Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9912626, 17 pages
https://doi.org/10.1155/2021/9912626

Research Article

C^2S^2-LOOP: Circular Chessboard-Based Secure Source Location Privacy Model Using ECC-ALO in WSN

Naveed Jan,[1] **Sarmadullah Khan**,[2] **Ali H. Al-Bayatti**,[2] **Madini O. Alassafi**,[3] **Ahmed S. Alfakeeh**,[3] **and Mohammad A. Alqarni**[4]

[1]*Department of Information Engineering Technology, Shuhada-e-APS University of Technology Nowshera, Pakistan*
[2]*School of Computer Science and Informatics, De Montfort University, The Gateway, Leicester LE1 9BH, UK*
[3]*Faculty of Computing and Information Technology, King Abdul Aziz University, Jeddah 21589, Saudi Arabia*
[4]*College of Computer Science and Engineering, University of Jeddah, Jeddah 23218, Saudi Arabia*

Correspondence should be addressed to Naveed Jan; jannaveed@gmail.com

Received 11 March 2021; Accepted 7 May 2021; Published 25 May 2021

Academic Editor: Sungchang Lee

Source location privacy (SLP) is a serious issue in wireless sensor networks (WSN) since Eavesdroppers tries to determine the source location. Hunting Animals in Forest is considered as an example for SLP. Many conventional schemes have been proposed for SLP in WSN, namely, Random Walk Routing, and Fake Messages Transmission, which cause critical issues (less safety period, packet delivery latency, and high energy consumption). Furthermore, the security analysis is not properly investigated in any previous work. In this paper, we propose a new model called the circular chessboard-based secure source location privacy model (C^2S^2-LOOP) with the following tasks: key generation, network topology management (clustering), intercluster routing (travel plan), and data packets encryption. All sensor nodes are deployed in a circular chessboard (Circular Field) and the key generation ($\boldsymbol{PU}_K, \boldsymbol{SE}_K$) is invoked using elliptic curve cryptography (ECC) with Ant Lion Optimization algorithm, which mitigate the issues of conventional ECC. Then, the network topology is managed using clustering where residual energy of the nodes is used for Cluster Head (CH) selection. Intercluster routing is implemented using packet traversing using clockwise and anticlockwise directions, which are mainly concerned with establishing a secure route between the source to the destination node. To ensure data security, we present the Chaotic Artificial Neural Network (C-ANN) in which encryption is executed. Assume that CH near to the source node has a high trust value, then it traverses (clock-wise) real packets towards sink node and similarly in the left side region (anticlockwise), fake packets are transmitted. Network simulations (OMNeT++) are evaluated and compared with the previous approaches, and finally, our proposed scheme concludes that it maintains not only source node location privacy (large safety period) and also reduces energy consumption by more than 40% and latency by more than 35%.

1. Introduction

WSN is a kind of wireless network that is comprised by a grouping of sensor nodes that can sense, collect, and broadcast information to adjacent nodes through direct communication or relay nodes [1, 2]. Source location privacy is an emerging area in event-driven applications such as military and wildlife tracking applications. At any time, the sensor node becomes a source node, and thus when event is detected by a node, the message for a specific event is transmitted to the sink node [3–5]. In many cases, the source node can be easily located through the shared wireless transmission medium. Hence, the objective of this source location privacy is to protect the source node location [6]. The safety period is the main concern in SLP, i.e., how long until the node is discovered [7]. To address this concern, several methods have been proposed for SLP in the sensor network. SLP can be classified into the following: flooding-based approach, phantom routing, and fake/dummy messaging approach. Most of the authors have used Random Walk Routing for source location in which nodes are selected in random and adversary/attacker cannot find the source location [8, 9]. Previously,

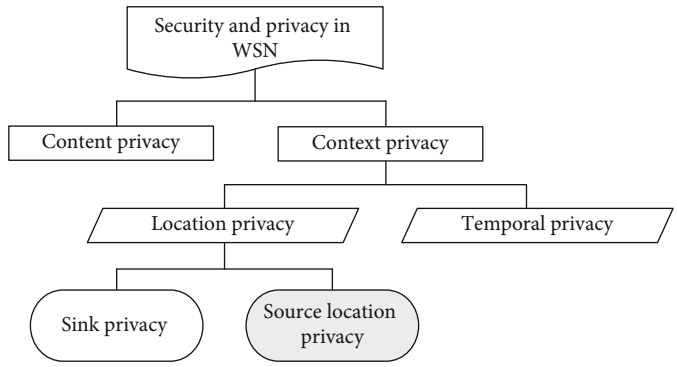

Figure 1: Security and privacy in WSNs.

dummy message injection method is presented which improves the location privacy but it causes more overhead among sensor nodes [10].

Other approaches are geographic routing, cyclic entrapment, in-network location anonymization, cross-layer routing, separate path routing, network coding, and limit node detectability. These approaches are consuming more energy, large delay, and decreased safety period [11–13]. Source node location privacy becomes important for message transmission, but confidentiality of data packets must be ensured through encryption strategy, which is much more necessary to adequately address the problem of source location privacy. Then, we discussed the concepts [14] include safety period, unlikability, identity privacy, timing privacy, route privacy, and contextual privacy. However, context privacy is used for source location identification. Figure 1 indicates the security and privacy of WSN, while Figure 2 shows an example of animal tracking providing a good example of SLP in the sensor network.

1.1. Source Location Privacy. SLP is an important issue and enormous works have been undertaken in this field. A number of attacks related to SLP in WSN. Privacy of source node location is ensured with the use of context protection. Adversaries may use packet tracing to determine the source node location, while the data is being sent from the source to the sink node. However, two adversaries are involved in SLP that is as follows:

(i) *Local Attacker.* This type of attacker can only eavesdrop within range and back-trace the routing path until it reaches the source node

(ii) *Global Attacker.* This type of attacker learns about the whole network traffic and who can make use of temporal consistency and the correlation between packets. Hence, it makes use of the following:

(a) Received signal strength indicator

(b) Direction of the packets

(c) Inter-packets time

(d) Packet's occurrence time

Furthermore, the global attacker is near to the sink node of the sensor network and tries to find out the location of the source node of the message [15]. Security is a challenging operation in SLP. Obtaining some parameters such as safety period may improve location privacy, but it may lead to severe issue on the other side such as residual energy. Hence, a balanced trade-off between location privacy and energy consumption is more desirable to obtain high QoS performance and fewer computations in SLP. However, modeling a secure and robust scheme to address these parameters is a difficult process. Very popular routing protocols are required and we need to be augmented these routing protocols with a novel scheme. Energy consumption is still an important issue in accomplishing SLP. To address these issues and show better performance (minimum energy consumption, minimum latency, and maximum safety period) for the source location privacy and easy and flexible network topology management, C^2S^2-LOOP provides an efficient solution.

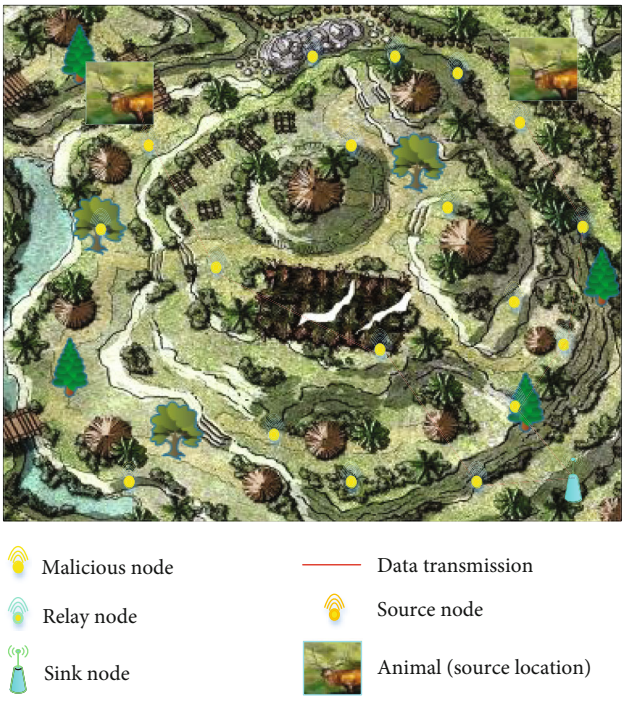

Figure 2: Example for SLP in sensor network.

1.2. Contributions and Organizations. The main contributions of this paper are as follows:

(i) We propose a circular chessboard based secure source routing (C^2S^2-LOOP) to protect a source's location privacy against an attacker

(ii) We propose an elliptic curve cryptography-based ant lion optimization algorithm for key generation in which public and secret keys are generated. This solves issues of the traditional ECC algorithm

(iii) Equal number of nodes are deployed in each cluster and CH is selected based on residual energy

(iv) Transmission of packets from source to sink is done using clockwise and anticlockwise directions for real and fake packets depending on the value of random number R_n

(v) Before packets transmission from the source node, it will be encrypted using a chaotic artificial neural network and then forwarded to adjacent nodes

(vi) We evaluate the performance by a comprehensive set of experimentations for the proposed vs. previous approaches, and our proposed scheme demonstrates the effectiveness and improvement to source location privacy preserving in terms of energy consumption, latency, safety period, and network lifetime

The remainder of this paper is as follows: in Section II, we present the state of the art in the field of SLP in WSN. In Section III, we describe the problems and effects of analysis for protecting source location privacy. In Section IV, we present our proposed system model where we elaborate the proposed approach in further detail by presenting subsections. An experiment of the proposed approach is concentrated in Section V, and also, the simulation results obtained by the proposed as well as the previous approaches are described. Section VI concludes our proposed approach, and future directions of this proposed approach are highlighted in Section VII.

2. State of the Art

Over the last few decades, several vulnerabilities have been determined in terms of SLP in WSN. Protecting source location privacy is not only abundant for preserving source location but also some other metrics have been presented in the current literature. In this section, we present this state of the art.

The authors in [16] presented a dynamic SLP algorithm to achieve a high level of SLP with a high number of messages. The proposed dynamic hybrid approach uses a random walk procedure for packet transmission to the base station and a fake source allocation strategy for energy consumption reduction. A dynamic SLP approach is more energy-efficient, but it is suitable for the deployment of WSN environments. It increases communication overhead since the whole network is dynamic in nature, and also, the hybrid approach is the combination of fake source nodes and random walks, which also increases network overhead and delay. In [17], a differentially private framework-based differential privacy was presented to protect the location of event occurrence. Privacy of event occurrence location is required that requires that an adversary must not able to distinguish between real and dummy traffic messages. The proposed approach produces reduced sensitivity to a single node transmission, which is achieved through real dummy and cumulative reporting to the same event (fake/real events). The first component mechanism generates dummy events to protect source location privacy in which the attacker can easily find the source location by receiving more dummy messages. The authors in [18] proposed a ring-loop routing for a source location privacy scheme in IoT-assisted WSN. It increases the backtracking time of the adversary; a confounding time-domain transmission was introduced to transmit real packets. In addition to Phantom nodes and fake packets transmission, a confounding ring was also utilized to protect the source location privacy. Firstly, real packets are forwarded in the basic ring using confounding time-domain transmission, and secondly, phantom nodes forward using confounding with the shortest path. The proposed scheme is suitable for a local adversary, but it is not suitable for global attackers and it follows the basic ring for packet transmission to the sink node.

A multiobjective optimization model was proposed for SLP [19], which is based on two criterions such as pareto efficiency (selection either) and confirm efficiency. A genetic algorithm (GA) was employed to generate Pare-to-Optimal schedules. In addition, two functions were derived in which the main purpose is to minimize total slot usage and also reduces coupled slot usage, which follows the time division multiple access (TDMA) procedure. It directs the predicted attacker path away from the source node. Its advantage is that near-optimal capture radio coupled with path creation that causes no extra messages overhead. This approach was led to high energy consumption and latency. The authors in [20] designed a new protocol called redundancy-based convergence based preserved source location privacy (RBCPSLP) technique in energy harvesting WSN. It improves the privacy preservation by creates as many interference sources. A branch convergence-based SLP preserving strategy was proposed, and hence, routes merge into few routes before arrival at the sink node. In this work, the route is not effective to preserve SLP.

A trace cost-based SLP protection (TCSLP) scheme was proposed in WSN [21]. Initially, authors built a phantom area, which consists of phantom nodes far away from the source node. Then, two routing schemes were integrated (shortest path routing and random walking) for packets transmission, which improves source node location privacy. Phantom node may not be at the right place of the network, which results in the reduction of privacy levels as well as an increment in energy consumption. A new source location privacy protection scheme was proposed in [22], which is implemented in a more practical adversarial model, i.e., smart adversary. This scheme was implemented under both local and global attackers. In order to defend against these adversaries, the authors proposed a lightweight message sharing approach, and then, each message is mapped to a set of shares. Message sharing is not more reliable and scalable for large-scale networks. Energy-efficient and optimum

routing is a critical and general issue in WSN. An improved version of routing for WSN was proposed over cluster-based WSN [23]. Initially, a network is divided into number cells, and then, GA is applied to find an optimum number of nodes. To increase the speed of clustering, the *k*-means algorithm was proposed. Both GA and *k*-means clustering are time-consuming processes. In [24], the authors presented a dynamic routing scheme for source node location protection. It aims at improving paths for data transmission, and the proposed dynamic routing scheme aims to choose maximum paths for data transmission. Firstly, it selects an initial node from the boundary of the network and every packet traverse by a greedy route and a directed route to the sink node. It causes high complexity and high energy consumption. The authors in [25] focused on SLP by introduced suitable modifications to sensor routing protocols that make it hard for an adversary to backtrack the origin of the source node. This paper jointly considers the issues of energy consumption and location privacy in WSN. The drawbacks of this approach are to lack of security and privacy leakage.

In [26], all-direction routing algorithm (ARR) was proposed for SLP which against parasitic WSN. In ARR, agent nodes are randomly selected in directions by the source nodes based on local decisions rather than knowing the whole topology of the networks. In this work, proper agent node selection is difficult, and it is difficult for agent to transmit packets from the source node to the destination agent node. In [27], the authors proposed two novel methods such as angle protocol for source location (APS) and EAPS (enhanced protocol for source location). These methods adjust dynamically emission radius in routing. APS protocol provides geographically dispersed phantom source nodes and utilizes the energy from energy-abundant regions to create the path. In this work, the dynamical adjustment of node emission radius is complex. Koh et al. [28] have proposed multipath routing named optimal privacy-enhancing routing algorithm (OPERA). The authors have considered global adversary for both lossy and lossless observations that used Bayesian Maximum Posteriori (MAP) estimation scheme. The biggest strength of OPERA is that it provides a good trade-off between energy consumption and privacy but leads to high computational complexity. A novel tree-based diversionary routing scheme was proposed [29] to preserve SLP based on hide-and-seek strategy. The proposed tree-based routing provides strong resistance to reverse trace of the adversary and also resistance to direction-oriented attack. The proposed tree-based routing scheme utilizes remaining energy only at different remote regions and creates diversionary routes as more and then sent to one route in regions near to sink node. A list of nomenclature is shown in Table 1

A confused arc-based SLP scheme was proposed in [30], which is implemented in WSN assisted Internet of Things. The main scope of this paper is to finish packets transmission via random walk based on the node direction. In this scheme, nodes select their next relay nodes in a particular communication range. The proposed scheme is compared with the ring routing, which reduces energy consumption and delays at the expense of safety time for WSN. In this work, the safety period is very less for packet transmission. On the other hand, a *K*-means clustering scheme based on SLP was proposed in WSN enabled IoT [31]. To protect the source location, fake source nodes are deployed in the network for sensing dummy messages. To increase the safety period, *k* -means clustering was proposed, which forms clusters. Fake packets are transmitted via fake source nodes to reach the destination node. This scheme is failed to increase the safety period and reduce the latency at minor energy consumption, but lack of security.

Table 1: List of nomenclature.

Symbol	Meaning
$C_1, C_2, C_3 \cdots$	No. of circular fields
$C_{ID1}, C_{ID2}, C_{ID3} \cdots$	Circular identifier
a	Area of circular field
$N(SN) \in C$	No. of nodes in each circular field
SN_i	Sensor nodes
S_{INK}	Sink node
HL_p	Hello packet
$c_1, c_2, c_3 \cdots$	No. of clusters
CH	Cluster head
CH_C	Current CH
CH_l	New CH
c_M	Cluster member
S_T	Sensing time
A_T	Aggregation time
S_{ps}	Packet size for sensor node
E_R	Sensor residual energy
P_T	Plain text
C_T	Ciphertext
T_S	Time stamp
PSRN	Pseudorandom number
x, y	Sensor position
S	Source node
SE_k	Private key
PU_k	Public key
X, Y, a, b	Domain parameters
BP	Base point
p	Prime number
MAX_E_R	Node with maximum residual energy

3. Problem Description

We firstly evaluate the effect of overheads (routing and communication between nodes) during SLP using different methods (random walk, fake message transmission, dummy message injection, and so on). Then, we investigate the effect of energy consumption and also considered some optimal ethics for introducing a new scheme for protecting source location information [32]. In [33], a novel chess-board

alternation (CBA) was proposed for SLP against global attacker. Initially, the network is partitioned into two sets and each set operates in an alternating fashion. This CBA has obtained perfect privacy, but it decreases energy cost up to 50% and transmission delay by more than 40%. This method follows a random walk procedure, which is a simple method that increases delay when the probability of adjacent random walk nodes is high. Global attacker can easily capture source node location due to random walk routing (node direction and RSSI). In [34], grid-based cluster methodology was proposed in which the network is divided into a number of clusters. In a grid-based clustered environment, three techniques were proposed such as Dynamic Tree (DT), Dynamic Shortest Path Tree (DSP), and Hybrid Scheme. The proposed hybrid scheme used dummy messages to mislead the adversary since it tracks the source node location, which wastes the energy of sensor nodes. A large packet delay is due to the process of three schemes. Cluster head selection is not effective since it only considers the residual energy of a node. It leads to cluster-based SLP is not effective. A two-phase routing was proposed for SLP [35]. The basic idea behind this routing is to consume less amount of energy with the use of random walks and escape angle (total sequitur angle $2\alpha_1$ and escape angle α_1). Energy consumption of a node is high since it uses multiple virtual source nodes, and also, this routing scheme delivers the packet to the base station through random-multipaths, and thus, it utilizes an excess amount of energy for transmission to the sink node. A dynamic routing scheme was proposed in [36], which firstly chosen an initial node from the network boundary and every packet is traverse using greedy routing and then used directed route before reaching to the sink node. Event packet is encrypted using a secret key, which is shared between the sink node and the source node. Packets are forwarded through boundary nodes, which consumes more time (number of hops) for packet transmission. In this work, a strong security framework was required which is used for packet encryption and secret key generation. A new scheme called strategic location-based random routing was presented. Here, routing paths are not optimal since it selects random routes which results large delay for packets delivery at the sink node, and also, random nodes are selected by node position, which does not always result in accurate location protection. Energy consumption of the whole network is high due to the packet's transmission through different paths.

4. C^2S^2-Loop System Model

In this section, we describe our proposed model of circular chessboard-based secure routing for SLP. The proposed system architecture is shown in Figure 3.

4.1. System Overview. C^2S^2-LOOP is comprised of four entities such as Sensor Nodes (SNs), Cluster Heads (CHs), Global Attacker, and Sink Node (SN). Global attacker used to track the location of the source node, which tends to leak the privacy and also leakage of information. We implement the following operations: (i) key generation, (ii) network topology management, (iii) travel plan, and (iv) data packets encryption. The initial step is held once because it does not need to repeat the process until the transmission range of the network is changed.

4.2. Assumptions for C^2S^2-LOOP

(1) All sensor nodes are deployed randomly over the circular region with equal initial energy

(2) All sensor nodes are homogeneous (nodes having similar functionalities of processing and communication)

(3) All sensor nodes are moving randomly at constant speed and location are aware

(4) All sensor nodes have a frame header of 104 bits and transmit packet based on time interval

(5) Sink is placed at the center of region, which is stationary

(6) Adversary (Global Attacker) is near to the sink node of network, which tries to find out the source location

(7) It has a global view, and thus, it can view the whole communication patterns of the network

4.3. C^2S^2-LOOP Network Setup. In C^2S^2-LOOP, the circular region is divided into M circular fields. We consider $M = 3$, which means the sensor network is divided into three circular fields c_1, c_2, c_3. The radius of circular fields are denoted as r_1, r_2, r_3, and the ratio is 1 : 2 : 3, respectively. We deployed sensor nodes in a circular chessboard c_1, c_2, c_3. However, there are two shapes are identified in chessboard (white and gray). In each gray and white space, we can see a fair distribution of sensor nodes and does not deploy densely. In a circular chessboard, nodes are deployed in the ratio of 1 : 2 : 3. Area a is determined for each circular field is a critical concern due to deployment and location determination. The sensing area for circular field 1 is depicted in Figure 4.

The area computation for all c_1, c_2, c_3 is as follows:

$$\begin{aligned} a(c_1) &= \prod R^2, \\ a(c_2) &= \prod (2R)^2 - \prod R^2 = 4\prod R^2 - \prod R^2 = 3\prod R^2, \\ a(c_3) &= \prod (3R)^2 - \prod (2R)^2 = 9\prod R^2 - 4\prod R^2 5\prod R^2, \end{aligned} \tag{1}$$

where R is the radius of the circular fields. After sensor nodes deployment, SN_i is responsible for executing sensing S_T and transmitting data packets D_T at time T. The sink node S_{INK} issues public and private keys for all sensor nodes. S_{INK} aggregated all data packets with the packet length S_{ps} through CHs while reducing energy consumption. Other sensor nodes transmit the sensed packets to CH. The process of key generation, network topology management, travel plan, and packet encryption are implemented in many works, but C^2S^2-LOOP incurs a large safety period, minimum packet delay, and minimum energy consumption. Improvement of these QoS

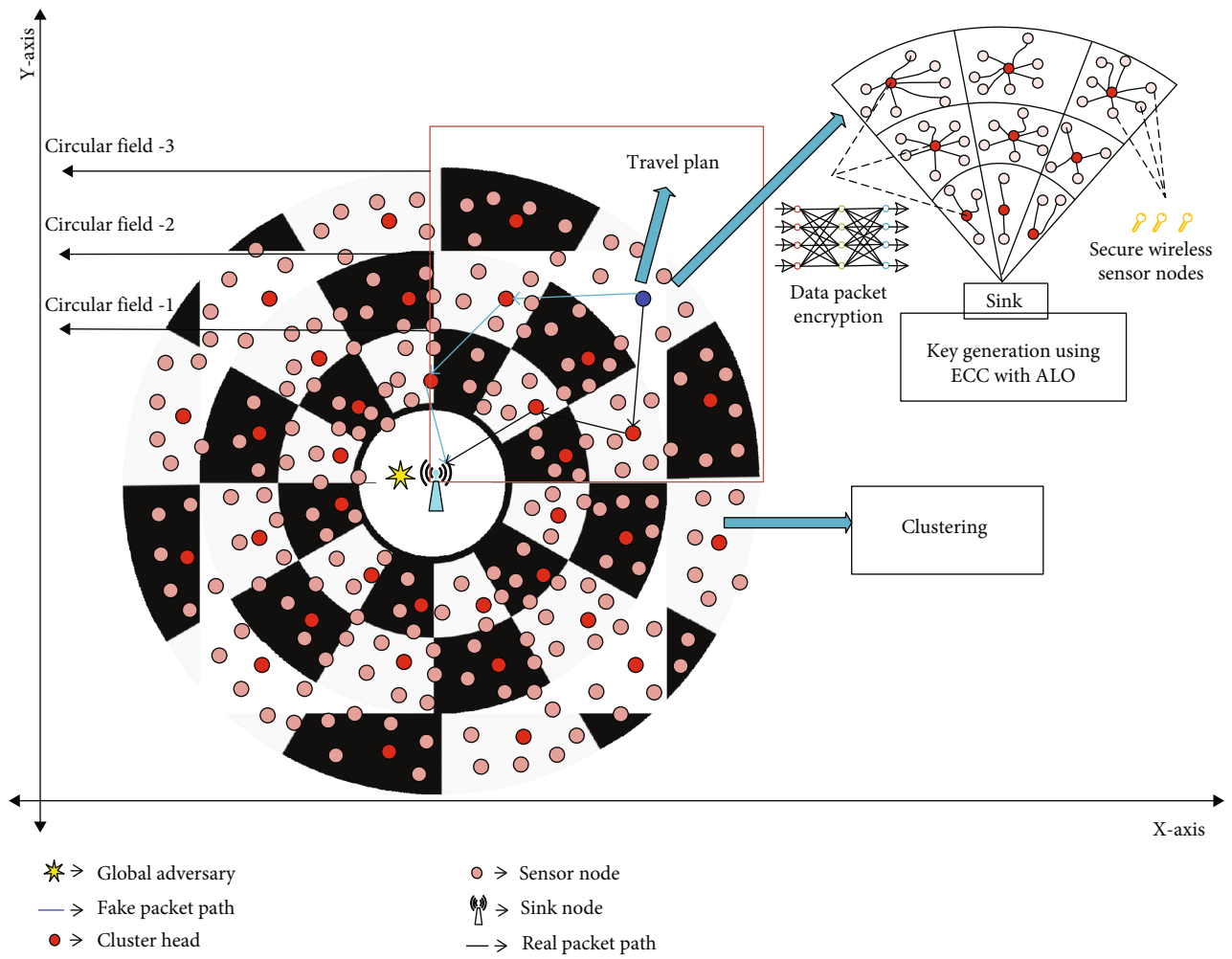

Figure 3: System architecture.

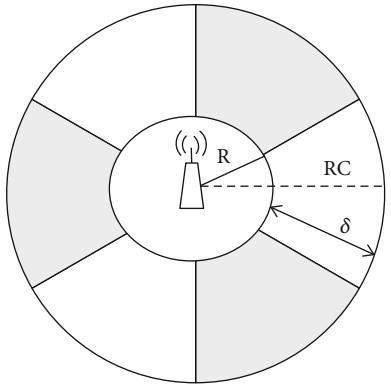

Figure 4: Sensing area for circular field 1.

metrics in the circular chessboard and protecting source location privacy is the main focus of this paper.

4.4. Key Generation. Firstly, registration is performed using ECC with ALO algorithm in which private key and public keys are generated, which is highly secured than the conventional ECC algorithm. ECC is a public-key cryptography system that performs computation by elliptic curve instead of polynomial arithmetic or integer. It provides strong security compared to RSA. Elliptic curve is expressed by an equation of two variables with coefficients. Elliptic curve over real numbers satisfies the set of points, which must satisfy the following equation:

$$Y^2 = X^3 + aX + b, \tag{2}$$

where X, Y, a, b are real numbers, applying different sets of values for a and b.

Definition 1. Elliptic curve.

The elliptic curve over Z_p, $p > 3$ is the set of all pairs $(X, Y) \in Z_p$ which satisfy

$$Y^2 \equiv X^3 + a \times X + b \mod p, \tag{3}$$

where $a, b \in Z_p$ $(0, 1, \cdots p-1)$, i.e., set of integer values with

modulo p arithmetic, and the condition is the following

$$4a^3 + 27b^2 \neq 0 \mod p. \tag{4}$$

For example, $a = -4, b = 0.67$ gives the elliptic curve with the following equation:

$$Y^2 = X^3 - 0.4x + 0.67, \tag{5}$$

However, ECC is demonstrated by two fields such as prime field and binary field. In order to deal with the cryptographic operations, a suitable finite field is selected with contains a large number of points. Some of the benefits of using ECC are as follows: (1) it uses a smaller key size for ciphertexts and signatures, (2) it supports very fast key generation, (3) fast encryption and decryption process than RSA, and (4) for computations, ECC required less memory and CPU cycles than RSA. Therefore, it is suitable for all applications.

Key generation is a significant process where we generate both public key and private key PU_K, SE_K, respectively. This SE_K is generated using the ALO algorithm. ECC key generator description is as follows [37]:

$$\begin{aligned} SE_K &= I \times \text{Selected from the interval } (1, p-1), \\ PU_K &= \quad SE_K \times BP, \end{aligned} \tag{6}$$

where BP is the base point taken from the elliptic group. However, ECC selects private key in a random manner, which leads to the incorrect generation of ciphertext. To mitigate such issues, ALO is proposed for private key generation, and then, the private key and base point are used to generate the public key, written in equation. The process of ALO is described underneath: ALO is a new metaheuristic algorithm released in 2015 by Seyedali Mirjalili [38]. It is based on the behaviors of Ant Lions Hunting mechanism. The major steps involving in ALO for hunting prey are (1) Ants random walk, (2) Building traps, (3) Entrapment of Ants in Traps, and (4) Catching Preys, and rebuilding traps are executed. In order to determine the private key (optimal solution), ALO follows the following process:

(i) *Initialization.* Firstly, initialize the population of Ants and Antlions in a random way

(ii) *Fitness Computation.* Compute the fitness of Ants and Antlions and determine the best antlion is the optimum solution (Elite)

(iii) *Update Ants Position.* Choose an antlion by Roulette Wheel. Then updates Ants position using random walk around choose Antlion and Elite. In addition, we compute fitness value for all Ants

(iv) *Replace an Antlion.* In this step, replace an antlion with its corresponding ant (only when it becomes fitter)

(v) *Update Elite.* When an action becomes fitter compared to Elite

(vi) *Termination Condition.* When termination condition is reached, return the Elite as the optimum solution for the given problem. Else, update ant's position and continue until the termination condition is reached

In ALO, fitness is computed based on SN_i coordinates (x, y), Identity, i.e., PSRN, and current time stamp T_S. Hence, it is defined by the following:

$$f = \{SN_i(x, y), PSRN, T_S\}, \tag{7}$$

where f is the fitness value for private key selection.

Pseudocode 1: SE_K key generation using ALO.1) Begin

2) Initialize population of Ants and Antlions

3) Compute f for Ants and Antlions

4) Determine the Best_Antlions

5) Consider the current Best_AntLion is the Elite//Optimum Solution

6) While (End Criterion) is fulfilled

7) For every Ant

8) Select an Antlion via Roulette Wheel strategy

9) Update C and D using following

10) $C^t = C^t/I$ & $D^t = D^t/I$(11)

11) Make random walk and normalize it using eqn. (11)

12) $x(t) = [0, \text{cumsum}\,(2r(t_1) - 1) \cdots cumsum(2r(t_n) - 1)]$

$$X_i^t = \frac{(X_i^t - w_i) \times (D_i - C_i^t)}{(D_i^t - w_i)}$$

13) Update ant position using $Ant_i^t = R_a^t + R_e^t/2$

14) End for

15) Compute f for all Ant_i

16) Substitute an Antlion by corresponding ant becomes fitter using eqn

17) $\text{Antlion}_j^t = \text{Ant}_i^t$ if $f(\text{Ant}_i^t) > f(\text{Antlion}_j^t)$

18) Update e^t when Antlion fitter than the Elite

19) End while

20) Return Elite

Pseudocode of the proposed ALO is illustrated as follows: in the ALO algorithm, Ants and Antlions are initialized randomly. In pseudocode, w_i denotes minimum random walk of the ith variable. C_i^t denotes the maximum of the random walk at ith iteration. R_a^t and R_e^t are the random walk around the Antlion chosen by the Roulette Wheel, and elite at tth

1) Begin
2) Initialize population of Ants and Antlions
3) Compute f for Ants and Antlions
4) Determine the Best_Antlions
5) Consider the current Best_AntLion is the Elite//Optimum Solution
6) While (End Criterion) is fulfilled
7) For every Ant
8) Select an Antlion via Roulette Wheel strategy
9) Update C and D using following
10) $C^t = C^t/I$ & $D^t = D^t/I$(11)
11) Make random walk and normalize it using eqn. (11)
12) $x(t) = [0, \text{cumsum}\,(2r(t_1) - 1) \cdots cumsum(2r(t_n) - 1)]$

$$X_i^t = \frac{(X_i^t - w_i) \times (D_i - C_i^t)}{(D_i^t - w_i)}$$

13) Update ant position using $Ant_i^t = R_a^t + R_e^t/2$
14) End for
15) Compute f for all Ant_i
16) Substitute an Antlion by corresponding ant becomes fitter using eqn
17) $\text{Antlion}_j^t = \text{Ant}_i^t$ if $f(\text{Ant}_i^t) > f(\text{Antlion}_j^t)$
18) Update e^t when Antlion fitter than the Elite
19) End while
20) Return Elite

Pseudocode 1: SE_K key generation using ALO.

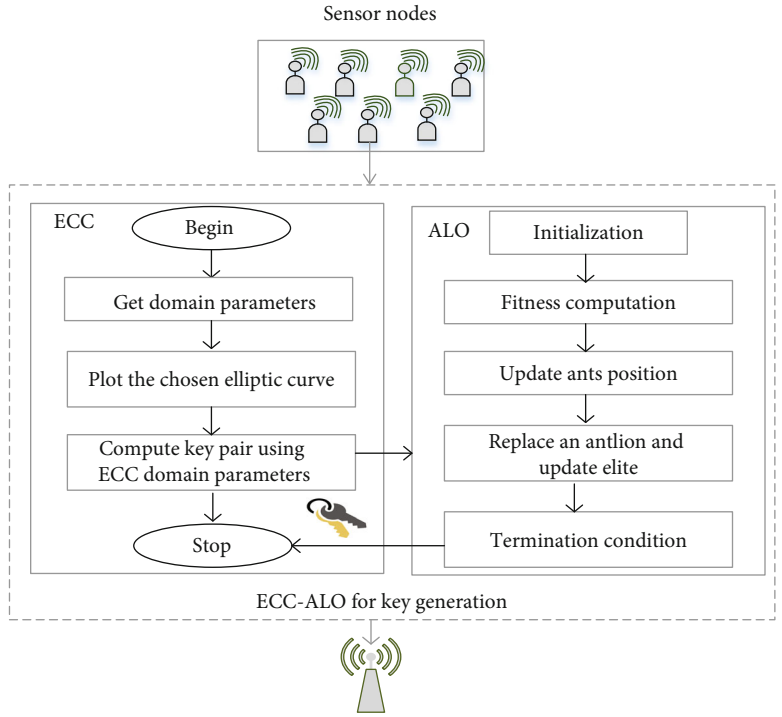

Figure 5: Key generation using ECC with ALO algorithm.

iteration variable, Ant_i^t indicates the current position of ith ant at tth iteration. Figure 5 depicts the flow diagram for ECC with ALO for key generation.

4.5. Network Topology Management. Network topology is managed by the selection of optimal CH. For CH selection, node residual energy E_R is considered.where E_I is the initial energy of a node and E_i is the energy left after the process of round 1 [39].

Definition 2. Node residual energy.

Node residual energy is the energy left after the process of data transmission. It is denoted as E_R, which is computed as follows:

$$E_R = E_I - E_{i=1}, \quad (8)$$

4.5.1. Cluster Formation. To form clusters, SN_i broadcasts hello packet HL_P to collect adjacent node information. In each circular field area, SN_i presented within the gray and white shape is considered as a cluster.

4.5.2. Cluster Head Selection. With the passage of time or in other words as the network lifetime increases, the node energy decreases. If CH remains static, it will soon die out of the battery power and will not remain part of the network. Therefore, dynamic CH selection is used. The node with maximum residual energy is elected in each round (SN_i having MAX_E_R) as CH. Each individual gray and shape area of nodes involved in the CH election process. This helps in improving the overall life of the network by equally utilizing the energy of all nodes and minimizes the energy hole problem in the network.

4.6. Travel Plan. Before packet transmission, we determine the travel plan between the source node to the sink node, which is not virtual or uses fake source nodes. In this work, we called routing is a travel plan. However, routing is the most fundamental issue in WSN since routing schemes play an important role in WSN. Attackers use the backtracking technique to catch the source node. In backtracking at some node, if the attacker is not able to hear any packet, then it requires to turn back and traverse to other directions. The communication range of the attacker and sensor node is the same. A random number R_n is generated by the source node which is compared with the already selected number P_n. If the $R_n \geq P_n$, then the real packet is sent in a clockwise direction and a fake packet in anticlockwise direction and vice versa. With the use of a fake path, an attacker cannot find the source location. It requires a greater number of backtracks, and finally, it receives fake packets and we also encrypt the fake messages and forwarded to the fake path. Real packets and fake packets are encrypted in the same manner so that the attacker cannot differentiate between them. It helps to increase the safety period of the network and unable to find the source location.

4.7. Data Packets Encryption. Data packets are encrypted and forwarded using a chaotic artificial neural network where we obtain chaotic sequences as a ciphertext. C-ANN is a combination of two algorithms such as Chaos Theory and Artificial Neural Network. There are several reasons to combine Chaos Theory with ANN: (1) it provides promising and efficient results for encryption and decryption, (2) Imitate function and structure of the human brain to be better, and (3) Chaos theory time series are considered as learning rate in ANN, which provide efficient results. In this work, we proposed a Hop Field Neural Network in ANN. With the use of keys generated using ECC with ALO, packets are encrypted using C-ANN.

Pseudocode 2 demonstrates the encryption process of packets using C-ANN. We generate encrypted packets by the following pseudocode.

Pseudocode 2: C-ANN Algorithm.1) Begin

2) Compute the length of key for encryption

3) Split the key into subsequences of 8 bytes

4) Initialize parameters μ and the initial point $X(0)$

5) For input message M (P_T)

6) Chaotic Sequence is follows: $X(1), X(2), X(3)\ldots$

7) $X(n+1) = \mu \mathrm{X(n)}(1 - \mathrm{X(n)})$

//Transforms binary representation

8) Binary Sequence is follows: $X(1), X(2), X(3)\ldots$

$B = (8n-8)b(8n-7)\cdots B(n-2)B(8n-1)$

9) $WF = B$

10) $WF + I/P$ function $\rightarrow C_T$

Few other biological-inspired routing protocols are also mentioned in [40].

5. Performance Evaluation

In this section, we evaluate the performance of C^2S^2LOOP by conducting various experiments. Firstly, we demonstrate how the simulations will impact the network performance. Then, we define the parameter description in terms of safety period, latency, energy consumption, total energy consumption, and network lifetime. Lastly, we illustrate the comparison of C^2S^2LOOP with previous works.

5.1. Simulation Model. Experiments conducted using the OMNeT++ model which consists of the following four parts: (1) network topology definition (NED) describes the module structure which consists of gates and parameters. It is saved in .ned, (2) message definitions (.msg) in which we can define various message types and insert more data fields; (3) it will convert message definitions into full-fledged C++ classes (.ini); and (4) it consists of simple module sources. They are C++ files with an extension of .h and .cc. The configuration files (omnet.ini, NED) for simulation are depicted in Figures 6 and 7.

Figure 8 shows the simulation environment and experiments conducted over Windows 7 (Ultimate-x86) Operating System. The sink node is located at the center of circular region X, Y = 3000m, 3000m. The number of sensor nodes deployed is 200, and nodes are uniformly and randomly distributed over the circular field. Nodes' initial energy level is equipped with 100 J. Some of the parameters used for simulation are given in Table 2.

5.2. Case Study: Panda Hunter Game. This paper provided a case study of SLP for the Panda-Hunter Game model. Sensor nodes are deployed in a large environment to monitor the behavior of Panda. Panda is a source here, which sends messages to the sink node and Hunter is an adversary. Figure 9 pictorial representation of Panda Game is implemented using our proposed model.

The Hunter observes data packets and traces panda location from the sink node same as mentioned in [41, 42]. Our

1) Begin
2) Compute the length of key for encryption
3) Split the key into subsequences of 8 bytes
4) Initialize parameters μ and the initial point $X(0)$
5) For input message M (P_T)
6) Chaotic Sequence is follows: $X(1), X(2), X(3)\ldots$
7) $X(n+1) = \mu \mathrm{X(n)}(1 - \mathrm{X(n)})$

//Transforms binary representation

8) Binary Sequence is follows: $X(1), X(2), X(3)\ldots$
   $B = (8n-8)b(8n-7)\cdots B(n-2)B(8n-1)$
9) $WF = B$
10) $WF + I/P$ function $\rightarrow$ C_T

Pseudocode 2: C-ANN Algorithm.

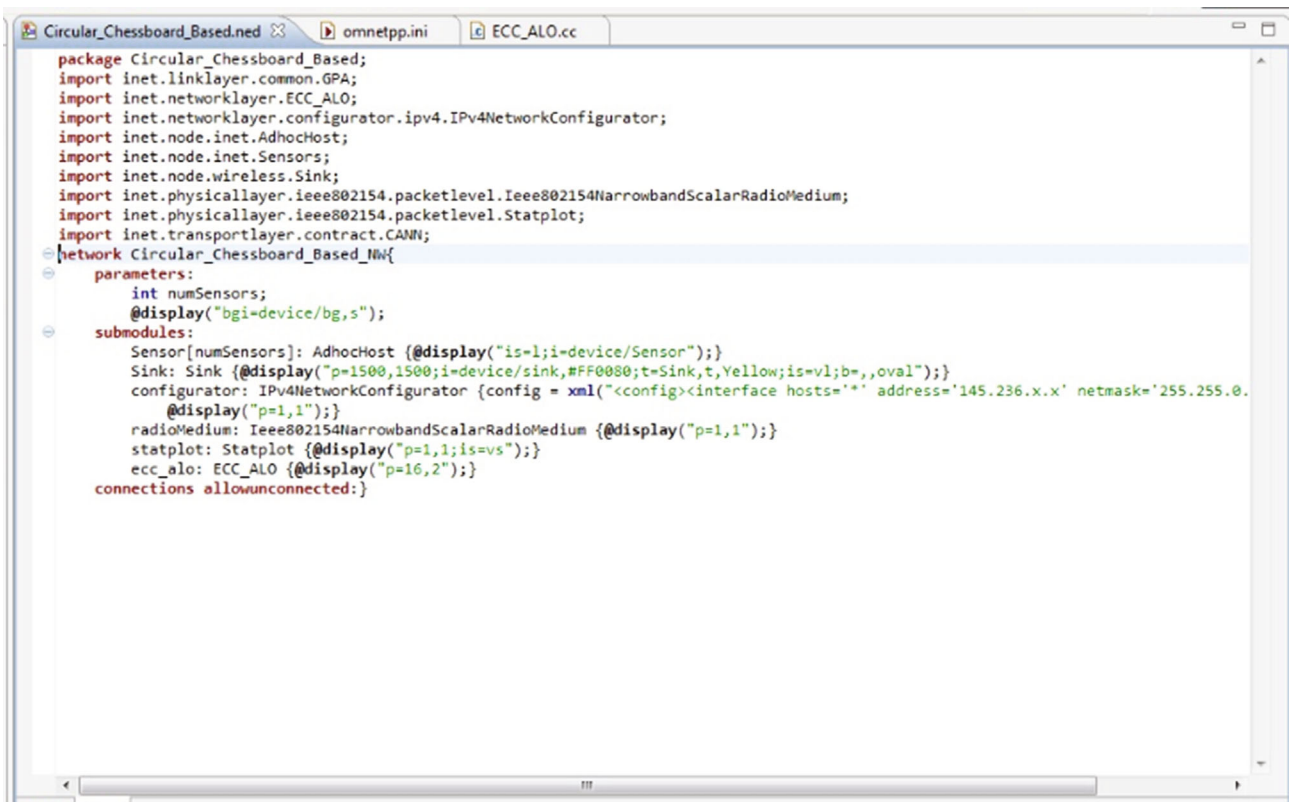

Figure 6: NED file for simulation.

SLP goal here is to increase the time required for Hunter to capture the location of the Panda (Safety Period). While sending messages to the sink node, energy usage is an important concern. Some of the functionalities of the Hunter are as follows: (1) it does not interfere with the sensor network, (2) it contains devices to measure Angle of Arriving message, (3) it moves at any rate and unlimited power, and (4) it has a global view of how the network works.

5.3. Definition of Simulation Metrics. In order to estimate the performance of C^2S^2LOOP, we consider the following QoS parameters.

5.3.1. Safety Period. It is the time duration taken to deliver a number of data packets from S to the S_{INK} before global attacker reaches the source location. Hence, this parameter is gauged from the number of packets successfully received at the S_{INK} before tracing of the attacker. It is computed by the following:

$$S_P = \sum_{i=1}^{n} T\left(P\left(S\right), P(S_{\mathrm{INK}})\right) + R(P\left(S\right), P(S_{\mathrm{INK}})), \quad (9)$$

where S_P is the safety period, $T(P\left(S\right), P(S_{\mathrm{INK}}))$ is the transmission time of packet P sending from S to S_{INK} node, and $R(P\left(S\right), P(S_{\mathrm{INK}}))$ is the packet received time at S_{INK} node.

5.3.2. Latency. It is defined as the amount of time duration is taken by a packet to reach its destination from the source to

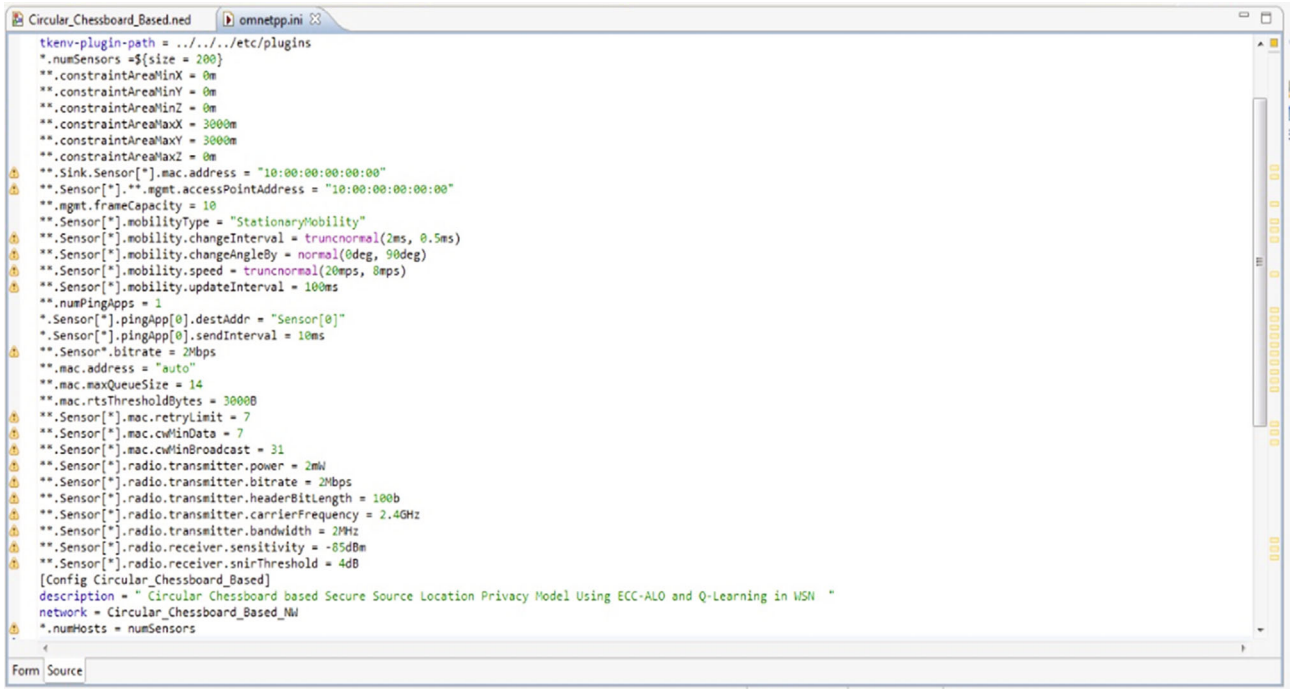

Figure 7: OMNETPP file used in simulation.

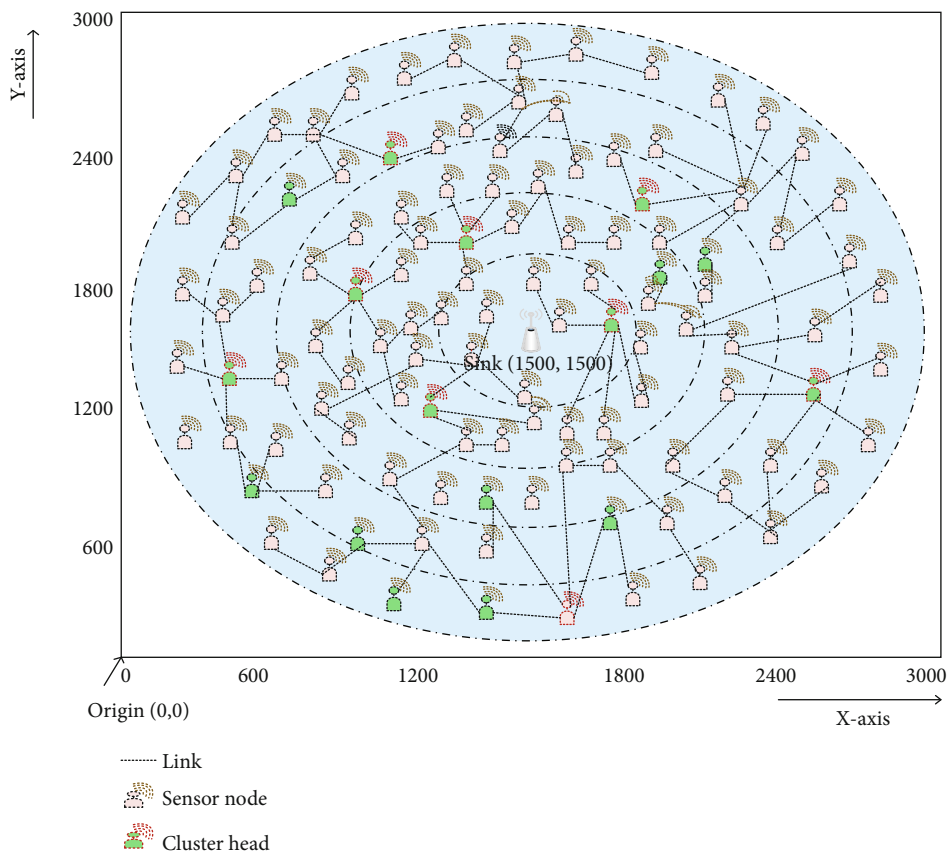

Figure 8: Simulation environment.

Table 2: Simulation parameters.

Parameter	Values
Simulation tool	OMNeT++4.6
Number of nodes	200
Number of circular fields	5
Simulation area	3000 m × 3000 m
MaxQueueSize	14
Sink mobility model	Random waypoint
Packet interval	10 ms
Number of packets	400
Packet size	1280 bytes
Path loss model	Free space path loss
Frequency	2.4 GHz
Channel bandwidth	20 MHZ
Transmission range	500 m
Header length	20B
Network layer protocol	IPv4
Key size	512 bytes
Simulation time	1000 ms
Bit rate	2 Mbps
Sensor mobility change angle	0-90 degrees
MAC protocol	IEEE 802.15.4
ALO	
No. of ants (population N)	50
Max iterations (t)	500
No of variables	6
Random number	(0,1)

the sink node. The computation of latency is based on the latency of queuing, processing, propagation, and transmission. It is computed by the following:

$$L = \mathrm{TR}_{S-\mathrm{SINK}} - \mathrm{TS}_{S-\mathrm{SINK}} \quad (10)$$

Where L is the latency, $\mathrm{TR}_{S-\mathrm{SINK}}$ is the time taken for packets transmission from the source node to the sink node, and $\mathrm{TS}_{S-\mathrm{SINK}}$ is sending time of packets transmitted from the source node to the sink node.

5.3.3. Energy Consumption. Let consider SN be the set of all nodes present in the network.

$$SN_i = \{SN_1, SN_2, SN_3 \cdots SN_{n-1}, SN_n\}. \quad (11)$$

Energy consumption E_C of SN_i is computed by the following:

$$E_C = E_I - E_R. \quad (12)$$

5.4. Comparative Study. In this section, a comparative study is conducted for the proposed and previous works such as CBA scheme [33], grid-based clustering [34], SLP-R [32], and two-phase routing [35]. Table 3 shows the comparison.

5.4.1. Safety Period Analysis. In a lot of previous works, source location privacy level is estimated in terms of safety period. It must be higher for better network performance. However, it increases when the distance between S and S_{INK} increases. Previous approaches are failed that achieved poor performance in terms of privacy level.

Figure 10 shows safety period analysis for hop count and distance between source node to the sink node. When the hop count increases, the safety period increases. CBA is designed with more privacy criteria for preserving source location privacy since it keeps only homogeneous sensor nodes for network deployment.

The safety period of CBA is closer to our C^2S^2LOOP which works well for global attacker and dummy message transmitted through random walk routing. In SLP-R, the source node can transmit a greater number of data packets before reaches the adversary to source origin. Furthermore, two-phase routing and grid-based clusters increase privacy level (safety period), but it decreases while the distance to S and S_{INK} increases. The average safety period regarding of it shows 156.66 s, 159.83 s, 87.5 s, 188.66 s, and 245.16 s for two-phase routing, SLP-R, grid-based clusters, CBA, and the proposed scheme, respectively.

Figure 11 indicates the performance of the safety period with respect to the distance between S to S_{INK}. Distance between S to S_{INK} increases gradually for all four previous works considered in this paper. In this case, the position of the source node is varied between 20 and 120 min intervals of 20 m. From the graph, it can be observed that the safety period of the proposed scheme increases as the distance increase compared to previous works. This is due to the fact that we determine the optimum route instead of random walk routing, phantom routing, and fake source routing. If a number of circular field increases, the safety period also increases with the help of distance between S to S_{INK}. The average safety period with respect to distance is 192.85 s, 194.14 s, 105 s, 214.28 s, and 290.42 s for two-phase routing, SLP-R, grid-based clusters, CBA, and the proposed scheme, respectively.

5.4.2. Latency Analysis. The latency in terms of the number of hop counts taken by the packets transmitted from the S to reach the S_{INK} is depicted in Figure 12. Our proposed approach shows minimal latency while all four previous works show maximal. The minimal delay in the proposed approach can be attributed to the fact that random routing paths are longer and selecting next-hop is not an optimal way. When the degree of randomness of the network is high, hop count is also high. However, we remark that the proposed scheme is best and it can adopt for Delay Tolerant Source Location Privacy Applications where privacy level and latency are sacrificed than previous works. In CBA, packet transmission is delayed due to alternating fashion of 50% nodes in the active stage and 50% of nodes in the sleep stage. Alternating fashion required large computations, and hence, packet delay is high.

Figure 13 depicts the performance of latency with respect to distance between S to S_{INK} node. From the plots, it can be seen that the proposed approach causes minimal latency for

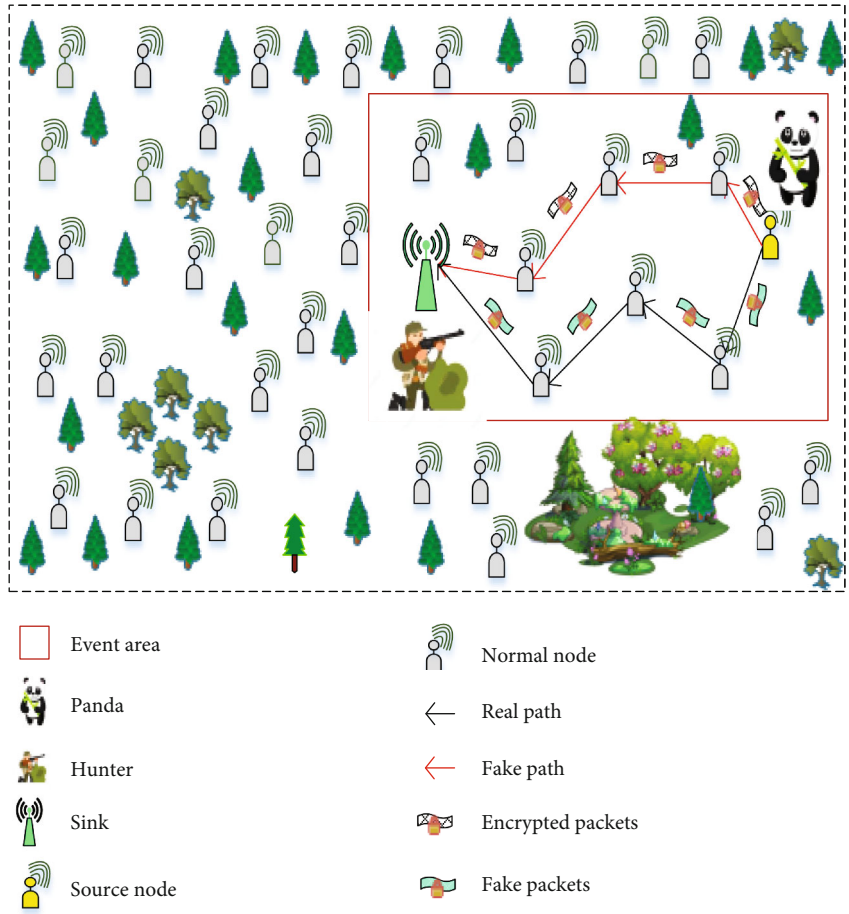

Figure 9: Panda game (proposed model use case).

Table 3: Comparison of proposed and previous approaches for different QoS parameters.

Method	Description	Parameters S_p	L	E_c	Demerits
CBA scheme	Source location privacy protection scheme is proposed against global attacker	→	↑	↑	(i) High energy consumption (ii) High delay
Grid-based clusters	The network is divided into number of clusters	↓	↑	↑	(i) Wastage of energy (ii) Large packet delay
SLP-R	Source location privacy using random routing	→	↑	↑	(i) Increases energy consumption due to random paths (ii) Privacy leakage
Two-phase routing	Escape angles based random walk routing	→	→	↑	(i) It utilized an excess amount of energy (ii) Network lifetime suffers due to multiple virtual source nodes

↑ = High, ↓ = Low, → = Medium.

packet transmission. Two-phase routing, SLP-R, grid-based clusters, and CBA require maximal delay. We proposed a circular chessboard-based SLP scheme, which main intention is to reduce packet delay and energy consumption. Among previous works, CBA and SLP-R require large latency. This can be attributed by random routing paths. Our solution here is the optimum formation of clusters in a circular chessboard and construct travel plan for routing packets. Thus, we obtained minimal latency when the distance between sensor nodes to the S_{INK} node is high.

The average latency with respect to hop count is 0.25 s, 0.49 s, and 0.131 s for the proposed approach and previous approaches. Similarly, the average latency with respect to distance is 0.25 s, 0.491 s, 0.465 s, 0.475 s, and 0.131 s for two-phase routing, SLP-R, grid-based clusters, CBA, and the proposed approach, respectively.

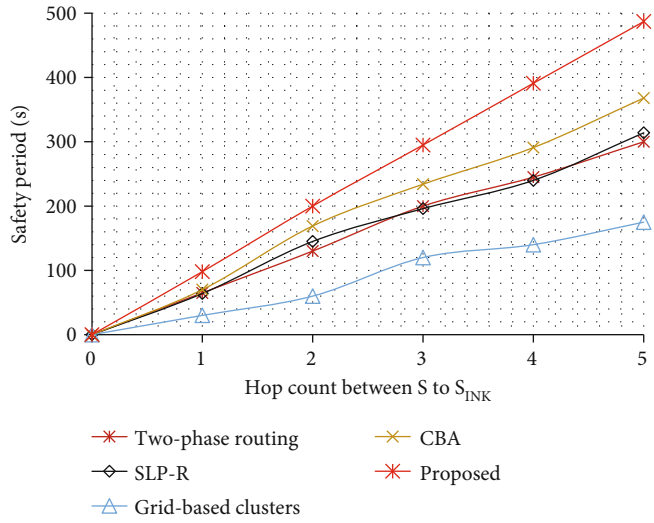

Figure 10: Safety period vs. hop count between SN to sink node.

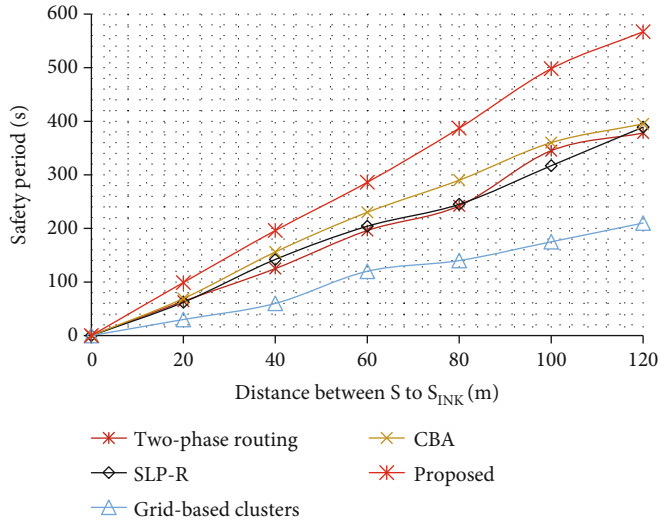

Figure 11: Safety period vs. distance between S to SINK.

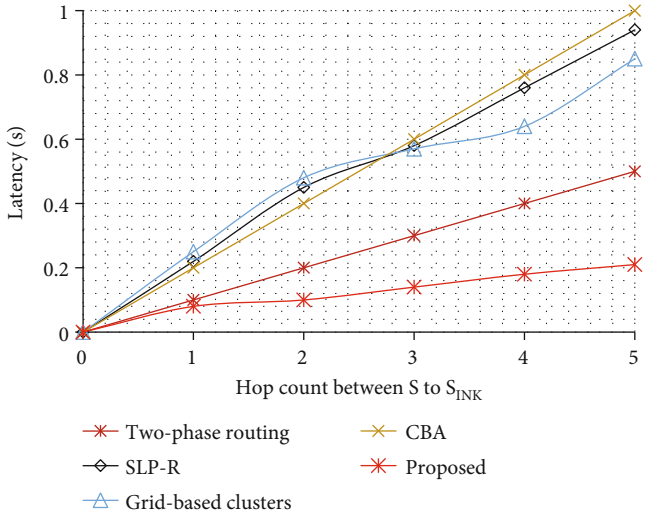

Figure 12: Latency vs. hop count between S to SINK.

5.4.3. Energy Consumption Analysis. Energy consumption to transmit a single bit of data packet is equal to processing 800 instructions. The energy consumption due to transmission of data packets from S to S_{INK} node is depicted in Figure 14. A large energy consumption primarily depends on the hop count the packets take to reach the S_{INK} node from source node S.

The energy consumption of the previous works is the maximum, and we obtained the least for the proposed approach. The reason for this least energy consumption by our proposed approach is as follows: (i) hop count between S to S_{INK} is less in the proposed approach compared to two-phase routing, SLP-R, grid-based clusters, and CBA. (ii) Our proposed approach forward aggregated packets through CH, which reduces large energy consumption than previous works. The average energy consumption for node-sending "n" packets is 935 J, 1010 J, 1250 J, 1041.66 J, and 524 J for two-phase routing, SLP-R, grid-based clusters, CBA, and the proposed approach.

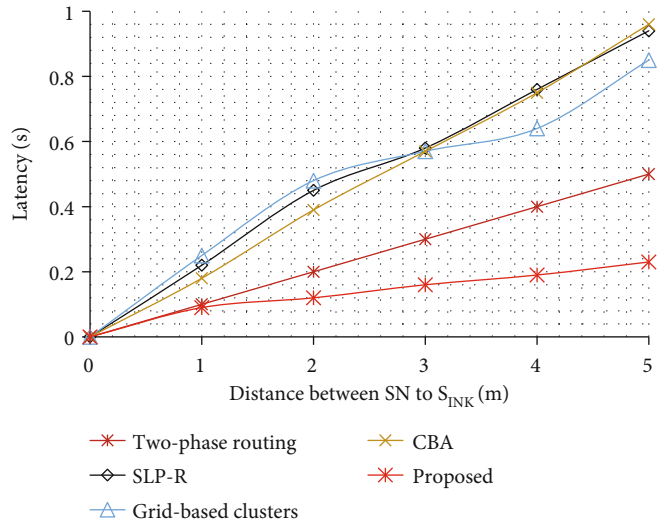

Figure 13: Latency vs. distance between SN to sink node.

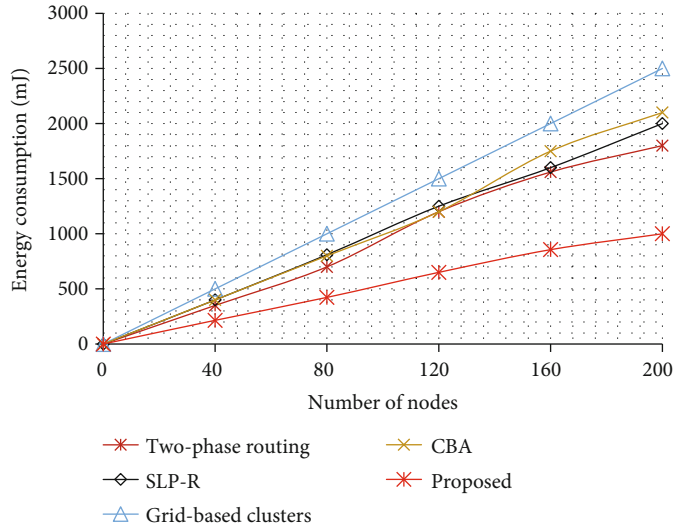

Figure 14: Energy consumption vs. number of nodes.

Table 4: Comparison between proposed vs. previous works.

Metric		Two-phase routing	SLP-R	Grid-based clusters	CBA	Proposed
Average safety period (s)	Hop count	156.66	159.83	87.5	188.66	245.16
	Distance	192.85	194.14	105	214.28	290.42
Average latency (s)	Hop count	0.25	0.49	0.465	0.5	0.11
	Distance	0.25	0.491	0.465	0.475	0.131
Energy consumption (mJ)		935	1010	1250	1041.667	524

6. Results Discussion

The efficiency of SLP in WSN is based on QoS requirements. Depends upon routing and network configuration (sensor node deployment and simulation values of each parameter), performance is varied. Energy is one of the important metrics, because sensor nodes are not replaceable and rechargeable. Hence, harvesting in WSN is considered for preserving source location privacy. Our proposed scheme does not harvest since we perform energy-efficient clustering for network management.

Table 4 illustrates the comparison between proposed and previous works in terms of average safety period, and latency based on hop count and distance, average energy

consumption, average total energy consumption, and average network lifetime.

The advantages of C^2S^2-LOOP are as follows: (i) a large safety period is obtained if the number of circular fields increases, safety period also increases with the aid of our proposed model (key generation, network topology management, travel plan, and packet encryption). (2) Low packet delivery delay from source to the sink node. This is due to our proposed algorithms such as ECC with ALO and chaotic-based ANN algorithm. These algorithms perform speedily and produce accurate and better performance than the earlier works. (3) C^2S^2-LOOP ensures full security and privacy of source node location. (4) In the case of data packet redundancy, energy consumption is minimized using clustering and hence the whole network is managed and also minimizes load at each sensor node. In addition, the individual transmission of packets to sink node is inefficient so a global attacker can be easily tracing packets through adjacent sensors.

7. Conclusion

In this paper, a novel C^2S^2-LOOP scheme is designed to protect the source location privacy in WSN. In SLP, QoS requirements are important such as safety period, packet delay, and energy consumption. Previous works in SLP do not consider all these parameters, which affects the network performance. These parameters are achieved with the aid of our C^2S^2-LOOP scheme. C^2S^2-LOOP invoked with the following operations: key generation, network topology management, travel plan, and data packets encryption. Sensor nodes authenticated using the elliptic curve ALO algorithm, which selects optimum secret keys, which are verified at the sink node. Next, the network topology is managed by the formation of clusters. In clusters, node residual energy is used for CH election. Intracluster communication is initiated by single-hop and intercluster routing (from source to the sink node) is implemented using clockwise and anticlockwise directions. To ensure data confidentiality, chaotic ANN is used in which data packets are encrypted and transmitted to the next-hop. Extensive experimentation is conducted using the OMNeT ++ network simulator that shows the that proposed C^2S^2-LOOP maximizes the safety period while minimizing energy consumption and latency as compared to previous works such as two-phase routing, SLP-R, grid-based clusters, and CBA.

8. Future Work

In the future, we have planned to extend our research in the following aspects:

(i) We deploy IoT sensors for monitoring SLP in real-time applications (disaster monitoring and control). Hence, we combine IoT and WSN environments

(ii) We prevent the network from security attacks (spoofing attacks, DoS attacks, and more)

(iii) We also protect sink location privacy against both global and local attackers

Data Availability

The data that support the findings of this study are all briefly introduced and all information are available in the manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia under Grant No. (KEP-19-611-38). The authors acknowledge with thanks the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia, for technical and financial support.

References

[1] Z. Qian, Q. Xiaolin, and D. Youwei, "Intelligent silent zone for source-location privacy based on context-awareness in WSNs," *Transactions of Nanjing University of Aeronautics and Astronautics*, vol. 35, no. 1, pp. 203–218, 2018.

[2] W. Chen, M. Zhang, G. Hu, X. Tang, and A. K. Sangaiah, "Constrained random routing mechanism for source privacy protection in WSNs," *IEEE Access*, vol. 5, pp. 23171–23181, 2017.

[3] M. Bradbury and A. Jhumka, "A near-optimal source location privacy scheme for wireless sensor networks," in *2017 IEEE Trustcom/BigDataSE/ICESS*, Sydney, NSW, USA, August 2017.

[4] A. Bushnag, A. Abuzneid, and A. Mahmood, "Source anonymity in WSNs against global adversary utilizing low transmission rates with delay constraints," *Sensors*, vol. 16, no. 7, p. 957, 2016.

[5] B. Chakraborty, S. Verma, and K. P. Singh, "Staircase based differential privacy with branching mechanism for location privacy preservation in wireless sensor networks," *Computers & Security*, vol. 77, pp. 36–48, 2018.

[6] C. Gu, M. Bradbury, J. Kirton, and A. Jhumka, "A decision theoretic framework for selecting source location privacy aware routing protocols in wireless sensor networks," *Future Generation Computer Systems*, vol. 87, pp. 514–526, 2018.

[7] Y. He, G. Han, H. Wang, J. Adu Ansere, and W. Zhang, "A sector-based random routing scheme for protecting the source location privacy in WSNs for the Internet of Things," *Future Generation Computer Systems*, vol. 96, pp. 438–448, 2019.

[8] G. Han, X. Miao, H. Wang, M. Guizani, and W. Zhang, "CPSLP: a cloud-based scheme for protecting source-location privacy in wireless sensor networks using multi-sinks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2739–2750, 2019.

[9] L. Mutalemwa and S. Shin, "Achieving source location privacy protection in monitoring wireless sensor networks through proxy node routing," *Sensors*, vol. 19, no. 5, p. 1037, 2019.

[10] Q. Wang, J. Zhan, X. Ouyang, and Y. Ren, "SPS and DPS: two new grid-based source location privacy protection schemes in wireless sensor networks," *Sensors*, vol. 19, no. 9, pp. 2074–2093, 2019.

[11] A. Jhumka, M. Bradbury, and M. Leeke, "Fake source-based source location privacy in wireless sensor networks," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 12, pp. 2999–3020, 2015.

[12] J. Wang, R. Zhu, S. Liu, and Z. Cai, "Node location privacy protection based on differentially private grids in industrial wireless sensor networks," *Sensors*, vol. 18, no. 2, pp. 410–425, 2018.

[13] S. Li, Y. Xiao, Q. Lin, and Z. Qi, "A novel routing strategy to provide source location privacy in wireless sensor networks," *Wuhan University Journal of Natural Sciences*, vol. 21, no. 4, pp. 298–306, 2016.

[14] A. Proano, L. Lazos, and M. Krunz, "Traffic decorrelation techniques for countering a global eavesdropper in WSNs," *IEEE Transactions on Mobile Computing*, vol. 16, no. 3, pp. 857–871, 2017.

[15] Y. Wang, L. Liu, and W. Gao, "An efficient source location privacy protection algorithm based on circular trap for wireless sensor networks," *Symmetry*, vol. 11, no. 5, pp. 632–646, 2019.

[16] M. Bradbury, A. Jhumka, and M. Leeke, "Hybrid online protocols for source location privacy in wireless sensor networks," *Journal of Parallel and Distributed Computing*, vol. 115, pp. 67–81, 2018.

[17] B. Chakraborty, S. Verma, and K. P. Singh, "Differentially private location privacy preservation in wireless sensor networks," *Wireless Personal Communications*, vol. 104, no. 1, pp. 387–406, 2019.

[18] H. Wang, G. Han, L. Zhou, J. A. Ansere, and W. Zhang, "A source location privacy protection scheme based on ring-loop routing for the IoT," *Computer Networks*, vol. 148, pp. 142–150, 2019.

[19] J. Kirton, M. Bradbury, and A. Jhumka, "Towards optimal source location privacy-aware TDMA schedules in wireless sensor networks," *Computer Networks*, vol. 146, pp. 125–137, 2018.

[20] C. Huang, M. Ma, Y. Liu, and A. Liu, "Preserving source location privacy for energy harvesting WSNs," *Sensors*, vol. 17, no. 4, 2017.

[21] H. Wang, G. Han, C. Zhu, S. Chan, and W. Zhang, "TCSLP: a trace cost based source location privacy protection scheme in WSNs for smart cities," *Future Generation Computer Systems*, vol. 107, pp. 965–974, 2020.

[22] N. Wang, J. Fu, J. Zeng, and B. K. Bhargava, "Source-location privacy full protection in wireless sensor networks," *Information Sciences*, vol. 444, pp. 105–121, 2018.

[23] S. Dehghani, B. Barekatain, and M. Pourzaferani, "An enhanced energy-aware cluster-based routing algorithm in wireless sensor networks," *Wireless Personal Communications*, vol. 98, no. 1, pp. 1605–1635, 2018.

[24] G. Han, L. Zhou, H. Wang, W. Zhang, and S. Chan, "A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things," *Future Generation Computer Systems*, vol. 82, pp. 689–697, 2018.

[25] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, Washington, DC, USA, 2004.

[26] N. Wang and J. Zeng, "All-direction random routing for source-location privacy protecting against parasitic sensor networks," *Sensors*, vol. 17, no. 3, 2017.

[27] Z. Jia, X. Wei, H. Guo, W. Peng, and C. Song, "A privacy protection strategy for source location in WSN based on angle and dynamical adjustment of node emission radius," *Chinese Journal of Electronics*, vol. 26, no. 5, pp. 1064–1072, 2017.

[28] J. Y. Koh, D. Leong, G. W. Peters, I. Nevat, and W.-C. Wong, "Optimal privacy-preserving probabilistic routing for wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 9, pp. 2105–2114, 2017.

[29] J. Long, M. Dong, K. Ota, and A. Liu, "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.

[30] G. Han, H. Wang, J. Jiang, W. Zhang, and S. Chan, "CASLP: a confused Arc-based source location privacy protection scheme in WSNs for IoT," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 42–47, 2018.

[31] G. Han, H. Wang, M. Guizani, S. Chan, and W. Zhang, "KCLP: a k-means cluster-based location privacy protection scheme in WSNs for IoT," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 84–90, 2018.

[32] M. Raja and R. Datta, "An enhanced source location privacy protection technique for wireless sensor networks using randomized routes," *IETE Journal of Research*, vol. 64, no. 6, pp. 764–776, 2018.

[33] Q. Zhou, X. Qin, and X. Xie, "Hiding contextual information for defending a global attacker," *IEEE Access*, vol. 6, pp. 51735–51747, 2018.

[34] M. F. Al-Mistarihi, I. M. Tanash, F. S. Yaseen, and K. A. Darabkh, "Protecting source location privacy in a clustered wireless sensor networks against local eavesdroppers," *Mobile Networks and Applications*, vol. 25, no. 1, pp. 42–54, 2020.

[35] R. Manjula and R. Datta, "A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs," *Pervasive and Mobile Computing*, vol. 44, pp. 58–73, 2018.

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

[37] O. P. Verma, N. Jain, and S. K. Pal, "Design and analysis of an optimal ECC algorithm with effective access control mechanism for big data," *Multimedia Tools and Applications*, vol. 79, no. 15-16, pp. 9757–9783, 2020.

[38] S. Mirjalili, "The ant lion optimizer," *Advances in Engineering Software*, vol. 83, pp. 80–98, 2015.

[39] M. Lemos, R. Filho, R. Rabêlo, C. de Carvalho, D. Mendes, and V. Costa, "An energy-efficient approach to enhance virtual sensors provisioning in sensor clouds environments," *Sensors*, vol. 18, no. 3, 2018.

[40] S. Ahmed, "Nature Inspired Optimization Techniques, a review for FANETs," *Sukkur IBA Journal of Emerging Technologies*, vol. 3, no. 2, pp. 40–58, 2020.

[41] N. Jan, A. Al-Bayatti, N. Alalwan, and A. I. Alzahrani, "An enhanced source location privacy based on data dissemination in wireless sensor networks (DeLP)," *Sensors*, vol. 19, no. 9, article 2050, 2019.

[42] N. Jan and S. Khan, "Energy-efficient source location privacy protection for network lifetime maximization against local eavesdropper in wireless sensor network (EeSP)," *Transactions on Emerging Telecommunications Technologies*, no. article e3703, 2019.