Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 5539382, 17 pages
https://doi.org/10.1155/2021/5539382

Research Article

Node Location Privacy Protection in Unattended Wireless Sensor Networks

ZhiGang Zhou,[1] Yu Wang,[1] PanPan Li,[2] XinGong Chang,[1] and JiWei Luo[1]

[1]*Shanxi University of Finance & Economics, No. 696, Wucheng Road, Taiyuan, Shanxi, China*
[2]*Jiaxing University, No. 56, Yuexiu South Road, Jiaxing, Zhejiang, China*

Correspondence should be addressed to Yu Wang; soberwy666@163.com

Received 19 February 2021; Revised 25 March 2021; Accepted 20 May 2021; Published 31 May 2021

Academic Editor: Paul Honeine

Node location protection is critical to the wireless sensor networks (WSN), especially for unattended environment. However, due to most of the static deployment and the limitations in energy, storage, and communication capabilities of the sensors, WSNs are vulnerable to various location (and derivative) attacks. In this work, we study the node location privacy protection issue from both aspects of attacks and defenses. First, we present a new two-phase location attack for two important types of nodes (including base station and source node). It can locate a base station node within few amounts of local wireless transmission monitoring and then reversely trace the location of the source node. Different from existing methods, the proposed attack determines the node location based on the transmission direction, which can break through existing defenses. Then, to defend against such attacks, we design a pseudospiral-based routing protocol for WSN. We analyze the performance of parameters such as routing probability, maximum detectable angle, hop count, and number of loops based on PU SBRF, MoRF, and PLAUDIT methods. The theory analysis and confrontation experiment of attack and defense show that the proposed scheme can protect the location privacy of the target node with moderate communication and computation overhead.

1. Introduction

As an important part of the Internet of things [1], unattended wireless sensor networks (UnWSNs) have been widely used in a variety of civilian and military applications (such as environmental monitoring, marine disaster warning, offshore oil, and gas exploration) [2]. However, due to the characteristics of static layout of sensors in unattended environment and the limitations in energy, storage, and communication capabilities of the sensors, UnWSNs are vulnerable to various location attacks [3]. Moreover, UnWSNs often involve the collection and transmission of large amounts of sensitive data, which concerns the national information security [4]. Once node location (including source node and base station) is leaked or captured by an attacker, it will result in a series of derivative attacks, such as sensitive data theft and military target intelligence collection. Therefore, privacy protection of node location becomes the top priority of UnWSNs security.

In wireless sensor networks [5], node location privacy-preserving technology is to protect the location of some important nodes (such as source node and base station) in the network. Specifically, locating the source node means that an attacker can discover valuable information nearby the source node [6], while locating the SINK node (also called base station) means that an attacker can attack the SINK node and steal important information [7]. Anonymous communication technology protects the location of the source node or base station by hiding the identity of the nodes in the communication process [8]. Although much work has been done for protecting sensor location privacy (such as LPSS (phantom source nodes) [9, 10], flooding [11], and pseudoinformation injection [12]), these technologies are either computational intensive schemes (such as large-scale broadcasting-based protocols and public-key cryptosystems [13]) or linear growth in communication costs. They are not suitable for UnWSNs, since most of the sensor nodes consist of low-cost and low-power radio devices.

In fact, many technologies have lost efficacy facing new challenges:

First, unattended sensors are mostly statically deployed in the absence of shelter environment; compared to traditional IOTs, node location information is more easily positioned. It makes the source node location privacy expose to the risk of a steep.

Second, the traditional single, fixed source node location privacy protection mode is difficult to resist the large sample of knowledge-related attacks. By the technique of data mining and analysis, such as area sampling monitor, association analysis, and neural network, adversaries can identify the relatively accurate location privacy protection pattern. It threatens the security of the location privacy of the node.

Last but not the least, most of the existing node location privacy protection technologies require complex angle calculation and routing computation, which is difficult to implement on a large scale under the existing UnWSN environment.

The objective of this paper is to provide a bidirectional location privacy protection mechanism for both source nodes and SINK nodes in an unattended wireless sensor network environment. Therefore, we first propose a new bidirectional node location attack(BDLA), including SINK attack and source node attack, which to the best of our knowledge, cannot be defended by existing node location protection schemes, especially in the case of multiple adversaries conspiring. Subsequently, in a targeted manner, we design a pseudospiral routing protocol based on Archimedes Curve for UnWSNs, in which we use Voronoi rule to partition the SINK nodes in the UnWSN. Through such data spiral routing, it not only improves the strength of SINK privacy protection but also balances the end-to-end communication quality. Furthermore, to cope with the data sampling attack, sensors generate and send pseudomessages to disturb the attackers on an irregular basis. It improves the ability of the source node location privacy resisted. The theory analysis and confrontation experiment of attack and defense show that the proposed scheme owns capable of protecting the location privacy of the target node with moderate communication and computation overhead. The contributions of the paper are summarized as follows:

(1) We first study a new bidirectional node location attack (BDLA) scheme in UnWSNs, and accordingly, we propose a pseudospiral-routing protocol based on the Archimedes curve to protect the location privacy of both source nodes and SINK nodes

(2) We construct a one-by-one mapping relationship between Vcell and SINK based on the Voronoi rule, aiming to minimize the communication overhead of sending information from a given source node to the nearest SINK

(3) To respond to data sampling attacks, we design a strategy in which the sensors generate and send false messages to disturb the attacker from time to time, making our mechanism more efficient

(4) Furthermore, our extensive experiments on a test bed demonstrate the effectiveness and practicality of the scheme

The rest of the paper is organized as follows. Section 2 overviews related work in current decades. Section 3 introduces the network model, attack capability hypothesis, and attack strategy proposed for important sensor nodes. Section 4 provides the detailed description of the proposed mechanism designs for node location privacy protection in UnWSNs. Section 5 gives thorough analysis of privacy guarantee. Section 6 reports our experimental study that evaluates the performance of our solution, followed by the concluding remarks in Section 7. Symbols are summarized in Table 1.

2. Related Work

Over the past few decades, there has been a lot of interest in technologies related to WSN. Nayyar et al. [14] provide in-depth analysis of simulation tools available for simulating almost everything considering underwater sensor network and comparing the features provided by every simulation tool, and routing protocols for UWSN are presented. In addition, comparison of protocols is also mentioned by Nayyar et al. [15] on the basis of various characteristics such as routing technique, packet delivery ratio, energy efficiency, packet delay, and localization to give a clear picture of the benefits and shortcomings of each and every enlisted protocol for UWSN. Furthermore, John et al. [16] discussed the functioning of various location-based opportunistic routing protocols proposed for UWSNs and evaluated the performance of two major protocols and VBF and HH-VBF using simulations in Aqua-Sim, but the performance of these protocols comes down with communication voids in the network.

In recent years, a series of inspiring techniques have sprung up. Current location privacy protection strategies are mainly classified into path camouflage technology, trap-inducing technology, and access control technology.

In the research field of path camouflage technologies, Ozturk et al. [11] proposed a privacy protection method for source node location based on the random walk thought "phantom routing," but the overhead is too large. In [9], authors made further improvements to "phantom routing" and proposed a directional walking technique based on sectors and skipping steps, and it is greatly reduced overhead. PUSBRF protocol [17] can generate phantom source nodes that are far away from the real source node and geographically diverse. It increases the cost of backtracking by attackers and can effectively resist local traffic attacks. SPENA protocol [18] makes it difficult for an attacker to trace the source node by modifying the packet and dynamically selecting a routing node. However, the implementation process of using the encryption technology to hide the source information is complex, similar methods include the EELP protocol [19]. The LPMS protocol [20] uses a random data receiving scheme to implement a dynamic

Table 1: List of symbols used in this work.

Symbol	Explanation
R, r	Radius
L, l	Line and tangent
D	Domains
N, n	Node set and nodes
C	Class
B	SINK
V	Vcell
H	Index set
$k_{i,B}$	Pairwise key
h_{fake}	The maximum number of times a pseudomessage is forwarded
T	Timer
p	Routing probabilities

SINK node, which has high privacy protection intensity, but has a greater impact on the end-to-end communication quality. Long et al. [21] propose a routing strategy based on tree structure, which is used to hide the location privacy of the source node, and this scheme is effective to improve the privacy protection while maximizing the network lifetime. The literature [22] hides the location information of the source node by randomly selecting intermediate nodes and a network mixing ring, but it consumes too much energy. The literature [23] also adopts the random walking strategy of camouflage packets and real packets. The real data packets would randomly walk in a certain stage to hide the transmission direction, while the camouflage data packets are injected into the intersecting nodes of two or more shortest paths so that the attacker cannot determine the real route.

In the field of trap-inducing technologies, the PeCo protocol [24] protects the privacy of source node and base station by using camouflage routing path based on pseudobase station, but the use of flooding in backbone network leads to high energy consumption. In [25], authors propose a routing scheme based on the loop, where the network topology consists of multiple routing and routing paths. The data is sent to the receiving node via the nearest routing loop to protect the location privacy of the base station. The data in the SRCRR protocol [26] is stored randomly in the middle node in the routing process, and the SINK node periodically collects the data sent by the intermediate node in the semicircle circular movement, so as to prevent the attacker from predicting and tracking its position and moving mode. Similar to the SRCRR protocol, the literature [27] uses a receiving SINK toroidal region route, and the source node randomly selects nodes within the star region around the SINK node. If the star region is large enough, the attacker could not monitor the entire zone to protect the source node location information. The literature [28] protects the location privacy of the base station by introducing false data that balances the traffic density in the network. In addition to protecting the location of the source node privacy, the literature [29] adopts the strategy of random walking and bidirectional tree to protect the location privacy of the destination base station.

In the research field of access control technology, the STAP protocol [30] uses the packet forwarding strategy of the joint layer to implement data forwarding and grouping under unknown node location, which can resist local and global attacks. However, it needs to lay out storage nodes, and the quality of communication is unstable. To improve the network energy consumption and its communication efficiency, the ADRing protocol [31] based on anonymous quantization dynamic obfuscation ring uses the dynamic obfuscation loop and the anonymous measure evaluation mechanism based on the location quadrant to protect the location privacy of source node. MQA Protocol [32] uses encryption technology to realize the anonymity of node IDs, but the frequent process of encryption and decryption leads to an inefficient system. The PPSNC protocol [8] based on GEVs (global encoding vectors) carries on the homomorphic encryption to the data stream. Because the ciphertext data flow is not detectable, it can effectively prevent the traffic analysis attack, but this method is computationally expensive.

In summary, existing techniques have many shortcomings, such as reducing the communication quality while protecting the source node location privacy, or not enough to reduce the energy consumption while protecting the source node location privacy, so in this paper, we design a high-performance location privacy protection method, which improves the ability to protect the privacy of the source node location and ensures a moderate communication and computation overhead.

3. Network Model

The wireless sensor network consists of many sensor nodes and several SINK nodes deployed in the monitoring area. The sensor node forms a multihop and self-organizing network system by means of wireless communication, which aims to perceive, collect, and process the information of the objects in the network coverage area and send to the user. The network model is similar to the Panda_Hunter game [11] (as shown in Figure 1), where the sensor network is used to monitor panda activity and location. Once the panda is discovered, the nearest sensor, as the source node, will send the observations periodically or immediately to the SINK nodes in the form of messages. The SINK nodes send information to the user via the Internet or satellite.

The goal of this work is to make it difficult for an attacker to locate the target object (such as a panda) by locating SINKs and stealing the message or reversely locating the source node. Without loss of generality, in this work, we make the following assumption for the entire UnWSNs:

(1) The sensor nodes are distributed uniformly across the network. Assume that each sensor node has a transmission range r_s, which is the same with the distance of the nearest neighbor nodes, and any two nodes in the network can communicate by one hop or multihop mode.

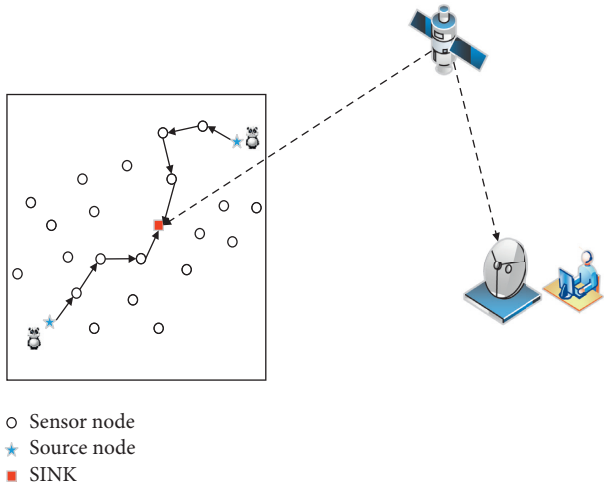

Figure 1: The Panda_Hunter game model.

(2) The whole network may have several SINKs, and the location of the base station is random.

(3) At the same time, the network may have multiple source nodes, and the mapping relationship between source nodes and SINKs is not fixed (i.e., given a source node, it can send messages to any SINK in the network).

(4) Sensor nodes and SINKs are indistinguishable from appearance, but the difference is that a sensor has limited computation and power, while the base station is not constrained in these aspects.

4. Attack Model

4.1. Attack Capability Hypothesis. In this work, we assume that the adversaries have strong hardware configurations and may be colluded in the network. Specifically, the adversaries have the following characteristics:

(1) Passive attack: each adversary can monitor the messages sent by nodes within its communication scope. Assume that each sensor has the same communication radius r_s, and the adversary's monitoring radius is denoted by $r_d\,(r_d = k \times r_s\,(k > 1))$.

(2) Limited local attack capability: sensor nodes are deployed in a wide range of areas, making it difficult for attackers to monitor global traffic on such a large UnWSN. That is, we assume that the coverage of the whole UnWSN is a circle area with radius $r_u\,(r_u = n \times r_s\,(n \gg k))$.

(3) Node locating: an attacker can locate nodes that are outside its monitoring scope through existing node-locating techniques (such as the sending signal strength [33]).

(4) Collusion attack: in order to locate the nodes (i.e., source nodes or SINKs) with high precision, several adversaries may collude with each other to share nodes' location information they obtained. However, we assume that the monitoring scope of the adversaries cannot cover the entire network. In fact, if the adversaries could monitor the whole UnWSN, then they can monitor the target object's activity directly without relying on the network.

4.2. Overview of Node Attack Strategy. Based on attack capability hypothesis, we propose a bidirectional node location attack (BDLA) scheme. BDLA first determines the location of the SINK by the direction of the message adversaries monitored. Let $L(n_i, n_j)$ be the line through the nodes n_i and n_j. For any two independent lines L_i and L_j, if L_i and L_j intersect, then the intersection is the candidate SINK. More generally, if there are $m\,(m > 2)$ monitoring regions for conspirators who generate m fitted lines, then they compute all the intersections, and estimate the locations of the SINKs from these intersections. Based on this, BDLA reversely traces the location of the source nodes. Specifically, BDLA consists of five steps:

(1) Location sampling with multimonitoring regions: in the network, conspirators choose m $(m > 1)$ regions as the monitoring domains $\mathbf{D}\{D_1, \ldots, D_m\}$, where any $D_i \in \mathbf{D}$ has a node set N_i, and each node $n_i \in N_i$ locates in the monitoring domain D_i. As shown in Figure 2(a), four monitoring domains locate close to nodes $\{n_1, n_2, n_3, n_4\}$, respectively. The adversaries try to find several short forwarding paths $\{\langle n_i, n_j\rangle, \ldots, \langle n_k, n_t\rangle\}$ via passive attacks (such as eavesdropping) or compromising on some nodes.

(2) Candidate SINK location discovery based on multiparty coordination: according to the location sampling information of the nodes monitored, the attacker can use the least squares method to fit the position into a line l: $y = ax + b$, where a and b can be expressed as follows:

$$a = \frac{N\mp \sum_{n=1}^{N}(x_n \times y_n) - \left(\sum_{n=1}^{N} x_n\right)\left(\sum_{n=1}^{N} y_n\right)}{N\left(\sum_{n=1}^{N}(x_n)^2\right) - \left(\sum_{n=1}^{N} x_n\right)^2},$$
$$b = \frac{\left(\sum_{n=1}^{N} y_n\right)}{N} - a\frac{\left(\sum_{n=1}^{N} x_n\right)}{N}. \quad (1)$$

(3) SINK location estimation: by fitting the position sampling of the nodes monitored and removing noise, the attackers can locate the SINKs. Let the position set of k estimate SINKs be LS. The attack can use a certain clustering method to clean the noise point in LS. The main steps of the denoising process are divided into 3 steps: (1) using agglomerative hierarchical clustering to LS, (2) finding the maximum class $C_{\max}$, and (3) locating the cluster means $\mathrm{Loc}(C_{\max})$, which are the location estimation of the SINKs after denoising, as shown in Figures 2(c) and 2(d).

(4) Based on SINKs' location, the source node can be backtracked by data acquisition and fitting, as shown in Figure 2(e).

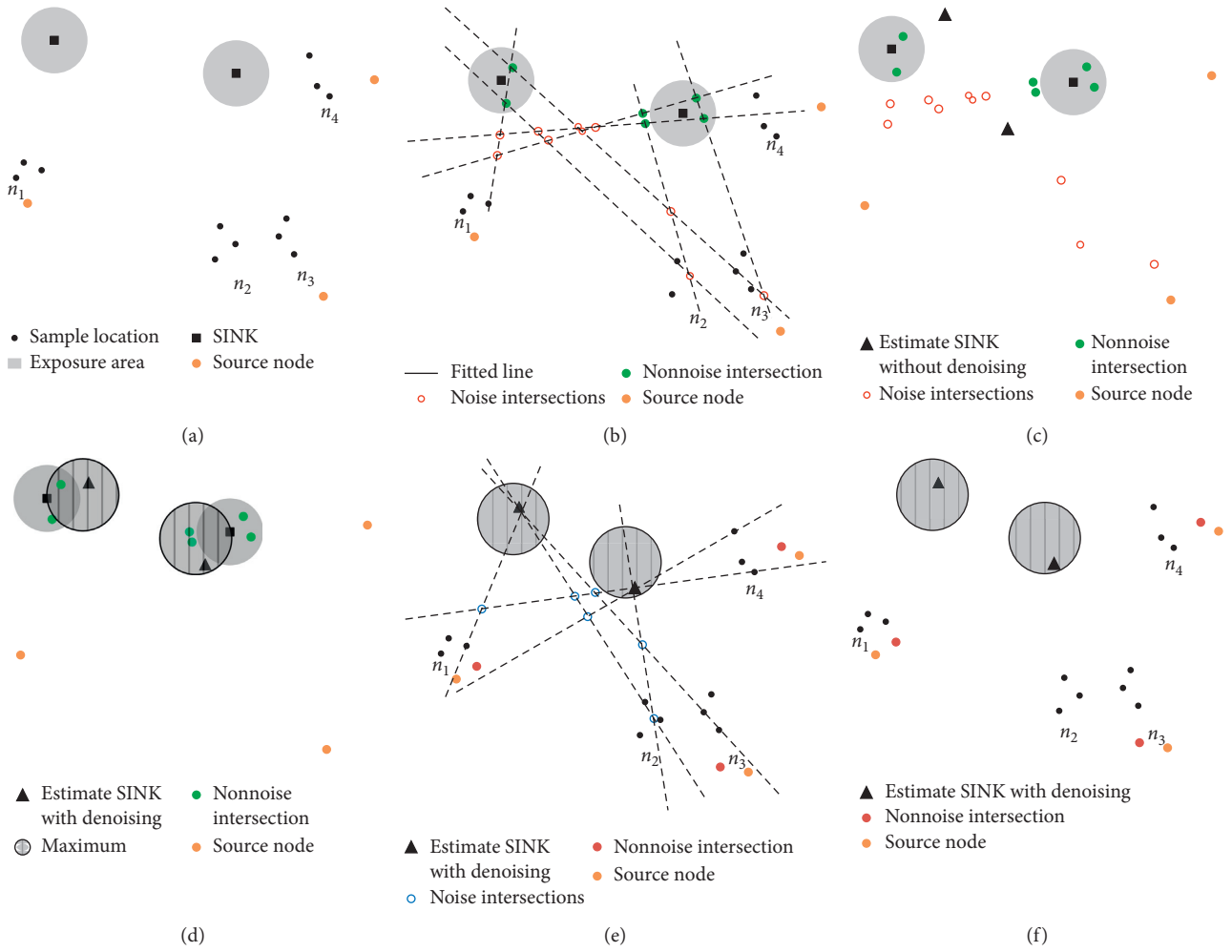

FIGURE 2: Bidirectional node location attack (BDLA) scheme procedure. (a) Location sampling. (b) Line fitting. (c) SINK estimation without denoising. (d) SINK estimation with denoising. (e) Source node estimation without denoising. (f) Source node estimation with denoising.

(5) Based on the source node set with noise, in the same way, the attacks use cluster cleaning again to get the denoising location of the source nodes with high probability, as shown in Figure 2(f).

5. Node-Location Privacy Protection Protocol in UnWSNs

5.1. Observation. In the proposed attack model, the adversary can locate the location of the source nodes mainly by backtracking the transmission path of the information in the detection range. By observation, it has become the focus of contention between the two sides for the attacks and defenses of the information transmission directions and the traces. Therefore, how to find the balance between the communication cost and the privacy-aware transmission path in all the candidate paths from the source node to the SINK is a question.

Intuitively, in all 2D graphics, the circle has the following two characteristics: (1) in the European rectangular coordinate system, for any two nodes on it, the tangent directions are different and (2) the integral of all angles between the adjacent nodes and the center of the circle is 360. Therefore, routing strategies with a (partial) ring in the path become the mainstream privacy protection solution for UnWSNs.

As shown in Figure 3, we denote by d the distance between the source node and SINK, by $\phi x_1 + (1-\phi)x_2\,(0<\phi<1)$ the center of the circle and by R the radius of the circle. Let D be the possible monitoring domain of adversaries. Comparing Figures 3(a) and 3(b), the suspected range covering the source node depends on the value of the parameter ϕ and R. Make R a fixed value, and when $\phi \longrightarrow 0$, the center of the circle becomes closer to the SINK. According to the attack model, the larger the angle θ formed by the tangent l_1 and l_2, the wider the scope of the suspected range $S = \phi\pi l^2/360$ (and vice versa). For ϕ to be fixed, when R increases, the angle θ will increase, and the scope of the suspected range S will increase as θ increases (and vice versa). However, in real scenarios, due to the limitation of the communication overhead, the size of the circle radius R is restricted correspondingly, and the value of ϕ is positively correlated with D. From the perspective of the actual effect of privacy protection, the value of ϕ is also restricted. Therefore, the existing location privacy protection

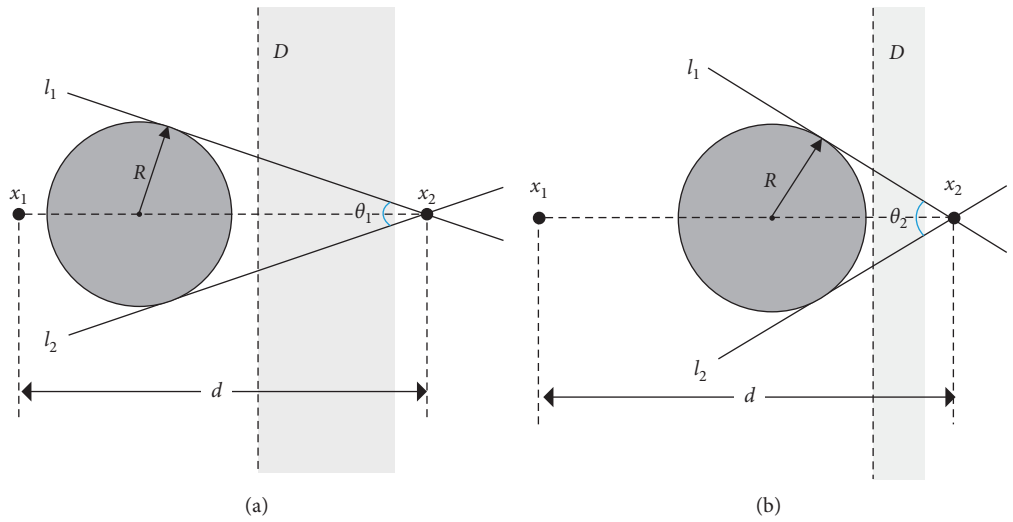

Figure 3: The relationship between the proposed privacy protection policy and attacker's monitoring domain.

scheme for WSNs cannot realize the theoretically optimal routing strategy that takes account of the node location privacy protection and communication overhead in ideal environment.

Based on the above observation, focusing on multi-SINK scenario, we propose a pseudospiral-based node location privacy protection routing protocol for UnWSNs. As shown in Figure 4, each node divides the other nodes within its perceived range into three subnode sets, including the loop-left node set (take the clockwise spiral as an example), the centripetal node set, and the centrifugal node set, where the loop-left node set is not required. In the hop-by-hop information routing, each relay selects a node in the corresponding loop-left node set or other node set to send the message with the given probability. It should be noted that the information is encrypted transmission, and the decision of which set would be chosen between the centripetal node set and centrifugal node set is set in the encrypted state bit of the information. Therefore, adversaries cannot infer the relative position among the relay and SINKs by the message forwarding relationship. Specifically, the proposed routing protocol includes two stages, namely, network initialization and message transmission.

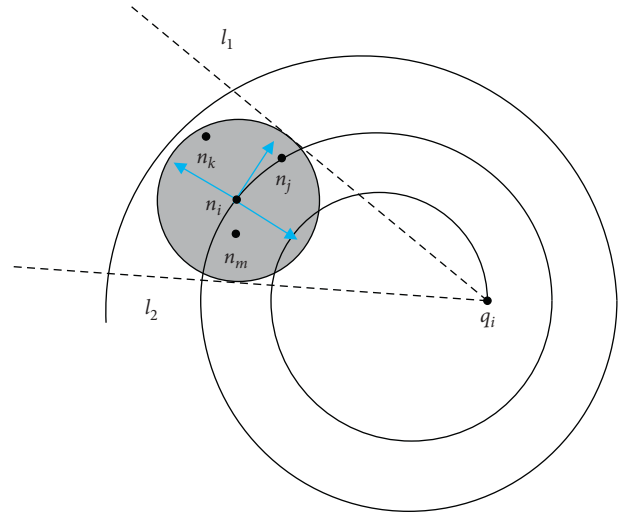

Figure 4: Schematic diagram of a pseudohelix-based node location privacy protection routing protocol.

5.2. Network Predeployment Initialization. We assume that the network is secure in the stage of predeployment and initialization. According to Voronoi rule [34], the whole network is divided into a set of Voronoi cells (Vcell), where each SINK B_i in the network is assigned to a Vcell. It makes the following:

(1) Each subspace Vcell has and only has a SINK

(2) Given a Vcell_i and the corresponding SINK B_i, for any node n_i assigned to Vcell_i, B_i is the nearest SINK compared with the others; if n_i is at the boundary node between the two Vcells, the equation is established

Based on the Voronoi rule, we build a one-by-one mapping relationship between a Vcell and a SINK, which aims at reducing the communication overhead of sending information from a given source node to the nearest SINK as much as possible. Figure 5 shows a network space partitioning instance, and $\{B_1, B_2, B_3, B_4\}$ are four SINKs in the network which are divided into four Vcells $\{V_1, V_2, V_3, V_4\}$, respectively. Given the source node n_i located in Vcell V_1, B_1 is the nearest SINK. However, it gives rise to the following problems: (1) due to the irregular shapes of the generated subspaces, it is difficult to be transformed by the coordinate representation; (2) as a result of the number of subspaces partitioned by the Voronoi rule is equal to the number of

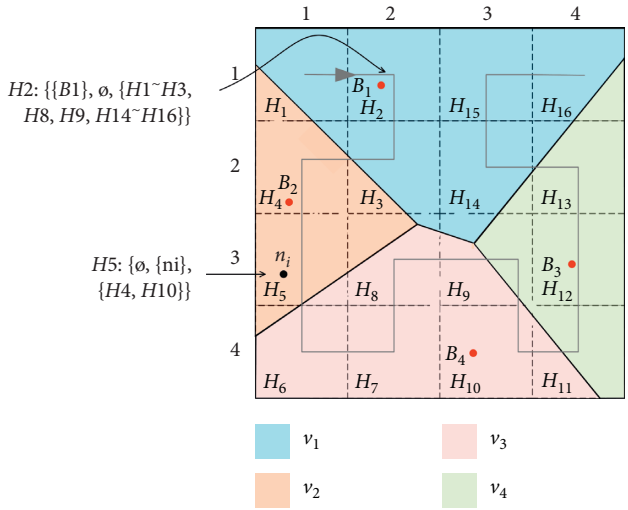

Figure 5: An example of Voronoi-based domain division.

SINKs, it could not to be fine-grained refinements to regional division.

To solve these problems, on top of the Voronoi diagram, we superimpose a regular $M \times M$ grid of arbitrary granularity, where each grid cell (Gcell) stores information about the Vcells intersecting it. The information recorded in each Gcell G_{ij} can be viewed as a tuple (B, N, H), where B is SINKs contained in this Gcell, N is the sensors contained in this Gcell, and H is an index set that records such Gcells: (1) when $B = \varnothing$, H records such Gcells that contain SINKs in the Vcells intersecting of the target Gcell G_{ij}; (2) $B \neq \varnothing$, and H records all Gcells in the Vcells covering B. For example, Figure 5 depicts a 4×4 grid, where G_{12} containing B_1 stores $(\{B_1\}, \varnothing, \{G_{11}, G_{12}, G_{13}, G_{14}, G_{21}, G_{22}, G_{23}, G_{24}, G_{32}, G_{33}\})$, G_{31} intersected by $\{V_2, V_3\}$ stores $(\varnothing, \{n_i\}, \{G_{21}, G_{43}\})$, etc. In practical, we use the Hilbert filling curve [10] to map the 2D regions into 1D values. The benefit of using Hilbert curve is that it describes the proximity relation among Gcells by using Hilbert ordering. 1-D values based on Hilbert ordering can be indexed by a $B+$-tree as well [35, 36]. Therefore, H of G_{12} (H_2 corresponding with the Hilbert value of G_{12}) records $(\{B_1\}, \varnothing, \{H_1 \sim H_3, H_8, H_9, H_{14} \sim H_{16}\})$.

Figure 6 depicts the data structure for the network. The core idea is to employ a grid-based $B+$-tree (gB+-tree) that hierarchically decomposes the spatial space into l levels tree structure, where the ith level has 4^i Gcells. The root node of the gB+-tree is of height zero and covers the whole spatial space. The internal nodes located in the $[1, l-1]$th level dynamically maintain a tuple $(|B|, |N|)$, respectively, where $|B|$ records the number of SINKs within its subregion and $|N|$ keeps the number of sensors within its subregion. The leaf nodes located in the lth level maintain a triple (B, N, H), respectively. And, leaf nodes use Hilbert filling curve that maps the 2D space to 1D. The 1D values can be arranged in a $B+$tree. For example, in Figure 6, there are 8×8 grid, and the capacity of each node is 4. Each entry in a node has a key, a value domain, and a pointer to its child node. For the leaf level, the Hilbert values are the keys of the corresponding Gcells, while all the keys in a leaf node are less or equal to the key of the corresponding parent node. For the value domains in leaf nodes, each entry maintains a triple (B, N, H) (e.g., H_7: $(\varnothing, \{n_3, n_4\}, \{H_3, H_{11}\})$), whereas the value domains in internal nodes, each entry maintains the statistics from its child node, e.g., in the level 1, the value of the entry with key = 8 is $(0, 2)$ which means that, at the moment, there exists 0 SINK and 2 sensor nodes in the subregions $\{H_5, H_6, H_7, H_8\}$.

Obviously, the geographical location of the region with similar Hilbert line sequence is also neighboring. Combining the Voronoi rule and the Hilbert space filling curve, SINKs initialize the UnWSN with the following steps (as shown in Figure 7).

(1) Each SINK in the deployment domain divides the network space into several subdomains and sorts by using the Voronoi rule and the Hilbert space fill curve. Each sensor records its Hilbert serial number H_i and the Voronoi partitioning domain number Vcell_i, respectively, in the corresponding state code.

(2) Sensors in each Gcell boundary perceives the minimum upper Gcell sensor set and the maximum lower Gcell sensor set in its coverage range and marks them, respectively, as the centripetal node set and the centrifugal node set according to the relative position between sensors and the target SINK with the same Vcell.

(3) Each SINK calculates the sensor of the Archimedes Helix which is centered by itself and the radius of R and broadcasts it, while each sensor only receives the information sent by the target SINK with the same Vcell and marks it in the corresponding SINK.

(4) Each sensor perceives whether there are left (or right) sensors labeled as loop nodes. If it exists, it is recorded in the loop-left (or -right) node set.

5.3. Message Transmission. Each sensor n_i is preloaded with two pairwise keys $k_{i,B}$ and k_i and a hashing function F, where $k_{i,B}$ is shared between the node n_i and the SINK B; k_i is n_i's broadcast key that is shared between n_i and its neighbors. In addition, Wang et al. [37] proposed the concept of exposure domain, that is, the adversary is easy to trace the nodes nearby the source node to the location of the source node. To this end, massage transmission mainly includes the following three stages:

(1) $G(h)$-hops finite flooding: $G(h)$ is a random function, which randomly transmits message; $[0, h]$ hops away from the source node. Different from literature [9] that aims at finding a phantom source node away from the source node for h-hops, the purpose of this step is to generate random location disturbances, which prevent the adversary from the reverse derivation of the proposed strategy.

(2) (k, p)-routing: we denote by k the maximum number of loops required for routing, which is designed to prevent information from being lost in the circle and to effectively reduce communication

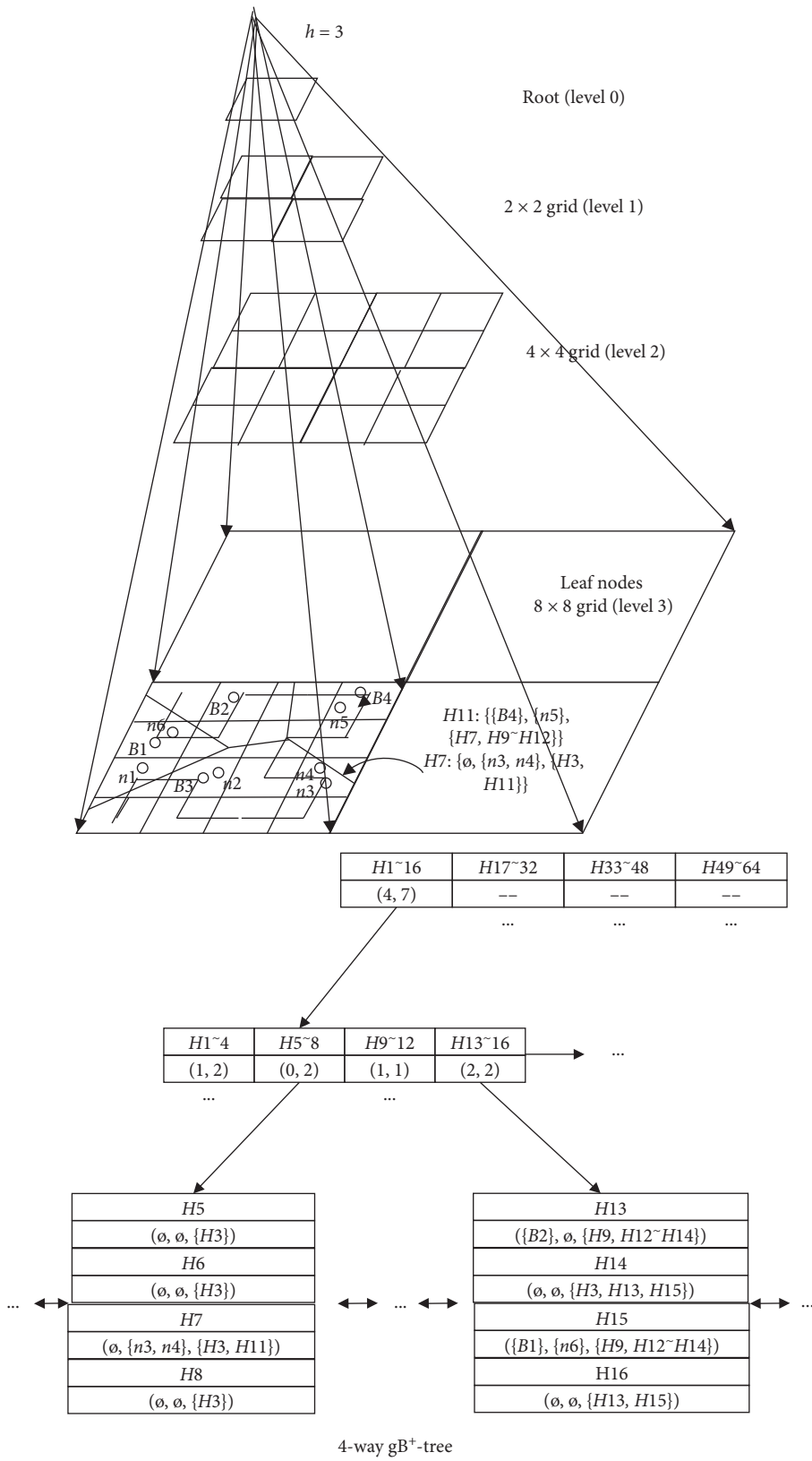

Figure 6: An example of Grid-based $B+$-tree.

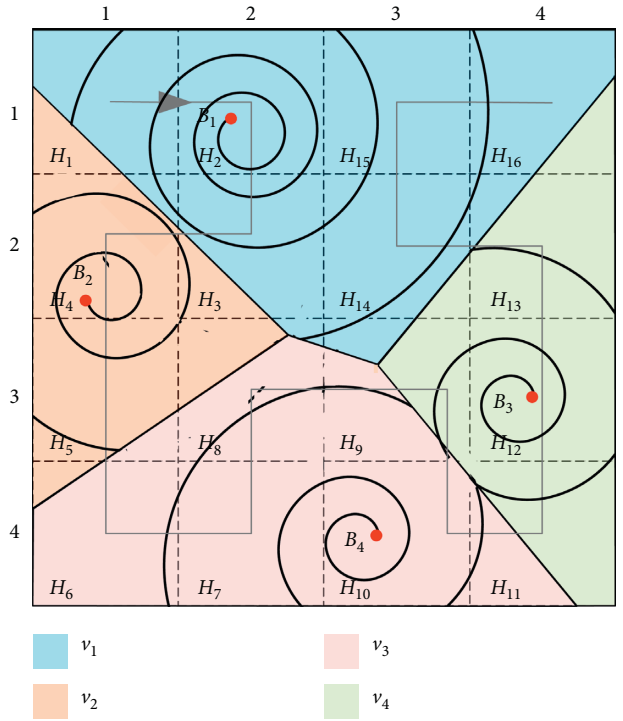

Figure 7: An example of pseudohelix-based message routing.

overhead, and by p the routing probability of choosing the node from the loop-left node set as the next relay. Correspondingly, $(1 - p)$ is the routing probability of choosing the node from the centripetal node set or the centrifugal node set as the next relay. It is determined by the status bits of the information for the selection of the centripetal node set or the centrifugal node set. When the message has not been routed to the SINK, the corresponding state bit is set to 1 (representing the centripetal node set); when the SINK receives the message, it would change its corresponding state bit to 0 (representing the centrifugal node set). Noted that, in real scenarios, to prevent location leakage problem that the angle θ spanned by the circle tangents is too small, the value of the parameter p is often not a fixed value, but is determined by a function $Q(h)$ with the reverse trend of the number of the message forwarding hops h.

(3) $G(h)$-hops SINK camouflage: because SINKs are only responsible for receiving information in the process of message transmission, it shows the in-degree is much larger than the out-degree. Therefore, we need to disguise it as an ordinary relay node. When the message is received by the SINK, similar to step (1), the SINK would continue to forward the message with limited hops $G(h)$.

The details of the algorithm are shown in Algorithm 1, and the algorithm flowchart is shown in Figure 8.

5.4. Pseudomessage Generation. In addition, to prevent adversaries from analyzing the message routing rules through big data monitoring and sampling technology, the sensors need to generate and send pseudomessages periodically to disturb the adversaries. To this end, each sensor node n_i preloads two random numbers during initialization: $\lambda\,(0 < \lambda < 1)$, h_{fake}, where λ represents the probability of generating a pseudomessage and h_{fake} represents the maximum number of times a pseudomessage is forwarded. However, it could cause message congestion in the network. Therefore, we introduce the trigger mechanism and the inhibition mechanism into the pseudomessage generation strategy:

(i) Trigger mechanism: each sensor contains a timer T_i. When the sensor node does not forward message as the source node or relay node for a long time $(T_i > T)$, the pseudomessage generation mechanism will be triggered, and the corresponding state value of the pseudomessage and its own state are changed to *Fake*. The value of the timer set for each sensor node varies, and when the pseudomessage is sent, the sensor's state value "*Fake*" will revert to *True* after m timer cycles.

(ii) Inhibition mechanism: when the node is forwarding message with the state value of "True" if receiving a message with the state value of "Fake" at the same time, the node will discard directly, regardless of the parameter settings (e.g., h_{fake}).

INPUT: n_i: start sensor node; k: the maximum number of loops passed;
p: routing probability; U_x: the centripetal node set of n_i;
U_l: the centrifuge node set of n_i; U_c: the loop-left (or -right) node set of n_i;
Vcell_i, Gcell_i: the corresponding Vcell and Gcell in which n_i is located;
$W(*)$: random function;
OUTPUT: n_j target sensor node;
PROCEDURE:

```
(1)  while k > 0 do
(2)    n_j = n_i;
(3)    if n_j ≠ SINK then
(4)      if n_j · U_c ≠ ∅ & W(*) ≥ p then
(5)        randomly choose a node n_k from n_j · U_c, let n_j = n_k
(6)      else
(7)        randomly choose a node n_k from n_j · U_x, let n_j = n_k
(8)      if SINK · |Gcell_SINK| > n_i · |Gcell_i| then
(9)        let n_i · Vcell_i be the subset that is bigger than |Gcell_i|
(10)       n_j · Gcell_i = |min(n_i · Vcell_i)|
(11)     else
(12)       let n_i · Vcell_i be the subset that is smaller than |Gcell_i|
(13)       n_j · Gcell_i = |max(n_i · Vcell_i)|
(14)   else
(15)     let n_j's state be 0
(16)     randomly choose a node n_k from n_j · U_l, let n_j = n_k
(17)     if SINK · |Gcell_SINK| > n_i · |Gcell_i| then
(18)       let n_i · Vcell_i be the subset that is smaller than |Gcell_i|
(19)       n_j · Gcell_i = |max(n_i · Vcell_i)|
(20)     else
(21)       let n_i · Vcell_i be the subset that is bigger than |Gcell_i|
(22)       n_j · Gcell_i = |min(n_i · Vcell_i)|
(23) return n_j
```

Algorithm 1: Message security transmission algorithm.

6. Experiments

We implemented experiments to evaluate our routing protocol (named MST for ease of description). The simulation experiments use Ubuntu 16.04LTS. We adopt simulation software NS2 to build UnWSN, where 10,000 sensors (including 10 SINKs) are randomly deployed in the region of $1000\,\text{m} \times 1000\,\text{m}$. The position coordinates of each node is added a random disturbance ε, which follows a Gaussian distribution, that is, $\varepsilon \sim N(\mu, \varepsilon^2)$. In addition, in order to compare and verify our proposed protocol MST with PU SBRF [17], MoRF [38], and PLAUDIT [28] in the simulation environment, all of experimental results are the average of three experiments. We analyze the performance of parameters such as routing probability, maximum detectable angle, and the number of loops passed on different methods in terms of communication overhead and security time.

6.1. Comparison and Analysis for Communication Overhead. The communication overhead is the basis for measuring the usability of the privacy protection method. In this work, the communication overhead is measured by the hops which messages passed from the source node to the SINK.

In the case of given the minimum communication overhead $d = 50$ (that is, it is 50 hops from source nodes to the SINK), Figure 9 shows the maximum number of loops passed by the MST algorithm under different routing probabilities p. As can be seen from Figure 9, the communication overhead of the MST protocol increases as the maximum number of loops required by the route increases. It indicates that the more the maximum number of loops passed by messages, the more hops is, due to the longer routing path. It is consistent with the theoretical analysis. In addition, when $k > 8$, the number of hops remains basically constant. This is because in the experiment setting, the number of rings between the source node and the SINK remains around 8. According to the proposed node location protection routing algorithm, when the information is close to the SINK, the routing will no longer be limited to the set of k. It is designed to prevent the information from being lost in the rings and effectively reduce the communication overhead.

In conjunction with Figure 10, it can be seen that when $p = 70\%$, the superior performance was obtained, which comprehensively compares the three indexes: hop number, ring number passed, and amplitude of the detectable angle. Moreover, compared with the case of $\{p = 50\%,\ k = 5\}$ and the case of $\{p = 30\%, k = 5\}$, the communication overhead of the case of $\{p = 70\%,\ k = 5\}$ increases slightly, but its detectable angle increases by 45%. Furthermore, we can reach the following conclusion that the size of the detectable

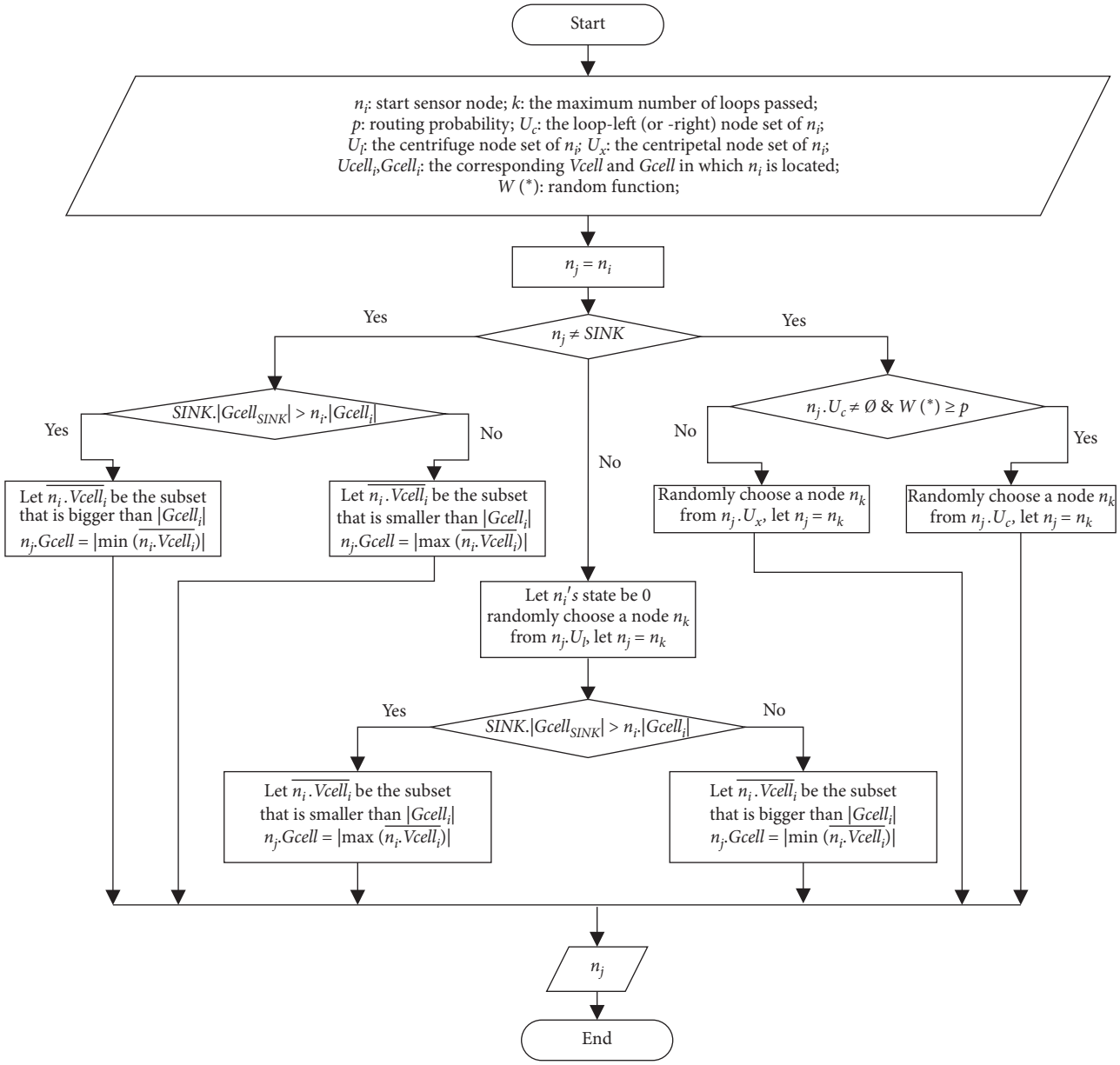

Figure 8: The flowchart of Algorithm 1.

angle is positively correlated with the number of hops along the rings in the early stage of routing. And, as the increase of the routing probability p that chooses the node from the loop-left node set, this positive correlation also tends to be significant. Furthermore, as the increase of hops, we found two kinds of interesting phenomena. (1) The detectable angle is suddenly enlarged. It is due to the fact that, in the multi-SINK network, message may leap from one helix formed by a certain SINK to another during the routing process (details in Algorithm 1: line 8–13), named the transition phenomenon of message routing between rings. (2) The detectable angle gradually expands to a certain maximum and then gradually shrinks. It mainly occurs in the events with high probability p. Due to the characteristics of helix, it is understandable that messages have higher chances of routing along the rings in a roundabout way. It is noted that, in this stage, the decrease of the detectable angle has no explicit relation with the change of detectable domain obtained by attackers. There are two main scenarios in our observations. (1) The distance between the focuses of routing paths and the source node is greater than the distance between the source node and the SINKs. In the multi-SINK network, it means that the source node and all the SINKs would be in the ipsilateral open sector, which results in the bidirectional node location attack failure. (2) The source node may be outside the detectable domain formed by attackers, due to the transition phenomenon. In short, under the MST protocol, along with the routing of the packets, the probability of the source node being traced back is reduced. Correspondingly, the risk of node location exposure is reduced. It is consistent with previous theoretical analyses.

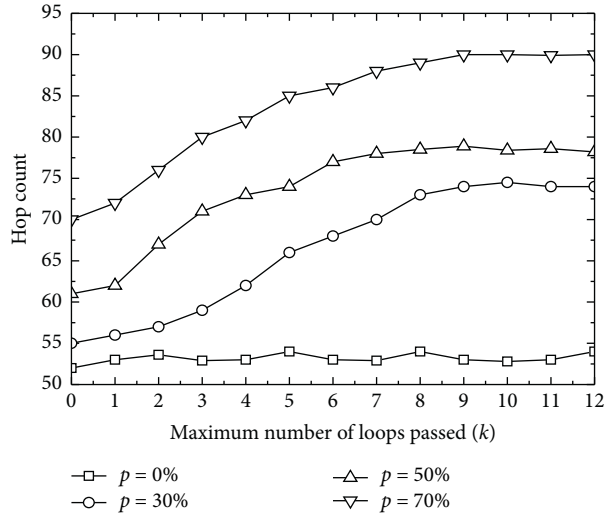

Figure 9: The communication overhead of the MST method in different routing probabilities along rings (the specific experimental data are shown in Table 2 in the Appendix).

Table 2: The communication overhead of the MST method in different routing probabilities along rings.

K	P/%			
	0	30	50	70
0	52.23	54.81	61.54	70.01
1	52.74	56.13	62.24	72.13
2	52.91	56.76	66.93	75.84
3	52.67	57.84	71.14	79.93
4	52.64	62.16	72.85	82.59
5	53.73	66.14	73.26	84.95
6	52.52	67.54	77.33	86.14
7	52.32	70.10	77.83	87.96
8	53.73	72.83	78.01	88.32
9	52.38	73.90	78.52	90.12
10	52.27	74.33	78.01	90.16
11	52.33	73.83	78.18	90.07
12	53.83	73.84	77.92	90.13

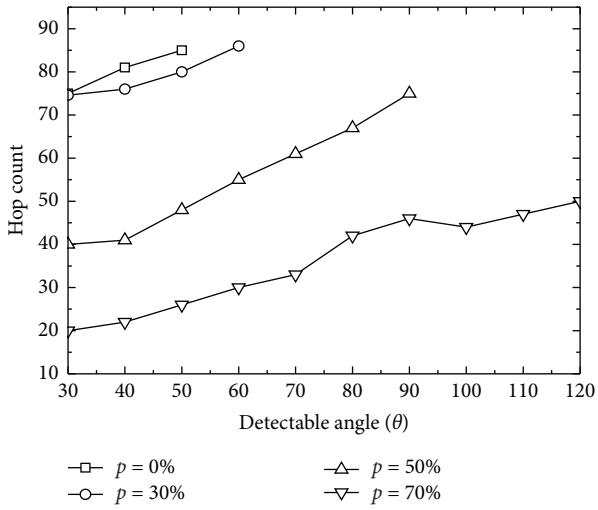

Figure 10: The communication overhead of the MST method at different detectable angles (the specific experimental data are shown in Table 3 in the Appendix).

In addition to the maximum number of rings required that affects the communication overhead, the distance (the count of hops) between the source node to the SINK is also an index that uses to investigate the communication overhead of different routing protocols. Figure 11 illustrates the impact of distance on the communication overhead, using the same experiment settings as before. The experiment shows that when $p = 70\%$, MST algorithm has a lower hop count and communication overhead than other cases. Specifically, in the case of $p = 90\%$, the routing path along the spiral ring is too long. It directly leads to a larger detectable angle but with more communication overhead. While in the case of $p = 50\%$, the routing path along the spiral ring maybe too short, even causing the strategy probability to failure. Although communication overhead is low, in this case, the detectable domain formed by the detectable angle becomes smaller, and the risk of exposure of the resource node is greater.

In addition, given $p = 70\%$, we compared MST and the other three well-known algorithms in the communication

Table 3: The communication overhead of the MST method at different detectable angles.

θ	P/%			
	0	30	50	70
30	75.00	75.02	40.00	20.12
40	82.30	76.28	40.82	21.10
50	85.03	78.54	48.94	25.33
60		86.19	55.07	30.05
70			60.52	33.15
80			65.98	41.28
90			75.13	45.76
100				44.37
110				47.24
120				50.26

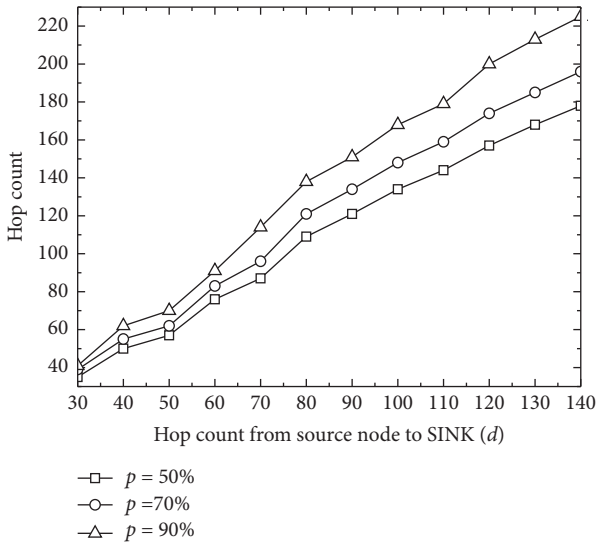

Figure 11: The communication overhead of the MST method in different distances from the source node to SINK (the specific experimental data are shown in Table 4 in the Appendix).

Table 4: The communication overhead of the MST method in different distances from the source node to SINK.

d	P/%		
	50	70	90
30	32.21	36.54	40.12
40	50.10	55.12	62.82
50	57.30	62.15	70.90
60	72.92	82.80	91.44
70	85.38	94.62	112.81
80	89.16	121.32	139.31
90	120.14	132.32	150.56
100	131.89	148.64	168.80
110	142.53	158.56	180.07
120	158.14	173.65	201.35
130	167.59	183.27	214.25
140	178.29	195.71	223.57

overhead with different detectable angles. As shown in Figure 12, the communication overhead of four methods increases with the increase of the detectable angle. Specifically, the communication overhead of MoRF and PLAUDIT increases linearly with the increase of the detectable angle, while MST only presents sublinear growth. As PU SBRF adopts flooding protocol to generate multiple phantom source nodes that causes a large initial angle, the detectable angle formed by MST is smaller than that of PU SBRF in the early stage of routing; however, in this stage, the communication overhead of PU SBRF is a linear function of the parameter n (n represents the number of the phantom source nodes generated), which is much larger than the communication overhead of the other three algorithms. Moreover, under the same experimental settings, the maximum detectable angle that can be formed by MST is much larger than that of the other three algorithms. The experiment result shows that MST can reach a detectable angle of more than 120 degrees, while MoRF, PU SBRF, and PLAUDIT can only reach 60 degrees, 50 degrees, and 80 degrees, respectively. In general, the communication overhead of MST increases with the increase of the detectable angle, but the increasing trend is gentle, which is acceptable in the real environment.

6.2. Comparison and Analysis for Security Time. In this work, we use the security time to measure the security performance of protocols. The security time means the sum of hops that attackers need to trace from the SINK to the source node [17]. Similar to Section 5.1, given a certain distance (100 hops with 12 rings in the experiment setting), we verify the relationship between the number of rings passed and the detectable angle formed, as shown in Figure 13.

The experiment result shows that, with the increase of the maximum number of rings passed, the detectable angle increases gradually. The larger the detectable angle is, the smaller the detectable domain the attacker gets and the less the probability of the source node being exposed, and vice versa. A relatively small detectable domain would improve the nontraceability of the source node, guaranteeing the location privacy of the source node. When the detectable angle $\theta = 75$ with $\{p = 70\% \text{ and rings} = 8\}$ or $\theta = 110$ with $\{p = 70\% \text{ and rings} = 9\}$, MST obtains the superior comprehensive performance. It should be noted that a detectable angle that is too large or too small can cause the routing protocol to fail, as it is an art of balance between privacy protection and the communication overhead.

Theoretically, track-back hop number [18], average track-back time [26], and traffic confusion degree [8] can all be used as evaluation indexes to measure the security time. In order to unify, we take the track-back hop number as the evaluation indicator. The following experiment evaluated the security time of each algorithm with the track-back hop number for different detectable angle θ, as shown in Figure 14. The PU SBRF, in the initial routing stage, adopts flooding protocol, in which each hop is routed in a direction that deviates from the real source node. It makes the security time of the PUSBRF significantly improved in this stage. MoRF and PLAUDIT adopt the traffic balancing to hide the source node sending messages. It is noted that, in this experiment, we filter out the interference of the traffic-

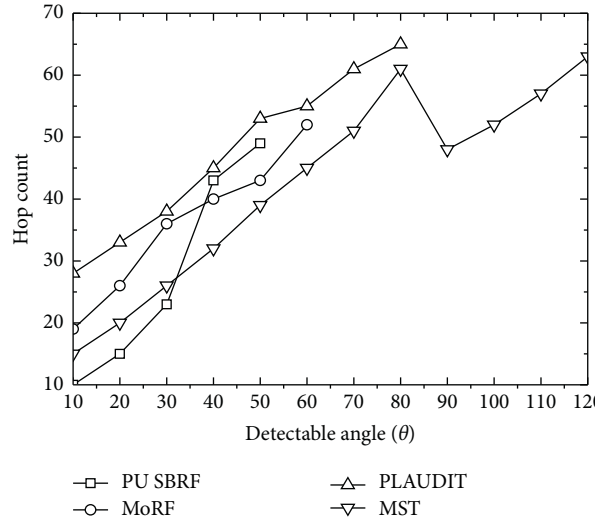

Figure 12: Compare the communication overhead of the four methods at different detectable angles (the specific experimental data are shown in Table 5 in the Appendix).

Table 5: Compare the communication overhead of the four methods at different detectable angles.

θ	Methods			
	PU SBRF	MoRF	PLAUDIT	MST
10	10.03	18.83	27.93	14.54
20	14.26	26.03	33.15	20.02
30	23.12	35.44	38.23	25.29
40	43.22	40.08	45.14	31.68
50	47.92	42.95	53.23	38.44
60		52.34	55.27	45.03
70			62.16	51.32
80			65.32	61.87
90				47.28
100				51.75
110				57.44
120				63.00

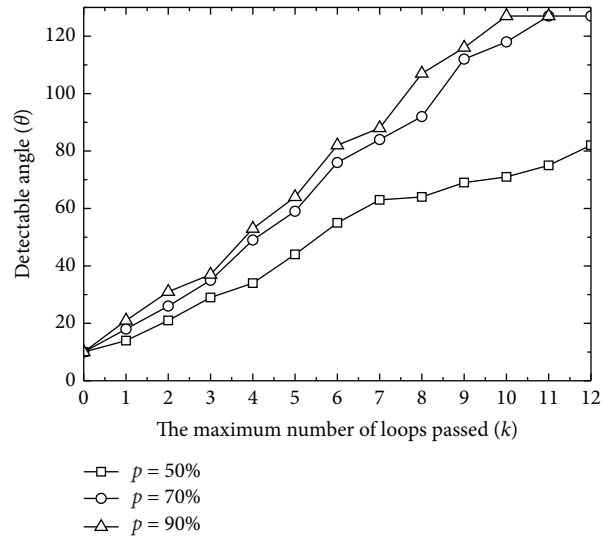

Figure 13: The maximum detectable angle formed by the MST method in different routing probabilities along rings (the specific experimental data are shown in Table 6 in the Appendix).

Table 6: The maximum detectable angle formed by the MST method in different routing probabilities along rings.

k	P/%		
	50	70	90
0	10.00	10.00	10.00
1	13.40	18.20	21.31
2	21.23	25.14	31.94
3	28.90	32.63	37.82
4	32.27	49.78	52.33
5	43.19	58.84	65.09
6	52.99	75.36	82.30
7	63.22	83.56	85.98
8	63.95	92.16	107.63
9	68.39	112.33	115.29
10	70.38	117.65	126.89
11	75.36	126.89	126.89
12	81.33	126.89	126.89

Table 7: Compare the track-back error hop number (security time) of the four methods at different detectable angles.

θ	Methods			
	PU SBRF	MoRF	PLAUDIT	MST
30	5.00	2.59	2.68	3.91
40	7.58	5.76	7.45	6.92
50	10.02	6.65	7.38	7.78
60		7.50	7.75	12.10
70			7.65	12.65
80			8.13	13.46
90				13.46
100				16.35
110				18.29
120				18.94

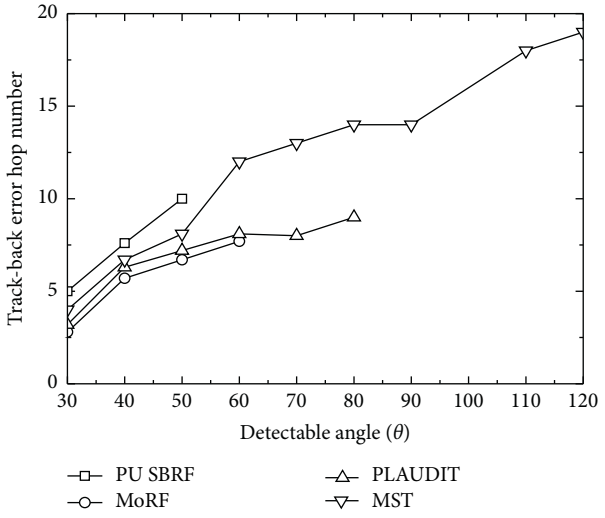

Figure 14: Compare the track-back error hop number (security time) of the four methods at different detectable angles (the specific experimental data are shown in Table 7 in the Appendix).

balancing strategy to the security time. We observed that MoRF and PLAUDIT have no dominant strategy for increasing the detectable angle. The MST method in this work uses the pseudohelix routing method to effectively expand the detectable angle in each stage of routing.

7. Conclusion and Future Scope

In this paper, we presented a kind of bidirectional location privacy attack and defense mechanism for UnWSNs. Specifically, to prevent adversaries from reasoning or backtracking the source nodes and SINK nodes based on the message propagation path, we propose a pseudospiral routing protocol based on the Archimedes curve. In addition to this, the paper constructs a one-by-one mapping relationship between Vcell and SINK based on the Voronoi rule, aiming to optimally balance routing paths with privacy-preserving capabilities given the routing tolerance parameters.

Till date, there is no proper secure routing mechanism for UnWSNs capable of dynamically adapting message routing to the evolution of the adversary's attack capabilities. And, even very limited work (including the current version of this paper) implements pseudomessage obfuscation assuming only that adversary attack capabilities do not accumulate with observations.

So, in the next version, we plan to dynamically evolve the adversary's attack capability by incorporating the historical information distribution behavior of each sensor in the previous time window into the adversary's observation knowledge and use Stackelberg game to guide the sensors in generating pseudomessage as a way to achieve an optimal balance of node location privacy protection and effectiveness in UnWSNs.

Appendix

The data of the experimental results in this paper are shown in Tables 2–7.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

The author greatly appreciates the support of Shanxi University of Finance and Economics. This work was supported by the Shanxi Province Applied Basic Research Program (Youth Science and Technology Research Fund) (Grant no. 201901D211415), the Science and Technology Innovation Project of Higher Education Institutions in Shanxi Province (Grant no. 2019L0478), the Youth Scientific Research Foundation of Shanxi University of Finance and Economics

(Grant no. QN-2019020), and Graduate Student Innovation Project of Shanxi Province (Grant no. 2020SY177).

References

[1] S. Shah, M. Khan, and A. Almogren, "Security measurement in industrial IoT with cloud computing perspective: taxonomy, issues, and future directions," *Scientific Programming*, vol. 2020, no. 1, 2020.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[3] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: a state-of-the-art survey," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1501–1514, 2009.

[4] M. A. M. Ahsan, I. Ali, and M. Imran, "A fog-centric secure cloud storage scheme," *IEEE Transactions on Sustainable Computing*, vol. 1, 2019.

[5] M. S. Adam, L. Y. Por, M. R. Hussain et al., "An adaptive wake-up-interval to enhance receiver-based ps-Mac Protocol for wireless sensor networks," *Sensors*, vol. 19, no. 17, p. 3732, 2019.

[6] C. Huang, M. Ma, Y. Liu, and A. Liu, "Preserving source location privacy for energy harvesting WSNs," *Sensors*, vol. 17, no. 4, p. 724, 2017.

[7] J. Chen, H. Zhang, X. Du, B. Fang, and L. Yan, "Designing robust routing protocols to protect base stations in wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 14, no. 17, pp. 1613–1626, 2014.

[8] Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "An efficient privacy-preserving scheme against traffic analysis attacks in network coding," in *Proceedings of the INFOCOM 2009, IEEE*, pp. 2213–2221, IEEE, Rio de Janiero, Brazil, April 2009.

[9] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proceedings. 25th IEEE International Conference on Distributed Computing Systems, 2005. ICDCS 2005*, pp. 599–608, IEEE, Columbus, OH, USA, June 2005.

[10] L. Kang, "Protecting location privacy in large-scale wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications ICC'09*, pp. 1–6, IEEE, Dresden, Germany, June 2009.

[11] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 88–93, ACM, Washington, DC, USA, October 2004.

[12] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks SecureComm 2005*, pp. 113–126, IEEE, Athens, Greece, September 2005.

[13] M. Ahsan, I. Ali, and M. Idris, "Countering statistical attacks in cloud-based searchable encryption[J]," *International Journal of Parallel Programming*, vol. 48, no. 3, 2020.

[14] A. Nayyar and V. E. Balas, "Analysis of simulation tools for underwater sensor networks (UWSNs)," in *Proceedings of the International Conference on Innovative Computing and Communications*, pp. 165–180, Springer, Singapore, December 2019.

[15] A. Nayyar, V. Puri, and D.-N. Le, "Comprehensive analysis of routing protocols surrounding underwater sensor networks (UWSNs)," in *Proceedings of the Data Management, Analytics and Innovation*, pp. 435–450, Springer, Singapore, August 2019.

[16] S. John, V. G. Menon, and A. Nayyar, "Simulation-based performance analysis of location-based opportunistic routing protocols in underwater sensor networks having communication voids," in *Proceedings of the Data Management, Analytics and Innovation*, pp. 697–711, Springer, Singapore, January 2020.

[17] J. Chen, B.-X. Fang, L.-H. Yin, and S. Su, "A source-location privacy preservation protocol in wireless sensor networks using source-based restricted flooding," *Chinese Journal of Computers*, vol. 33, no. 9, pp. 1736–1747, 2010.

[18] K. Pongaliur and L. Xiao, "Maintaining source privacy under eavesdropping and node compromise attacks," in *INFOCOM, 2011 Proceedings IEEE*, pp. 1656–1664, IEEE, Shanghai, China, April 2011.

[19] L. Zhou and Q. Wen, "Energy efficient source location privacy protecting scheme in wireless sensor networks using ant colony optimization," *International Journal of Distributed Sensor Networks*, vol. 10, no. 3, Article ID 920510, 2014.

[20] E. C.-H. Ngai and I. Rodhe, "On providing location privacy for mobile SINKs in wireless sensor networks," *Wireless Networks*, vol. 19, no. 1, pp. 115–130, 2013.

[21] 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.

[22] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 7, pp. 1302–1311, 2012.

[23] J. Wang, F. Wang, Z. Cao, F. Lin, and J. Wu, "Sink location privacy protection under direction attack in wireless sensor networks," *Wireless Networks*, vol. 23, no. 2, pp. 579–591, 2017.

[24] K. Mehta, D. Donggang Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 320–336, 2012.

[25] J. Long, A. Liu, M. Dong, and Z. Li, "An energy-efficient and SINK-location privacy enhanced scheme for WSNs through ring based routing," *Journal of Parallel and Distributed Computing*, vol. 82, pp. 47–65, 2015.

[26] A. Liu, X. Liu, Z. Tang, L. T. Yang, and Z. Shao, "Preserving smart sink-location privacy with delay guaranteed routing scheme for WSNs," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 3, p. 68, 2017.

[27] L. Lightfoot, Y. Li, and J. Ren, "Preserving source-location privacy in wireless sensor network using STaR routing," in *Proceedings of the Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pp. 1–5, IEEE, Miami, FL, USA, December 2010.

[28] N. Baroutis and M. Younis, "Load-conscious maximization of base-station location privacy in wireless sensor networks," *Computer Networks*, vol. 124, pp. 126–139, 2017.

[29] H. Chen and W. Lou, "On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, pp. 36–50, 2015.

[30] X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: a social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs," in *INFOCOM, 2011 Proceedings IEEE*, pp. 2147–2155, IEEE, Shanghai, China, April 2011.

[31] X. Niu, C. Wei, and Y. Yao, "Energy-consumption-balanced efficient source-location privacy preserving protocol in WSN," *Journal on Communications (In China)*, vol. 37, no. 4, pp. 23–33, 2016.

[32] R. Di Pietro and A. Viejo, "Location privacy and resilience in wireless sensor networks querying," *Computer Communications*, vol. 34, no. 3, pp. 515–523, 2011.

[33] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, R. L. Moses, and N. S. Correal, "Locating the nodes: cooperative localization in wireless sensor networks," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 54–69, 2005.

[34] L. Hu, W.-S. Ku, S. Bakiras, and C. Shahabi, "Spatial query integrity with voronoi neighbors," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 4, pp. 863–876, 2013.

[35] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, no. 12, pp. 1719–1733, 2007.

[36] G. Ghinita, P. Kalnis, and A. Khoshgozaran, "Private queries in location based services: anonymizers are not necessary," in *Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data*, pp. 121–132, ACM, Vancouver, Canada, June 2008.

[37] W. P. Wang, L. Chen, and J. X. Wang, "A source-location privacy protocol in WSN based on locational angle," in *Proceedings of the IEEE International Conference on Communications, 2008. ICC'08*, pp. 1630–1634, IEEE, Beijing, China, May 2008.

[38] N. Baroutis and M. Younis, "Using fake sinks and deceptive relays to boost base-station anonymity in wireless sensor network," in *Proceedings of the IEEE 40th Conference on Local Computer Networks (LCN)*, pp. 109–116, IEEE, Beach, FL, USA, October 2015.