where,τ represents the cooling factor, which remains constant throughout the process.

(iii) EW-DHOA algorithm

The traditional DHOA workson the basis of the hunting techniques used by humans to pursue deer. DHOA is highly effective in solving comprehensive test problems and stands out as a competitive and logical algorithm compared to others. On the other hand, Earthworm Optimization Algorithm (EWA) is well-suited for parallel computing and offers a balanced approach between reinforcement and diversification. However, the conventional DHOA has certain limitations, such as a higher probability of getting trapped in local optima and a gradual decrease in search speed. To address these drawbacks, EW-DHOA is proposed by integrating EWA with DHOA. This exhibits a high level of balance, exceptional searching ability in favourable regions, and high reliability. Furthermore, the input parameters of the proposed EW-DHOA are independent, making it versatile for application in large-scale and nonlinear power systems. The earthworms explore the search space by traversing different routes, and the deer exploit the best routes found by the earthworms to refine the solutions.

Furthermore, the solution is updated according to the position of the leader fitness. Once the solution is updated, the next update procedure is conducted using the EWA approach. In this process, the fitness is computed for all the solutions, and the position of the leaderis selected. The selected position of the leader is then updated using Eq. (27).

To prevent getting stuck in local optima as well as toenhance the search efficiency, the EWA method incorporates the use of the CM technique. The integration of the CM in EWA is described by Eq. (27) and Eq. (28). Throughout the process, the fitness function is constantly assessed, and when the minimum fitness is attained, the algorithm concludes. The fitness evaluation is carried out for all the solutions that have been updated through DHOA, and the leader position is chosen based on this assessment. The position of

the selected leader is subsequently updated by utilizing the CM technique from the conventional EWA.

$$Wt_n = \sum_{o=1}^{T_{pop}} P_{o,n}/T_{pop} \tag{27}$$

$$P'_{o,n} = P_{o,n} + Wt_n * y \tag{28}$$

where, the n^{th} position of the o^{th} earthworm is represented as $P_{o,n}$. The whole population is denoted by T_{pop}, Wt_n indicates weight vector, and$y$ indicates a random number extracted from the Cauchy distribution. On comparison, if the new fitness is better than the old fitness, the existing solution isupdated with the new ones. This iterative process continues until the termination criteria are met, resulting in the identification of optimal routing solutions in the WSN.

4 Simulation results and analysis

The efficacy of the suggested method is validated using the MATLAB platform, employing a configuration of 100 sensors in the designated area of$200m \times 200m$. The simulations is carried out in a NS3 simulator. The attack is executed by inundating the sensors with RREQ packets. Each node possesses a communication range of 30 m. The comparison of existing WSN routing protocols and the simulation parameters can be found in Tables 1 and 2.

4.1 Evaluation metrics

The metrics used for evaluating the performance are given as follows:

(i) Throughput: It is the rate at which data is successfully transmitted from source nodes (sensors) to the destination or sink node over the network. It measures the amount of useful data that can be transferred within a given time frame.

$$Throughput = \frac{\mathrm{T_{dp}}}{\mathrm{T}} \tag{29}$$

where, T signifies the time period and $\mathrm{T_{dp}}$ denotes the sum of delivered packets.

(ii) Delay: It refers to the time it takes for data to travel from a source node (sensor) to a destination or sink node in the network. It represents the latency or time delay experienced by the data packets during transmission.

$$Delay = \frac{T_{arrival} - T_{send}}{\mathrm{T_{conn}}} \tag{30}$$

where, $\mathrm{T_{conn}}$ denotes the quantity of connections, $T_{avrrival}$ indicates the arrival time, and T_{send}represents the timestamp indicating the time when the packet was transmitted.

(iii) Energy Consumption: It refers to the sum of energy consumed by individual sensor nodes or the network as a whole during their operation. Energy efficiency is a critical concern in WSNs due to the limited energy resources of the sensor nodes, typically powered by batteries or other energy-constrained sources. It is computed using Eq. (34).

$$E_{con} = E_{tx} + E_{rx} \tag{31}$$

where, the variable E_{rx}represents the energy dissipated during reception, while where the variable E_{tx}represents the energy dissipated during transmission.

(iv) Network Lifetime: The network lifetime is the duration during which 75% of the sensors in the network cease to function or, alternatively, as the duration when the remaining energy of 75% of the nodes reaches zero

(v) PDR: It is a metric that quantifies the efficiency of packet transmission within a WSN. PDR represents the ratio of successfully delivered packets to the total number of packets sent by a source node in the network.

$$PDR = \frac{p_{del}}{P_{sent}} \times 100 \tag{32}$$

where, P_{sent} represents the sum of data packets sent by the SN and p_{del} represents the sum of packets obtained at the DN.

(vi) Detection Rate: It refers to the effectiveness of a system or algorithm in detecting and identifying malicious or unauthorized activities within the network. It represents the percentage or proportion of detected malicious activities out of the total number of actual malicious events occurring in the network.

$$DR = \frac{T_{\mathrm{det}}}{T_{mal}} \times 100 \tag{33}$$

where, T_{det} indicates the count of detected malicious nodes, while T_{mal} represents the total number of malicious nodes.

In the design and simulation of our proposed Wireless Sensor Network (WSN) model for smart agriculture, we have strategically incorporated network overhead parameters to thoroughly analyze and optimize the system's performance. The consideration of the number of headers and footers per packet serves as a valuable metric, allowing us to delve into the intricacies of additional data transmitted for addressing, error-checking, and control purposes. This insight is instrumental in optimizing the efficiency of packet delivery within the network. Simultaneously, the

Table 1 Comparison of existing WSN routing protocols

Author Name	Proposed Method	Features	Limitation/Gap
Yao et al. [17]	EERPMS	Minimized energy usage.	It has higher computational and communication overhead due to the use of the multi-threshold segmentation algorithm and require accurate location information for optimal CH selection, which is not always be feasible in practical applications.
Sahoo et al. [18], 2021	GAPSO-H	Enables the selection of the most efficient CH nodes for improved network performance and optimizes sink mobility to minimize energy usage and prolong network lifetime	Data loss or corruption can occur during transmission, leading to inaccurate or incomplete data.
Maheshwari et al. [19], 2021	BOA-ACO	• Improved network lifespan due to the energy-efficient CH selection and data transmission route development. • Reduced nodes' energy usage while transferring the packets.	Using integrated optimization algorithms is complex and require additional computational resources.
Yadav and Mahapatra [20], 2021	CI-ROA	Conserve more energy.	Routing overhead is increased.
Zachariah and Kuppusamy [21], 2022	HOCK and HECK	Minimized energy consumption.	Enhancing security measures may increase energy consumption.
Han et al. [22], 2022	TAGA	Improves network security, energy efficiency, scalability, and reliability.	Complex and time-consuming process.
Anand and Sharma [23]	AgroKy	Enhanced network lifespan.	High computational time.
Hu et al. [24], 2021	TBSEER	Reduced energy usage.	Increased routing overhead
Thahniyath and Jayaprasad [25], 2022	SLBR	Minimize overhead among CH by utilizing a metric for load balancing routing.	Consuming additional energy resources.
Singh and Singh [26], 2021	HCR	Load balancing and a multi-level clustering design prevent the premature failure of WSNs.	Computationally intensive.
Gopinath et al. [27], 2021	SCEER	Balance between network security and energy efficiency is achieved by using a cryptography-based energy routing scheme.	Managing encryption keys is complex and time-consuming process.
Reddy et al. [28], 2021	ACI-GSO	Minimize energy usage by reducing the distance among selected node.	Implementing optimization algorithms require additional resources such as memory and energy.
Khot and Naik [29], 2021	P-WWO	• Reduced path failure due to PSO algorithm. • Uses only few number of parameters.	The packet loss ratio has increased, and the effectiveness in mitigating attacks is low.
Bangotra et al. [30], 2022	TBSIOP	• Conserving energy is accomplished by using an energy trust value calculator. • Reduce retransmissions by dividing up a node's transmission work among its neighbours.	More severe attacks on WSN are not handled by this approach.
Fang et al. [31], 2021	MSCR	The network lifespan is extended by the consideration of environmental factors.	Slow convergence rates and reduced reliability and accuracy due to complex network topologies
Lazrag et al. [32], 2021	Blockchain based routing	Decentralized, and tamper-proof way of managing transactions and data in WSNs	Increases the cost of node due to complex computations.

Table 1 (continued)

Author Name	Proposed Method	Features	Limitation/Gap
Revanesh and Sridhar [33], 2021	Integration of the Block chain based DCNN	Provides a high level of security against malicious attacks by integrating multiple algorithms	• Multiple complex algorithms, make it difficult to implement and maintain. • Use of multiple algorithms requires significant computational resources.

meticulous assessment of latency parameters provides a comprehensive understanding of the temporal delays introduced by overhead components. This analysis is pivotal for ensuring the responsiveness of our WSN, particularly in real-time applications critical to smart agriculture. Furthermore, the evaluation of energy consumption parameters is a cornerstone of our approach. By tracking the energy expended on processing control messages, transmitting acknowledgment packets, and managing routing information, we gain crucial insights into the energy efficiency of our model. This in-depth energy consumption analysis helps identify energy-intensive processes and informs potential avenues for optimization, contributing to the overall sustainability of the WSN in agricultural scenarios. In tandem with overhead considerations, our model employs various performance metrics to holistically evaluate the system's efficacy.

4.2 Comparative analysis

The proposed protocol demonstrates clear superiority over existing techniques, namely GA-PSO, CI-ROA, ACI-GSO, and P-WWO, as evidenced by a comprehensive comparative analysis illustrated in Fig. 4. The evaluation, conducted by varying sensor node density, underscores the remarkable performance of the proposed method in enhancing network lifetime. At a density of 100 nodes, the proposed protocol achieves an average of 2500 rounds, surpassing the performance of GA-PSO (1800 rounds), CI-ROA (2000 rounds), ACI-GSO (1900 rounds), and P-WWO (2100 rounds). This initial comparison already signifies the proposed method's capability to outperform existing protocols. As the node density increases to 500, the proposed protocol continues to excel, achieving an average of 3200 rounds, while GA-PSO, CI-ROA, ACI-GSO, and P-WWO attain 2500, 2800, 2600, and 2700 rounds, respectively. The graphical representation of this comparative analysis consistently places the proposed method's y-axis values higher than other methods across varying node densities on the x-axis, affirming its consistent and substantial improvement in network lifetime. The proposed protocol's success can be attributed to its optimized cluster formation, ensuring efficient resource utilization and balanced energy distribution, along with its adaptability to diverse node densities, positioning it as a robust and promising solution for enhancing the overall efficiency of WSNs.

Table 2 Parameter Setup

Parameter	Value
Nodes Deployed	100–500
Area	$200 \times 200 m^2$
Transmitter amplifierε_{amp}	0.0013 pJ/bit/m^4
The initial energy of the node	0.5 J
ε_{fs}	10 pJ/ bit/m^2
Packet Size (bits)	4000
Transmitter and Receiver ElectronicsE_{elec}	50 nJ/bit
Population size	50
Maximum iteration	100
No. of headers	200 headers
No. of footers	267 footers
Latency	7 ms

The energy consumption comparative analysis presented in Fig. 5 unequivocally establishes the superior performance of the proposed method when compared to existing techniques. At a node density of 100, the proposed method excels, achieving an average energy consumption of 0.3 mJ, outperforming GA-PSO, CI-ROA, ACI-GSO, and P-WWO, which register higher energy consumption levels of 0.4 mJ, 0.45 mJ, 0.5 mJ, and 0.55 mJ, respectively. This initial comparison underscores the proposed method's efficiency in resource utilization, resulting in significantly reduced energy consumption. As the node density escalates to 500, the energy consumption performance of the proposed method further strengthens. Remarkably, the proposed method attains the lowest energy consumption, averaging at 0.2 mJ, outshining GA-PSO, CI-ROA, ACI-GSO, and P-WWO, with consumption levels of 0.3 mJ, 0.35 mJ, 0.4 mJ, and 0.45 mJ, respectively. This consistent trend reinforces the proposed method's prowess in achieving enhanced energy efficiency, especially in scenarios with higher node densities. The underlying reasons for the improved energy efficiency of the proposed protocol are multi-faceted. Firstly, the optimized cluster formation embedded in the proposed method ensures judicious resource allocation and mitigates unnecessary energy dissipation. By strategically distributing energy-intensive roles within the network, the proposed method minimizes the risk of premature energy depletion

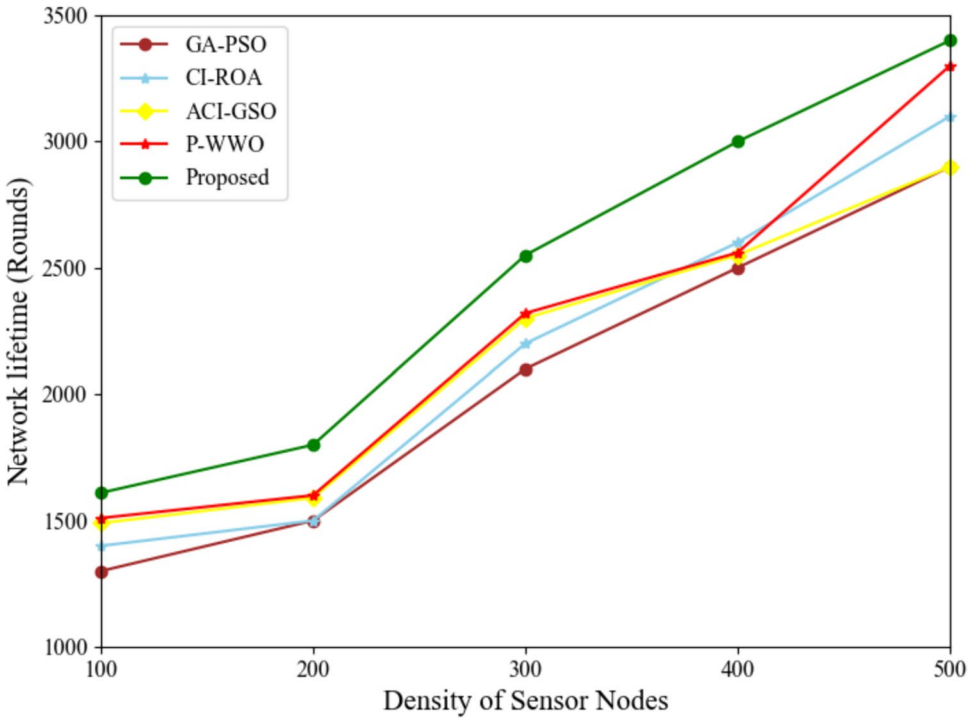


Fig. 4 Network lifetime

in specific nodes, thus contributing to prolonged network lifespan. Additionally, the incorporation of the Earthworm-based Deer Hunting Optimization Algorithm (EW-DHOA) in the routing protocol plays a pivotal role in achieving superior energy efficiency. The EW-DHOA routing protocol facilitates effective data transmission, optimizing the routing path and minimizing energy wastage. Its adaptive and bio-inspired approach allows for efficient adjustment to varying network conditions, further enhancing energy efficiency in data transmission. In summation, the proposed protocol's advantageous features, including optimized cluster formation and the incorporation of the EW-DHOA routing protocol, culminate in significantly improved energy efficiency, standing out as a promising and efficient solution.

Upon scrutinizing the performance depicted in Fig. 6, it becomes evident that the proposed method consistently outshines existing techniques, particularly in terms of packet delivery ratio (PDR). At a node density of 100, the proposed method excels with an average PDR of 98%, surpassing GA-PSO (94%), CI-ROA (93%), ACI-GSO (95%), and P-WWO (96%). This initial comparison underscores the proposed method's efficacy in ensuring reliable and efficient data transmission, leading to a higher PDR. Across different node densities, the proposed method maintains its superiority, consistently outperforming existing techniques in terms of PDR. This noteworthy trend emphasizes the robustness and adaptability of the proposed protocol to varying network conditions, solidifying its position as a reliable solution for achieving high PDR in Wireless Sensor Networks (WSNs). The proposed routing protocol plays a pivotal role in facilitating efficient and reliable data transmission by minimizing packet loss and optimizing routing paths. The integration of the blockchain-based integrity checking mechanism further contributes to the enhanced PDR by ensuring the integrity and authenticity of transmitted packets. This integration significantly reduces the chances of packet loss or corruption, thereby fortifying the reliability of data delivery in the proposed method. In summary, the proposed protocol's consistent outperformance in PDR is attributed to its efficient routing strategies, minimization of packet loss, and

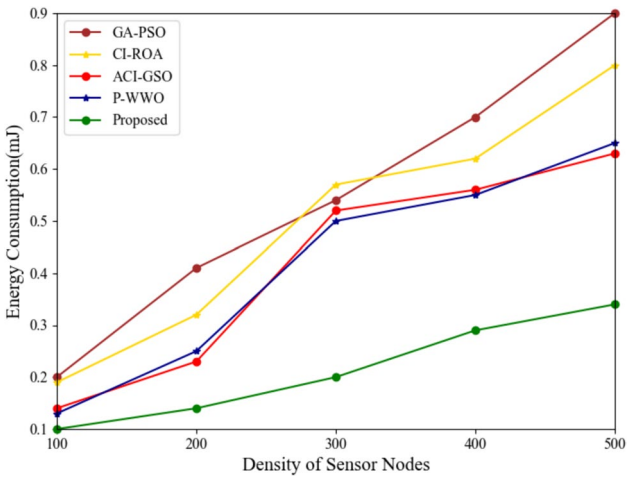
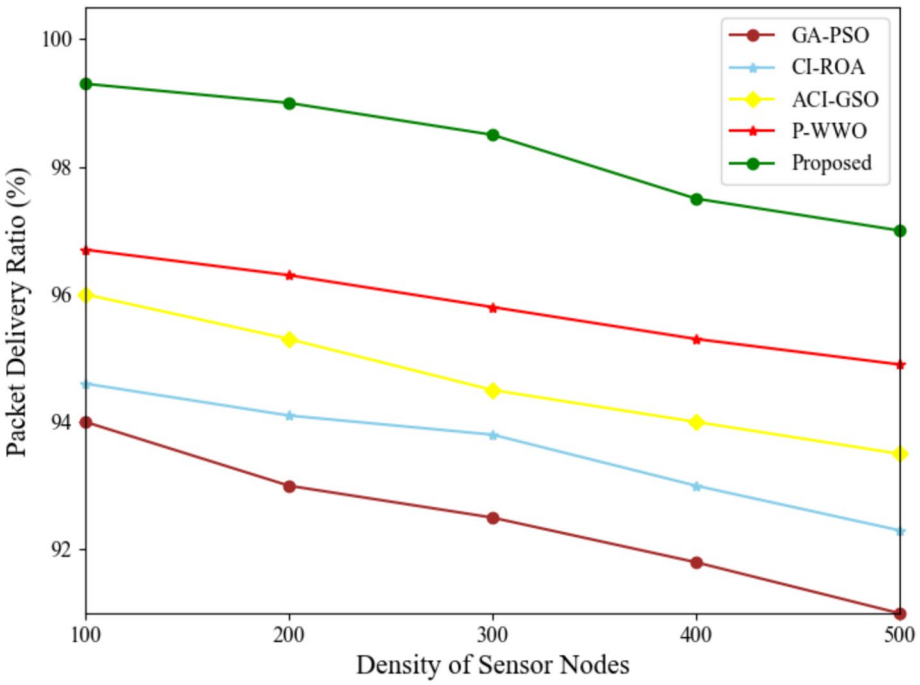


Fig. 5 Energy consumption

Fig. 6 Packet delivery ratio



the incorporation of a blockchain-based integrity checking mechanism. These features collectively position the proposed method as a superior choice for achieving reliable and robust data transmission compared to existing protocols.

In the realm of Wireless Sensor Networks (WSNs), achieving high throughput is paramount for efficient data transmission and communication. Figure 7 provides a comprehensive overview of throughput results, where the x-axis represents the density of sensor nodes ranging from 100 to 500, and the y-axis denotes throughput measured in megabits per second (Mbps). The results of the analysis unmistakably highlight a significant advantage of the proposed method over existing techniques in terms of achieving higher throughput. At a node density of 500, the proposed method exhibits an impressive average throughput of 0.8 Mbps. In comparison, GA-PSO achieves 0.6 Mbps, CI-ROA achieves 0.7 Mbps, ACI-GSO achieves 0.6 Mbps, and P-WWO achieves 0.7 Mbps. This substantial improvement in the performance of the proposed method can be attributed to the incorporation of the Earthworm-based Deer Hunting Optimization Algorithm (EW-DHOA). The EW-DHOA algorithm optimizes routing decisions, effectively reducing latency and maximizing the utilization of available network resources. The adaptive and bio-inspired nature of EW-DHOA allows the proposed method to dynamically adjust to varying network conditions, resulting in optimized routing paths that minimize delays and enhance overall throughput. By efficiently leveraging the routing capabilities of EW-DHOA, the proposed method outperforms existing protocols, ensuring a more efficient use of network resources and, consequently, achieving higher throughput. This strategic combination of optimized routing decisions and the adaptability of EW-DHOA positions the proposed protocol as a superior choice for enhancing throughput in WSN's.

In Wireless Sensor Networks (WSNs) dedicated to smart agriculture, the longevity and resilience of sensor nodes play a pivotal role in ensuring sustained network connectivity and functionality. The insightful analysis presented in Fig. 8 underscores the superiority of the proposed method in preserving a higher number of active sensor nodes compared to existing techniques, including GA-PSO, CI-ROA, ACI-GSO, and P-WWO. As the simulation progresses through an increasing number of rounds, the proposed approach consistently outperforms other methods in sustaining a greater number of alive sensor nodes. In the early stages of the simulation, all methods commence with the same number of nodes. However, the proposed method exhibits a slower decline in the number of alive nodes as the rounds advance, highlighting its resilience and efficiency in preserving network connectivity. The divergence in performance becomes more pronounced as the simulation unfolds. At the 3500th round, the proposed method sustains approximately 250 alive sensor nodes, whereas GA-PSO and CI-ROA have around 150 and 152 nodes, ACI-GSO has around 100 nodes,

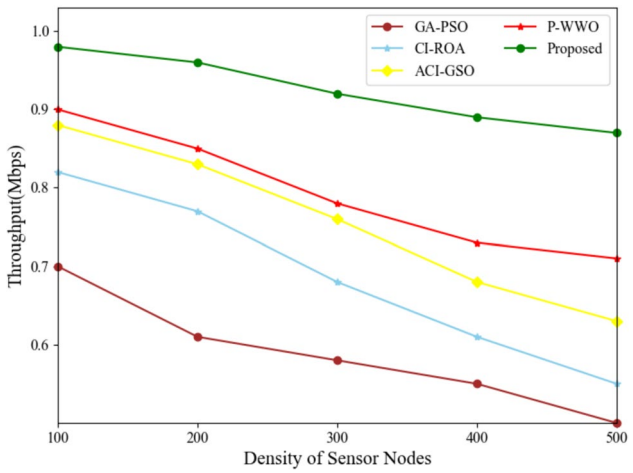
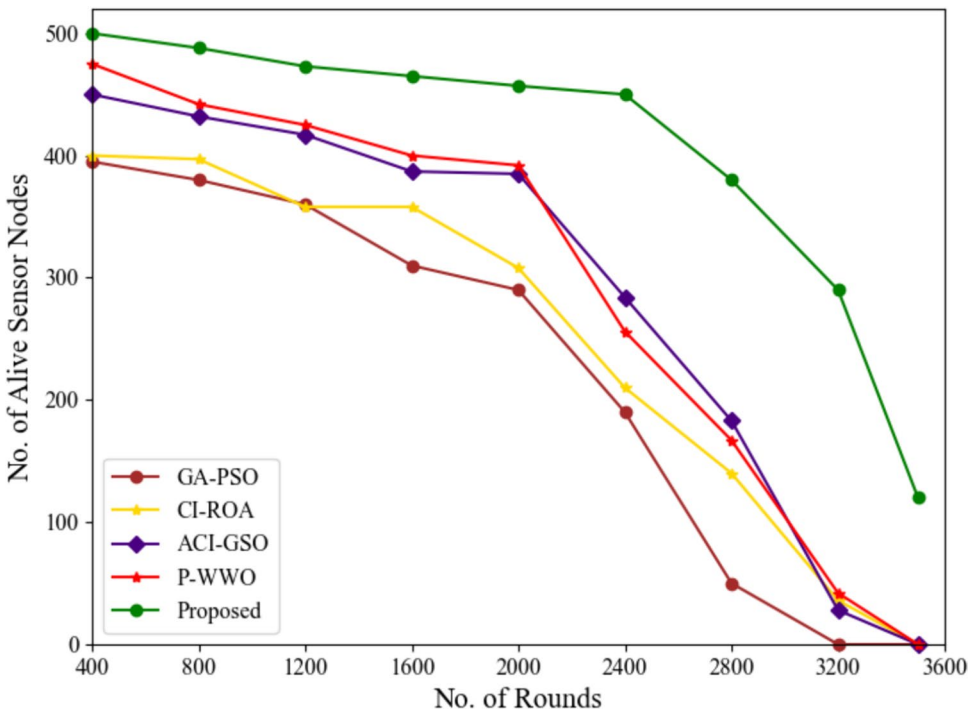


Fig. 7 Throughput

and P-WWO has around 120 nodes. This substantial difference is a testament to the efficacy of the proposed Distributed Fuzzy Cognitive Maps (DFCM) method in distributing and balancing energy usage among sensor nodes, thereby mitigating the risk of early energy depletion. Furthermore, the incorporation of the blockchain-based mechanism in the proposed protocol enhances the security and reliability of the network. This added layer of security prevents malicious attacks that could compromise the functionality of sensor nodes, contributing to the sustained vitality of the network over extended periods. In summary, the proposed protocol excels in maintaining a higher number of alive sensor nodes, attributed to the effective energy distribution facilitated by the DFCM method. The integration of blockchain-based security mechanisms further fortifies the network's reliability.

The evidence presented in Fig. 9 unequivocally establishes the consistent outperformance of the proposed method in terms of detection rate, solidifying its superiority over other examined methods. With a detection rate ranging from 75% to 90%, the proposed method excels in identifying malicious nodes within the network, showcasing a higher level of efficacy compared to alternative approaches. This superior detection rate underscores the proposed method's capability to effectively recognize and mitigate various security threats, contributing to the overall security and robustness of the Wireless Sensor Network (WSN). Achieving the highest detection rate among the examined methods emphasizes the proposed approach's prowess in safeguarding the network against potential malicious activities. This outcome is particularly significant in the context of WSNs used for smart agriculture, where data integrity and confidentiality are paramount. The proposed method's ability to consistently detect and address security threats enhances the overall security posture of the WSN, ensuring the trustworthiness and confidentiality of the transmitted data. The justification for the proposed protocol's superiority lies in its adeptness at implementing advanced security measures, possibly facilitated by the integration of the blockchain-based integrity checking mechanism. This additional layer of security

Fig. 8 Alive node analysis



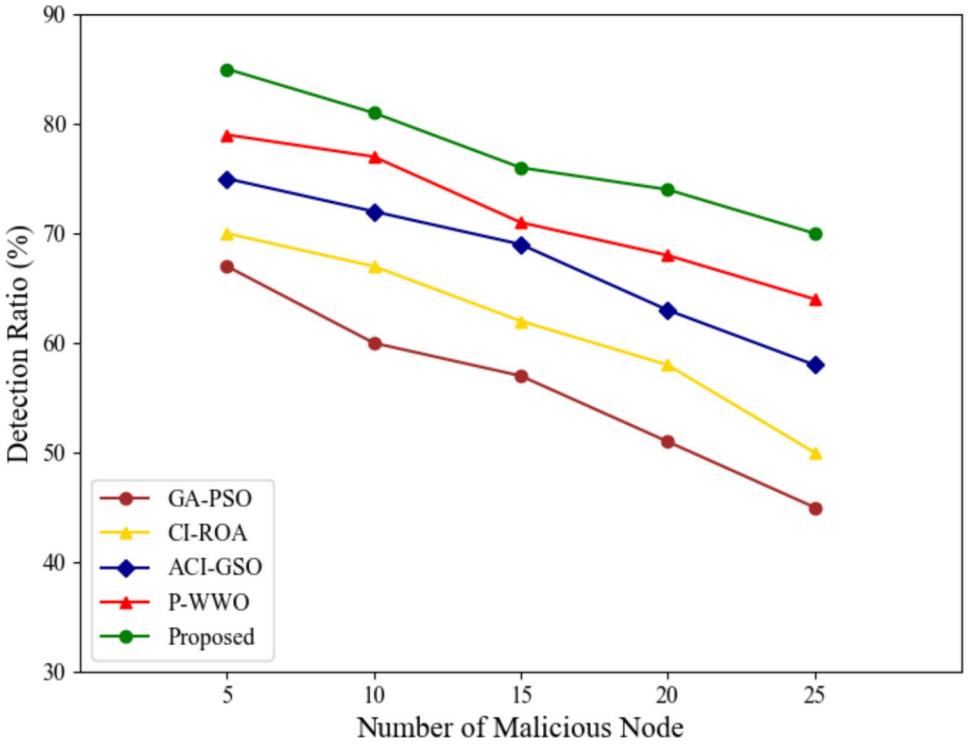


Fig. 9 Detection ratio

enhances the network's ability to detect and respond to malicious nodes effectively.

The assessment depicted in Fig. 10 unequivocally demonstrates the proposed method's exceptional convergence rate, establishing its superiority over other analyzed techniques. The innovative approach of combining the Deer Hunting Optimization Algorithm (DHOA) and Earthworm Algorithm (EWA) in the EW-DHOA algorithm contributes significantly to this high convergence rate. By harnessing the unique strengths and characteristics of both DHOA and

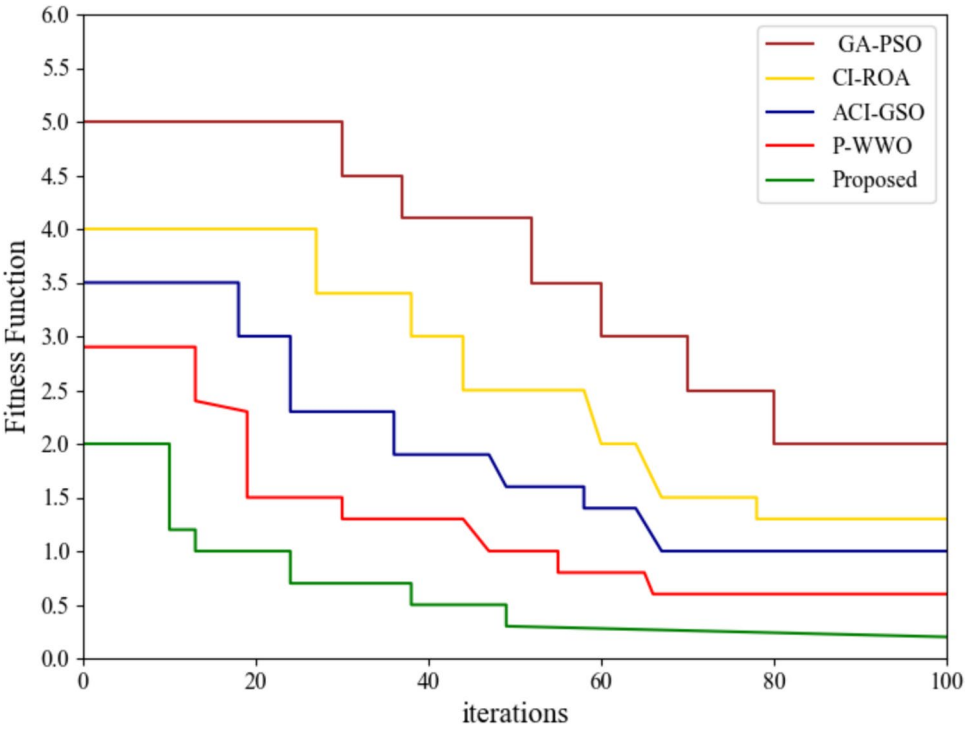


Fig. 10 Convergence analysis

EWA, the proposed method achieves a synergistic effect that surpasses the convergence rates of alternative approaches. DHOA's proficiency in updating solutions based on fitness and the position of the leader enhances the algorithm's ability to explore the search space effectively. This adaptability ensures that the algorithm can dynamically adjust to evolving conditions, preventing premature convergence and facilitating continuous exploration of potential solutions. On the other hand, EWA brings its own set of advantages by incorporating the Crowding Mechanism (CM), which prevents the algorithm from getting trapped in local optima and promotes a more thorough exploration of the solution space. The integration of these two powerful techniques within the EW-DHOA algorithm allows for a holistic and nuanced exploration of the solution space, leading to a remarkably improved convergence rate. This convergence rate is pivotal in optimizing the efficiency and effectiveness of the proposed protocol, particularly in scenarios where quick and accurate decision-making is essential. In summary, the proposed method stands out due to its ability to leverage the complementary strengths of DHOA and EWA, resulting in a superior convergence rate. This comprehensive exploration of the solution space ensures that the proposed protocol converges towards optimal solutions more effectively than other existing protocols.

5 Discussion and failure analysis

The proposed model represents a groundbreaking advancement in the domain of secure and efficient routing for Wireless Sensor Networks (WSNs) deployed in smart agriculture. A distinctive feature is the integration of the Earthworm-based Deer Hunting Optimization Algorithm (EW-DHOA) with blockchain technology, creating a resilient and tamper-proof routing infrastructure. This synergy ensures that data transmission in the network is not only secure but also optimized for the dynamic conditions of agricultural environments. The introduction of Distributed Fuzzy Cognitive Maps (DFCM) for Cluster Head (CH) selection marks another significant contribution, elevating the protocol's adaptability and intelligence. Unlike conventional routing protocols, our hybrid solution ingeniously combines bio-inspired algorithms with blockchain-based integrity checking, establishing a robust framework for data transmission. Moreover, the protocol introduces a novel mechanism through the dynamic updating of local blockchains, allowing real-time adjustments in routing decisions. This dynamic adaptation enhances the system's resilience in response to the ever-changing conditions of smart agriculture. In concert, these innovations tackle the challenges of energy efficiency, scalability, and security in WSNs, positioning our protocol as a pioneering and promising advancement in the realm of smart agriculture.

While the proposed hybrid protocol introduces innovative features and advancements in secure and efficient routing for Wireless Sensor Networks (WSNs) in smart agriculture, it is crucial to acknowledge certain limitations and potential failures that may impact its practical implementation.

a) Practical Implementation Challenges

- Failure Analysis: The practical implementation of the proposed model may encounter challenges related to computational and communication complexities, hindering its feasibility in dynamic wireless sensor network environments.
- Mitigation Strategy: Adopting a comprehensive approach that involves algorithmic optimizations, energy-efficient consensus mechanisms, and adaptive communication strategies addresses the practical implementation challenges. Integrating hardware optimizations and dynamic participation in consensus further enhances the model's adaptability to real-world constraints.

b) Communication Overhead

- Failure Analysis: Relying on blockchain for maintaining local blockchains and ensuring secure routing introduces communication overhead. The broadcasting of routing decisions and frequent updates across the network may result in additional message exchanges, impacting communication bandwidth and introducing latency.
- Mitigation Strategy: Implementing selective blockchain usage, batch processing, and compression techniques can significantly reduce communication overhead. Asynchronous communication, adaptive update frequencies, and dynamic participation in consensus mechanisms contribute to more efficient communication and reduced network congestion.

6 Conclusion

This paper presented an optimized secure EW-DHOA routing protocol for smart agriculture. The algorithm begins with an initialization phase, followed by the selection of CHs using a FCM approach. This approach enhances the selection process by considering distance from the BS, residual energy, and number of neighbours. The DF algorithm ensures balanced energy usage and increases the network's lifespan by distributing CHs evenly. The EW-DHOA algorithm determines optimal paths for data transmission, while the use of blockchain technology guarantees the integrity

and reliability of routing information. The comparative analysis show that the proposed method consistently outperforms the alternatives, achieving longer network lifetimes, lower energy consumption, higher packet delivery ratios, improved throughput, and a higher number of alive sensor nodes. In the future work, exploring techniques to incorporate mobility support in the proposed method would enable more realistic modelling of dynamic network topologies.

Author contribution All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Ashutosh Kumar Rao, Kapil Kumar Nagwanshi, Manoj Kumar Shukla. The first draft of the manuscript was written by Ashutosh Kumar Rao and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript. Conceptualization: Ashutosh Kumar Rao, Kapil Kumar Nagwanshi; Methodology: Ashutosh Kumar Rao, Manoj Kumar Shukla; Formal analysis and investigation: Ashutosh Kumar Rao, Kapil Kumar Nagwanshi; Writing - original draft preparation: Ashutosh Kumar Rao, Kapil Kumar Nagwanshi; Writing - review and editing: Ashutosh Kumar Rao, Kapil Kumar Nagwanshi, Manoj Kumar Shukla; Supervision: Manoj Kumar Shukla.

Funding There is no funding for this study.

Declarations

Ethics approval This article does not contain any studies with human participants and/or animals performed by any of the authors.

Consent to publish There is no consent to publish for this study.

Conflict of interest The authors declare no competing interests.

References

1. Azadi H, Moghaddam SM, Burkart S, Mahmoudi H, Van Passel S, Kurban A, Lopez-Carr D (2021) Rethinking resilient agriculture: From climate-smart agriculture to vulnerable-smart agriculture. J Clean Prod 319:128602
2. Sanjeevi P, Prasanna S, Siva Kumar B, Gunasekaran G, Alagiri I, Vijay Anand R (2020) Precision agriculture and farming using internet of things based on wireless sensor network. Trans Emerg Telecommun Technol 31(12):e3978
3. Sinha BB, Dhanalakshmi R (2022) Recent advancements and challenges of internet of things in smart agriculture: a survey. Futur Gener Comput Syst 126:169–184
4. Gsangaya KR, Hajjaj SS, Sultan MT, Hua LS (2020) Portable, wireless, and effective internet of things-based sensors for precision agriculture. Int J Environ Sci Technol 17:3901–3916
5. Santhosh J, Balamurugan P, Arulkumaran G, Baskar M, Velumani R (2021) Image driven multi feature plant management with FDE based smart agriculture with improved security in wireless sensor networks. Wirel Pers Commun 127(2):1–17
6. Gheisari M, Yaraziz MS, Alzubi JA, Fernández-Campusano C, Feylizadeh MR, Pirasteh S, Abbasi AA, Liu Y, Lee CC (2022) An efficient cluster head selection for wireless sensor network-based smart agriculture systems. Comput Electron Agric 198:107105
7. Hosseinzadeh M, Tanveer J, MasoudRahmani A, Yousefpoor E, SadeghYousefpoor M, Khan F, Haider A (2022) A cluster-tree-based secure routing protocol using dragonfly algorithm (DA) in the internet of things (IoT) for smart agriculture. Mathematics. 11(1):80
8. El Khediri S, Khan RU, Nasri N, Kachouri A (2020) MW-LEACH: low energy adaptive clustering hierarchy approach for WSN. IET Wireless Sens Syst 10(3):126–129
9. Shafiq M, Ashraf H, Ullah A, Tahira S (2020) Systematic literature review on energy efficient routing schemes in WSN–a survey. Mobile Netw Appl 25:882–895
10. Hossan A, Choudhury PK (2022) DE-SEP: distance and energy aware stable election routing protocol for heterogeneous wireless sensor network. IEEE Access 10:55726–55738
11. Sadhana S, Sivaraman E, Daniel D (2021) Enhanced energy efficient routing for wireless sensor network using extended power efficient gathering in sensor information systems (E-PEGASIS) protocol. Procedia Comput Sci 194:89–101
12. Kaur K, Sharma ES (2020) : Enhanced Distributed Energy Efficient Clustering Protocol. In: 2020 International Conference on Computer Communication and Informatics (ICCCI). IEEE, pp 1–5
13. Villas LA, Boukerche A, Ramos HS, De Oliveira HA, de Araujo RB, Loureiro AA (2012) DRINA: a lightweight and reliable routing approach for in-network aggregation in wireless sensor networks. IEEE Trans Comput 62(4):676–689
14. Yuan X, Chen Y (2022) Secure routing protocol based on dynamic reputation and load balancing in wireless mesh networks. J Cloud Comput 11(1):77
15. Kumar R, Tripathi S, Agrawal R (2020) An analysis and comparison of security protocols on wireless sensor networks (WSN). In: Design Frameworks for Wireless Networks. Springer, pp 3–21
16. Nagappan K, Rajendran S, Alotaibi Y (2022) Trust aware multi-objective metaheuristic optimization based secure route planning technique for cluster based IIoT environment. IEEE Access. 10:112686–112694
17. Yao YD, Li X, Cui YP, Wang JJ, Wang C (2022) Energy-efficient routing protocol based on multi-threshold segmentation in wireless sensors networks for precision agriculture. IEEE Sensors J 22(7):6216–6231
18. Sahoo BM, Pandey HM, Amgoth T (2021) GAPSO-H: a hybrid approach towards optimizing the cluster based routing in wireless sensor network. Swarm Evol Comput 60:100772
19. Maheshwari P, Sharma AK, Verma K (2021) Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization. Ad Hoc Netw 110:102317
20. Yadav RK, Mahapatra RP (2021) Energy aware optimized clustering for hierarchical routing in wireless sensor network. Comput Sci Rev 41:100417
21. Zachariah UE, Kuppusamy L (2022) A hybrid approach to energy efficient clustering and routing in wireless sensor networks. Evol Intel 15(1):1–3
22. Han Y, Hu H, Guo Y (2022) Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm. IEEE Access 10:11538–11550
23. Anand S, Sharma A (2022) AgroKy: an approach for enhancing security services in precision agriculture. Measurement: Sensors 24:100449
24. Hu H, Han Y, Yao M, Song X (2021) Trust based secure and energy efficient routing protocol for wireless sensor networks. IEEE Access 10:10585–10596
25. Thahniyath G, Jayaprasad M (2022) Secure and load balanced routing model for wireless sensor networks. J King Saud Univ-Comput Inform Sci 34(7):4209–4218

26. Singh H, Singh D (2021) Hierarchical clustering and routing protocol to ensure scalability and reliability in large-scale wireless sensor networks. J Supercomput 77:10165–10183
27. Gopinath S, Kumar KV, Elayaraja P, Parameswari A, Balakrishnan S, Thiruppathi M (2021) Sceer: secure cluster based efficient energy routing scheme for wireless sensor networks. Mater Today: Proc 45:3579–3584
28. Reddy DL, Puttamadappa C, Suresh HN (2021) Merged glowworm swarm with ant colony optimization for energy efficient clustering and routing in wireless sensor network. Pervasive Mobile Comput 71:101338
29. Khot PS, Naik U (2021) Particle-water wave optimization for secure routing in wireless sensor network using cluster head selection. Wirel Pers Commun 119:2405–2429
30. Bangotra DK, Singh Y, Selwal A, Kumar N, Singh PK (2022) A trust based secure intelligent opportunistic routing protocol for wireless sensor networks. Wirel Pers Commun 127(2):1045–1066
31. Fang W, Zhang W, Chen W, Liu J, Ni Y, Yang Y (2021) MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks. EURASIP J Wireless Commun Netw 2021:1–20
32. Lazrag H, Chehri A, Saadane R, Rahmani MD (2021) Efficient and secure routing protocol based on Blockchain approach for wireless sensor networks. Concurr Comput: Pract Exp 33(22):e6144
33. Revanesh M, Sridhar V (2021) A trusted distributed routing scheme for wireless sensor networks using blockchain and metaheuristics-based deep learning technique. Trans Emerg Telecommun Technol 32(9):e4259
34. Tabatabaei S (2020) A novel fault tolerance energy-aware clustering method via social spider optimization (SSO) and fuzzy logic and mobile sink in wireless sensor networks (WSNs). Comput Syst Sci Eng 35(6):477–494
35. Tabatabaei S, Rajaei A, Rigi AM (2019) A novel energy-aware clustering method via lion pride optimizer algorithm (LPO) and fuzzy logic in wireless sensor networks (WSNs). Wirel Pers Commun 108:1803–1825
36. Tabatabaei S (2021) A new routing protocol for energy optimization in mobile ad hoc networks using the cuckoo optimization and the TOPSIS multi-criteria algorithm. Cybern Syst 52(6):477–497
37. Akbari Y, Tabatabaei S (2020) A new method to find a high reliable route in IoT by using reinforcement learning and fuzzy logic. Wirel Pers Commun 112(2):967–983
38. Gorgich S, Tabatabaei S (2021) Proposing an energy-aware routing protocol by using fish swarm optimization algorithm in WSN (wireless sensor networks). Wirel Pers Commun 119(3):1935–1955
39. Ebrahimi S, Tabatabaei S (2020) Using clustering via soccer league competition algorithm for optimizing power consumption in wsns (wireless sensor networks). Wirel Pers Commun 113:2387–2402
40. Allahverdi Mamaghani A, Ebrahimi Dishabi MR, Tabatabaei S, Abdollahi Azgomi M (2021) A novel clustering protocol based on willow butterfly algorithm for diffusing data in wireless sensor networks. Wirel Pers Commun 121(4):3425–3450
41. Tabatabaei S, Rigi AM (2019) Reliable routing algorithm based on clustering and mobile sink in wireless sensor networks. Wirel Pers Commun 108(4):2541–2558
42. Tabatabaei S (2022) Provide energy-aware routing protocol in wireless sensor networks using bacterial foraging optimization algorithm and mobile sink. PLoS One 17(3):e0265113
43. Miri ST, Tabatabaei S (2020) Improved routing vehicular ad-hoc networks (VANETs) based on mobility and bandwidth available criteria using fuzzy logic. Wirel Pers Commun 113:1263–1278
44. Tabatabaei S (2023) Introducing a new routing method in the MANET using the symbionts search algorithm. PLoS One 18(8):e0290091
45. Kanna SR, Sivakumar K, Lingaraj N (2021) Development of deer hunting linked earthworm optimization algorithm for solving large scale traveling salesman problem. Knowl-Based Syst 227:107199
46. Sajay KR, Babu SS, Vijayalakshmi Y (2019) Enhancing the security of cloud data using hybrid encryption algorithm. J Ambient Intel Human Comput 1–10

Ashutosh Kumar Rao is presently doing PhD From Amity School of Engineering & Technology, Amity University, Rajasthan and has completed his post graduation from Technocrats Institute of Technology, Bhopal Affitalted to Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal (MP) and graduation from Sachdeva Institute of Technology, mathura Affitalted to Uttar Pradesh Technical University,Lucknow (UP). His research area is Machine Learning, Internet of Things, I. He has more research papers in national and international journals and conferences. He has more than 14 years of experience in teaching. He is Member of ISTE, CSI. He has guided 02 M-Tech scholars.

Kapil Kumar Nagwanshi has received his PhD from the Chhatisgarh Swami Vivekanand Technical University Bhilai, India. He is currently working as an Associate Professor at SoS E&T Guru Ghasidas Vishwavidyalay (A Central University), Bilaspur, India. His primary domain of teaching and research includes the internet of things, digital image processing, cyber forensics, data science and engineering, AI, and computer networking. He has guided 15 MTech scholars and currently supervising six PhD scholars. He is a senior member of IEEE, YHAI, and a life member of CSI, IETE, and members of IAENG, IACSIT, and some other professional bodies. He is a reviewer of reputed journals such as IEEE Access, Imaging Science Journal, Journal of Real-Time Image Processing, and International Journal of Computer and Electrical Engineering.

Dr. Manoj Kumar Shukla is a Professor in Department of Computer Science & Engineering, Amity School of Engineering and Technology Amity University, Noida. Dr. Shukla has done his Ph.D from ISM-Dhanbad in the area of Computer Science. He is Member of ISTE, CSI, IETE, IANG, UACEE, WSEAS, IACSIT, ACM, etc. He has guided 22 M-Tech scholars and currently supervising six PhD scholars. He has been editorial board Member for a number of premier conferences and journals including American Journal of Database Theory and Application, International Journal of Scientific and Engineering Research, IJAIS, IJCIIS, IJCST, IJCST, IJETTCS, IJCSE, WASET, CSJEERS, IJACT, etc. He has been referee and reviewer for a number of premier conferences and journals including IEEE sponsored conferences, CSI Journal of Computing, International Journal of Emerging Trends & Technology in Computer Science, International Journal of Soft Computing and Engineering, Computer Science Journal Excellence in Education, Research & Service, and International Journal of Advancements in Computing Technology etc.