Wireless Personal Communications (2021) 119:2405–2429
https://doi.org/10.1007/s11277-021-08335-0

Particle-Water Wave Optimization for Secure Routing in Wireless Sensor Network Using Cluster Head Selection

Pradeep Sadashiv Khot[1] · **Udaykumar Naik**[2]

Accepted: 19 February 2021 / Published online: 12 March 2021

Abstract

Wireless sensor network (WSN) has some great advantages, such as flexible communication, low power consumption, and low cost. In view of the WSN clustering algorithm, the dynamic cluster head selection methods are put forward in order to solve the problem of the unreasonable cluster head selection that may lead to the overlapping coverage and unbalanced energy consumption in the cluster communication. Also, security is an important aspect in the WSN. Various security and routing protocols are developed for increasing the efficiency of packet transmission, but discovering the optimal path without degrading transmission reliability poses a challenging task in the sensor network. Hence, an effective and optimal secure routing algorithm named Particle-Water Wave Optimization (P-WWO) is developed in this research for routing the data packets in secure path. The proposed P-WWO algorithm is designed by integrating the Particle Swam Optimization (PSO) with the Water Wave Optimization (WWO). The secure route needed to broadcast the data packets is determined through the selection of Cluster Head using the PSO-based cellular automata with fitness measure. However, the fitness measure is computed by considering the factors, like energy, delay, trust, consistency factor, and maintainability factor. Accordingly, the routing path with the minimal distance and less delay is accepted as the optimal path using the proposed P-WWO based on the fitness value. The route maintenance process enables the proposed optimization to decide whether the packets can be transmitted in the selected route or need to re-route the data. Moreover, the proposed P-WWO obtained better performance using the metrics, such as energy balancing index, coverage, number of alive-nodes, and average energy left with the values of 0.9246 99.9%, 144, and 0.666 J, respectively.

Keywords Secure routing · Wireless sensor network (WSN) · Water wave optimization (WWO) · Cellular automata · Particle swarm optimization (PSO)

✉ Pradeep Sadashiv Khot
pradeepsadashivkhot@gmail.com

[1] Department of Computer Science and Engineering, Sanjay Ghodawat University, Kolhapur, Maharashtra 416118, India

[2] Department of Electronics and Communication Engineering, KLE Dr. M.S. Sheshgiri College of Engineering & Technology, Belagavi, Karnataka 590008, India

1 Introduction

WSN is the most commonly used communication device is the past decades, due to the rapid deployment and its strength. The sensor network can be dispersed in the environment at very short time in order to perform various activities. Various applications are considered from warfield network to the industrial activities. However, WSN can be effectively used for the private purposes [1]. WSN contains number of cooperating and geographically distributed sensor nodes. Accordingly, the requirement of intelligent, small sized and the inexpensive sensors are integrated into technological advances in the networking model to perform ubiquitous computing [2]. The modern user can access different service using their mobiles and through sensor networks. It is the collection of sensor nodes that are dispersed in different locations such that each node has its own transmitting and receiving operation in the fixed d or transmission range with fixed power. At each data communication, the node will loss certain quantity of energy and performs limited number of data transmission [1, 3, 4]. WSN is widely utilized in various research areas, like internet of vehicles, smart cities, and body area networks [2, 5, 6]. The availability of limited energy is the major problem of WSN. The sensor node gets the required amount of energy from the attached battery such that the battery is not rechargeable [2, 7]. However, the battery power specifies the lifespan of sensor node and hence the energy required by the sensor node can be used judiciously [2, 8].

WSN is considered as the promising technology to be widely used in various applications, like emergency response, health care monitoring, environmental monitoring, and battlefield monitoring. WSN is vulnerable to different threats, as it is usually distributed in the harsh or hostile environment [9, 10]. However, the sensor nodes can be captured by the attackers easily and acts as the malicious nodes and launch different types of attacks, like wormhole attacks, hello flooding stacks, Sybil attack, sinkhole, and the selective forwarding attack [9, 11, 12]. The presence of malicious nodes in the network will drop the packets such that essential data will not reach the sink node is the security is not provided in the network [9, 13, 14]. Secure routing is highly essential in the sensor network and it can be used to identify the occurrence of malicious node before forwarding the data packet to sink node. However, the malicious nodes can be identified based on the previous data transmission. However, the performance or routing can be increased by tracing, the number of previous communication, total number of data transmission involved, number of neighboring nodes, and successful transmission. Accordingly, the transmission analysis enables to find the exact route to achieve data transmission [1]. The data congestion is reduced by the congestion management methodologies for error free transmission [15]. Various routing protocols are developed in the sensor network to route the data to other nodes through secure communication [16].

Based on the organization of sensor network, data routing can be done using three techniques, namely, location based routing, flat based routing and hierarchical based routing. However, the position of the nodes is used for adapting the routing mechanism in location based routing, whereas the nodes are allocated with equivalent roles in flat based routing. Moreover, the nodes in the network tend to play various network activities in the hierarchical based routing. When the system parameters are controlled to define the energy level and the network conditions, the routing protocol can be specified as adaptive. Based on routing protocol, the routing techniques are classified into various types, like QoSbased, negotiation-based, multipath-based, query-based, and coherent-based routing methods. The reactive protocol identifies the path in advance before transmitting the data, whereas the reactive protocol finds the path in an on-demand basis [16]. Some of the major routing protocols used in the sensor network are ad hoc on-demand distance vector (AODV), destination sequence distance vector (DSDV) routing [17], dynamic source routing (DSR) [18], Traffic-aware Routing Protocol [19] and link quality source routing (LQSR) [16, 20]. In [21], a distributed algorithm named ambient trust sensor routing (ATSR) is designed for evaluating the reliability of node. To design the secure routing protocol, various routing techniques based on the trust of node are developed for finding the credibility of nodes [16]. Most of the routing protocols depend on the trust and the encryption mechanism in order to assurance security [22]. However, encryption helps the network to resist various categories of network attacks [9]. In literature, several optimization algorithms [23] are used for solving the routing problem. Real-time communication is necessary in many WSN applications. The real-time routing protocols have time constrain, which is important to consider when designing real-time routing in WSNs. WSN demands real-time forwarding, which means messages in the network are delivered according to their end-to-end deadlines [24]. WSNs are used in many real life applications, such as health monitoring, disaster management, defense security, and so on. For real life application, the homogeneous WSNs are not suitable because of the rechargeable battery support, very limited, and less energy resources are available that is why researchers tries to enhancing or increasing the lifetime of WSNs to prolong the network lifetime.

This research is focused to design a secure routing mechanism using the proposed P-WWO for routing the data packets in a secure path. However, the proposed P-WWO performs the routing process by involving four different phases, namely active node identification, Cluster Head (CH) selection, finding secure path, and secure data transmission. The sensor nodes that are simulated in the network are effectively identified such that the active nodes are used to perform the routing process. Once the active nodes are identified, the CH is selected from the nodes and the routing process is effectively achieved using the selected CH. However, the selection of CH is carried out by the newly designed PSO-based cellular automata. The routing path used to transmit the data securely is identified using the proposed P-WWO based on the fitness measure. The optimal selected is selected from the number of routes and the data transmission is progressed using the optimal path using double wave encryption model.

The major contribution of this research is explained as follows:

- *Proposed P-WWO* An effective and optimal secure routing mechanism named P-WWO is designed to perform the routing process in the sensor network. The proposed P-WWO determines the optimal route by selecting the CH using the PSO-based cellular automata. However, the secure routing path is effectively identified based on the minimum distance using the fitness measure. Accordingly, the routing path that consumes less delay and minimal distance is accepted as the best solution.

The research is organized as follows: Sect. 2 elaborates the existing routing protocols in WSN, and Sect. 3 describes the system model of WSN. Section 4 discussed the selection of CH, and Sect. 5 describes the proposed P-WWO for secure routing in the sensor network. Section 6 explains the result and discussion of proposed P-WWO algorithm and finally Sect. 7 concludes the paper.

2 Motivation

In this section, some of the conventional routing protocols to find the secure path is explained along with their advantages and drawbacks, which motivate the researchers to develop the P-WWO algorithm for routing the packets in secure path.

2.1 Literature Survey

Various conventional secure routing algorithms in WSN are surveyed in this section. Rathee et al. [2] developed an QoS aware energy balancing secure routing (QEBSR) algorithm for finding the optimal path in the network. This algorithm used some increased model to calculate the end-to-end delay and the trust factor. However, the end-to-end delay was measured based on the delay encountered in the node and delay in the path. It effectively increased the lifetime of network and reduced the delay. This algorithm used the weight vector for deciding the objective factor, but using the weight vector is nontrivial task. Sun et al. [25] modeled a secure routing protocol using ant colony optimization to minimize the energy usage in the sensor network. It used the pareto multi-objective strategy to solve the security issues in WSN. It effectively reduced the energy usage and enhanced the trust factor of the nodes. It increased the diversity of solution and obtained better performance in packet loss rate. It failed to consider the probability failure and reliability of network. Shi et al. [9] modeled an information aware secure routing protocol for finding the secure path in WSN. It specified the multi-hop communication between sink node and the sensor node. It computed the trust between the neighboring nodes in order to select the route. Moreover, it failed to consider the transmission delay. Selvi et al. [26] modeled an energy aware trust secure routing model for detecting the malicious users in WSN. Here, the intruders were detected based on the trust score and the optimal path was selected using the decision tree-based routing approach. It reduced the energy consumption, but failed to use the fuzzy constraints.

Stephen et al. [1] developed a sectional transmission analysis (STA) model for increasing the performance of reliability in routing. It performed the route discovery process and selected the route based on the reliable transmission support (RTS) measure. It increased the security and reliable transmission more effectively, but failed to find the malicious node. Kalidoss et al. [27] introduced a QoS aware trust based routing protocol for increasing the security in WSN. Here, the trust scores were used to select the genuine node in such a way that genuine node acts as the CH, which was used to find the malicious nodes. It achieved increased performance in terms of packet transmission, delay and throughput. However, it failed to handle the uncertainty. Mythili et al. [28] developed a Spatial and Energy Aware Trusted Dynamic Distance Source Routing (SEAT-DSR) algorithm to enhance the lifetime of network. Here, the energy level, data quality, and the spatial information were effectively equalized. It failed to achieve fast data communication. Beheshtiasl and Ghaffari [29] developed a secure and trust aware routing model to find the secure route based on fuzzy logic. This method increased the lifetime of network and reduced the energy consumption. It does not perform attack and intrusion detection strategy. Ahmed et al. [24] proposed a real-time routing in wireless sensor networks here a real-time with load distributed routing protocol (RTLD) that computes optimal forwarding choice based on packet reception rate (PRR), remaining power of sensor nodes and packet velocity that moving through one-hop. This paper presents the RTLD designed for real-time routing in WSNs. In general, the finding concludes that RTLD provides a good performance in term of delivery ratio, power consumption and packet overhead. This is primarily due to its forwarding strategy considers the problem of real-time routing protocols whereas it is not energy efficient [24].

Singh et al. [30] developed a fuzzy link cost estimation based adaptive tree algorithm for Routing Optimization. Here, fuzzy link cost estimation based Adaptive Tree routing algorithm (Fuzzy AT) has been introduced, which uses the concept of fuzzy logic based link cost estimation. The performance of this algorithm has been evaluated with traditional reinforcement learning based algorithms. The results shows that Fuzzy AT algorithm is most appropriate reinforcement learning based routing algorithm for ensuring energy efficient, reliable, and QoS aware routing in dynamically changing, asymmetric and unreliable wireless environment of WSNs. However, it failed to handle uncertainty. Rodrigues and John [31] developed a Joint trust approach for trust-aware routing in WSN. Here, WSN is considered as an infrastructure-less network, which contains inexpensive sensor nodes for monitoring the WSN network. Sensor nodes in the WSN are allocated randomly. Additionally, they developed a Chicken-Dragonfly (CHicDra) optimization algorithm for assisting secure communication by finding the optimal cluster heads (CHs) in the network. However, it fails to include parameters, like coverage, link quality, and several other related parameters.

Singh and Malhotra [32] developed a reinforcement learning- based real time search algorithm for routing optimization in WSN using fuzzy link cost estimation. This paper uses the concept of fuzzy logic-based link cost estimation depending upon physical layer and Medium Access Control (MAC) layer parameters, such as residual energy, packet drop rate, and Received Signal Strength Indicators (RSSI) The performance of this algorithm is evaluated along with traditional RL-based algorithms, such as real time search, adaptive tree, ant-based flooded forward routing and constrained flooding algorithms. Moreover, it fails to consider the link quality. Pattnaik and Sahu [33] developed assimilation of fuzzy clustering approach and EHO-Greedy algorithm for efficient routing in WSN. The simulation results demonstrate that the suggested system delivers better performance than other existing algorithms. In addition, to focus on the reduction in high frequency of re-clustering and distribution of CHs, the areas, such as determining the best way with maximum energy for intercluster multihop communication, employing multiple BSs, to reduce the burden on CHs, which closer to a single BS may be considered to bring further improvement.

Vinitha et al. [34] proposed an energy-efficient multihop routing in WSN using the hybrid optimization algorithm. The research established an effective routing protocol using the cat and salp swarm optimization (C-SSA). The selection of the optimal hops to progress the routing in WSN is based on the hybrid optimization, named as C-SSA optimization, which is the integration of the cat swarm optimization (CSO) and salp swarm optimization (SSA). The C-SSA exhibits better convergence, and operates based on the constraints, such as energy, delay, intercluster distance, intracluster distance, link lifetime, delay, and distance. The intrusion and attack detection are failed to perform in this method. Elhoseny et al. [35] developed swarm intelligence–based energy efficient clustering with multihop routing protocol for sustainable WSNs. The Grey Wolf Optimization (GWO) algorithm–based routing process takes place to select the optimal paths in the network. The presented approach incorporates the benefits of both the clustering and routing processes, which leads to maximum energy efficiency and network lifetime. It fails to perform fast data communication.

2.2 Challenges

Some of the drawbacks faced by the conventional routing protocols are discussed as follows:

- The error prone nature of network channels and the resource constraint of sensor nodes, like limited energy, less processing capability, short communication range, and low bandwidth poses number of challenges in the WSN applications [2].
- Due to various network attacks, routing strategy in WSN can get damage and causes irreparable loss, which is a challenging issue in the sensor network [25].
- Routing the major issue in sensor network, and it tends to make error due to the reasons, like continuous node failure, changing network conditions, less battery power, and the behavior of malicious nodes [26].
- To deploy the sensor nodes under various situations, such as disaster area, remote harsh and hostile field result a challenging task [28]. Due to the presence of attackers, designing the secure routing algorithm result a challenging issue in WSN [27].
- Security is the major issue in WSN, as unreliable channels and unattended operation render the sensor nodes vulnerable to attack. Moreover, to establish the routing path that maximizes the network lifetime is the key challenge in WSN.

3 System model

WSN is the wireless network that contains number of distributed services for monitoring the physical and the environmental changes, like vibration, temperature, pollutants, and sound using the sensor nodes. WSN is the collection of sensor nodes that enables to send and receive the information through wireless path. The places where the sensors nodes are to be located are engineered and pre-determined, as it can be randomly deployed in terrain or the disaster management system. However, the key feature of WSN is the facility of self-organizing and the cooperative effort of the nodes. Accordingly, the nose uses the processing capability for carrying the information and broadcast only the required data to recipient. The sensor node needs less computing power and is usually non-replaceable. The nodes in the sensor network hold various order of magnitude, as it is randomly and densely deployed in the network in such a way that the topology of WSN frequently varies. However, the sensor nodes are adopted to perform actuator control, event detection, and location sensing. The nodes the sensor network have the facility to sense and process the information and also it receive the data from different nodes. Accordingly, each node in this network is accountable for exchanging the data with neighboring nodes. The nodes in the sensor network contains three different subsystems, namely communication, processing and sensor subsystem. Figure 1 portrays the system model of WSN.

3.1 Energy Model

The network lifetime is increased using the energy of nodes, as sensor nodes use battery power [36]. The energy model of WSN performs our modes of operations, namely idle, transmitting, sleeping, and receiving mode. The node that consumes maximal energy is selected for discovering the route. However, the routing path with minimum energy is used

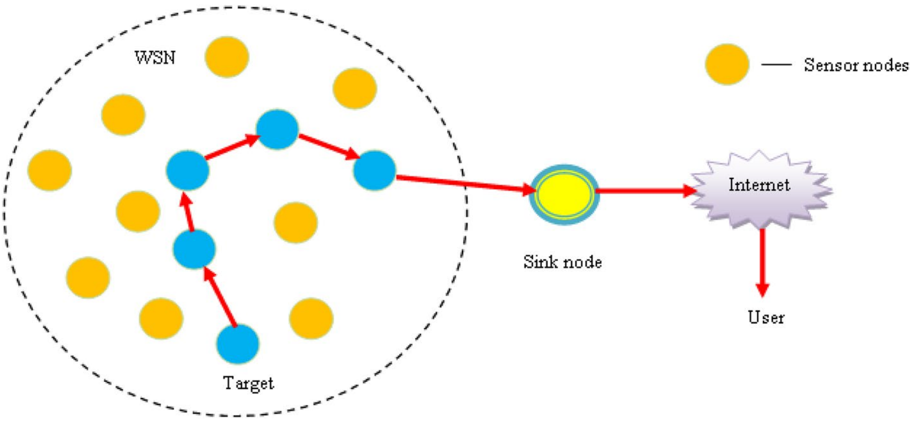


Fig. 1 System model of WSN

for data transmission such that this path is accumulated in routing table. The energy value of each node is calculated with respect to time interval. Accordingly, the node that consumes the energy is specified as,

$$P^a(t) = A^a_g * P^a_g + A^a_h * P^a_h \tag{1}$$

where $P^a(t)$ specifies the energy consumed by ath node at time t, A^a_g signifies the number of data packets send by ath node, A^a_h represents the number of data packets received by ath node, P^a_h represents the energy needed to receive the packets, and P^a_g specifies the energy needed to send the packets. However, the term P^a_g and P^a_h is calculated as,

$$P^a_g = A * \tau \tag{2}$$

$$P^a_h = \beta * \kappa \tag{3}$$

where A specifies the time required to send the packets, τ represents the power required for sending data packets,β signifies the time needed to receive the packets, and κ indicates the power needed to receive the packets. Therefore, the residual energy is computed as,

$$P_\lambda = PP - P^a(t) \tag{4}$$

where PP signifies initial energy of sensor nodes. For each node, P_λ is computed and the energy of the nodes is verified with threshold value such that the nodes with less energy is used for data transmission.

3.2 Link Lifetime Model

Due to the dynamic topology changes, it is required to calculate the lifetime of the path in WSN [36]. At each hop, the lifetime of the link is calculated during path traversal of route request. Let us consider the nodes as a and b lies within the transmission range. The link lifetime equation is expressed as,

$$L = \frac{-\left(pq + xy + \sqrt{\left(p^2 + x^2\right)l^2 - (py - xq)^2}\right)}{\left(p^2 + x^2\right)} \tag{5}$$

Here, $p = S_a \cos\,\theta_a - S_b\,\cos\,\theta_b$

$$q = u_a - u_b$$
$$x = S_a \sin\,\theta_a - S_b\,\sin\,\theta_b$$
$$y = v_a - v_b$$

where $\left(u_a, v_a\right)$ denotes the coordinate of sensor node a, $\left(u_b, v_b\right)$ specifies the coordinate of node b, S_a specifies the mobility speed of node a, S_b indicates the mobility of speed of node b, θ_a represents the direction of motion of node a, θ_b specifies the direction of motion of node b, and l represents the transmission range.

3.3 Mobility Model

The movement of nodes is specified with the mobility model [37]. However, the mobility patterns of WSN evaluate the performance of routing process in data transmission. However, the mobility model imitates the nodes movements in real-time applications. Accordingly, random mobility scheme is the optimal way of analyzing the performance in sensor network due to their simplicity and wide availability. Let us consider two sensor nodes as a and b with the initial position as $\left(r_1, s_1\right)$ and $\left(r_2, s_2\right)$, respectively. However, the nodes a and b moves in the network with varying velocity at certain direction using angle θ_1 and θ_2 with respect to x-axis. Here, the node a move with the distance d_1 and the node b move with the distance d_2 at time interval t, respectively. After performing the mobility process, the nodes a and b move to the new location at tth time. Therefore, the distance among the nodes $a\left(r_1, s_1\right)$ and $b\left(r_2, s_2\right)$ is specified as,

$$\alpha_{(a,b)} = \sqrt{\left|r_1 - r_2\right|^2 + \left|s_1 - s_2\right|^2} \tag{6}$$

where $\alpha_{(a,b)}$ specifies the distance between the nodes $a\left(r_1, s_1\right)$ and $b\left(r_2, s_2\right)$.

4 CH Selection Using PSO-Based Cellular Automata

Once, the active nodes are selected, it is required to find the CH for each active node set, as the data transmission is progress only the CH nodes. The CH is selected based on minimum distance between the nodes using the newly designed CH selection mechanism named PSO-based cellular automata. The PSO-based cellular automaton is developed by integrating the PSO algorithm with the cellular automata approach. PSO [38] is the swarm intelligence paradigm that mimics the behavior of swarm for guiding the particles in search of global optimum solution. In PSO, the particle swarm is specified as the potential solution such that each particle j is specified with two vectors, namely velocity and position vector. The position vectors is represented as $Y_j = \left[Y_j^1, Y_j^2, \ldots, Y_j^N\right]$, and the velocity vector is specified as $J_j = \left[J_j^1, J_j^2, .., J_j^N\right]$. Here, N indicates the dimension of solution space. However, the position and the velocity of each particle j are initialized by the random vectors in the corresponding ranges. During evolutionary process, the location and the velocity of particle j at dimension m is updated as,

$$J_j^m = \alpha . J_j^m + w_1 z_1^m \left(R_j^{best(m)} - Y_j^m \right) + w_2 z_2^m \left(T_j^{best(m)} - Y_j^m \right) \tag{7}$$

$$Y_j^{m+1} = Y_j^m + J_j^m \tag{8}$$

where α represents the inertia weight, w_1, and w_2 represents the acceleration coefficients, and z_1 and z_2 are the uniformly distributed random number that lies in the range between 0 and 1, respectively. R_j^{best} represents the position of swarm with best fitness, and T_j^{best} denotes the best neighborhood position of particle j, respectively.

Learning automata (LA) [39] is an approach that receives the input from the sensor nodes and performs some operations to generate the output. It encompasses the ability to find out the features from network environment and find the suitable action among the set of pre-defined actions in order to execute the necessary operation. Here, the threshold value called as cut-off value is used for protecting the nodes energy at various levels. However, the upper threshold value is specified as $\left(\omega^{cutoff}\right)$ that lies in the range of $\left[0, \partial^2\right]$, here ∂ represents the cell. However, the cut-off value of the nodes present in the CH contains energy remained and the location of the nodes. However, the success or the failure of cut-off is evaluated based on the probability value, which is calculated using the angular position and the energy level. Accordingly, the probability of cur-off is specified as,

$$G = E\mu^c + \sum_{k=1}^{E} k\mu^I \tag{9}$$

$$G = E \sum_{i=0}^{n} \left(1 - H^i\right) + H^i \sum_{k=1}^{i-1} \left(1 - H^k\right) k \tag{10}$$

where H^i represents blocking probability, μ^c denotes success probability, and μ^I specifies failure probability. Based on the automaton criteria, the action vector probability gets updated. With the cellular automata, the participation degree of each node in CH is calculated by considering the number of transmitted packets. However, the PSO-based cellular automata select the CH to perform secure routing process in WSN. However, the CH that is selected using the PSO-based cellular automata is represented as,

$$\eta = \sum_{v=1}^{10} K \tag{11}$$

Here, K denotes CH. Algorithm 1 represents the pseudo code of PSO-based cellular automata for CH selection.

Algorithm 1. Pseudo code of PSO-based cellular automata

Sl. No	Pseudo code of PSO-based cellular automata for CH selection
1	Initialize the energy level of nodes
2	Select CH with minimum distance using PSO
3	Assign the automata to CH
4	$for(c=1;c\leq n;c++)$
5	$for(\rho=1;\rho\leq \max;\rho++)$
6	Compute participation degree
7	Select the node with highest participation degree
8	Calculate the success or failure probability
9	if
10	LA receives the award
11	then
12	Increment the participation degree
13	else
14	Decrement the participation degree
15	Compute cumulative probability using Eq. (10)
16	Apply the first level of cut-off to the selected nodes
17	Mark the CH node
18	Perform the second level of cut-off based on the cut-off values.
19	End
20	end

5 Proposed P-WWO Algorithm for Secure Routing in WSN

In WSN, the sensor node broadcast the data to the destination through secure route with minimum distance and maximum lifetime. To route the data in a secure path and to increase the lifetime span of link poses a great challenge in WSN. To solve these issues, secure routing protocol named P-WWO is developed in this research for selecting best routing path to achieve data transmission in wireless network. At first, the active nodes in the network are selected based on minimum distance. After selecting the active nodes, the next step is to select the CH using PSO-based cellular automata. The CH is passed to the routing stage, where the routing process is carried out using the proposed P-WWO, which is designed using PSO [38], and WWO [40], respectively. However, the optimal path is effectively selected based on the parameters, like energy, delay, trust, maintainability factor, and consistency factor, respectively. However, the proposed P-WWO find the optimal path using the fitness function. Finally, the data transmission is securely carried out using double wave encryption model. Figure 2 portrays the block diagram of the proposed P-WWO routing protocol.

5.1 Solution Encoding

It is the representation of solution vector used to determine the optimal CH. With the solution vector, the optimal route can be effectively selected in order to achieve data transmission more efficiently. The secure path is estimated using the fitness function, which considers some optimization parameters and enable the proposed P-WWO routing protocol to find the best solution.

5.2 Fitness Function

The fitness function is calculated using the factors, like energy, delay, trust [41] [42], maintainability factor [43], and consistency factor. However, the function with the maximum fitness valued is declared as the best solution, which is evaluated by considering the minimal distance. Accordingly, the fitness function is expressed as,

$$F = P + (1 - \gamma) + G + B + MF \tag{12}$$

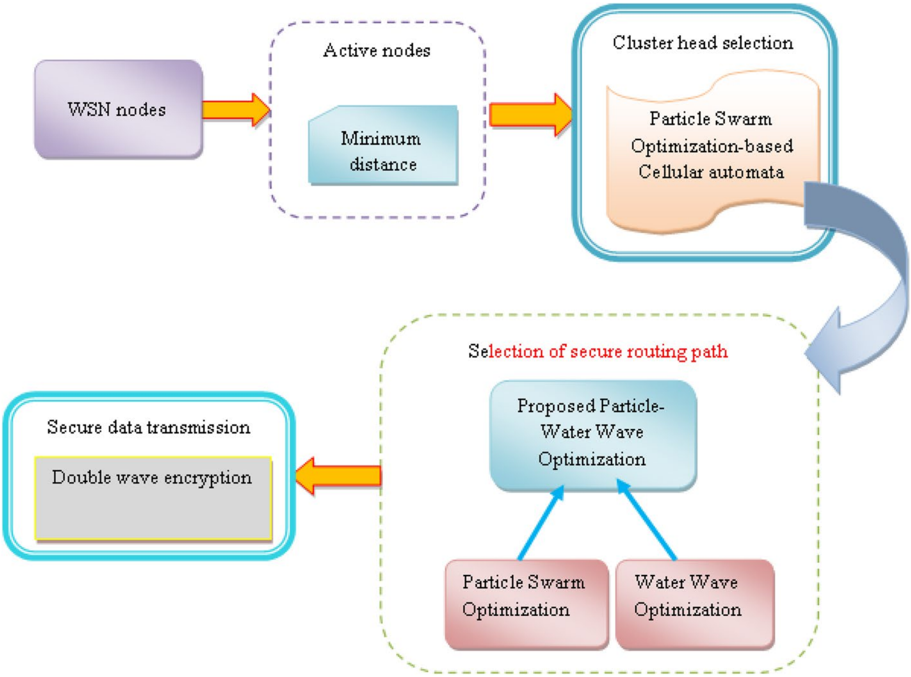

WSN nodes
Active nodes
Minimum distance
Cluster head selection
Particle Swarm Optimization-based Cellular automata
Selection of secure routing path
Proposed Particle-Water Wave Optimization
Particle Swarm Optimization
Water Wave Optimization
Secure data transmission
Double wave encryption

Fig. 2 Block diagram of the proposed P-WWO routing protocol

where P represents energy, γ indicates delay, G specifies the consistency factor, MF represents the maintainability factor, and B is the trust.

$$P = \sum_{e=1}^{Q} \left(\frac{P_j^j - P_e^j(t)}{O} \right) \tag{13}$$

where j represents jth CH, Q specifies the number of CH, and O signifies the number of rounds.

$$\gamma = \frac{\max\limits_{e=1}^{Q} \left(V^e\right)}{ZZ} \tag{14}$$

where V^e indicates the cluster member of eth CH, and ZZ specifies the total number of nodes.

$$G = \sum_{\substack{i=1 \\ j=i+1}}^{Q-1} \left(\frac{M_{i,j}(t)}{M_{i,j}(t) + \vartheta M_{i,j}(t)} \right) \tag{15}$$

where $\vartheta M_{i,j}(t)$ indicates the inconsistent packet, and $M_{i,j}(t)$ indicates the number of nodes.

$$B = \sum_{\substack{i=1 \\ j=i+1}}^{Q-1} \left[(1 - \chi) * \sigma_{i,j}(t) * G * PP_{i,j}(t) + \varepsilon * M_{i,j}(t-1) + B_1 + B_2 \right] \tag{16}$$

where χ denotes a constant factor that lies in the interval of [0,1], $\sigma_{i,j}(t)$ specifies the sending rate, and $pp_{i,j}(t)$ indicates packet loss rate.

$$B_1 = CN(a, b) \tag{17}$$

where B_1 denotes direct trust, and CN indicates the satisfaction of nodes

$$B_2 = \left\{ \begin{matrix} \dfrac{\sum_{U \in A_1 - \{A_r\}} FC(a, sn) \times B_1}{\sum_{U \in A_1 - \{A_r\}} FC(a, sn)} & , \mathit{if} \left| A_1 - \{A_r\} > 0 \right| \\ 0 & \mathit{if} \left| A_1 - \{A_r\} = 0 \right| \end{matrix} \right\} \tag{18}$$

where B_2 specifies indirect trust, U indicates the set of nodes interacted with node b, and FC represents feedback credibility.

$$MF = e^{-\sigma v} \tag{19}$$

where $\sigma = \frac{1}{L}$.

Here, σ denotes the average link failure rate, MF denotes the maintainability factor, v represents the time during the link at work L signifies the link lifetime of network.

5.3 Secure Routing Using Proposed P-WWO Algorithm

The proposed P-WWO algorithm is developed by integrating the PSO [38], with the WWO [40], respectively. The WWO takes the inspiration of shallow water model and solve the optimization problem more effectively in search space. The solution space of WWO is analogous to seabed area such that the fitness is computed based on seabed depth. WWO maintains the population of solution in such a way that each of the solution is analogous to the wave. The WWO involves three different operations on wave, like refraction, breaking, and propagation, respectively. The algorithmic steps involved in the proposed P-WWO algorithm are explained as follows:

(1) *Population initialization* Let us consider the population V of n waves in the solution space and is represented as,

$$V = \left\{ Y_1, Y_2, ...Y_j, ...Y_n \right\} \tag{20}$$

(2) *Propagation operation* At each iteration the waves propagated exactly at once. However, the propagation operator generates the new wave by shifting the dimension j of original wave Y as,

$$Y_j^{m+1} = Y_j^m + rand(-1, 1).\eta.D_j \tag{21}$$

where *rand* represents the random number that lies in the range of $[-1, 1]$, and D_j represents the length.

(3) *Breaking operation* The breaking operation can be performed on the wave Y for finding the best solution and performs the local search process for simulating the wave breaking. However, the breaking operation of WWO is expressed as,

$$Y_j^{m+1} = Y_j^m + X(0, 1).\eta.D_j \tag{22}$$

where η denotes the breaking coefficient. In PSO, the position and velocity of particle j on dimension m is expressed as,

$$Y_j^{m+1} = Y_j^m + J_j^{m+1} \tag{23}$$

$$Y_j^{m+1} = Y_j^m + \alpha.J_j^m + w_1 z_1 \left(R_j^m - Y_j^m \right) + w_2 z_2 \left(T^m - Y_j^m \right) \tag{24}$$

$$Y_j^{m+1} = Y_j^m + \alpha.J_j^m + w_1 z_1 R_j^m - w_1 z_1 Y_j^m + w_2 z_2 T^m - w_2 z_2 Y_j^m \tag{25}$$

$$Y_j^{m+1} = Y_j^m \left(1 - w_1 z_1 - w_2 z_2 \right) + \alpha.J_j^m + w_1 z_1 R_j^m + w_2 z_2 T^m \tag{26}$$

$$Y_j^m \left(1 - w_1 z_1 - w_2 z_2 \right) = Y_j^{m+1} - \alpha.J_j^m - w_1 z_1 R_j^m - w_2 z_2 T^m \tag{27}$$

$$Y_j^m = \frac{Y_j^{m+1} - \alpha.J_j^m - w_1 z_1 R_j^m - w_2 z_2 T^m}{\left(1 - w_1 z_1 - w_2 z_2 \right)} \tag{28}$$

By substituting the Eq. (28) in Eq. (22), the resultant equation is specified as,

$$Y_j^{m+1} = \frac{Y_j^{m+1} - \alpha.J_j^m - w_1 z_1 R_j^m - w_2 z_2 T^m}{\left(1 - w_1 z_1 - w_2 z_2\right)} + X(0,1).\eta.D_j \tag{29}$$

$$Y_j^{m+1} = \frac{Y_j^{m+1}}{1 - w_1 z_1 - w_2 z_2} - \frac{\alpha.J_j^m + w_1 z_1 R_j^m + w_2 z_2 T^m}{\left(1 - w_1 z_1 - w_2 z_2\right)} + X(0,1).\eta.D_j \tag{30}$$

$$Y_j^{m+1} - \frac{Y_j^{m+1}}{1 - w_1 z_1 - w_2 z_2} = X(0,1).\eta.D_j - \frac{\alpha.J_j^m + w_1 z_1 R_j^m + w_2 z_2 T^m}{\left(1 - w_1 z_1 - w_2 z_2\right)} \tag{31}$$

$$Y_j^{m+1}\left(\frac{1 - w_1 z_1 - w_2 z_2 - 1}{1 - w_1 z_1 - w_2 z_2}\right) = X(0,1).\eta.D_j - \frac{\alpha.J_j^m + w_1 z_1 R_j^m + w_2 z_2 T^m}{\left(1 - w_1 z_1 - w_2 z_2\right)} \tag{32}$$

$$Y_j^{m+1}\left(\frac{-\left(w_1 z_1 + w_2 z_2\right)}{1 - w_1 z_1 - w_2 z_2}\right) = -\left(\frac{\alpha.J_j^m + w_1 z_1 R_j^m + w_2 z_2 T^m}{\left(1 - w_1 z_1 - w_2 z_2\right)} - X(0,1).\eta.D_j\right) \tag{33}$$

$$Y_j^{m+1} = \frac{1 - w_1 z_1 - w_2 z_2}{w_1 z_1 + w_2 z_2}\left[\frac{\alpha.J_j^m + w_1 z_1 R_j^m + w_2 z_2 T^m}{1 - w_1 z_1 - w_2 z_2} - X(0,1).\eta.D_j\right] \tag{34}$$

where η specifies the breaking coefficient, D_j represents the length of search space, w_1, and w_2 represents the learning rates, r_1 and r_2 are the random numbers that lies in the range of [0, 1], R_j^m represents the personal best, T^m denotes the global best, and α represents the inertia weight, respectively.

(4) *Refraction operation* The direction of waves will be deflected when it is not perpendicular to isobath. The position of wave after performing the refraction process is represented as,

$$Y_j^{m+1} = X\left(\frac{Y^*(m) + Y(m)}{2}, \frac{|Y^*(m) - Y(m)|}{2}\right) \tag{35}$$

After performing the refraction process, the wavelength is specified as,

$$\eta' = \eta.\frac{F(Y)}{F(Y*)} \tag{36}$$

where Y^* denotes the best solution, $X()$ represents the Gaussian random number with the mean and standard deviation.

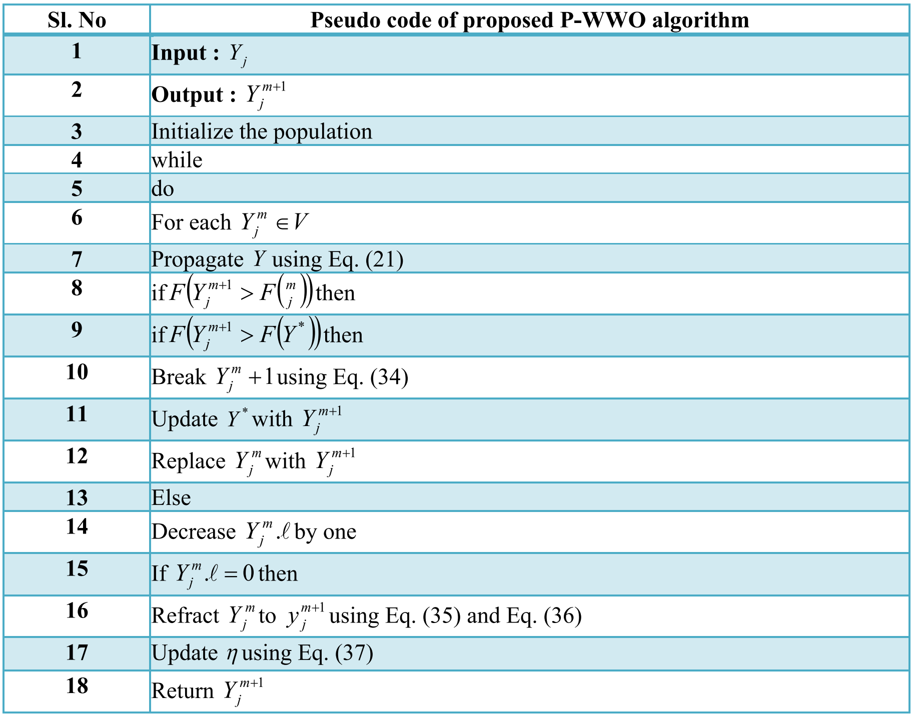
(v) *Update wavelength* After each iteration, it is required to update the wavelength using the below equation as,

$$\eta = \eta.\,\mathfrak{R}^{-\left(F\left(Y_j\right)-F_{\min}+f\right)/\left(F_{\min}-F_{\min}+f\right)} \tag{37}$$

where $F_{\max}$ and $F_{\min}$ represents the maximum and minimum values, $\mathfrak{R}$ denotes the wavelength reduction coefficient, and f represents the small positive integer, respectively.

(vi) *T1ermination* The above steps are repeated until the best path is obtained for routing the data. Algorithm 2 portrays the pseudo code of proposed P-WWO algorithm for secure routing.

Algorithm 2. Pseudo code of proposed P-WWO for secure routing



Sl. No	Pseudo code of proposed P-WWO algorithm
1	**Input :** Y_j
2	**Output :** Y_j^{m+1}
3	Initialize the population
4	while
5	do
6	For each $Y_j^m \in V$
7	Propagate Y using Eq. (21)
8	if $F\left(Y_j^{m+1} > F\left({}_j^m\right)\right)$ then
9	if $F\left(Y_j^{m+1} > F\left(Y^*\right)\right)$ then
10	Break $Y_j^m + 1$ using Eq. (34)
11	Update Y^* with Y_j^{m+1}
12	Replace Y_j^m with Y_j^{m+1}
13	Else
14	Decrease $Y_j^m.\ell$ by one
15	If $Y_j^m.\ell = 0$ then
16	Refract Y_j^m to y_j^{m+1} using Eq. (35) and Eq. (36)
17	Update η using Eq. (37)
18	Return Y_j^{m+1}

By integrating the parametric features from PSO and WWO, secure routing can be effectively achieved with faster convergence speed. The run time of the proposed algorithmic parameters increases the routing performance by finding the optimal path. The fitness function is used to find the best path with minimum distance and delay.

5.4 Secure Data Transmission Using Double Wave Encryption

Once the optimal route is identified between source and destination end, the data transmission can be progressed in a secure manner using double wave encryption. Here, the encryption process is carried out in a two-way encryption model using the secret key. The steps involved in the two-way encryption are described as follows:

(1) Generate the matrix F, which contains the observed data.
(2) Encrypt the matrix F.
(3) Receive the ceiling value for each word in the matrix.
(4) Convert the ceiling value into binary number.
(5) Store the final result in the form of decimal value in a new matrix Z.

5.5 Route Maintenance

Once, the secure route is identified using the proposed P-WWO then it is required to find the lifespan of nodes. While forwarding the data packets to nearest node, it is significant for the node to detect whether its path to the next hop is broken. If the node determines that the path is broken then it is required to perform route maintenance process by computing the lifespan of the link. However, the link life of the node is computed using Eq. (5). Moreover, the maintainability factor of the path is computed using Eq. (19). However, the maintainability factor MF is compared with the threshold value $\wp$. When $MF > \wp$, re-routing process can be achieved using the proposed P-WWO and if $MF < \wp$, the node broadcast the data with the already selected route.

6 Results and Discussion

This section elaborates the results and discussion of proposed P-WWO algorithm for routing the data in WSN.

6.1 Experimental Setup

The implementation of proposed P-WWO is carried out in PYTHON tool with windows 10OS, 4 GB Ram, and intel I3 processor.

6.2 Evaluation Metrics

The performance revealed by the proposed P-WWO algorithm is analyzed by considering the number of alive-nodes, coverage, energy balancing index, and average energy left based on number of rounds.

- *Alive nodes* This is the nodes that comprise the facility to acquire new routing path in the network.
- *Coverage* It is the measure used for finding the fixed number of targets.
- *Energy balancing index* It is the available energy performance in the sensor network and is specified as,

$$\mathrm{X} = \frac{\left(\sum_{v-1}^{Z} \varpi_v\right)^2}{Z.\ \sum_{v-1}^{Z} \varpi_v^2} \tag{29}$$

where Z specifies the number of nodes, and ϖ_v denotes the consumed energy of vth node.

- *Average energy left* It is the remaining energy left by sensor nodes in the network

6.3 Comparative Methods

The performance improvement is analyzed using the existing approaches, like CA-based malware propagation model [44], cellular automata (CA)-based node scheduling algorithm [45], and Dynamic Irregular Cellular Multiple Learning Automata (DICMLA) [46].

6.4 Comparative Analysis

This section explains the comparative analysis of proposed P-WWO routing algorithm with respect to the number of rounds.

a. Analysis using 50 nodes

This section describes the analysis made using 50 nodes with respect to number of rounds. Figure 3a portrays the analysis of number of alive nodes. For 500 rounds, the proposed P-WWO has the alive-nodes as 49. The nodes alive in the existing CA-based node scheduling are 49, CA-based malware propagation is 49, DICMLA is 49, and P-SMO is 49, while. For 1500 rounds, the number of nodes alive for the existing CA-based node scheduling is 22, CA-based malware propagation is 6, DICMLA is 2, and P-SMO is 41, while the proposed P-WWO has the number of alive-nodes as 47.

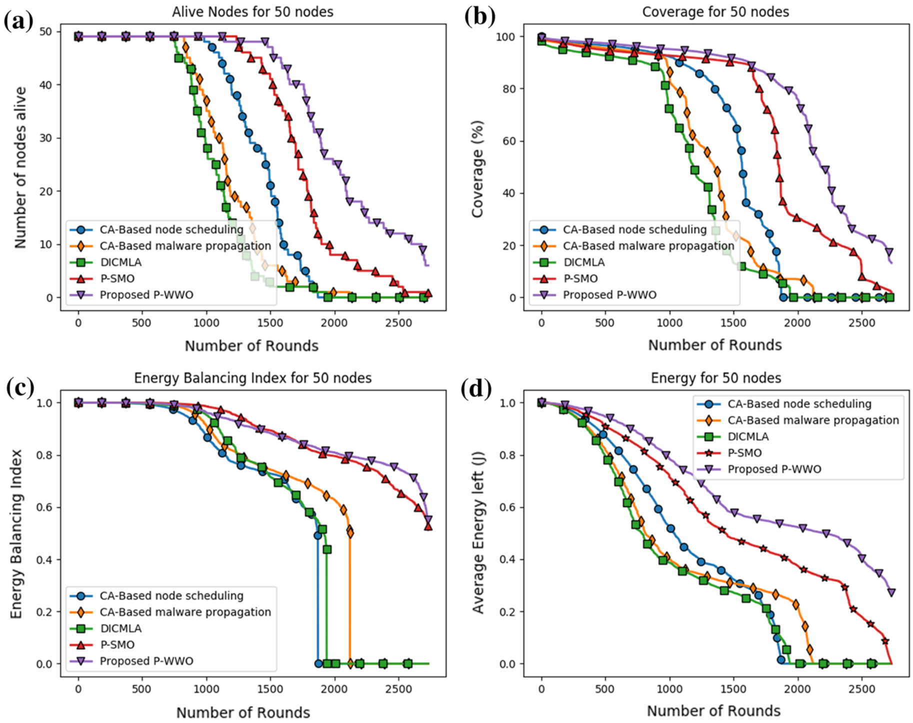


Fig. 3 Comparative analysis based on 50 nodes, **a** alive nodes, **b** coverage, **c** energy balancing index, **d** average energy left

Figure 3b depicts the analysis of coverage of proposed P-WWO routing algorithm. For 500 rounds, the proposed P-WWO has the coverage of 97.257%, which is better when compared to the other existing methods, and the coverage of the existing CA-based node scheduling is 96.43%, CA-based malware propagation is 95.3475%, DICMLA is 92.535%, and P-SMO is 94.6275%. The performance of the proposed method 0.8% higher than the CA-based node scheduling, 1.9% improved than CA-based malware propagation, 4.8% higher than DICMLA, and 2.7% than P-SMO. For 1500 rounds, the coverage of the existing CA-based node scheduling is 68.355%, CA-based malware propagation is 24.0275%, DICMLA is 13.1825%, and P-SMO is 90.1575%, while the proposed P-WWO has the coverage of 91.7025%.

Figure 3c represents the analysis based on energy balancing index. For 500 rounds, the energy balancing index of the existing CA-based node scheduling is 0.9952, CA-based malware propagation is 0.9994, DICMLA is 0.9969, and P-SMO is 0.9996, while the proposed P-WWO has the energy balancing index of 0.9985. For 1500 rounds, the energy balancing index of the existing CA-based node scheduling is 0.7281, CA-based malware propagation is 0.7436, DICMLA is 0.7161, and P-SMO is 0.8936, while the proposed P-WWO has the energy balancing index of 0.8830.

Figure 3d depicts the analysis based on average energy left. For 500 rounds, the average energy left by the existing CA-based node scheduling is 0.8713 J, CA-based malware propagation is 0.8187 J, DICMLA is 0.7934 J, and P-SMO is 0.9097 J, while the average energy left by the proposed P-WWO is 0.9461 J. For 1500 rounds, the average energy left by the existing CA-based node scheduling is 0.3232 J, CA-based malware propagation is 0.3075 J, DICMLA is 0.2714 J, and P-SMO is 0.4792 J, while the average energy left by the proposed P-WWO is 0.5778 J.

b. Analysis using 100 nodesAnalysis using 100 nodes

This section describes the analysis made using 100 nodes with respect to number of rounds. Figure 4a portrays the analysis of number of alive nodes based on the rounds. For 500 rounds, the nodes alive in CA-based node scheduling are 100, CA-based malware propagation is 100, DICMLA is 100, and P-SMO is 100, while the proposed P-WWO has the alive-nodes of 100. For 2000 rounds, the number of nodes alive for the existing CA-based node scheduling is 14, CA-based malware propagation is 4, DICMLA is 8, and P-SMO is 48, while the proposed P-WWO has the number of alive-nodes as 64.

Figure 4b depicts the analysis based on coverage. For 300 rounds, the coverage of the existing CA-based node scheduling is 99.8625%, CA-based malware propagation is 99.89%, DICMLA is 99.855%, and P-SMO is 99.8875%, while the proposed P-WWO has the coverage of 99.88%. For 1500 rounds, the coverage of the existing CA-based node scheduling is 79.6375%, CA-based malware propagation is 62.57%, DICMLA is 55.8775%, and P-SMO is 98.025%, while the proposed P-WWO has the coverage of 98.555%.

Figure 4c represents the analysis based on energy balancing index. For 500 rounds, the energy balancing index of the existing CA-based node scheduling is 0.9989, CA-based malware propagation is 0.9939, DICMLA is 0.9996, and P-SMO is 0.9991, while the proposed P-WWO has the energy balancing index of 0.9984. For 1500 rounds, the energy balancing index of the existing CA-based node scheduling is 0.8124, CA-based malware propagation is 0.7383, DICMLA is 0.7553, and P-SMO is 0.8737, while the proposed P-WWO has the energy balancing index of 0.8826.

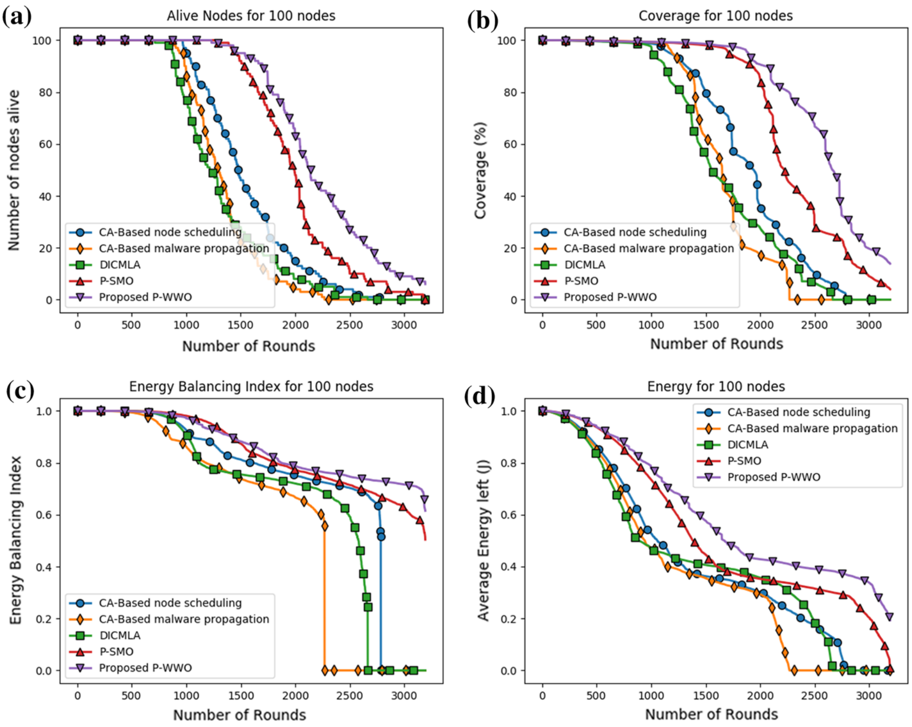


Fig. 4 Comparative analysis with 100 nodes, **a** alive nodes, **b** coverage, **c** energy balancing index, **d** average energy left

Figure 4d depicts the analysis based on average energy left. For 500 rounds, the average energy left by the existing CA-based node scheduling is 0.8655 J, CA-based malware propagation is 0.8504 J, DICMLA is 0.8321 J, and P-SMO is 0.9374 J, while the average energy left by the proposed P-WWO is 0.9379 J. For 1500 rounds, the average energy left by the existing CA-based node scheduling is 0.3631 J, CA-based malware propagation is 0.3552 J, DICMLA is 0.4060 J, and P-SMO is 0.4462 J, while the average energy left by the proposed P-WWO is 0.5769 J.

c. Analysis using 150 nodes

This section describes the analysis made using 150 nodes based on the rounds. Figure 5a portrays the analysis based on number of alive nodes. For 1000 rounds, nodes alive in the existing CA-based node scheduling are 103, CA-based malware propagation is 135, DICMLA is 90, and P-SMO is 144, while the proposed P-WWO has the alive-nodes of 144. For 2000 rounds, the number of nodes alive for the existing CA-based node scheduling is 5, CA-based malware propagation is 14, DICMLA is 4, and P-SMO is 64, while the proposed P-WWO has the number of alive-nodes as 128.

Figure 5b depicts the analysis based on coverage. For 500 rounds, the coverage of the existing CA-based node scheduling is 99.96%, CA-based malware propagation is 99.995%, DICMLA is 99.995%, and P-SMO is 100%, while the proposed P-WWO has the coverage of 100%. For 1700 rounds, the coverage of the existing CA-based node scheduling is

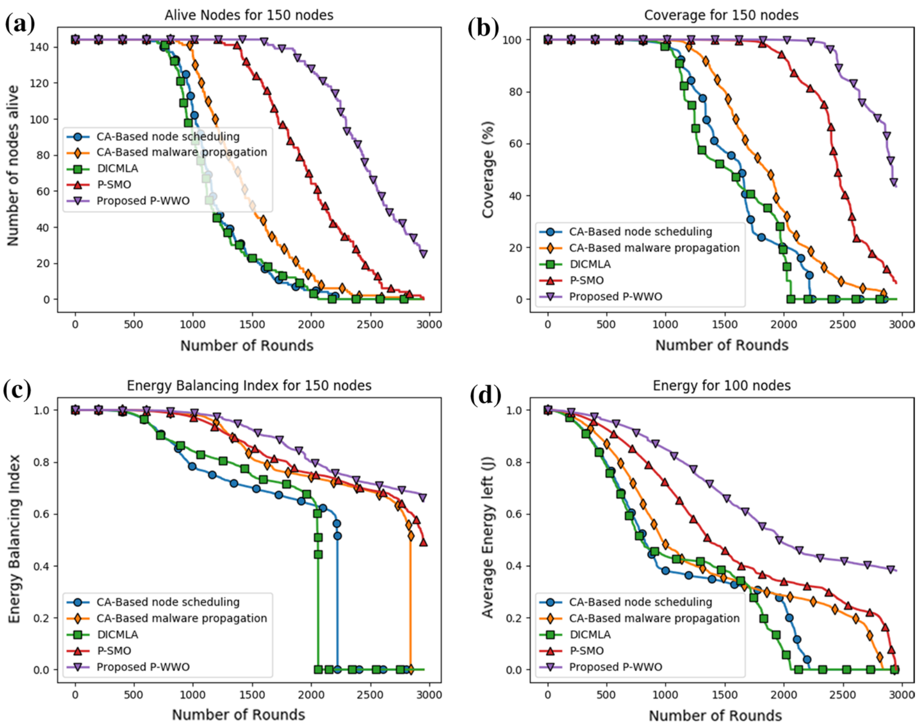


Fig. 5 Comparative analysis with 150 nodes, **a** alive nodes, **b** coverage, **c** energy balancing index, **d** average energy left

33.452%, CA-based malware propagation is 58.122%, DICMLA is 40.89%, and P-SMO is 99.472%, while the proposed P-WWO has the coverage of 99.992%.

Figure 5c represents the analysis based on energy balancing index. For 500 rounds, the energy balancing index of the existing CA-based node scheduling is 0.9822, CA-based malware propagation is 0.9996, DICMLA is 0.9842, and P-SMO is 0.9984, while the proposed P-WWO has the energy balancing index of 0.9992. 1500 rounds, the energy balancing index of the existing CA-based node scheduling is 0.7006, CA-based malware propagation is 0.8139, DICMLA is 0.7466, and P-SMO is 0.8564, while the proposed P-WWO has the energy balancing index of 0.9246.

Figure 5d depicts the analysis based on average energy left. For 500 rounds, the average energy left by the existing CA-based node scheduling is 0.7932 J, CA-based malware propagation is 0.8653 J, DICMLA is 0.7820 J, and P-SMO is 0.9268 J, while the average energy left by the proposed P-WWO is 0.9596 J. For 1500 rounds, the average energy left by the existing CA-based node scheduling is 0.3372 J, CA-based malware propagation is 0.3539 J, DICMLA is 0.3815 J, and P-SMO is 0.4602 J, while the average energy left by the proposed P-WWO is 0.6661 J.

6.5 Comparative Discussion

Table 1 portrays the comparative discussion of proposed P-WWO algorithm made using 50 nodes. It is shown that the number of nodes alive with the existing CA-based node

Table 1 Comparative discussion made using 50 nodes

Number of rounds	Metrics	CA-based node scheduling	CA-based malware propagation	DICMLA	P-SMO	Proposed P-WWO
1500	Energy balancing index	0.7281	0.7436	0.7161	0.8936	0.8830
	Coverage (%)	68.36	24.03	13.18	90.16	91.70
	Number of nodes alive	22	6	2	41	47
	Average energy left (J)	0.3232	0.3075	0.2714	0.4792	0.5778

scheduling is 22, CA-based malware propagation is 6, DICMLA is 2, and P-SMO is 41, while the proposed P-WWO has the number of alive-nodes of 47, where the proposed method is 53% better than CA-based node scheduling, 87.2% better than CA-based malware propagation, 95.7% better than DICMLA, and 12.76% better than P-SMO.

Table 2 portrays the comparative discussion of proposed P-WWO algorithm made using 100 nodes. The coverage obtained by the existing CA-based node scheduling is 79.6375%, CA-based malware propagation is 62.57%, DICMLA is 55.8775%, and P-SMO is 98.025%, while the proposed P-WWO has the coverage of 98.555%. Here, the performance of the proposed method is 19% better than the existing CA-based node scheduling, 36% better than CA-based malware propagation, 43% better than DICMLA, and 0.5% better than P-SMO for 1500 rounds.

Table 3 depicts the comparative discussion of proposed P-WWO algorithm made using 100 nodes. For 1500 rounds, the energy balancing index of the existing CA-based node scheduling is 0.7006, CA-based malware propagation is 0.8139, DICMLA is 0.7466, and P-SMO is 0.8564, while the proposed P-WWO has the energy balancing index of 0.9246. Here, next to the proposed method P-SMO has better result and the CA-based node scheduling has the worst performance.

From the analysis, it is depicted that the proposed method offers the high performance than the existing methods. The reasons for the high performance of the proposed P-WWO algorithm are described here. The PWWO algorithm not only has the optimization efficiency of the basic PSO and WWO but can also has strong stability and robustness. It can avoid threat areas with a minimum cost to obtain the optimal path. In

Table 2 Comparative discussion made using 100 nodes

Number of rounds	Metrics	CA-based node scheduling	CA-based malware propagation	DICMLA	P-SMO	Proposed P-WWO
1500	Energy balancing index	0.8124	0.7383	0.7553	0.8737	0.8826
	Coverage (%)	79.64	62.57	55.88	98.03	98.56
	Number of nodes alive	46	22	28	92	95
	Average energy left (J)	0.3631	0.3552	0.4060	0.4462	0.5769

Table 3 Comparative discussion made using 150 nodes

Number of rounds	Metrics	CA-based node scheduling	CA-based malware propagation	DICMLA	P-SMO	Proposed P-WWO
1500	Energy balancing index	0.7006	0.8139	0.7466	0.8564	0.9246
	Coverage (%)	56.802	80.18	50.83	99.79	99.9
	Number of nodes alive	23	52	23	126	144
	Average energy left (J)	0.3372	0.3539	0.3815	0.4602	0.6661

PSO algorithm, the lifetime factor of the node and link is taken into account for routing which gives the advantage of reduced data loss. The route failure is greatly minimized by using PSO algorithm thereby reducing the overhead. PSO algorithm is easier to implement and also it is very efficient in the global search. WWO is presented for global optimization problems. The WWO algorithmic framework of is simple, and easy to implement with a small-size population and it uses only a few control parameters.

7 Conclusion

To produce interruption less and efficient communication between source and destination nodes the routing protocols are necessary. Hence, in this research, an effective and optimal secure routing mechanism is modeled using the proposed P-WWO algorithm. Here, the routing process can be effectively achieved using the CH node. CH is selected using the newly designed PSO-based cellular automata. After selecting the CH, the path used to route the data securely is identified using the proposed P-WWO, which is developed by integrating the PSO with the WWO, respectively. However, the proposed P-WWO effectively identify the secure path using the fitness measure, which considers the factors like delay, energy, maintainability factor, consistency factor, and trust, respectively. Accordingly, the function with the maximum fitness value is accepted as the best route to transfer the data packets. Finally, the data transmission is carried out using the double wave encryption model. The implementation of proposed P-WWO algorithm is carried out and the performance is evaluated by varying the number of nodes, as 50, 100, and 150. Also, the performance of the proposed method is compared with the existing methods, such as CA-based node scheduling, CA-based malware propagation, DICMLA and P-SMO and the analysis results shows that the performance of the proposed method is better than the existing methods. The proposed P-WWO obtained better performance using the metrics, like energy balancing index, coverage, number of alive-nodes, and average energy left with the values of 0.9246, 99.9%, 144, and 0.666 J, respectively. The future extension of the routing process can be focus to reduce the packet loss ratio and increase the efficiency to avoid malicious attacks.

References

1. Stephen, R. K., Sekar, A. C., & Dinakaran, K. (2019). Sectional transmission analysis approach for improved reliable transmission and secure routing in wireless sensor networks. *Cluster Computing, 22*(2), 3759–3770.
2. Rathee, M., Kumar, S., Gandomi, A. H., Dilip, K., Balusamy, B., & Patan, R. (2019). Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks. *IEEE Transactions on Engineering Management, 68*(1), 170–182.
3. Saini, K., & Ahlawat, P. (2019) A trust-based secure hybrid framework for routing in WSN. In: *Recent findings in intelligent computing techniques*. Singapore: Springer (pp. 585–591).
4. Krishnaveni, M. M., Selvakumar, G., & Devi, M. S. A. (2019). Reliable data transmission in wireless network using secure trust based routing.
5. Kaiwartya, O., Abdullah, A. H., Cao, Y., Altameem, A., Prasad, M., Lin, C. T., & Liu, X. (2016). Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. *IEEE Access, 4,* 5356–5373.
6. Cao, Y., Wang, T., Kaiwartya, O., Min, G., Ahmad, N., & Abdullah, A. H. (2016). An EV charging management system concerning drivers' trip duration and mobility uncertainty. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 48*(4), 596–607.
7. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*(4), 393–422.
8. Kavitha, M., & Geetha, B. G. (2019). An efficient city energy management system with secure routing communication using WSN. *Cluster Computing, 22*(6), 13131–13142.
9. Shi, Q., Qin, L., Ding, Y., Xie, B., Zheng, J., & Song, L. (2020). Information-aware secure routing in wireless sensor networks. *Sensors, 20*(1), 165.
10. Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks.
11. Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications, 35*(3), 867–880.
12. Vasudeva, A., & Sood, M. (2018). Survey on sybil attack defense mechanisms in wireless ad hoc networks. *Journal of Network and Computer Applications, 120,* 78–118.
13. Dhanvijay, R., Pande, M., & Wajurakar, S. (2019). Energy optimization in wireless sensor networks using trust-aware routing algorithm.
14. Tang, D., Jiang, T., & Ren, J. (2010). Secure and energy aware routing (sear) in wireless sensor networks. In *IEEE global telecommunications conference GLOBECOM* (pp. 1–5).
15. Abdulrahman, S., & Raisi, J. A. (2020) A review on congestion management methodologies and its applications. *Journal of Computational Mechanics, Power System and Control* 3(3).
16. Rodrigues, P., & John, J. (2020). Joint trust: An approach for trust-aware routing in WSN. *Wireless Networks, 26*(3), 3553–3568.
17. Perkins, C. E., & Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *ACM SIGCOMM Computer Communication Review, 24*(4), 234–244.
18. Johnson, D. B., Maltz, D. A., & Broch, J. (2001). DSR: The dynamic source routing protocol for multihop wireless ad hoc networks. *Ad hoc Networking, 5*(1), 139–172.
19. Rewadkar, D., & Doye, D. (2018). Traffic-aware routing protocol in VANET using adaptive autoregressive crow search algorithm. *Journal of Networking and Communication Systems, 1*(1), 36–42.
20. Draves, R., Padhye, J., & Zill, B. (2004). Comparison of routing metrics for static multi-hop wireless networks. *ACM SIGCOMM Computer Communication Review, 34*(4), 133–144.
21. Zahariadis, T., Leligou, H., Karkazis, P., Trakadas, P., Papaefstathiou, I., Vangelatos, C., & Besson, L. (2010). Design and implementation of a trust-aware routing protocol for large WSNs. *International Journal of Network Security & Its Applications (IJNSA), 2*(3), 52–68.
22. Mohan, C. R., & Reddy, A. V. (2018). T-whale: Trust and whale optimization model for secure routing in mobile ad-hoc network. *International Journal of Artificial Life Research., 8*(2), 67–79.
23. Srinivas, S., & Santhirani, Ch. (2020). Hybrid particle swarm optimization-deep neural network model for speaker recognition. *Multimedia Research, 3*(1), 1–10.
24. Ahmed, A. A., Latiff, L. A., Sarijari, M. A., Fisal, N. (2008). Real-time routing in wireless sensor networks. In *Wireless sensor networks*.
25. Sun, Z., Wei, M., Zhang, Z., & Qu, G. (2019). Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks. *Applied Soft Computing, 77,* 366–375.
26. Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Nehemiah, H. K., & Kannan, A. (2019). An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. *Wireless Personal Communications, 105*(4), 1475–1490.

27. Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., & Kannan, A. (2020). QoS aware trust based routing algorithm for wireless sensor networks. *Wireless Personal Communications, 110*(4), 1637–1658.
28. Mythili, V., Suresh, A., Devasagayam, M. M., & Dhanasekaran, R. (2019). SEAT-DSR: Spatial and energy aware trusted dynamic distance source routing algorithm for secure data communications in wireless sensor networks. *Cognitive Systems Research, 58,* 143–155.
29. Beheshtiasl, A., & Ghaffari, A. (2019). Secure and trust-aware routing scheme in wireless sensor networks. *Wireless Personal Communications, 107*(4), 1799–1814.
30. Singh, K., & Malhotra, J. (2018). Fuzzy link cost estimation based adaptive tree algorithm for routing optimization in wireless sensor networks using reinforcement learning. *Wireless Sensor Networks Using Reinforcement Learning, 8*(3), 151–164.
31. Rodrigues, P., & John, J. (2020). Joint trust: An approach for trust-aware routing in WSN. *Wireless Networks, 26,* 3553–3568.
32. Singh, K., & Malhotra, J. (2019). Reinforcement learning-based real time search algorithm for routing optimisation in wireless sensor networks using fuzzy link cost estimation. *International Journal of Communication Networks and Distributed Systems, 22*(4), 363.
33. Pattnaik, S., & Sahu, P. K. (2020). Assimilation of fuzzy clustering approach and EHO-Greedy algorithm for efficient routing in WSN. *Wireless Sensor Networks, 33*(8), 20.
34. Vinitha, A., Rukmini, M. S. S., & Sunehra, D. (2020). Energy-efficient multihop routing in WSN using the hybrid optimization algorithm. *Wireless Sensor Networks, 33*(12), 20.
35. Elhoseny, M., Rajan, R. S., & Hammoudeh, M. (2020). Swarm intelligence–based energy efficient clustering with multihop routing protocol for sustainable wireless sensor networks. *International Journal of Distributed Sensor Networks, 16,* 1550147720949133.
36. Balachandra, M., Prema, K. V., & Makkithaya, K. (2014). Multiconstrained and multipath QoS aware routing protocol for MANETs. *Wireless Networks, 20*(8), 2395–2408.
37. Yadav, A. K., & Tripathi, S. (2017). QMRPRNS: Design of QoS multicast routing protocol using reliable node selection scheme for MANETs. *Peer-to-Peer Networking and Applications, 10*(4), 897–909.
38. Zhan, Z. H., Zhang, J., Li, Y., & Chung, H. S. H. (2009). Adaptive particle swarm optimization. *IEEE Transactions on Systems, Man, and Cybernetics Part B (Cybernetics), 39*(6), 1362–1381.
39. Kumar, N., & Kim, J. (2013). ELACCA: Efficient learning automata based cell clustering algorithm for wireless sensor networks. *Wireless Personal Communications, 73*(4), 1495–1512.
40. Zheng, Y. J. (2015). Water wave optimization: A new nature-inspired metaheuristic. *Computers & Operations Research, 55,* 1–11.
41. Chen, Z., He, M., Liang, W., & Chen, K. (2015). Trust-aware and low energy consumption security topology protocol of wireless sensor network. *Journal of Sensors, 6,* 7.
42. Wang, B., Chen, X., & Chang, W. (2014). A light-weight trust-based QoS routing algorithm for ad hoc networks. *Pervasive and Mobile Computing, 13,* 164–180.
43. Palaniappan, S., & Chellan, K. (2015). Energy-efficient stable routing using QoS monitoring agents in MANET. *EURASIP Journal on Wireless Communications and Networking, 1*, 1–11.
44. Wang, Y., Li, D., & Dong, N. (2018). Cellular automata malware propagation model for WSN based on multi-player evolutionary game. *IET Networks, 7*(3), 129–135.
45. Byun, H., & Yu, J. (2014). Cellular-automaton-based node scheduling control for wireless sensor networks. *IEEE Transactions on Vehicular Technology, 63*(8), 3892–3899.
46. Zhang, F., Wang, X., Li, P., & Zhang, L. (2016). An energy aware cellular learning automata based routing algorithm for opportunistic networks. *International Journal of Grid and Distributed Computing, 9*(2), 255–272.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Pradeep Sadashiv Khot received his B.E. degree in Computer Engineering from Mumbai University, Mumbai, Maharashtra State, India in 2007 and M.Tech. Degree in Computer Science and Engineering from SRM University, Chennai, Tamilnadu State, India in 2013. Pradeep Khot is currently pursuing the Ph.D. degree in Computer Science and Engineering with the Visvesvaraya Technological University (VTU) Belagavi, Karnataka State, India. With a broader scope of Cellular automata in Wireless Sensor Networks, his main field of interest is Cellular Automata, Wireless Sensor Networks, Data Analytics, Artificial Intelligence. He has presented papers in various National and International conferences.

Udaykumar Naik is currently Professor, Electronics and communication Engineering department at KLE DRMSSCET, Belagavi, Karnataka, India.Prof. Udaykumar Naik received B.E. degree in Electronics and Communication Engineering, from the Karnataka University, Dharwar, India in 1988, M.Tech. degree in Digital Electronics and Advanced Communications, from National Institute of Technology-Karnataka (NIT-K), Surathkal, India, in 1996 and Ph.D. degree in Electronics Engineering, Shivaji University, Kolhapur, India, in 2014. His research interests include Indoor Wireless Location Technologies, Antenna design and Wireless Systems Modeling and Design, Wireless Sensor Networks. He is the author of 30 research papers in peer reviewed reputed international journals and conferences. He has over 30 years of teaching experience. Professor Udaykumar Naik is a Fellow of the Institution of Electronics and Telecommunications Engineers, New Delhi, India.