International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/218511 Volume 10, Issue 1, January – February (2023)

RESEARCH ARTICLE

Hybrid Optimization Enabled Routing Protocol for Enhancing Source Location Privacy in Wireless Sensor Networks

Chinnu Mary George
Department of Computer Science and Engineering, Dayananda Sagar University, Bangalore, India.
gchinnu2@gmail.com

Gayathri K M
Department of Electronics and Communication Engineering, Dayananda Sagar University, Bangalore, India
gayathri-ece@dsu.edu.in

Reeja S R
School of Computing Sciences and Engineering, VIT-AP University, Andhra Pradesh, India.
reeja.sr@vitap.ac.in

Received: 27 November 2022 / Revised: 26 December 2022 / Accepted: 31 December 2022 / Published: 26 February 2023

Abstract – Wireless sensor networks (WSN) are utilized in various application domains concerning monitoring and smart application, in which highly sensitive information in healthcare and military applications is also employed using the WSN. The openness and unattended nature of the WSN make security as a challenging task. The information eavesdropping is employed by the network intruder from the source node; hence the location of the source node needs to be protected for the acquisition of information security. Thus, this research introduces a privacy preservation of the source location method using the hybrid optimization based secure routing. For this, Shuffled Shepherd-Coot (SS-Coot) optimization is proposed by hybridizing the foraging behavior of the Coot, a water bird, with the shepherd's behavior in herding the animal community. The incorporation of the herding behavior of the shepherd with Coot's foraging behavior helps to enhance the diversification phase to obtain the best solution by avoiding premature convergence. In the proposed source location privacy preservation, the network boundary radiuses are obtained optimally using the SS-Coot algorithm during the network initialization. Then, the routing through the various boundaries of the network with multi-hop helps to protect the location of the source by confusing the intruder's backtrace process. The analysis is performed based on Packet Delivery Ratio (PDR), throughput, energy consumption, and delivery latency and obtained the values of 1.02867, 1.02909, 0.30171, and 0.00165, respectively.

Index Terms – Source Location, Privacy, Shuffled Shepherd Optimization Method, Wireless Sensor Network, Coot Optimization.

1. INTRODUCTION

The Internet of things (IoT) and sensing systems require the support of a wireless sensor network (WSN) for processing the application that leads to the popularity of WSNs in recent years. The sensor nodes are utilized by the WSN for the information exchange, which is a low-powered and small sensing device [1]. Communication, sensing, computing, and mobilizing the information are the major capabilities of the sensor nodes, in which the higher consumption of energy and a minimum lifetime of the network is the challenging task [2]. The intelligent transportation systems, controlling of water quality, healthcare, industrial monitoring, and several monitoring applications are performed through the WSN. Besides, the WSN is applicable in complex, harsh, and unattended environments due to the usage of batteries, which degrades performance due to the changes in environmental and energy factors [3][4][5]. In unprotected areas, the WSNs are utilized with an enormous number of nodes using distributed interconnections between the devices [6]. The nodes responsible for the information gathering are termed sink nodes [7], and communication takes place through the wireless nodes. Finally, the collected information is stored by the sink node [8]. The interception and detection of information are employed in the WSN using the relevant receiver due to its openness and unattended nature. Thus, security issues exist in the network because the intruder employs an illegal approach to the information threat, which leads to the requirement of security measures in the network

[8]. Security is highly necessary for the application domains, like healthcare and the military for safeguarding the sensitive information [9]. The degradation of the application is employed by the attacker by interfering with the proper functioning of the network [10]. The location information concerning the important nodes is obtained by the intruder during the network traffic [11] [12] [13]. Thus, the preservation of privacy with efficient communication based on energy is essential for the WSN [14][15][16]. Due to the drastic changes in the environment, the performance is affected, and the limited battery usage limits the performance; thus, the reliability of the network needs to be guaranteed for the WSN [17][6]. The transmission of the single data packet without making the data redundancy needs to be performed for the reduction of energy consumption [18].

The observability and traceability of the source location are minimized through the source location privacy preservation method in the WSN [19]. The compromised nature of the WSN is easily exposed to the attacker by identifying the source location; thus, security is a challenging task. Several routing protocols were developed for the preservation of the location of the source [12][6]. The detection of the source location is employed by the attacker for the information gathering because the location of the asset is directly related to the location of the source. The relay ring routing (ReRR) protocol for the protection of the source location uses two methods of routing based on the dynamic strategy. The detection of the source node is employed based on the sink location. The better efficiency in routing for the protection of the source location is employed through the random routing strategy. The goal of the research is to devise a source location privacy preservation for the efficient routing of sensitive information in the WSN environment. The routing of the data to the sink node from the source node with enhanced security is employed through the multi-hop transmission, in which the intermediate diversion and mediate nodes are utilized. Here, the region of the network is divided into outer and inner boundaries with the mediate, diversion, and normal layers. The regions of these layers are found optimally using the hybrid optimization algorithm. The major contributions of the research are:

- **Proposed SS-Coot Algorithm**: The proposed SS-Coot optimization algorithm is designed by combining the shepherd's behavior in herding the animal community based on the instinct of the animal in the Shuffled Shepherd Optimization (SSO) [20] and the foraging behavior of the Coot water birds in Coot Optimization [21] for the enhancement of the exploration phase to obtain the global best solution.
- **Proposed SS-Coot-based Network Initialization**: The proposed SS-Coot-based network initialization is utilized to identify the network regions, in which the radiuses of the network regions are obtained optimally using the proposed SS-Coot optimization algorithm.
- **Proposed Multi-objective Fitness Function**: The fitness function for the SS-Coot optimization is derived based on the packet delivery ratio, throughput, and energy to obtain enhanced solution.

1.1. Motivation

The WSN is widely utilized in sensitive information sharing in applications, like military, environment monitoring, and various smart applications. Still, security is a challenging task, which can be eliminated through the privacy preservation of the source location. Hence, this research reviews the conventional methods of privacy preservation of the source location and identifies the challenges of designing a novel framework by overcoming challenges faced by them.

The secure source location-aware routing protocol based on the SS-Coot is organized as follows: Section 2 provides the related method along with its challenges, and the network model is presented in Section 3. Section 4 details the SS-Coot-based routing of data, and section 5 details the analysis of source location privacy preservation methods. Finally, section 5 concludes the work.

2. RELATED WORKS

The privacy preservation of the source location for the highly secure information routing in the WSN is developed by [22] using the random routing technique, which is difficult to back trace to identify the source node's location. The path diversity and the shortest path was evaluated using the phantom single path routing technique. The diversion of the nodes was employed near the sink node to enhance the security of the source location and obtained better performance in terms of delivery ratio and latency, but it failed to enhance the computation overhead and the consumption of energy, which is considered as a limitation of the method. The capture likelihood and the safety period-based source location privacy were employed in [23][24] to prevent network tracking. In this, the energy overhead was minimized using the phantom routing with the flexible tracking preventing mechanism. The evaluation was performed by considering the single path routing and flood-based approach and acquired elevated performance; still, the communication overhead concerning the method was high. The data flooding with the real and the fake data packets to show the high path diversity of the method using the relay ring routing was developed by [3] for the preservation of source location. The safeguarding of the relay node was employed by incorporating the relay nodes among the source and destination. The method obtained reliability and high efficiency, and the estimation of the delay and reliability were not evaluated by the method, which is the drawback. The random routing-based preservation of privacy was presented by [11], in which the fake packet was routed initially through the random nodes. Finally, using the ring routing, the real data packet was transmitted. The analysis of the method showed better results for the network's lifetime, transmission delay, and safety time; still, the multiple nodes for privacy preservation were not evaluated by the method.

The sector Phantom-based privacy preservation of the source location in routing was presented by [12] using the coordinates of the central node. The phantom node was placed between the base station and the source node to acquire enhanced privacy concerning the source location. Minimal communication overhead was obtained, due to the consideration of minimal region but failed to balance the consumed energy and the overhead of communication to acquire the security for a longer time. The encryption-based method for information authentication was designed by [3] using the trust model for the privacy preservation of the source location. The enhanced longevity with the minimal attack was estimated by the method, but the network's delay is still higher. The hash-based technique was presented by [6] for sharing sensitive information. In this, the location of the source is hidden using the encoding technique for the acquisition of enhanced security. The method accomplished minimal delay in delivering the data with minimal consumption of energy and a larger number of data packets; still, the computation complexity of the method is higher, which is the drawback of the method. The fuzzy-based node clustering and CH selection using the optimal routing were developed by [5], in which the integrity and confidentiality were obtained through the secure data aggregation criteria. The minimal overhead of computation and the consumption of energy were obtained by the method; still, the method can't be applicable for monitoring applications.

2.1. Challenges

The prior privacy preservation of source location for the secure routing techniques has faced several challenges like:

- The privacy preservation of the source location designed by [21] has a better tolerance over the communication overhead; still, the consumption of higher energy by the method is a challenging issue.
- The minimal PDR, along with higher delay in data exchange in the end-to-end delivery of the data, is considered as a challenge in the method [10], but it acquired efficient energy utilization in the regions of the near sink.
- With the higher hops, the efficient routing and confusing the intruder is employed by [11], in which the analysis of the tradeoff between the lifetime of the network and privacy was not employed, and the consideration of multiple sources was also not employed in the method.
- The overlapping of the routing along with the multiple paths routing through the random directions are obtained by [12], in which the higher energy consumption and the communication overhead limit the performance of the method.
- The method with additional measures, like computation overhead, memory, and communication provides the enhanced security model; still, it is not applicable for the resource constraint methods.

2.2. Problem Statement

With the several challenges seen across in wireless sensor networks. This research will develop a new method for routing the data packets using proposed Shuffled Shepherd-Coot (SS-Coot) algorithm. WSN is consisted of a set of nodes and links. A wireless sensor node is a computing device equipped with a wireless interface, a limited set of computational capabilities and has a unique identifier. Communication from a node is typically modeled with a circular communication range centered at the node.

A node can exchange packets with all its neighboring nodes. A link exists between the two neighboring nodes. The network model is a large, two-dimensional coordinate network, represented by an undirected graph G = (V, W) with a set of vertices V that represent the nodes, and a set of edges W that represent the communication links between the neighboring nodes. Initially, the nodes will be simulated in the network and thereby source node and the target node will be identified to make the data communication process.

3. NETWORK MODEL

The WSN comprises several distributed sensors, named nodes for processing applications, like asset tracking and monitoring, military, agriculture, medical applications, and so on. Thus, for sensitive application processing, the security of the information transmission plays a crucial role that is ensured by preserving the privacy of the source location. The open nature of the WSN helps the intruder to monitor the information through the back tracing process from the sink to the source node.

Hence, the location of the source node needs to be preserved to preserve the sensitive information shared through the network. Thus, this research introduces a hybrid optimization-enabled routing protocol for preserving the source location of the network. The information exchange from a node in the network with its neighbor is employed using the link.

Thus, the network comprises of the nodes and the links for the information exchange and is notated as, $A = (vertices, edges)$, where the nodes in the network is referred as vertices and the links in the network are referred as edges, while representing the network using the undirected graph. The nodes in the introduced method utilize the same range of communication, and hence, the homogeneous structure is considered for the privacy preservation of the source node. The various nodes utilized in the proposed SS-Coot-based privacy preservation of source location are:

3.1. Source Node

The node that starts the information exchange is termed as the source node, and the information exchange from the source to the sink is performed using only one source node to avoid the redundancy of data. Suppose multiple sources detect the same asset in the network and start information exchange to the sink node. In that case, data redundancy occurs, and the back tracing becomes easier for the intruder when the same multiple pieces of information are received by the sink simultaneously. In addition, the source node is not aware by the subsequent nodes. Thus, in the proposed SS-Coot method, a single source is utilized for exchanging the information in the network.

3.2. Sink Node

The node that receives the information is termed the sink node, in which the intruder monitors the sink node for the eavesdropping of the information without any interference in the network and performs back tracing by obtaining the signal strength and angle. Thus, the efficient routing mechanism using the proposed SS-Coot provides the efficient privacy preservation of the source location through the proposed routing protocol. Besides, the sink node act as the communication link between the network and the external world and is responsible for the information gathering.

3.3. Diversion Node

The random nodes are termed as diversion nodes, which are present in both the network's inner and outer boundary regions. The information exchange occurs in these nodes, which are considered as intermediate nodes.

3.4. Mediate Node

The random nodes are termed mediate nodes, which are present in the network's inner and outer boundary region. The information exchange occurs in these nodes and is considered as the intermediate node. The mediate nodes are far away from the sink node and are also beyond the dispersion node.

3.5. Normal Node

The normal nodes in the network are present in the inner and outer boundary region of the WSN, which is present near the sink node in the inner boundary and beyond the mediate nodes in the outer boundary of the network. Each node in the network has a unique ID for the exchange of information and follows the sleeping schedule, which means the node becomes inactive when no asset is detected by them.

4. PROPOSED SS-COOT BASED ROUTING PROTOCOL FOR PRIVACY PRESERVATION OF SOURCE LOCATION

The WSN is widely utilized in several application domains, like environmental monitoring, healthcare, grids, smart homes, event/asset monitoring, and also in various sensitive applications like military monitoring and so on, in which security and limited resources are challenging tasks. In this, the adversary performs asset poaching using the backtrace process from the sink node to reach the source to eavesdrop on the information. Hence, this research introduces the secure source-aware routing protocol using hybrid optimization for the privacy preservation of the source location. In the proposed SS-Coot routing protocol, the efficient routing technique confuses the adversary, and hence the back tracing of the source location is impossible with the introduced method. Initially, the network initialization is employed using the proposed SS-Coot optimization for the estimation of the radius of the network region for the data routing. The SS-Coot is designed by combining the herding behavior of the shepherd based on several animal communities with the foraging behavior of the Coot, a water bird, for the accomplishment of enhanced exploration to obtain the global best solution without premature convergence. Here, the SS-Coot is utilized for the network initialization, in which the radius of the network region is found optimally using the proposed optimization algorithm. After initializing the network, efficient routing through the various network regions is employed based on four different steps for the privacy preservation of the source location. The workflow is portrayed in Figure 1.

4.1. Network Initialization Using Hybrid SS-Coot

The proposed SS-Coot-based Privacy Preservation of Source Location of the network performs the initialization process initially for the implementation process, in which the location of their own position in the network along with the sink and neighboring node's locations are initialized. Besides, all the nodes are assigned with a unique ID, and the destination nodes obtain the position of the nodes in the network through the global positioning system (GPS). Then, the hop count is initialized as zero for all the nodes by sending a beacon message by the sink to all other nodes. The count is incremented upon the reception of another beacon packet from the nodes, which is utilized to identify the node's location from the sink node. Let us consider, that when a node obtains several packets of information, it ignores the information from the node with a higher hop and stores the minimum hop information. Also, the radius of the network decides the availability of the nodes in the inner or outer boundary, in which the sink node is located at the center of the network and is defined as $L(S_i)$, the radius of the normal node at the inner boundary is defined as r_{ni}, the radius of the diversion node at the inner boundary is notated as r_{di}, the radius of the mediate node at the inner boundary is defined as r_{mi}, the radius of the diversion node at the outer boundary is defined as r_{do}, the radius of the mediate node at the outer boundary is notated as r_{mo}, the radius of the normal node at the outer boundary is notated as r_{no} and is portrayed in Figure 2. As per Figure 2, the proposed WSN is subdivided into two divisions named (i) inner boundary region and (ii) outer boundary region. Here, both the inner and outer boundary has the corresponding normal, mediate, and diversion nodes. Here, the initialization of the radius of the network is considered as the problem and is solved optimally using the proposed SS-Coot optimization algorithm.

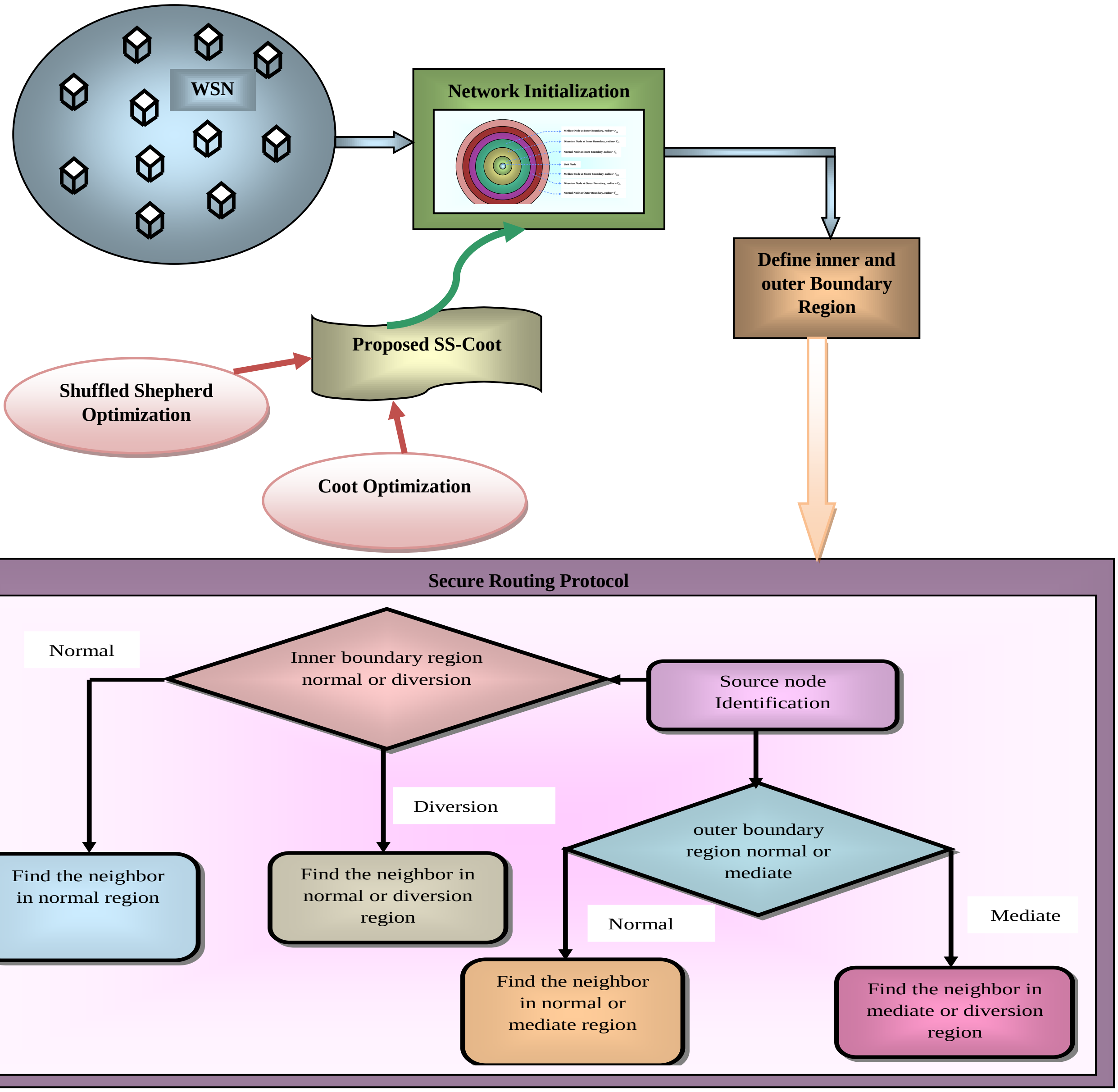

WSN
Network Initialization
Define inner and outer Boundary Region
Proposed SS-Coot
Shuffled Shepherd Optimization
Coot Optimization
Secure Routing Protocol
Normal
Inner boundary region normal or diversion
Source node Identification
Diversion
outer boundary region normal or mediate
Find the neighbor in normal region
Find the neighbor in normal or diversion region
Normal
Mediate
Find the neighbor in normal or mediate region
Find the neighbor in mediate or diversion region

Figure 1 Proposed SS-Coot-Based Privacy Preservation of Source Location

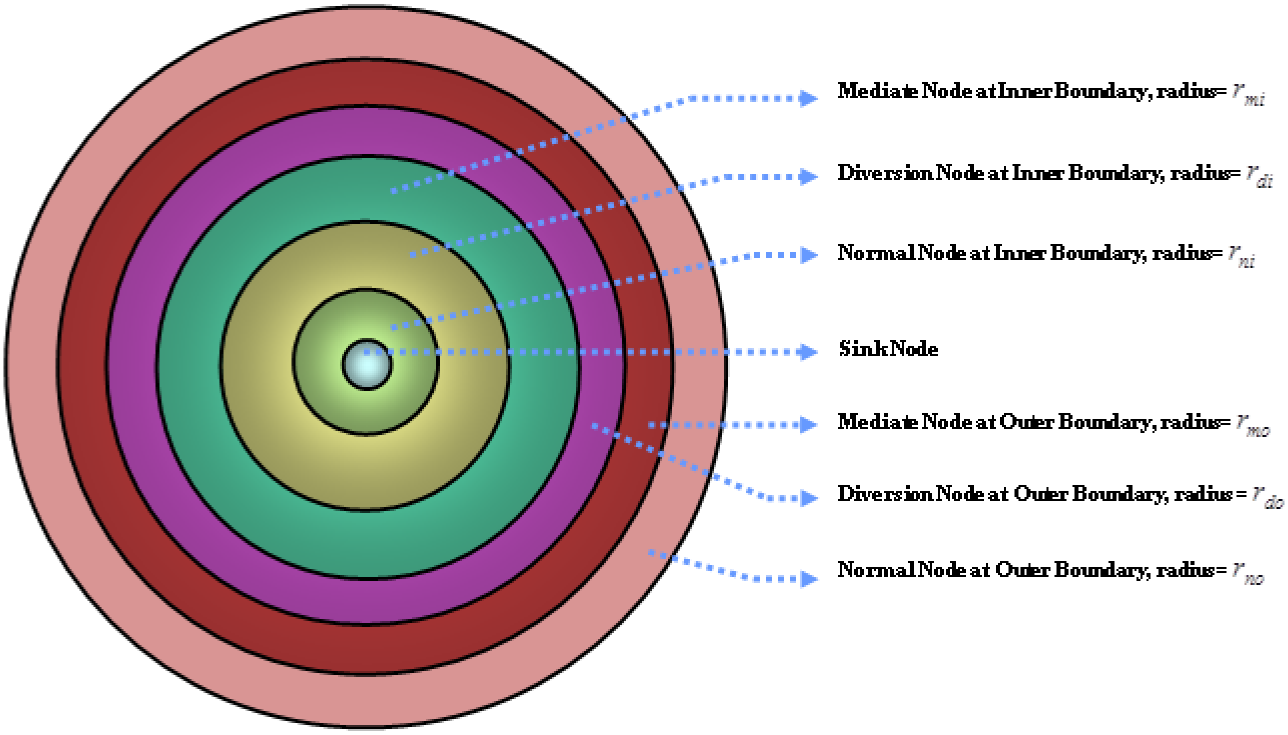

Mediate Node at Inner Boundary, radius= r_{mi}
Diversion Node at Inner Boundary, radius= r_{di}
Normal Node at Inner Boundary, radius= r_{ni}
Sink Node
Mediate Node at Outer Boundary, radius= r_{mo}
Diversion Node at Outer Boundary, radius = r_{do}
Normal Node at Outer Boundary, radius= r_{no}

Figure 2 Distribution of Nodes in the Proposed Network Model

4.2. Solution Encoding

The solution encoding of the proposed SS-Coot-based privacy preservation of the source location in WSN is portrayed in Figure 3. The problem to be solved using optimization is the estimation of the radius of the network for the network initialization. Here, the optimal estimation of the radius is employed using the SS-Coot algorithm. Here, the radius $r_n, r_{di}, r_{mi}, r_{do}, and\ r_{mo}$ should be in ascending order, and its value ranges between (0-100).

r_n	r_{di}	r_{mi}	r_{do}	r_{mo}

Figure 3 Solution Encoding of Proposed SS-Coot Based Privacy Preservation of Source Location

4.3. Fitness Function

The factors, like PDR, throughput, and energy are considered to evaluate the fitness function. The closeness of the obtained solution compared to the optimal target solution is estimated through the fitness measure. Here, in the proposed SS-Coot privacy preservation of the source location, the fitness is formulated as in equation (1),

$$SL_{fit} = \frac{1}{3}\left[\left(1 - SL_{PDR}\right) + \left(1 - SL_{Throughput}\right) + SL_{Energy}\right] \quad (1)$$

Where, the fitness function is expressed as SL_{fit}, the packet delivery ratio is defined as SL_{PDR}, the throughput is defined as $SL_{Throughput}$ and the energy is defined as SL_{Energy}. Here, the data packet received by the sink node with respect to the data packets shared by the source node is estimated through the PDR measure and is expressed as in equation (2),

$$SL_{PDR} = \frac{\sum_{i=1}^{Total_{\sin k}} T_{PD}}{\sum_{j=1}^{Total_{ssource}} T_{PS}} \quad (2)$$

where, the PDR of privacy preservation of the source location is notated as SL_{PDR}, the total number of source node is referred as $Total_{ssource}$, the total number of destination node is referred as $Total_{\sin k}$, the total packets received by all destination nodes is referred as T_{PD}, and total packets send by all source nodes is referred as T_{PS}. Then, the amount of data shared within the particular time to the sink from the source is defined as throughput and is expressed as in equation (3),

$$SL_{Throughput} = \frac{Packets_{S-D}}{Packets_{Total}} \qquad (3)$$

Where, the total number of packets is notated as $Packets_{Total}$, the packets shared to the destination from the source is notated as $Packets_{S-D}$, and the throughput is defined as $SL_{Throughput}$. Finally, when the data is transferred to the sink from the source, some amount of energy is consumed by the network [15], which depends on the number of bits in the packet and is expressed as in equation (4),

$$SL_{energy} = Energy_{Transmission} \times N_{Bits} \qquad (4)$$

Where, the energy is notated as SL_{energy}, the total number of bits in the packet is notated as N_{Bits} and the energy loss during the transmission is notated as $Energy_{Transmission}$.

4.4. Proposed SS-Coot Optimization for Network Initialization

The proposed SS-Coot for the network initialization of privacy preservation of the source location is designed by incorporating the Shepherds behavior in the animal community based on the instinct of the animal in herding [20] with the foraging behavior of the Coot Bird in the swarm [21].

4.4.1. Motivation of SS-Coot

The Coot is a small bird that lives in water and follows the swarm-based movement for foraging. The bird's movement in the water is synchronized or disordered while searching for food, and they also follow the leader. At the end of the movement, the Coot forms the chain structure, in which one Coot is behind another coot. The movement of the Coot is at an angle towards the motion direction in the food search. The Coot follows four movements in its food search; they are (i) Random motion (Exploration), (ii) Chain Movement, (iii), Position Adjustment by the member coots based on the leaders of the group, and (iv) Movement of the Leader towards food (Exploitation). Similarly, the shepherd shuffle method comprises of several communities of animals and is categorized based on the community, in which the shepherd's behavior in herding the animal based on instinct is considered. The animal horse is better at finding hard and fast pastures. Hence, the horse is utilized by the shepherd for the identification of the pasture in the search area in a fast and stiff way. Followed by the shepherd guides the sheep by providing food because the horses have the capability to find the pasture and return back.

Thus, in the proposed SS-Coot, the behavior of the shepherd in herding the sheep towards the horse in pasturing is hybridized with the foraging behavior of the Coot to enhance the exploration phase to avoid global convergence. The random movement of Coot towards the food search has the capability of striking at local optimal solution that leads to the inefficient solution in initializing the radius of the network to preserve the privacy of the source location. Thus, the exploration phase of the Coot is enhanced by integrating the shepherd's behavior in herding the animal community. Because, exploration capability of the horse in searching the pasture is higher that ensures the global best solution. Hence, by hybridizing the characteristic behavior, the balanced exploration and exploitation phases is obtained for the acquisition of the global best solution. In the proposed SS-Coot algorithm, the identification of food is nothing but the solution for the optimization issue, initialization of the network radius.

4.4.2. Mathematical Modeling of SS-Coot

The SS-Coot's mathematical modeling is detailed here, in which the initialization is the basic step. The initialization of the Coot's population in a random manner is notated as $\vec{a} = \left\{\vec{a_1}, \vec{a_2}, \ldots\ldots \vec{a_m}\right\}$. The Coot in the search space is move towards the food source and the solution for the optimization issue is can't able to achieve in a single iteration. Hence, the population of Coot in the sight area is expressed as in equation (5),

$$L(t) = rand(1, s) * (E - F) + F \qquad (5)$$

Where, the lower bound area is referred as F, the upper bound area is referred as E, the position of the Coot is notated as $L(t)$, and the dimension is defined as s. Then the representation of the $E \, and \, F$ is expressed as in equation (6),

$$F = [F_1, F_2, \ldots\ldots F_s], \qquad E = [E_1, E_2, \ldots. E_s] \qquad (6)$$

Fitness Measure: The fitness of the Coot in the sight area is measured through equation (1), and the position of the Coot is updated. Here, in the proposed SS-Coot-based privacy preservation of the source location, the minimal fitness value is considered.

Exploration: The Coot in the sight area explores through the random movement to identify the food source, and hence the random position of the Coot is expressed as in equation (7),

$$R = rand(1, s) * (E - F) + F \qquad (7)$$

The exploration of Coot based on the random movement has the capability to strike at the local solution, which updates the current position as in equation (8),

$$coot\ pos(i+1) = coot\ pos(i) + A * R_2 * (Q - Coot\ Pos(i))$$
(8)

Let us assume,

$coot\ pos(i+1) = L(t+1)$ and $coot\ pos(i) = L(t)$ for hybridizing the position updation and is expressed as in equation (9),

$$L(t+1) = L(t) + K \times M2 \times (R - L(t)) \qquad (9)$$

Where, the value ranges among $[0,1]$ is assigned for the random number $M2$. The factor K is obtained by evaluating in equation (10),

$$K = 1 - B \times \left(\frac{1}{\tau}\right) \qquad (10)$$

Where, the present iteration is notated as B and the maximal iteration is notated as τ. The equation (8) is re-written as in equation (11) and (12),

$$L(t+1) = L(t) + K \times M2 \times R - K \times M2 \times L(t) \qquad (11)$$

$$L(t+1) = L(t)[1 - K \times M2] + K \times M2 \times R \qquad (12)$$

Here, the local optimal solution with the pre-matured convergence is minimized by enhancing the food search through the incorporation of the shepherd's behavior in herding the animal community. The shepherd herds the animal community by knowing the instinct of the animal, and hence, the shepherd utilizes the horse for the identification of the food source, pasture. The horse finds the food faster with the best stiff, and hence, the shepherd guides the sheep community to follow the horse to find the pasture, which helps to enhance the exploration with fast convergence and to avoid trapping at the local solution of the Coot. Thus, the position of the shepherd is updated as in equation (13),

$$L(t+1) = L(t) + SS(t) \qquad (13)$$

Where, the current position is notated as $L(t+1)$, refers to the past location $L(t)$ and refers to the step size $SS(t)$. Here, the step size is estimated as in equation (14),

$$SS(t) = \alpha rand \circ (L_H(t) - L(t)) + \beta rand \circ (L_J(t) - L(t))$$
(14)

where, the random vector is notated as $rand$, the position of the sheep is referred as $L_J(t)$, the position of the horse is represented as $L_H(t)$, $\circ$ refers to the element-wise product, and the position of the shepherd is notated as $L(t)$. Here, the factors, $\alpha\ and\ \beta$ are defined as in equation (15) and (16),

$$\beta = \beta_0 - \frac{\beta_0}{\tau_{\max}} \times \tau \qquad (15)$$

$$\alpha = \alpha_0 - \frac{\alpha_0}{\tau_{\max}} \times \tau \qquad (16)$$

Where, the maximal iteration is notated as $\tau_{\max}$ and the current iteration is notated as τ. Initially, both the factors have zero value and is notated as $\alpha_0\ and\ \beta_0$. Then, the step size is substituted in the position updation of the shepherd and is expressed as in equation (17),

$$L(t+1) = L(t) + [\alpha rand \circ (L_H(t) - L(t)) + \beta rand \circ (L_J(t) - L(t))]$$
(17)

The equation is re-written as in equation (18),(19) and (20),

$$L(t+1) = L(t) + \alpha rand \circ L_H(t) - \alpha rand \circ L(t) + \beta rand \circ L_J(t) - \beta rand \circ L(t) \qquad (18)$$

$$L(t+1) = L(t)[1 - \alpha rand - \beta rand] + \alpha rand \circ L_H(t) + \beta rand \circ L_J(t) \qquad (19)$$

$$L(t) = \frac{L(t+1) - \beta rand \circ L_J(t) - \alpha rand \circ L_H(t)}{[1 - rand(\alpha + \beta]} \qquad (20)$$

The exploration phase is enhanced by minimizing the α and maximizing the β in the proposed SS-Coot algorithm. Then, the incorporation of the shepherd's behavior with the Coot's foraging behavior is employed by substituting equation (20) in equation (13) and is expressed as in equation (21),(22),(23),(24)and (25),

$$L(t+1) = \left[\frac{L(t+1) - \beta rand \circ L_J(t) - \alpha rand \circ L_H(t)}{[1 - rand(\alpha + \beta]}\right] [1 - K \times M2] + K \times M2 \times R$$
(21)

$$L(t+1) - \frac{L(t+1)[1 - K \times M2]}{[1 - rand(\alpha + \beta]} = K \times M2 \times R + \left[\frac{-\beta rand \circ L_J(t) - \alpha rand \circ L_H(t)}{[1 - rand(\alpha + \beta]}\right] \qquad (22)$$

$$L(t+1) - \frac{L(t+1)[1 - K \times M2]}{1} = K \times M2 \times R + \left[\frac{-\beta rand \circ L_J(t) - \alpha rand \circ L_H(t)}{1}\right] \tag{23}$$

$$L(t+1)[1 - rand(\alpha + \beta - 1 + K \times M2] = (K \times M2 \times R) \; [1 - rand(\alpha + \beta] - \begin{bmatrix} \alpha rand \circ L_H(t) + \\ \beta rand \circ L_J(t) \end{bmatrix} (1 - A * M2) \tag{24}$$

$$L(t+1) = \frac{1}{[K \times M2 - rand(\alpha + \beta)]} \begin{bmatrix} (K \times M2 \times R)[1 - rand(\alpha + \beta] - \\ [\alpha rand \circ L_H(t) + \beta rand \circ L_J(t)](1 - A * M2) \end{bmatrix} \tag{25}$$

Equation (23) portrays the newly designed position update equation by hybridizing the characteristic behavior of the shepherd and the Coot for the enhancement of the exploration criteria for the acquisition of the global best solution.

Average position Estimation: At the end of the swarm-based movement, the Coot forms the chain-based structure. The position of the Coot in the chain movement is obtained by averaging the position and is expressed as in equation (26),

$$L(t) = \frac{1}{2}[L(t-1) + L(t)] \tag{26}$$

Where, the current position is represented as $L(t)$ and the past position of the Coot is represented as $L(t-1)$.

Position Adjustment: The coots in the sight area adjust their location based on the leader's Coot to obtain the food. Here, the averaging of the position leads to the convergence at the local solution, which is minimized by selecting the leader using the formula in equation (27),

$$D = 1 + (tMODS) \tag{27}$$

Where, the index is notated as t, the total leaders in the swarm is notated as S, and the index number of the leader is represented as D. Thus, based on the index leader, the Coot updates the position as in equation (28),

$$L(t) = G(e) + 2 \times M1 \times \cos(2M\pi) \times G(e) - L(t) \tag{28}$$

Where, the interval $[-1,1]$ is assigned for the random number M and $M1$ has the value of $[0,1]$, the position of the leader is denoted as $G(e)$, and the position of the Coot is denoted as $L(t)$.

Exploitation: The leaders of the Coot update their location optimally in the present iteration, which helps to identify the location of the food for the members, and the position is updated as in equation (29),

$$G(t) = \begin{cases} W \times M3 \times \cos(2M\pi) \times L_{best} - G(t) + L_{best} & M4 < 0.5 \\ W \times M3 \times \cos(2M\pi) \times L_{best} - G(t) - L_{best} & M4 \geq 0.5 \end{cases} \tag{29}$$

Where, the best position is notated as L_{best}, $[0,1]$ be the range of the random number $M3 and M4$ and the factor W is estimated through in equation (30),

$$W = 2 - \tau \times \left(\frac{1}{\tau_{\max}}\right) \tag{30}$$

Re-Evaluation of Fitness: After updating the position of Coot, the fitness is re-calculated to identify the solution's feasibility.

Termination: The identification of the best solution or the accomplishment of $\tau_{\max}$ stops the iteration. The Pseudo-code of SS-Coot is presented in Algorithm 1.

```
Initialize the population of Coot $\bar{a}$ with the number of leaders $S$ and coots ( $\vec{a} - S$ )
Select leaders randomly
Estimate the fitness
Identify the $L_{best}$
While(termination not satisfied)
{
Estimate the parameters using equation (10) and equation (30)
Find the value $D$ using equation (27)
If( $rand > 0.5$ )
Update the position using equation (28)
else
If ( $rand < 0.5, t \sim= 1$ )
Update the position using equation (26)
else
Update the position using equation (25)
end
end
Update the position of leaders using equation (29)
}
end
$\tau = \tau + 1$
Stop
```

Algorithm 1 Pseudo-Code of SS-Coot

Thus, using the proposed SS-Coot optimization, the network initialization is employed, and then the secure routing is employed for the privacy preservation of the source location.

4.5. Source Location-Aware Routing Protocol

The data exchange in the network is initiated after the detection of the incoming data packet in the network. Here, in the proposed source location-aware routing, multi-hop routing is performed, in which the encryption of the incoming data packet is performed and forwarded to the sink node by the source node. The location of the source node in the network is employed through four-step process, which is portrayed in Figure 4.

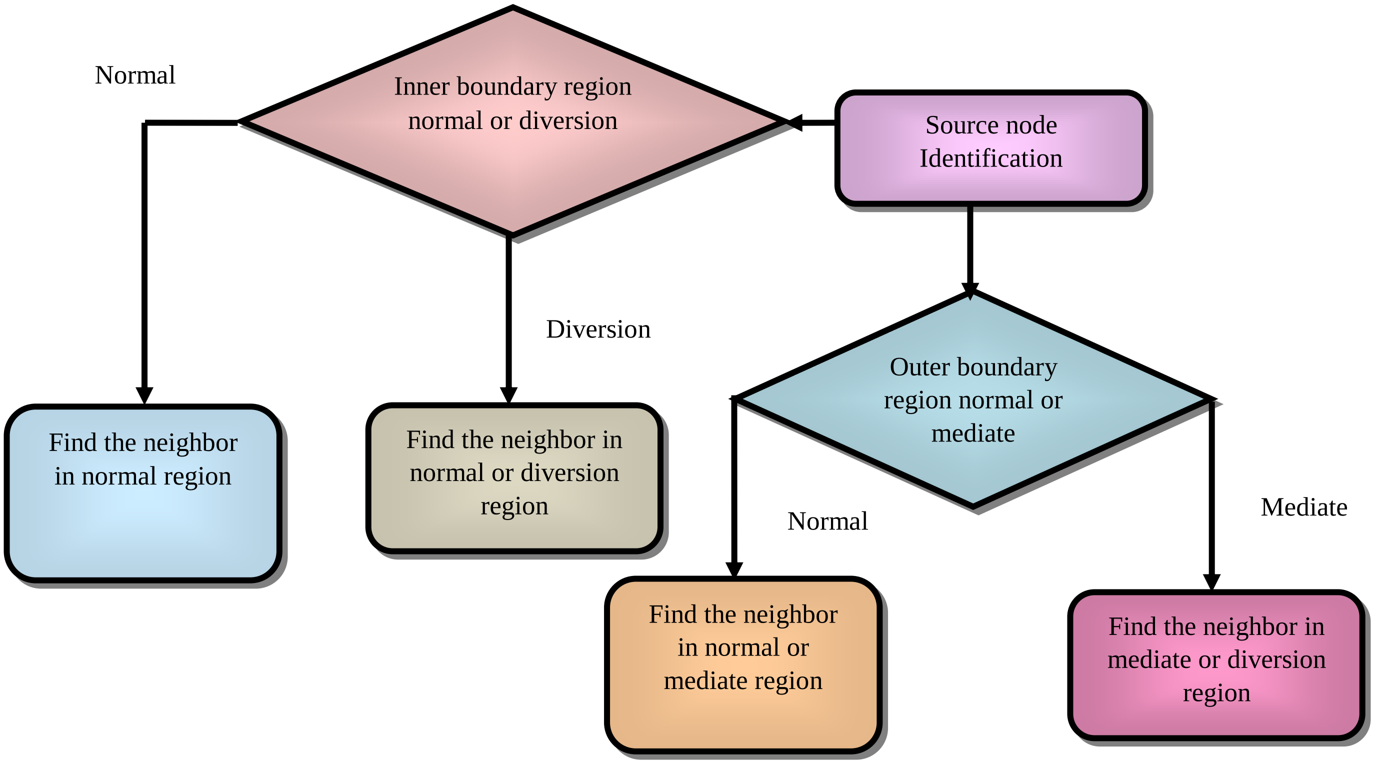

Normal
Inner boundary region normal or diversion
Source node Identification
Diversion
Outer boundary region normal or mediate
Find the neighbor in normal region
Find the neighbor in normal or diversion region
Normal
Mediate
Find the neighbor in normal or mediate region
Find the neighbor in mediate or diversion region

Figure 4 Source Location-Aware Routing Protocol

Step 1: Source Node of the packet: The source node is the node in the network which detects the asset and exchanges the information to the sink node through the intermediate node, which may be in the diversion or in the mediate region of the outer boundary to avoid source node localization. The routing of the data with privacy preservation utilizes the shortest path for energy-efficient transmission. The drawback of the method is the node near the sink is easy to backtrace by the intruder, which eases the identification of the source node. Hence, the routing through the long path in a random manner confuses the intruder in identifying the location of the source. Hence, in the proposed SS-Coot-based privacy preservation of the source location, the back tracing is avoided through the selection of source node in the network initialized using the SS-coot optimization.

Step 2: Identification of Next Node regions for packet: The source node in the network estimates the next node for exchanging the data based on the two different regions like: (i) inner boundary and (ii) outer boundary. The inner boundary comprises of three network regions named normal inner boundary region, mediate inner boundary region, and diversion inner boundary. Similarly, the outer boundary comprises of three network regions named normal outer boundary region, mediate outer boundary region, and diversion outer boundary. The estimation of the next node in the proposed SS-Coot-based source location-aware routing protocol is employed through any one of the following four phases.

Phase 1: Routing through the inner boundary in normal region: In this phase, the source node identifies the neighbour in the inner boundary and chooses the normal or mediate node in the inner boundary for data transmission.

Phase 2: Routing through the inner boundary in diversion region: In this phase, the source node identifies the neighbour in the inner boundary and it chooses the diversion or mediate node in the inner boundary for data transmission.

Phase 3: Routing through the outer boundary in normal region: In this phase, the source node is in the outer boundary and chooses the normal or mediate node in the outer boundary for data transmission.

Phase 4: Routing through the outer boundary in mediate region: In this phase, the source node is in the outer boundary and chooses the diversion or mediate node in the outer boundary for data transmission.

Step 3: Next node estimation using Neighbor: Thus, based on the above four conditions, the source node chooses the neighbor for the data transmission.

Step 4: Continue until reaching the sink node: The above mentioned steps continue till the data packet reaches the sink node.

Thus, the data routing through the proposed SS-Coot based routing provides the efficient routing of information through the mediate, and the diversion nodes with the longer path assure the back tracing a challenging task for the intruder and hence it provides the privacy preservation of the source location.

5. RESULTS AND DISCUSSION

The proposed SS-Coot based privacy preservation of the source location through the routing protocol is analyzed in this section.

5.1. Experimental Setup

The implementation of the proposed SS-Coot-based privacy preservation of the source location is employed in PYTHON in Windows 10OS, 8GB RAM PC.

5.2. Performance Metrics

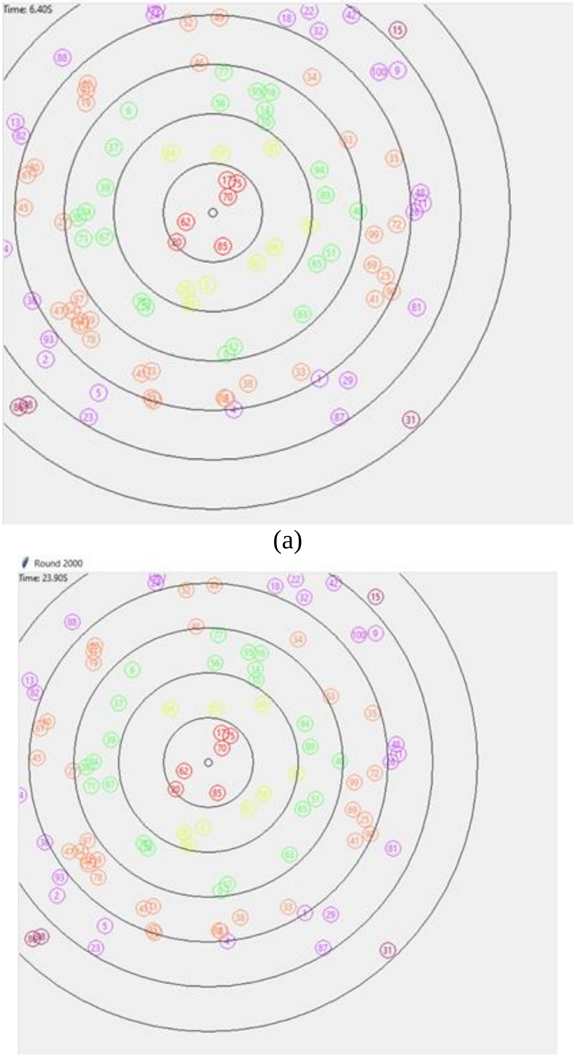
The Packet Delivery Ratio (PDR), Throughput, Energy Consumption, and Delivery Latency are utilized for the analysis of the proposed SS-Coot-based privacy preservation of the source location. The explanation of the PDR, throughput, and energy consumption are detailed in equation (2), equation (3), and equation (4) of section 4.3. The delivery latency is detailed below.

Delivery latency: The time elapsed between the sink node from the source node while exchanging the information is estimated through the delivery latency and is expressed as in equation (31),

$$Latency_{delivery} = T_t - A_t \qquad (31)$$

Where, the delivery latency is notated as $Latency_{delivery}$, the time taken by the source to reach the sink is notated as T_t, the actual targeted time is notated as A_t.

5.3. Experimental Analysis



(a)

(b)

Figure 5 Simulation Result of Proposed SS-Coot-Based Privacy Preservation of Source Location

Figure 5 portrays the simulation of the proposed SS-Coot based source location privacy preservation, in which Figure 5 (a) and 5(b) shows the network with various regions in inner and outer boundary. The simulation results depicts the sink node with three inner boundary regions and three outer boundary regions as explained in the network initialization detailed in section 4.1. The larger circles portray the boundary regions, wherein the smaller circles indicate the nodes in the network with its ID. The centre small node illustrates the sink node of the network.

5.4. Comparative Methods

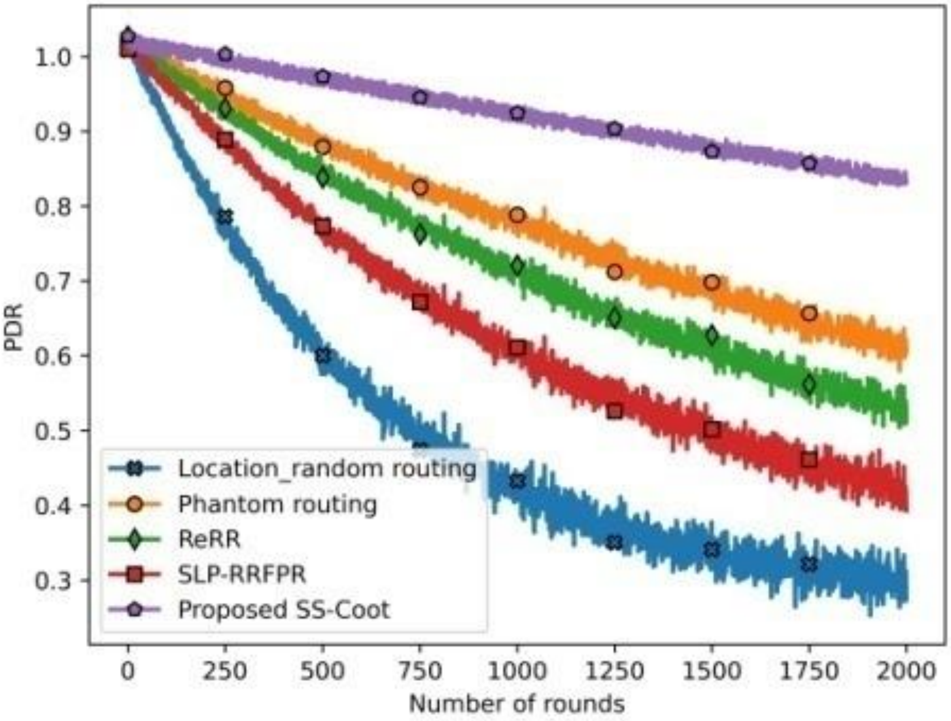
The SS-Coot-based privacy preservation of the source location is compared with the traditional methods like Location_random routing [1], Phantom routing [2], ReRR [3], and source location privacy protection scheme based on random ring and limited hop fake packet routing (SLP_RRFPR) [4].

5.5. Comparative Analysis

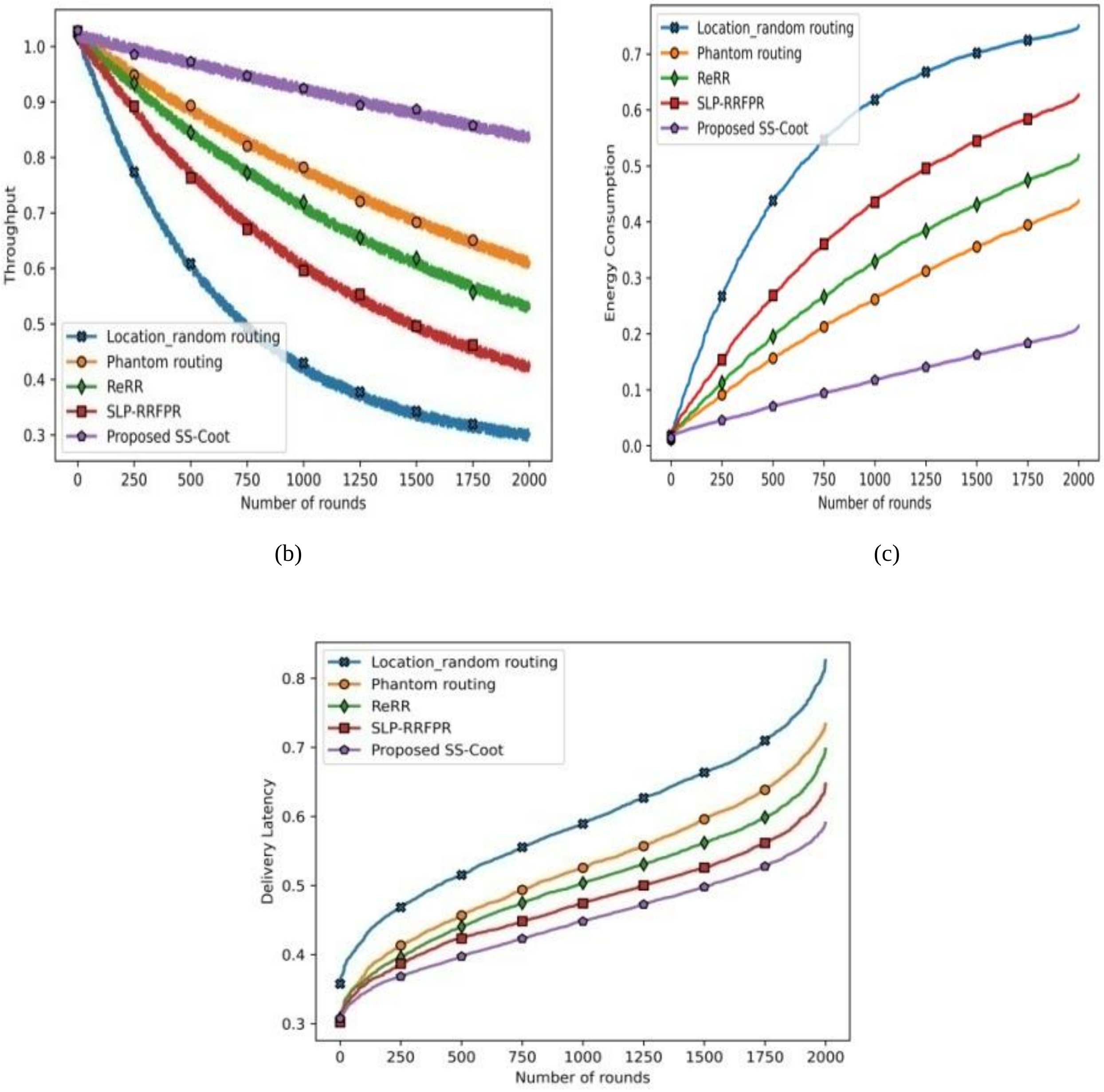
By varying the nodes of the network with 100 nodes, 150 nodes, and 200 nodes, the proposed SS-Coot-based privacy preservation of the source location is analyzed with the traditional method based on the performance metrics.

5.5.1. With 100 Nodes

The SS-Coot-based source location preservation using 100 nodes in the network is shown in Figure 6. The PDR is shown in Figure 6(a), the throughput in Figure 6(b), the Energy consumption in Figure 6(c) and finally delivery ratio in Figure 6(d). For the 120th round, the PDR acquired by SS-Coot is 1.0116, which is 12.11%, 1.67%, 3.34%, and 5.41% enhanced performance compared to Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods. Using 100th round, the throughput acquired by SS-Coot is 1.0016, which is 9.09%, 1.03%, 1.58%, and 3.44% enhanced performance compared to Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods. The energy consumption with 277th round is 0.04816, which is 83.38%, 50.29%, 60.48%, and 71.14% enhanced performance compared to Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods. The delivery ratio with 184th round is 0.3607, which is 20.46%, 9.27%, 6.21%, and 3.34% enhanced performance compared to Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods.



(a)



(b)

(c)

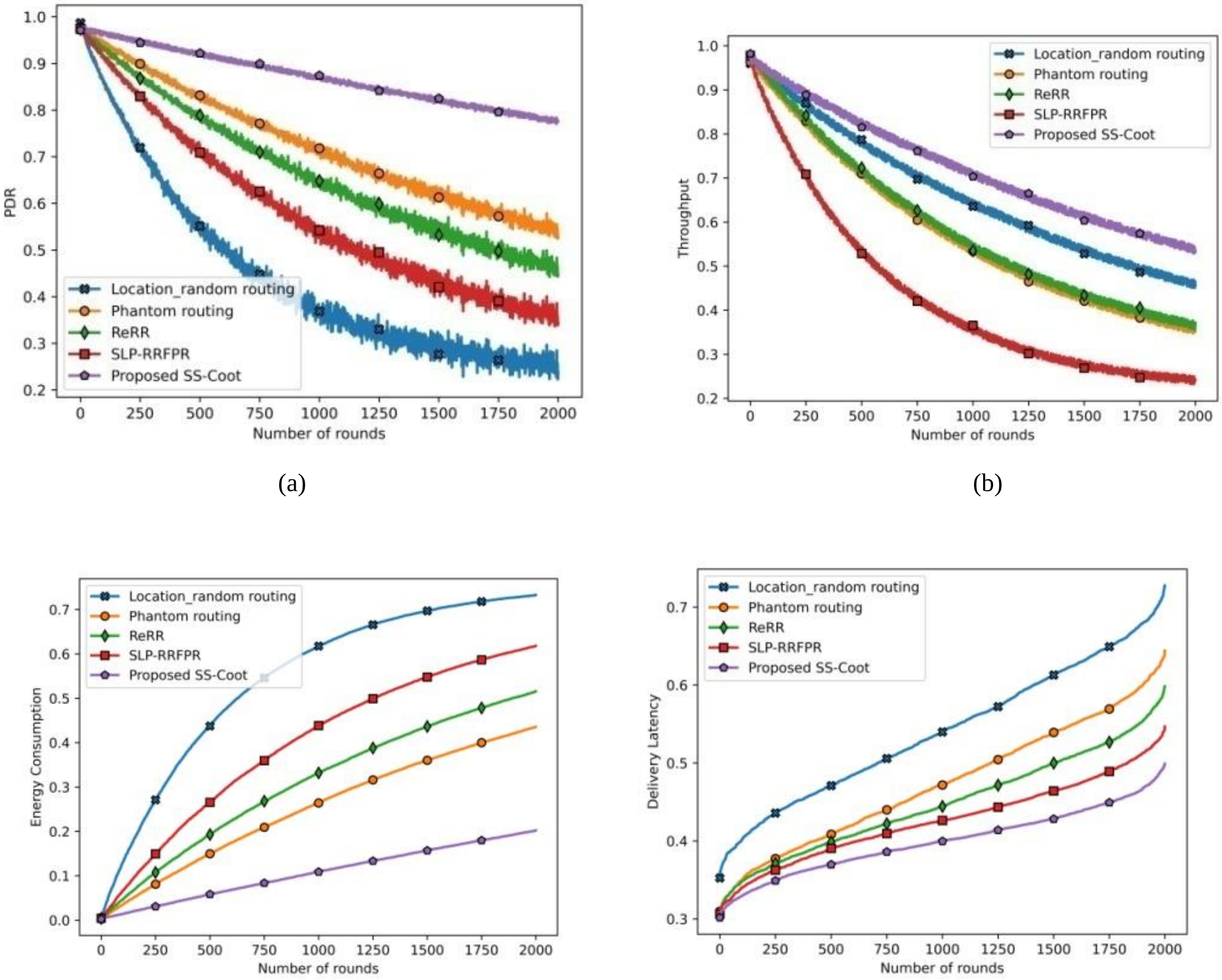
(d)

Figure 6 Analysis Using 100 Nodes Using a) PDR, b) Throughput, c) Energy Consumption and d) Delivery Latency

5.5.2. With 150 Nodes

The SS-Coot based source location preservation using 150 nodes in the network is shown in Figure 7. The PDR is shown in Figure 7(a), the throughput in Figure 7(b), the Energy consumption in Figure 7(c) and finally delivery ratio in Figure 7(d). The PDR obtained by SS-Coot is 0.9155 at 500th round that is higher that related methods like Location_random routing, Phantom routing, ReRR, and SLP_RRFPR with the percentage of 38.73%, 9.38%, 13.74%, and 20.69% respectively. The SS-Coot accomplished higher performance than Location_random routing, Phantom routing, ReRR, and SLP_RRFPR with the value of 0.7895 throughput for its 600th round, where the percentange enhancement is 4.48%, 14.91%, 13.54%, and 38.57% respectively. The delivery latency with

700th round is 0.3822, which is 23.20%, 12.00%, 8.35%, and 5.75% enhanced performance compared to Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods. 0.08836 energy consumption is generated by the SS-Coot in its 800th round, which is 84.30%, 59.73%, 68.49%, and 76.51% enhanced performance compared to Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods.



(a)

(b)

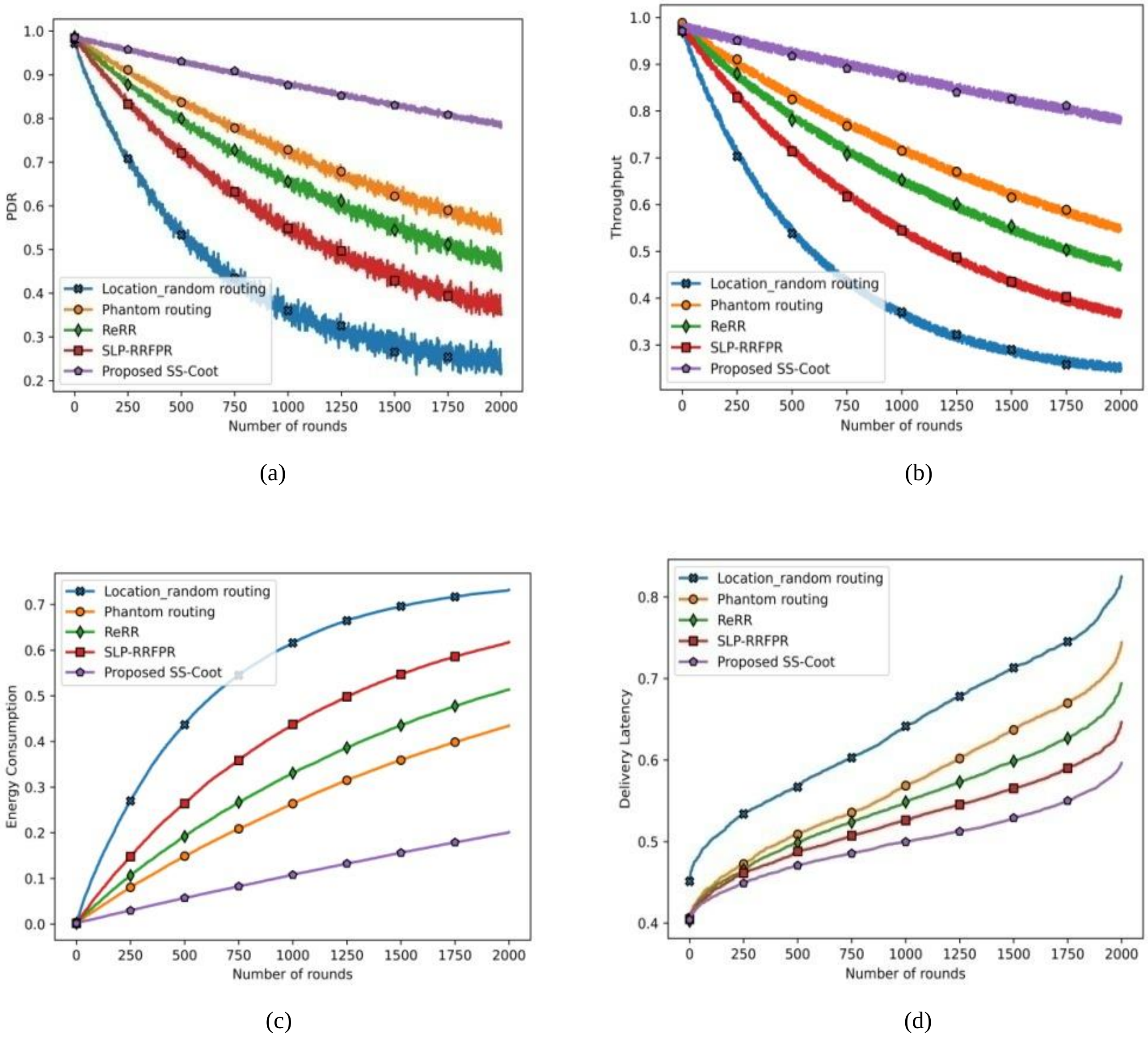
(c)

(d)

Figure 7 Analysis Using 150 Nodes Using a) PDR, b) Throughput, c) Energy Consumption and d) Delivery Latency

5.5.3. With 200 Nodes

The SS-Coot based source location preservation using 200 nodes in the network is shown in Figure 8. The PDR is shown in Figure 8(a), the throughput in Figure 8(b), the Energy consumption in Figure 8(c) and finally delivery ratio in Figure 8(d). The SS-Coot acquired 0.8789 PDR in 1000th round, which is 58.63%, 18.27%, 25.81%, and 38.08% enhanced performance compared to Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods. Likewise, 0.8238 throughput at 1500th round is acquired by SS-Coot that is 65.34%, 23.80%, 34.81%, and 48.24% enhanced performance compared to Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods. The delivery latency with 1750th round is 0.5497, which is minimal than related Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods with the percenmtage of 26.23%, 17.91%, 12.26%, and 6.81% respectively. At 2000th round, the energy consumption accomplished by the SS-Coot is 0.20108, which is 72.53%, 53.72%, 60.85%, and 67.44% enhanced performance compared to Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods.



(a)

(b)

(c)

(d)

Figure 8 Analysis Using 200 Nodes Using a) PDR, b) Throughput, c) Energy Consumption and d) Delivery Latency

5.6. Comparative Discussion

The best measures evaluated by the proposed SS-Coot method along with the comparative methods, are presented in Table 1. The maximal PDR acquired by the SS-Coot-based source location privacy preservation is 1.02867 with 100 nodes in the 9th round, which is 2.65%, 1.26%, 1.32%, and 0.70% better than Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods. The maximal throughput obtained by SS-Coot is 1.02909 with 100 nodes in the 1st round, which is 0.60%, 0.87%, 1.21%, and 0.20% better than Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods. The minimal energy consumption obtained by SS-Coot is 0.30171 with 150 nodes in the 1st round, which is 14.39%, 2.56%, 0.98%, and 1.46% better than Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods. The minimal delivery latency obtained by SS-Coot is 0.00165 with 200 nodes in the 1st round, which is 50.64%, 22.31%, 2.36%, and 1.12% better than Location_random routing, Phantom routing, ReRR, and SLP_RRFPR methods. Thus, the proposed method obtained enhanced performance compared to all the other comparative methods.

Table 1 Comparative Analysis

Round	Method/Metrics	Location_random routing	Phantom routing	ReRR	SLP-RRFPR	Proposed SS-Coot
Using 100 Nodes						
9	PDR	1.00141	1.01567	1.01504	1.02144	1.02867
1	Throughput	1.0229	1.02016	1.01662	1.027	1.02909
1	Energy consumption	0.35763	0.30698	0.30785	0.30178	0.30755
1	Delivery Latency	0.01887	0.01086	0.01391	0.01598	0.0141
Using 150 Nodes						
6	PDR	0.9739	0.97779	0.96885	0.96686	0.97911
1	Throughput	0.95975	0.96288	0.97504	0.97812	0.98207
1	Energy consumption	0.35244	0.30963	0.30469	0.30618	0.30171
1	Delivery Latency	0.00487	0.00259	0.00411	0.00428	0.00242
Using 200 Nodes						
8	PDR	0.96109	0.98571	0.98415	0.98024	0.98784
3	Throughput	0.97515	0.97391	0.98226	0.98128	0.98942
1	Energy consumption	0.45127	0.40657	0.40251	0.40477	0.40429
1	Delivery Latency	0.00334	0.00212	0.00169	0.00167	0.00165

6. CONCLUSION

This research introduced a privacy preservation method for source location preservation using the source-aware routing protocol to confuse the intruder in backtracing from the sink to the source node to avoid the eavesdropping of information. For this, a hybrid optimization named SS-Coot is utilized for the network initialization to route the data packet in a secure manner. The SS-Coot is designed based on the foraging behavior of the Coot, in which the herding behavior of the shepherd is based on the animal communities instinct to enhance the exploration. The SS-Coot has a balanced phase of diversification and intensification that helps to obtain a better solution for solving the optimization issue through the global best solution. Besides, the secure information exchange through the routing protocol with four phases helps to provide secure information sharing. The performance of the SS-Coot is evaluated in terms of PDR, throughput, Energy consumption, and delivery ratio and accomplished the higher value of PDR and throughput as 1.02867, and 1.02909 and the minimal value of Energy consumption, and delivery ratio as 0.30171, and 0.00165, respectively. The delivery latency of the method is higher, which will be minimized in the future using the novel framework with an enhanced routing strategy for source location privacy preservation.

REFERENCES

[1] Elshrkawey, M., Elsherif, S.M. and Wahed, M.E., "An enhancement approach for reducing the energy consumption in wireless sensor networks", Journal of King Saud University-Computer and Information Sciences, vol.30, no.2, pp.259-267, 2018.

[2] Babu, M.V., Alzubi, J.A., Sekaran, R., Patan, R., Ramachandran, M. and Gupta, D., "An improved IDAF-FIT clustering based ASLPP-RR routing with secure data aggregation in wireless sensor network", Mobile Networks and Applications, vol.26, no.3, pp.1059-1067, 2021.

[3] Liu, X. and Wu, J., "A method for energy balance and data transmission optimal routing in wireless sensor networks", Sensors, vol.19, no.13, pp.3017, 2019.

[4] Fu, X., Yang, Y. and Postolache, O., "Sustainable multipath routing protocol for multi-sink wireless sensor networks in harsh environments", IEEE Transactions on Sustainable Computing, vol.6, no.1, pp.168-181, 2020.

[5] Wang, F., Liu, W., Wang, T., Zhao, M., Xie, M., Song, H., Li, X. and Liu, A., "To reduce delay, energy consumption and collision through optimization duty-cycle and size of forwarding node set in WSNs", IEEE Access, vol.7, pp.55983-56015, 2019.

[6] Mutalemwa, L.C. and Shin, S., "Novel Approaches to Realize the Reliability of Location Privacy Protocols in Monitoring Wireless Networks", IEEE Access, vol.9, pp.104820-104836, 2021.

[7] Arivarasi, A. and Ramesh, P., "An improved source location privacy protection using adaptive trust sector-based authentication with honey encryption algorithm in WSN", Journal of Ambient Intelligence and Humanized Computing, pp.1-13, 2021.

[8] Chen, Y., Sun, J., Yang, Y., Li, T., Niu, X. and Zhou, H., "PSSPR: a source location privacy protection scheme based on sector phantom

routing in WSNs", International Journal of Intelligent Systems, vol.37, no.2, pp.1204-1221, 2022.

[9] Naghibi, M. and Barati, H., "EGRPM: Energy efficient geographic routing protocol based on mobile sink in wireless sensor networks", Sustainable Computing: Informatics and Systems, vol.25, pp.100377, 2020

[10] Manjunath, DR and Kumar, A., "Source Location Privacy for Geographical Routing in Wireless Sensor Networks: SLPGR", International Journal of Computer Networks and Applications, vol.8, no.4, pp.422-434, 2021.

[11] Tan, W., Xu, K. and Wang, D., "An anti-tracking source-location privacy protection protocol in WSNs based on path extension", IEEE internet of things journal, vol.1, no.5, pp.461-471, 2014.

[12] Jiang, J., Han, G., Wang, H. and Guizani, M., "A survey on location privacy protection in wireless sensor networks", Journal of Network and Computer Applications, vol.125, pp.93-114, 2019.

[13] Long, J., Dong, M., Ota, K. and Liu, A., "Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks", IEEE Access, vol.2, pp.633-651, 2014.

[14] Kamarei, M., Patooghy, A., Alsharif, A. and Hakami, V., "SiMple: A unified single and multi-path routing algorithm for wireless sensor networks with source location privacy", IEEE Access, vol.8, pp.33818-33829, 2020.

[15] Xiong, Z., Wang, H., Zhang, L., Fan, T. and Shen, J., "A ring-based routing scheme for distributed energy resources management in iiot", IEEE Access, vol.8, pp.167490-167503, 2020.

[16] Gu, C., Bradbury, M. and Jhumka, A., "Phantom walkabouts: A customisable source location privacy aware routing protocol for wireless sensor networks", Concurrency and Computation: Practice and Experience, vol.31, no.20, pp.e5304, 2019.

[17] Chakraborty, S., Goyal, N.K., Mahapatra, S. and Soh, S., "Minimal path-based reliability model for wireless sensor networks with multistate nodes", IEEE Transactions on Reliability, vol.69, no.1, pp.382-400, 2019.

[18] Shukla, A., Singh, D., Sajwan, M., Kumar, M., Kumari, D., Kumar, A. and Panthi, M., "SLP-RRFPR: a source location privacy protection scheme based on random ring and limited hop fake packet routing for wireless sensor networks", Multimedia Tools and Applications, pp.1-41, 2022.

[19] Mutalemwa, L.C. and Shin, S., "Secure routing protocols for source node privacy protection in multi-hop communication wireless networks", Energies, vol.13, no.2, pp.292, 2020.

[20] Naruei, I. and Keynia, F., "A new optimization method based on COOT bird natural life model", Expert Systems with Applications, vol.183, pp.115352, 2021.

[21] Kaveh, A. and Zaerreza, A. (2020), "Shuffled shepherd optimization method: a new Meta-heuristic algorithm", Engineering Computations, Vol. 37 No. 7, pp. 2357-2389.

[22] Mutalemwa, L.C. and Shin, S., "Strategic location-based random routing for source location privacy in wireless sensor networks", Sensors, vol.18, no.7, pp.2291, 2018.

[23] Kamat, P., Zhang, Y., Trappe, W. and Ozturk, C., "Enhancing source-location privacy in sensor network routing", In 25th IEEE international conference on distributed computing systems (ICDCS'05), pp. 599-608, June 2005.

[24] Zhang, J., Tang, J. and Wang, F., "Cooperative relay selection for load balancing with mobility in hierarchical WSNs: A multi-armed bandit approach", IEEE Access, vol.8, pp.18110-18122, 2020.

Authors

Ms. Chinnu George, is a Research Scholar at Dayananda Sagar University, Bangalore. She has pursued her B.E in Computer Engineering from Shree Rayeshwar Institute of Engineering and Information Technology, Goa University in the year 2011. She has completed her MTech in Network and Internet Engineering from Karunya University in the year 2013.Her research interest is Wireless sensor networks, Data Analytics. She has published several international papers.

Dr. Gayathri K M is an Associate Professor in the Department of Electronics and Communication Engineering, School of Engineering, Dayananda Sagar University, Bangalore. She has obtained her bachelor’s degree in Medical Electronics from VTU, Bangalore in the year 2009. She has obtained her Master’s Degree in VLSI and Embedded Systems from VTU, Karnataka in the year 2011. Awarded PhD in 2018 from JAIN (Deemed-to-be University). She is having 9 years of teaching experience and 4 years of industry experience. She has published 20 research papers in both International and National Journals and presented papers in conferences. She has guided UG and PG students for their academic projects. Her areas of interest are VLSI, Wireless Communication, Satellite Communication and Navigation Systems. She was working as Principle Investigator for ISRO funded projects.

Dr Reeja S R, is a Professor in the Department of Computer Science and Engineering, VIT- AP University, She earned her Ph.D in Computer Science & Engineering from Visvesvaraya Technological University (VTU), Govt. of Karnataka for her thesis Real Time Video Denoising. She has nearly 12 years of teaching experience in various engineering colleges and 5 years of research experience in the concerned field. She has worked in VSSC/ISRO as a Research Assistant in QRSG (Quality Assurance & Reliability Software & mission Group) for 1 year.

How to cite this article:

Chinnu Mary George, Gayathri K M, Reeja S R, “Hybrid Optimization Enabled Routing Protocol for Enhancing Source Location Privacy in Wireless Sensor Networks”, International Journal of Computer Networks and Applications (IJCNA), 10(1), PP: 51-67, 2023, DOI: 10.22247/ijcna/2023/218511.