International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/210722 Volume 8, Issue 6, November – December (2021)

RESEARCH ARTICLE

Efficient and Reliable Routing With Cloud Based Source-Location Privacy Protection in Wireless Sensor Networks

R. Nagarajan
Department of Computer Science, Sri Ramakrishna College of Arts and Science, Coimbatore, Tamil Nadu, India
rnagarajan.snr@gmail.com

G. Maria Priscilla
Department of Computer Science, Sri Ramakrishna College of Arts and Science, Coimbatore, Tamil Nadu, India
mariajerryin76@gmail.com

Received: 17 September 2021 / Revised: 21 October 2021 / Accepted: 09 November 2021 / Published: 30 December 2021

Abstract – WSNs (Wireless Sensor Networks) have recently gained popularity. WSNs are typically deployed in insecure, unstructured areas where their source location reveals critical information about targets. Sensor deployment in WSNs has been seen in a variety of applications that oversee events and send information to base stations. Optimal route selection and source location privacy are critical issues in WSNs. If an intruder determines the source node by studying traffic mode, an attack could be conducted on a target with ease. Previous methods were based on MSROs (Mobile Sink-based Route Optimizations) and Cloud-Based WSN Protection Schemes. This research work chooses the optimum multi-sink node based on the BFAs (Bacteria Foraging Algorithms). But, it does not yield optimal paths to balance the PDRs (Packet Delivery Ratios) and energy dissipation. To seek a solution to this issue, this study proposes ERR-CSLPPs (Efficient and Reliable Routing with Cloud-based Source-Location Privacy Protections) using AAFBOA (Adaptive Adjustment Factor based Butterfly Optimization Algorithm), allowing the approach to choose the mobile sink node. Depending on the ETCs (Expected Transmission Counts), residual energy, and hop count, the optimal paths are chosen with the help of TOPSISs for efficient transmissions. The actual packets are sent over the preferred path. Next, the cloud-like false hotspot is formed to include counterfeit packets into the WSN to confuse the intruder and yield an elaborate privacy location. Counterfeit packets are included along the delivery path of the actual data packet to extend the time needed for tracing the traffic flow. The experiments reveal that the proposed system yields improved performance when matched with the earlier system in terms of overall energy dissipation, node utilization ratio, transmission delay, security, and network lifetimes.

Index Terms – Cloud Center, Mobile Sink, Adaptive Adjustment Factor, Fake Hotspot and Technique for Order Preference by Similarity to Ideal Solution.

1. INTRODUCTION

WSNs include many sensor nodes installed in remote target locations for data collection, processing, and communication to Base Station (BS) [1]. The sensor nodes largely represent WSNs. The sensor nodes' different features include portability, a low battery capacity, insufficient computing power, restricted memory and communication range, and so on [2]. WSNs are employed in monitoring applications in various ways, ranging from safety-oriented surveillance applications like asset monitoring, army, healthcare, radiation monitoring to non-critical applications like temperature and humidity management [3]. In safety-critical monitoring applications, it is critical to guarantee that data is securely transmitted among sensor nodes and that data like the asset location that is being watched is maintained secret [4-5].

In WSNs, several research directions range from corporeal design, routing mechanism, power management processes, security concerns, and sensing capacity of sensor nodes. The lifespan of the sensor nodes is a major challenge for WSNs since the power resources of sensor nodes are limited [6]. Routing protocol has a pivotal role to play in the lifespan of the sensor nodes. Routing in WSN is very different from other wireless networks due to its different distinct characteristics of sensor nodes such as energy limitations, processing capabilities, the transmission of information gathered from different nodes to a single base station, the uncertainty of global address, and random installation of sensor nodes, etc. To balance these kinds of characteristics, various kinds of routing protocols were designed. The routing protocol will choose the path from source to destination in the best-effort delivery model [7]. WSNs work in broadcast mode, with packets being transferred from source nodes to the sink using

RESEARCH ARTICLE

multi-hop communications the goal of these routing protocols is to attain energy competence and spread total network life spans. WSNs sensor node display communication behavior making it critical to maintain location information of the source node confidential since revealing this information to snooping adversaries helps them trace packet routes and source nodes in the network [8]. Source location privacy protection refers to keeping a source node's location information hidden from intruders [9]. Existing source node location privacy protection methods like cyclic entrapments [10], false data sources [11], phantom routings [12], and others assist in securing source position's privacy by enhancing path lengths or difficulty. Though these methods improve security in WSNs, they sacrifice network performances (increased communication complexities with reduced network stability). But, the overhead in communication constitutes the highest energy dissipation and is more compared to the computational complexity [13].

The primary contribution made by the proposed work is to develop an ERR-CSLPPs technique to attain an improved packet delivery ratio, network lifespan, and security. The proposed approach randomly chooses a sink from several sinks by employing Adaptive Adjustment Factor-based Butterfly Optimization Algorithm. The choice of sink helps modify the conventional traffic mode; changed traffic flow helps deal with the issue of a back-tracing attack. The use of TOPSISs helps achieve effective packet transmissions. Subsequently, the network generates cloud-shaped false hotspots and falsified branches so that the traffic pattern is made complex. The scene can also prolong the time for which the targets can be protected. It boosts energy efficiency to the maximum extent possible when guaranteeing the level of security.

The next sections of the work are systematized as given. In section 2, the overview of existing works on source location protection and path selection is provided. Section 3 describes the proposed ERR-CSLPPs technique. Section 4 discusses the simulation results of different approaches compared with various algorithms in terms of different metrics. Finally, Section 5 provides the conclusion of the technical work.

2. RELATED WORK

Here, review the advantages and disadvantages of the cloud-based source-location privacy safety in WSNs. Yao et al (2015) introduced a mechanism for safeguarding the source–location confidentiality based on a new application about the multiring topology. The study's source nodes select two arbitrary rings, one from their external rings and the other from internal rings, and two random angles totalling 180 degrees for packets to produce equally distributed traffic patterns in the network. Packets are then sent in any of the angles in each ring. The scheme also introduced false packets for route diversity and extended attack moments which can be defined as the time taken by an intruder to locate the source successfully. Their approaches protected source nodes from being traced and were also effective against traffic analysis attacks. Their results showed that their proposed approach could achieve improved spatial traffic uniformity and increased attack time, in addition to a moderate rise in hop count and energy dissipation [14].

Han et al (2019) presented an approach that depends on CPSLP to deal with the source location privacy problem. The researchers recommended an approach, which makes random modifications to the packet destinations during every transmission. Moreover, multiple sinks are used for forming several paths. Inclusion of an intermediate node makes the path have high randomness and flexible. Later, the cloud-like false hotspot is made to insert counterfeit packets into WSN so that intruders' will be confused and yield an elaborate privacy location. Every useful packet is routed via a path, which is very hard for the hotspot-finding opponent to locate in a straightforward manner. The results of the simulation show that the CPSLP approach can avoid intrusive seize and have a better degree of privacy protection simultaneously. The energy dissipation in this approach has very less effect on the network lifespan in comparison with a cloud-oriented approach and all-direction arbitrary routing approach [15].

Mutalemwa, L. C., and Shin, S. (2018) proposed a technique to safeguard source position's privacy with the use of arbitrary routing algorithms. Their random routing of packets from source to sink node is tactically positioned or mediated or diverted nodes to improve privacy. Node's positions influenced discretionary selections for mediations or diversions of nodes. Their scheme relayed packets in different portions of the network based on the position of originating nodes. The study's scheme ensured that subsequent packets were sent through dissimilar routing pathways, making it exceedingly difficult for attackers to trace originating node positions. The results of the simulation showed that the proposed approach helps in confusing the adversary strongly and yields better source location privacy so that its performance is better than other routing-based source location privacy approaches [16].

Sobral et al. (2013) used a fuzzy inference strategy to assist directed diffusion routing, which selected interaction paths amongst the system's nodes. The study's alternative methodology selected an ideal path depending on the fuzzy inference method and ACOs. The former determined a path's class depending on the number of hops and restricted power usage between nodes in the path. ACOs modified standard fuzzy frameworks to enhance path characterizations and increase energy efficiency and network's lifespan. Their results showed the scheme's efficiency in terms of energy, quantity of received packets, and the cost of received packets [17].

RESEARCH ARTICLE

EGRPM was developed by Naghibi and Barati (2020) for WSNs. The study divided the network geographically into numerous cells, and two mobile sinks were used to aggregate data from cell nodes. The study classified Cells into two types based on how they communicated with mobile sinks namely SCCs (Single-hop Communication Cells) and MCCs. Mobile sinks travelled in two concentric diamond-shaped circles, covering half of the network at any given moment. Initially, both sinks moved in one direction and stayed in the orbits' corners at certain periods to gather data from sensor nodes. SCCs directly sent data to static sinks, whereas MCCs transported data to mobile sinks using their suggested EGRPM algorithm. The performance of EGRPM resulted in a significant reduction of average energy dissipation and data delivery delay, leading to significant improvements in packet delivery rates and network lifespans [18].

Fu and He (2020) proposed an energy-efficient data collecting technique called (BIIE (Balanced Inter-cluster and Inner-cluster Energies) to extend network lifespan. Suggested BIIE was an enhanced hierarchical clustering method for reducing transmission costs. The scheme achieved energy balance amongst clusters by selecting the best RNs (Rendezvous Nodes) in clusters and building the mobile sink's routing path to reach all RNs using PSOs (Particle Swarm Optimizations). A local re-clustering approach based on remaining energy in sensor nodes balanced inner cluster energies. Their findings show the efficiency of suggested BIIE in increasing network lifespans [19].

In asynchronous WSNs, Cheng et al [20] (2019) developed a fast and efficient broadcast (FEB) protocol with a mobile sink. Examine the mobile sink's movement pattern and its travel speed. Furthermore, within two hops, examine the broadcast procedure, node position, and neighbour coverage information, and then provide an efficient broadcast method for mobile sink, as well as a heuristic movement approach. The suggested broadcast method must exchange node coverage information before transmission starts to eliminate the redundant packet transmissions. The suggested moving pattern strategy reduces network broadcast delay by moving the mobile sink to monitoring areas, where the broadcast process covers fewer nodes. The suggested technique considerably decreases broadcast delay and energy usage, according to simulation findings.

The energy balanced method in mobile WSNs redeployment has been studied by Ye et al [21] (2014). To increase the deployment's QoS, the virtual force method with an extended virtual force model is employed. An energy model is included to increase or limit the mobility of the nodes, allowing the energy of the entire WSN to be balanced and the network's lifetime to be extended. The simulated results show that the suggested technique is successful. Relying on Four Quadrants Deployment Model (FQDM), Al-Tabbakh et al [22] presented a self-deployment heuristic method for WSN. It investigates the impact of adding a realistic energy model to FQDM and suggests an expanded version of FQDM to improve border coverage. The suggested method relocates the sensors in a way that increases coverage whilst consuming the least amount of energy. The findings indicate that it provides good coverage for a specific region whilst conserving sensor energy.

2.1. Problem Identification

From the above discussion, it is identified that the existing techniques developed an optimal route selection and source location privacy methods in WSNs. If an intruder determines the source node by studying traffic mode, an attack could be conducted on a target with ease. Previous methods were based on MSROs (Mobile Sink-based Route Optimizations) and Cloud-Based WSN Protection Schemes. In this research work, the optimum multi sink node is chosen based on the BFAs (Bacteria Foraging Algorithms). But it does not yield optimal paths to balance the PDRs (Packet Delivery Ratios) and energy dissipation. So, the major objective of this work is to develop a WSN network model with source-location privacy protection in a cloud environment. Moreover, the Quality of Service (QoS) parameters are satisfied during data transmission with higher energy consumption, delay and network lifetime. The formulation of this proposed approach is carried out using a butterfly optimization approach.

3. PROPOSED METHODOLOGY

The proposed system developed ERR-CSLPPs to improve WSN's performances. The proposed system includes a network model, mobile sink selection, path selection and intermediate node, actual packet transmission, and construction of a cloud (which provides for fake packet broadcast and cloud center choice). Figure 1 shows the flow diagram of the proposed work.

3.1. Network and Adversary Model

The proposed system is developed with its modelling depending on the panda-hunter game. Authors assume that numerous sink nodes exist in-network to preserve the energy and enhance privacy protection capability instead of just a single sink. The proposed technique aims to prevent the attackers from being capable of examining the real packet transmission employing false traffic flow and averts them from getting the information on the positions of pandas. The assumptions on the proposed network model are given as,

Adversary model: A typical environment is illustrated in Figure 2. An intruder makes his best attempts to track the packet flow so that the location of the panda can be determined. This way, it can get considerable information regarding the target. Also, the intruder only makes passive attacks, indicating that it could monitor the packets. A passive

RESEARCH ARTICLE

attack would not obstruct the transmission happening among nodes or damage to any device. At first, the intruders are installed around the sinks. These sinks constitute the destinations for all the packets, and therefore the intruder will identify the packet flow and then track it by sequential hops to compute pandas. In this technical work, the adversaries are expected to wage the attack mode as provided as follows:

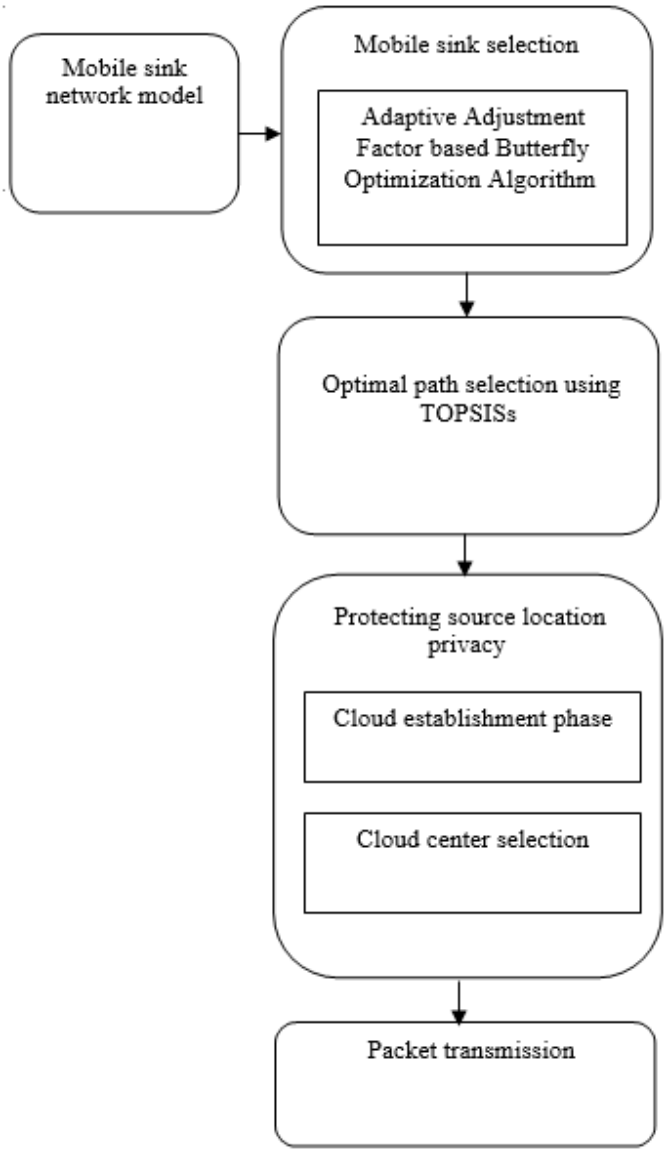

Figure 1 Flow Diagram of the Proposed Work

(1) Hotspot-locating attack: Once the panda appears, the source node generates multiple packets within a less amount of time. The packet transmission rate around the panda is found to rise instantly. The region that has high traffic is called a hotspot. An increased probability exists that the hotspot's centre makes the source node. By measuring the direction and wireless signal strength, the adversary can identify the packet's sender. Next, it travels towards the direction of the hotspot. The above-stated process will be performed again and again till the source node is identified.

(2) Back-tracing attack: As observed in Figure 2, when the intruder seizes three packet transfers, it will identify the target. This sort of intruder tracks the packet hop-by-hop using time correlation, content correlation, and inferences of data transmission rates. Hence, back-tracing helps the intruder to distinguish the sender and then traverses towards the location of the source. The intruder will continue the detection process till it successfully finds the source node.

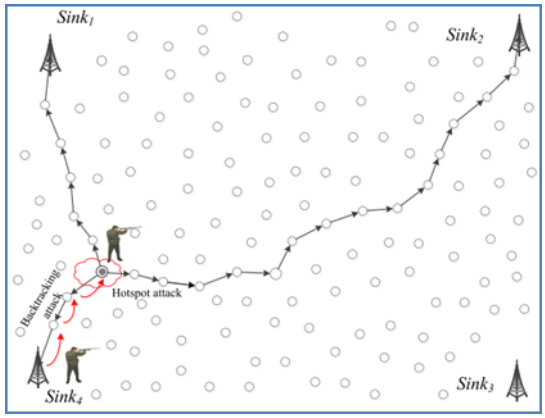

Figure 2 Backtracking and Hotspot Attack Utilized via Adversaries

Once the nodes are installed, every sink transmission starts beacon, which includes its position, sink ID, etc. When the node understands the sink coordinates, calculate the distance to every sink becomes easy. A neighbor list is defined by the hop count.

3.2. Selection of the Sink Node

In this proposed research work, AAFBOA (Adaptive Adjustment Factor based Butterfly Optimization Algorithm) is used for choosing the sink node for transmitting the packet. While a panda appears at a specific time and location, the source node starts broadcasting event packets to the sink. One crucial strategy that works well for source nodes is changing the eventual destination for each cycle. As a result, the source node uses a mechanism known as the destination sink to pick the ultimate destination sink of the current round. The cloud-based approach assigns a value to sink 'i' to determine which sink is chosen as destination sink, represented by $T(s_i)$. Assuming the distance among source and sink i is d, every sink computer $T(s_i)$ for a current period as shown below equation (1).

$$T(s_i)=\left[\gamma \times \frac{E_{ave-res_i}}{\sum_{i=1}^{4} E_{ave-res_i}} + (1-\gamma) \times \left(1-\frac{d_{s_i}}{\sum_{i=1}^{4} d_{s_i}}\right) \times \alpha \times \beta\right] \quad (1)$$

RESEARCH ARTICLE

Where, α specifies if $sink_i$ has been selected in the earlier transfer wherein α = 0 in the current round; else, α = 1, thus ensuring sinks are not selected repeatedly as the destination sink. When $d_{s_i}$is small, it is easy for intruders to find source locations using back-tracing attacks and hence the shortest distance of nodes transferring events is represented as d_s^{min}. When d_{s_i}>d_s^{min}, β = 1 and $d_{s_i} \leq d_s^{min}$, β = 0. It ensures the probability value of sink to get selected as destination sink is 0, since the use of β ensures packets reach protected locations. The length of d_s^{min} is linked to intermediate node's location and $E_{ave-res_i}$ depicts average residual energy of neighboring nodes to $sink_i$. γ is weight coefficient that balances distances and residual energies. Increase in the value of γ plays an important role in average residual energy $E_{ave-res_i,}$ choosing the destination sink, so that the selection process becomes more energy-specific. On the contrary, if γ becomes less, then the results of calculation hugely relies on d_{s_i} . The table 1. Specifies the symbols and its notation which is used in this work.

Symbol	Notation
$T(s_i)$	Destination Sink
d_{s_i}	Distance of Source Node i
$E_{ave-res_i}$	Average Residual Energy
f_i	Fragrance Level
S_{max}	Max Walk Step
θ	No. of Hops Required at Each Round

Table 1 Symbols and its Notation

BOAs (Butterfly Optimization Algorithms) are new nature-based meta-heuristics and mimic butterflies' general foraging and mating traits. BOAs model works on the fragrance discharged by butterflies, which is helpful to other butterflies while looking for food and mating partner. These sense receptors assist in the perception of fragrance/smell and are found throughout a butterfly's body. These receptors, known as chemoreceptors, are nerve cells located on the surface of butterflies' body.

In BOAs, butterflies generate a scent strength that correlates to their fitness, i.e., if a butterfly travels from one place to another, its fitness changes. Fragrance spread by butterflies is detected by other butterflies (unique data communication) and creates a collaborative social learning system. When a butterfly detects scent from another butterfly, it will migrate towards it (Global searches). In another case, if a butterfly cannot detect the smell, it will move at random (local searches). Every scent in BOA has its alluring fragrance and distinctive vibe. It is one of the characteristics which distinguish BOAs from other meta-heuristics. For using a specific true goal, BOAs are modified.

The entire idea of differentiating and using the procedure depends on three basic factors, namely stimulus intensity (I), sensory modality (c), power exponent (PE). Sensory modality approaches make tangible attempts to measure energy type with the raw information used by sensors and process it in various. Currently, other modalities might include temperature, light, and sound, and in BOA, the modality represents the scent released by the butterfly, where 'i' stands for the physical stimulation degree and is connected to the fitness of a solution/butterfly in BOAs. Sink nodes are viewed as butterflies, and T(s_i) stands for the objective function in this study. This implies that when a butterfly emits a detectable amount of scent, arbitrary butterflies in the vicinity can identify it and be drawn towards the butterfly. The butterfly power or solution is referenced to as a rise in intensity, while a refers to the parameter that considers normal expressions. Researchers conducted several tests on bugs, animals, as well as people for stimulus estimates, and it is told that when the amount gets high leveled, insects become less sensitive to environmental changes. In BOA, the scent is calculated using the equation given below equation (2):

$$f=cI^a \qquad (2)$$

Where, f_i implies fragrance level or i_{th} butterfly smells the scent to the degree that it is more grounded, c represents sensory modality, i represents objective function, a represents power exponent based on modality, that is responsible for changing extent of absorption. Algorithm is divided into two stages: global searches and local searches similar to scent rises in a population. Butterflies create scent that can be detected within a region. The sink node travels towards the fittest node g* in the first (global) search phase, which may be expressed as in equation (3),

$$x_i^{t+1} = x_i^t + (r^2 \times g^* - x_i^t) \times f_i \qquad (3)$$

The efficiency for the global and local search capability of the metaheuristic optimization algorithms should have a balance to improve the exploration and exploitation performances at the same time. To increase the global and local search ability, the adaptive adjustment factorα is expressed as in equation (4).

$$\alpha=\gamma^*\frac{S_{max}}{t^2} \qquad (4)$$

S_{max} -max walk step

t-number of the t^{th} iteration

RESEARCH ARTICLE

γ - variable coefficient related to the number of iterations

In favour of global exploration, mathematical expression (3) is re- written as below equation (5):

$$x_i^{t+1} = \alpha * x_i^t + (r^2 \times g^* - x_i^t) \times f_i \qquad (5)$$

Where, x_i^t refers to the solution vector for the i_{th} sink node in iteration number t. g denotes present optimal solution obtained from entire existing solutions in present phase. The fragrance of the i_{th} butterfly computed from f_i, r represents a arbitrary integer between [0, 1]. The neighbourhood (local searches) is denoted as in equation (6),

$$x_i^{t+1} = x_i^t + (r^2 \times x_j^t - x_k^t) \times f_i \qquad (6)$$

Where, x_j^t stands for j_{th} sink node in the search space and x_k^t stands for k_{th} sink node in the search space. If the minimum probability when sink positions are identical to swarm and *r is a* arbitrary value in the interval [0,1], Equation (6) forms a neighborhood arbitrary walk. Butterflies may seek for food and mates both locally and globally. As a result, a switch probability p is utilized as a part of BOAs to transit from regular global searches to focused local searches. The pseudocode of AAFBOA is illustrate in algorithm 1.

Input: Number of sink node

Output: Best sink node

1. Initialize the sink nodes
2. Compute T(s_i)
3. Specify sensor modality *c*, power exponent *a*, switch probability *p*
4. while stop condition not met do
5. for every sink node do
6. Compute fragrance for *bf*
7. end for
8. identify best *bf*
9. for every sink node
10. Form a arbitrary value *r* between [0, 1]
11. if *r* < *p* then
12. Go towards optimal solution applying Eq. (5)
13. else
14. Move arbitrarily using Eq. (6)
15. end if
16. end for
17. modify *c* value
18. end while
19. Best sink node

Algorithm 1 AAFBOA

Source node compares T(s_i) when each packet is to be transmitted. Next, the source node chooses sink with maximum T(s_i) to act as the destination sink.

3.3. Path Selection

Also, this study proposes TOPSISs for choosing the best communication paths. The selection of optimal path directly influences the energy dissipation and performance of the data forwarding process. In this, the paths are chosen by the objective function like ETCs, residual energy and hop count.

3.3.1. ETCs

The ETCs of a link is the anticipated number of data transmissions necessary to transfer a packet over that link, which includes retransmissions. ETCs can be computed as below equation (7):

$$\text{ETCs} = \frac{1}{d_f \times d_r} \qquad (7)$$

Where d_f is the forward delivery ratio, which describes the likelihood of successful packets reaching receivers, and d_r denotes the reverse delivery ratio, which specifies the probability of successfully received ACK packets.

3.3.2. Remaining Energy

Residual energy of a node is also a pivotal measure, and it is specified as the energy dissipated in every node after the present receiving and transmission step. The Residual energy R_e can be computed as:

$$R_e = I_e - (E_t + E_r) \qquad (8)$$

Where,

I_e −Initial Energy

E_t, E_r-energy needed for transmission and receiving correspondingly

3.3.3. Hop Count

The hop count is a vital factor to carry out optimal path selection. To get the hop count, distance among node and sink node must be computed using euclidean distance formulation as given:

$$\text{d(n,s)} = \sqrt{(x_n - x_s)^2 + (y_n - y_s)^2} \qquad (9)$$

here, d(n,s) is equivalent to Euclidean distance among node n and sink node. Also, hop count between node n and sink node is computed as below:

$$hc_n^s = \frac{d(n,s)}{avg(d(n,j))} \qquad (10)$$

RESEARCH ARTICLE

here, $avg(d(n,j))$refers to the average distance among node n and its adjacent nodes (j) distanced by one hop.

TOPSISs introduced in this study select the best way for sending data from sources to destinations. TOPSISs are used for handling issues in MCDM (Multiple Criteria Decision Making) underlying that selected option must have minimum Euclidean distance from PISs and greatest distance from NISs. For example, PISs enhances benefits while decreasing costs, but NISs add complexity while decreasing benefits. Every condition is assumed to be either raised or reduced. TOPSISs is an easy and quick approach for sorting potential alternates for closing in on an optimal solution.

Step 1: Define the decision matrix

Establishing a DM (Decision Matrix) is the first step in the proposed TOPSISs and it is denoted as in equation (11),

$$DM=\begin{array}{c} \\ L_1 \\ L_2 \\ \cdot \\ \cdot L_m \end{array}\begin{array}{c} \begin{array}{cccc} C_1 & C_2 & & C_n \end{array} \\ \begin{bmatrix} X_{11} & X_{12} \ldots & X_{1n} \\ X_{21} & X_{22} \ldots & X_{2n} \\ X_{m1} & X_{m2} \ldots & X_{mn} \end{bmatrix} \end{array} \quad (11)$$

Where "i'refers to the condition index (i = 1 . . . m); m indicates total probable sites and " j' specifies alternatee index (j= 1 . . . n). Elements C_1, C_2…, C_n indicates condition (objective function): whereas L_1, L_2…, L_n specifies number of sensor nodes. The matrix elements are associated with values of condition i corresponding to alternatee j.

Step 2: In the second step of the proposed TOPSISs a normalized DM encompassing nodes and objectives are computed where NDM (Normalized Decision Matrix) represents normalized values, indicating comparative performances of generated alternatives and given by the following equation (12),

$$NDM = R_{ij} = \frac{X_{ij}}{\sqrt{\sum_{i=1}^{m} X^2 ij}} \quad (12)$$

Step 3: TOPSISs generate a weighted decision matrix for sensor nodes as every selection criteria may be equally significant and hence are weighed before being used by AHP (Analytical Hierarchy Process), which measures the selected criterion's significance. This weighted decision matrix is generated by multiplying all elements of normalized decision matrix columns with arbitrary weights that is mentioned in equation (13),

$$V= Vij= Wj\times Rij \quad (13)$$

Step 4: PISs and NISs are found by TOPSISs in step four where positive ideal (S+) and negative ideal (S-) solutions are specified based on weighted decision matrix and given by the following expressions (14),(15)

$$PIS = S^{+}= \{ s_1^{+}, s_2^{+} \ldots\ldots, s_n^{+}\}: \text{where: } s_j^{+}=\{(\max_i (V_{ij}) \quad (14)$$

$$PIS = S^{-}= \{ s_1^{-}, s_2^{-} \ldots\ldots, s_n^{-}\}: \text{where: } s_j^{-}=\{(\min_i (V_{ij}) \quad (15)$$

Here, J corresponds to the beneficial features and J' corresponds to the non-beneficial features.

Step 5: TOPSISs compute separating distances between alternatives and ideal/non-ideal solutions in step five

$$D^{+} = \sqrt{\sum_{j=1}^{n}(V_{ij} - s_j^{+})^{2}}, \quad i=1,\ldots..,m \quad (16)$$

$$D^{-} = \sqrt{\sum_{j=1}^{n}(V_{ij} - s_j^{-})^{2}}, \quad i=1,\ldots..,m \quad (17)$$

Here, i = criterion index, j = alternative index.

Step 6: TOPSISs, in its penultimate step calculates relative proximities of alternatives to optimal solutions and using the Equation given below

$$RC_i=\frac{D^{-}}{D^{+}+D^{-}}, \quad i = 1, 2,.., n \quad (18)$$

Step 7: TOPSISs in its final step sorts preferences based on Ci where greater value of the relative proximity implies higher rank in the sequence, and hence indicates superior performance of alternative as rating options in decreasing order permits for a comparison of proportionally superior results.

3.4. Intermediate Node Selection

The intermediate nodes are meant to be separated from the original source nodes without concealing important information about source locations. The real packets are then routed to intermediate nodes by the originating nodes as node s have known coordinates represented by (x_i, y_i), the source node is presumed to be located at (x_s, y_s). After selecting the destination sink, the source node decides midpoint G $\left(\frac{x_s+x_{sink_i}}{2}, \frac{y_s+y_{sink_i}}{2}\right)$of the source node and destination sink. While the source node starts sending the actual packet, an arbitrary distance parameter d is expressed using Equation (19):

$$d=d_{min} \times (1 + |x|) \quad (19)$$

X refers to a standard normal random variable and adheres to a normal distribution with mean 0 and variance σ^2.

Once d is identified, the source node produces a point at random (x_{inter}, y_{inter}), which follows Eq (20). In every round, the placement of the intermediate nodes changes and is calculated by random integer x and the creation of coordinates at random. As a result, choosing an intermediate node is totally random

$$d^2 = \left(x_{inter} - \frac{x_s+x_{sink_i}}{2}\right)^2 + \left(y_{inter} - \frac{y_s+y_{sink_i}}{2}\right)^2 \quad (20)$$

RESEARCH ARTICLE

This must be ensured that the intermediate node IN1 is outside of the visual field at this point S and IN1 must be separated by a greater distance than d_{min}. As a result, Eq. (21) is utilized to limit the location of intermediate node IN1.

$$d+d_{min} < 0.5\, d_{s_t} \qquad (21)$$

3.5. Real Packet Transmission Stage

At the sensor domain, the source node chooses the intermediate node. Because each node only knows its neighbors, the source node is unaware of the precise location of other nodes greater than one hop away. A node, particularly, is unaware if a genuine node (x_{inter}, y_{inter}) which is nearby. To solve this challenge, a cloud-based method defines the nearest node to the problem as (x_{inter}, y_{inter}) to serve as an intermediary node that must be present in every round The nodes in the considered network are densely placed; the distance between them (x_{inter}, y_{inter}) is short because the distance to the intermediary node is less than one hop, this mistake may be disregarded

The best path selection entails creating massive routing pathways from source to destination node to send real packets per round. Real packet routing may easily choose which neighbour relay node will be the next recipient. After obtaining real event packet, the intermediate node broadcasts it immediately to target sink.

3.6. Cloud Center Node and Cloud Establishment Stage (Security Analysis)

The CPSLP method masks the source node within the group to prevent it from being discovered. This method depends on idea that the source node selects a node to serve as cloud center. Later, the cloud center node generates a high-traffic aggregation zone to act as an artificial hotspot, luring the invader. As a result, the intruder may highlight a region that is not used for packet transmission. Initially, the node acting as the cloud centerC_1 is determined where θ specifies the number of hops required to reach $C_1$and computed by Eq. (12). d_{sti} is the distance between IN1 and S andθ value is dependent on distance (d_{sti}) among source and an intermediate node. Due to the arbitrary position of intermediate nodes, the prediction of θbecomes complex, but the source node can determine hops from source to cloud center and the extent of cloud region.

$$\theta=\left[\frac{0.5 d_{sti}}{d_{min}}\right] \qquad (22)$$

When sending the real packet to destination sink, S transmits a cloud-event packet at random θhops to a nearby node, and current hop count decreases by one when adjacent node obtains this cloud event packet. node then restores the randomized characteristic while choosing next hop and continually reduces hop count. When the present hop count reaches zero, the node that received the cloud-event packet is designated as the cloud center node. Assume C1 exists at a distance of θ hops from the source node. Random routing is the proposed routing protocol of cloud-event packet. Provided the effect of irregular variation for the intermediate node, there is a constant change in θ each time a cloud packet is sent. As a result, cloud core location is continuous and hard to forecast. The goal of a cloud-event packet is to generate a bogus hotspot that seems like a cloud-like area. Following that, the CPSLP method produces a cloud structure with a large number of bogus packets in the network.

When C1 obtains a cloud-event packet from the source node, it encodes it and calculates the initial value of hop count $\theta$to send erroneous data packets to nearby nodes. Later, the adjacent nodes repeat the procedure till the hop count reaches zero. Because the cloud center broadcasts many bogus data packets quickly, traffic surrounding the cloud center is higher than the rest of the network areas.

3.7. Fake Branch Establishment and Fake Packet Transmission Stage

To extend the time needed for the traffic flow tracing, false packets are included in the delivery path of the actual data packet, represented by the primary path. The routing path taken by the false packet is regarded to be a counterfeit branch. The packet transmission is made up of various false branches having multiple hops along the primary path. When $n_i$it gets the original packet, it $n_i$produces a randomized number ranging between [0, 1] and later computes its threshold T (n_i which consists of a changeable number of nodes in the primary path for the generation of false branches, hop count between IN1 and $n_i$residual energy. In case, random value is lesser than T (n_i), $n_i$it produces false packets to transmit to the neighbor node. In case the intermediate node gets the actual packet, development of the false hotspot is either finished much before or will be in done in a short while. The fake hotspot creates confusion for the hotspot-locating intruder regarding the actual traffic pattern. The present original packet delivery is finished before its successful tracking; hence, intruders do not have sufficient time to find the source node and should stay put for the upcoming packet-transfer time period.

4. RESULTS AND DISCUSSION

The implementation of the proposed ERR-CSLPPs approach was done in MATLAB. The performance comparison between the proposed system and the existing MSRO-BFA and CPSLP approaches in terms of Total energy dissipation, node utilization ratio, transmission delay, security, and network lifetime is carried out. Table 2. Represents simulation parameter settings.

RESEARCH ARTICLE

4.1. Simulation Setting

In the tests, 2500 sensor nodes were installed randomly in an 800m*800m square area. Adversaries at first waited near four sinks to be deployed at four vertices, and the highest length of false branch is 10 (L ≤ 10); Transmission range (d_{min}) is 30m, Data bits per message (P_{bit}) is 1000bits, number of intruders are 1,4,8,12,16,20,24. The hearing range of adversaries is equivalent to d_{min},γ is 0.5 and Pfake is 0.1.Initially, there is only one intruder present in network. B. The overall energy dissipation is a constant issue in WSNs, as it restricts the data broadcast and network lifespan. Energy consumption depicts the difficulty exhibited by every algorithm, which is loaded with the help of sensor nodes. For example, the hotspot nodes consist of several packets that are forwarded per round compared to those existing along edges. The simulation in this work includes a full round of transmission, which includes transferring the actual packet to the destination sink and making counterfeit branches and a false hotspot.

Simulation Parameters	Range
Sensor Nodes	2500
Area	800m*800m square
Maximum Length of False Branch	10 (L ≤ 10);
Transmission range (d_{min})	30m
Data Bits Per Message (P_{bit})	1000 bits
Number of Intruders	1,4,8,12,16,20,24
Hearing Range of Adversaries d_{min},γ	0.5
Pfake	0.1

Table 2 Simulation Parameter Setting

4.2. Energy Consumption

The performance comparison between the proposed ERR-CSLPP scheme and the existing MSRO-BFA and CPSLP approaches is carried out in terms of overall energy consumption. The simulation time is plotted along the x-axis, and the energy consumption is plotted along the y-axis as shown in figure. 3. The simulation activity in this work included a full round of transmission, which provides for delivering the actual packet to the destination sink and making counterfeit branches and a false hotspot. Entire packet transfers were taken into consideration. Even though the energy consumption of ERR-CSLPP approach is a little more than the MSRO-BFA and CPSLP approach, it improved privacy preservation by utilizing false hotspots and packets. The major reason for this performance improvement is due to the exploitation of the butterfly optimization. The utilization of this optimization approach helps the proposed approach in consuming lesser energy of the nodes.

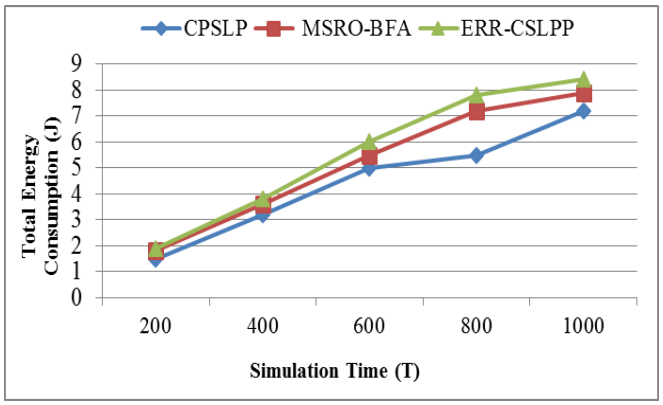

Figure 3 Total Energy Consumption

4.3. Node Utilization Ratio

The node utilization ratio is specified as ratio of network nodes whose residual energy is lesser than 99%.

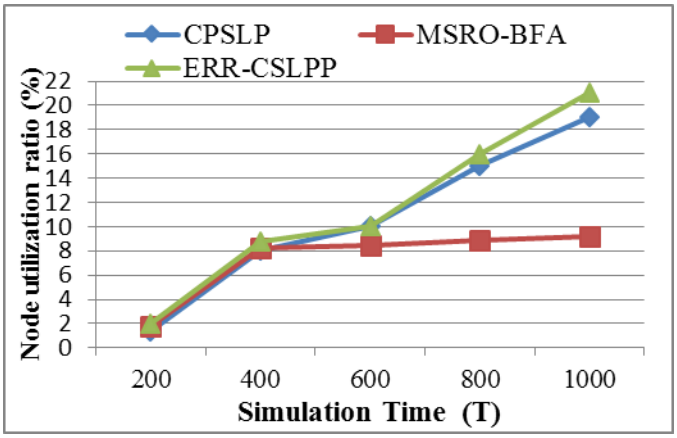

Figure 4 Node Utilization Ratio under Different Simulation Times

The comparison between the proposed ERR-CSLPP approach and the existing MSRO-BFA and CPSLP approaches is carried out in terms of Node utilization ratio, as illustrated in figure 4. The simulation time is plotted along the and node utilization ratio is plotted along the y-axis. A cloud-based routing form is constructed to avoid a hotspot issue in the region that surrounds the source node. It utilized nodes with increased residual energy to the maximum extent and create cloud-shaped hotspot balanced energy usage. The proposed approach consists of nodes in another region during packet

RESEARCH ARTICLE

broadcasts and yields the most significant node utilization ratio. The utilization of AAFBOA allows the proposed system to use the specific nodes that are appropriate for the data transmission without randomly using all the nodes.

4.4. Transmission Delay

Transmission delay refers to hop count in the primary path, corresponding to the source and sink node distance.

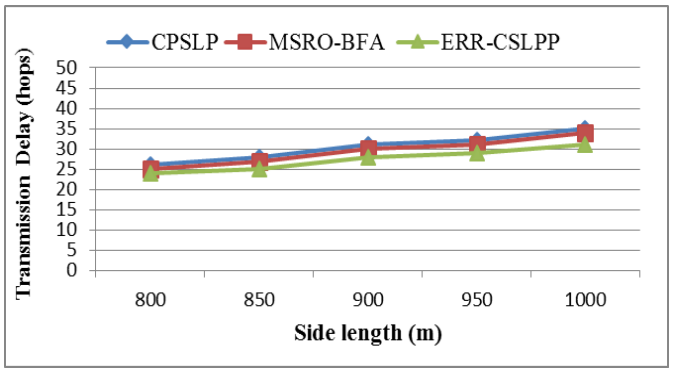

Figure 5 Transmission Delay

Figure 5 illustrates the transmission delay of the proposed ERR-CSLPP approach and the existing MSRO-BFAs and CPSLP approaches. The side length is taken along the x-axis, and transmission delay is considered along the y-axis. Proposed ERR-CSLPP, TOPSISs are presented with the intent of choosing the optimal paths for packet transmission. The paths are chosen based on the objective function like ETCs, residual energy, and hop count. It decreases the transmission delay. The setup in Figure 5 is meaningful since the network delay relies on the routing mode of three approaches. As the simulation time increases, there is also an increase in transmission delay. It can be proven from the experimental results that the proposed system yields very little transmission delay in comparison with the existing techniques. Delay is minimized in this approach by the usage of the optimization approach that helps in appropriate node utilization.

4.5. Network Security

The network security is specified as mean number of hops during full packet transfers to ensure security and privacy.

The performance comparison between the proposed ERR-CSLPP scheme and the existing MSRO-BFA and CPSLP approaches is carried out in security. As illustrated in Figure 6, the CPSLP approach yields the best level of protection. To guarantee the source location privacy is secured, it created false branches during the whole original packet transfer duration. The hotspot that the cloud center has produced gathered some more data transfer and resulted in fluctuations of traffic in a small region. This is confirmed from investigational findings that the suggested system yields improved security compared to earlier techniques.

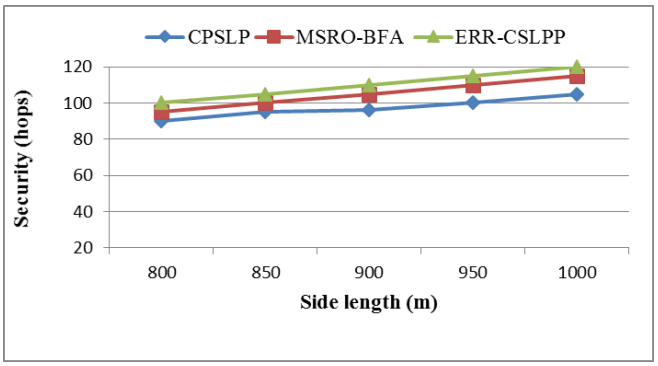

Figure 6 Security with Different Side Lengths

4.6. Network Lifetime

Network lifetime is improved by the use of optimization algorithm that minimizes the energy consumption of the nodes. Figure 7 shows network lifespan comparison between the proposed ERR-CSLPP and the existing MSRO-BFA and CPSLP approaches. If the sensor node's energy is depleted, the network lifetime decreases. In this proposed work, ETCs, residual energy, and hop count are considered for optimal route selection. Due to this consideration, the proposed system achieves improved network lifespan compared to the earlier MSRO-BFA and CPSLP techniques.

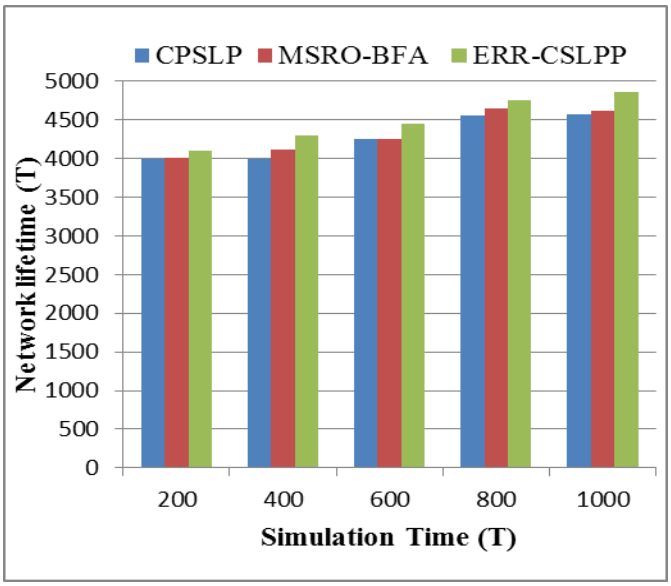

Figure 7 Network Lifetime

From the above discussion, it is mentioned that the proposed method is highly effective in all aspects of performance and security. The proposed AAFBOA is utilized in this study to choose the mobile sink node. TOPSISs are used to select optimal routes for transmission to enhance PDRs and minimize transmission delays. Based on the graph results from figure 3 to figure 7. It is clearly visualized that the

RESEARCH ARTICLE

proposed ERR-CSLPPs approach has high security and good network lifespan and energy utilization than the existing methods.

5. CONCLUSION

The proposed system developed an ERR-CSLPPs approach to prolong the network lifespan and increase the security strength against intruders. The proposed AAFBOA is utilized in this study to choose the mobile sink node. TOPSISs are used to choose optimal routes for transmission to enhance PDRs and minimize transmission delays. Furthermore, the CSLPP approach can safeguard source security during a back-track and hotspot-locating assault. For each period, the source node transmits the real packet. The usage of false branches provides adequate protection contrary to the back-tracing adversary. The experiments reveal that the proposed system yields improved performance compared to the earlier systems concerning overall energy dissipation, node utilization ratio, transmission delay, security, and network lifespan.

REFERENCES

[1] Khalaf, O. I., & Sabbar, B. M. (2019). An overview on wireless sensor networks and finding optimal location of nodes. Periodicals of Engineering and Natural Sciences (PEN), 7(3), pp.1096-1101.

[2] El Alami, H., & Najid, A. (2019). ECH: An enhanced clustering hierarchy approach to maximize lifetime of wireless sensor networks. IEEE Access, 7, pp.107142-107153.

[3] Numan, M., Subhan, F., Khan, W. Z., Hakak, S., Haider, S., Reddy, G. T., & Alazab, M. (2020). A systematic review on clone node detection in static wireless sensor networks. IEEE Access, 8, pp.65450-65461.

[4] Mostafaei, H. (2018). Energy-efficient algorithm for reliable routing of wireless sensor networks. IEEE Transactions on Industrial Electronics, 66(7), pp.5567-5575.

[5] Sangaiah, A. K., Sadeghilalimi, M., Hosseinabadi, A. A. R., & Zhang, W. (2019). Energy consumption in point-coverage wireless sensor networks via bat algorithm. IEEE Access, 7, pp.180258-180269.

[6] Sajwan, M., Gosain, D., & Sharma, A. K. (2018). Hybrid energy-efficient multi-path routing for wireless sensor networks. Computers & Electrical Engineering, 67, pp.96-113.

[7] Shokair, M., & Saad, W. (2017). Balanced and energy-efficient multi-hop techniques for routing in wireless sensor networks. IET Networks, 7(1), pp.33-43.

[8] Mutalemwa, L. C., & Shin, S. (2019). Achieving source location privacy protection in monitoring wireless sensor networks through proxy node routing. Sensors, 19(5), 1037.

[9] Wang, Y., Liu, L., & Gao, W. (2019). An efficient source location privacy protection algorithm based on circular trap for wireless sensor networks. Symmetry, 11(5), 632.

[10] Ouyang, Y.; Le, Z.; Chen, G.; James, F.; Fillia, M. Entrapping Adversaries for Source Protection in Sensor Networks. In Proceedings of the International Symposium on World of Wireless, Mobile and Multimedia Networks, Washington, DC, USA, 26–29 June 2006; pp. 23–34

[11] Ozturk, C.; Zhang, Y.; Trappe, W.; Ott, M. Source-Location Privacy for Networks of Energy-Constrained Sensors. In Proceedings of the Second IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems, Vienna, Austria, 12 May 2004; pp. 68–72.

[12] Ma, W.; Song, L. Source location privacy preservation routing protocol based on multi-path. Comput. Eng. Appl. 2018, 54, pp.81–85. (In Chinese).

[13] Cerpa, A.; Estrin, D. ASCENT: Adaptive Self-Configuring Sensor Networks Topologies. IEEE Trans. Mob. Comput. 2004, 3, pp.272–285.

[14] Yao, L., Kang, L., Deng, F., Deng, J., & Wu, G. (2015). Protecting source–location privacy based on multirings in wireless sensor networks. Concurrency and Computation: Practice and Experience, 27(15),pp. 3863-3876.

[15] Han, G., Miao, X., Wang, H., Guizani, M., & Zhang, W. (2019). CPSLP: A cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks. IEEE Transactions on Vehicular Technology, 68(3), pp.2739-2750.

[16] Mutalemwa, L. C and Shin, S. (2018). Strategic location-based random routing for source location privacy in wireless sensor networks. Sensors, 18(7), 2291.

[17] Ricardo A. L. Rabelo, Jose V. V. Sobral, Harilton S. Araujo, Rodrigo A. R. S. Baluz, and Raimir Holanda Filho, "An Approach Based on Fuzzy Inference System and Ant Colony Optimization for Improving the Performance of Routing Protocols in Wireless Sensor Networks," IEEE Congress on Evolutionary Computation, pp 3244-3245, 2013

[18] Naghibi, M., & Barati, H. (2020). EGRPM: Energy efficient geographic routing protocol based on mobile sink in wireless sensor networks. Sustainable Computing: Informatics and Systems, 25, 100377.

[19] Fu, X., & He, X. (2020). Energy-balanced data collection with path-constrained mobile sink in wireless sensor networks. AEU-International Journal of Electronics and Communications, 127, 153504.

[20] Cheng, H., Tao, L., & Zhang, X. (2019). A Fast and Efficient Broadcast Protocol With a Mobile Sink Node in Asynchronous Wireless Sensor Networks. IEEE Access, 7, 92813-92824.

[21] Ye, G., Zhang, B., & Chai, S. (2014, December). Energy balanced virtual force-based approach for mobile WSNs. In 2014 Seventh International Symposium on Computational Intelligence and Design (Vol. 1, pp. 496-500). IEEE.

[22] Al-Tabbakh, S. M., & Shaaban, E. (2017, September). Energy aware autonomous deployment for mobile wireless sensor networks: Cellular automata approach. In International Conference on Applied Physics, System Science and Computers (pp. 87-99). Springer, Cham.

Authors

Mr. R. Nagarajan is currently pursuing PhD in Sri Ramakrishna College of Arts & Science, Coimbatore since 2014 and currently working as an Assistant Professor in Department of Computer Science, Sri Ramakrishna College of Arts & Science (Formerly SNR Sons College), Coimbatore since 2012. He has completed the Bachelor of Computer Applications at Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore in the year 2005, M.Sc Information Technology at SNR Sons College, Coimbatore in the year 2009 and completed his M.Phil Computer Science, Bharathiar University, Coimbatore in the year 2013. He has published 4 research papers in reputed International Journals and also presented research articles in various international conferences. His area of Interest includes Networking and Cloud Computing. He has 10 years of Research experience.

Dr. G. Maria Priscilla is currently working as Associate Professor & Head, Department of Computer Science in Sri Ramakrishna College of Arts & Science (Formerly SNR Sons College), Coimbatore. She has finished her M.Sc. degree at Bharathiar University in 1998. She has been awarded M.Phil Degree at Bharathidasan University in 2005 and she has been awarded Ph.D at Mother Teresa University in 2014. Her area of interest in research is Computer Networks. She has 23 years of teaching experience in collegiate service. She has presented & published various papers in International & National conferences.

RESEARCH ARTICLE

How to cite this article:

R. Nagarajan, G. Maria Priscilla, "Efficient and Reliable Routing With Cloud Based Source-Location Privacy Protection in Wireless Sensor Networks", International Journal of Computer Networks and Applications (IJCNA), 8(6), PP: 730-741, 2021, DOI: 10.22247/ijcna/2021/210722.