

Article



SPS and DPS: Two New Grid-Based Source Location Privacy Protection Schemes in Wireless Sensor Networks

Qiuhua Wang ^{1,*}, Jiacheng Zhan ², Xiaoqin Ouyang ² and Yizhi Ren ¹

- ¹ School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China; renyz@hdu.edu.cn
- ² School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China;
- zhanjiacheng@hdu.edu.cn (J.Z.); xiaoqin_ouyang@163.com (X.O.)
- * Correspondence: wangqiuhua@hdu.edu.cn; Tel.: +86-0571-868-73820

Received: 3 April 2019; Accepted: 3 May 2019; Published: 4 May 2019



Abstract: Wireless Sensor Networks (WSNs) have been widely deployed to monitor valuable objects. In these applications, the sensor node senses the existence of objects and transmitting data packets to the sink node (SN) in a multi hop fashion. The SN is a powerful node with high performance and is used to collect all the information sensed by the sensor nodes. Due to the open nature of the wireless medium, it is easy for an adversary to trace back along the routing path of the packets and get the location of the source node. Once adversaries have got the source node location, they can capture the monitored targets. Thus, it is important to protect the source node location privacy in WSNs. Many methods have been proposed to deal with this source location privacy protection problem, and most of them provide routing path diversity by using phantom node (PN) which is a fake source node used to entice the adversaries away from the actual source node. But in the existing schemes, the PN is determined by the source node via flooding, which not only consumes a lot of communication overhead, but also shortens the safety period of the source node. In view of the above problems, we propose two new grid-based source location privacy protection schemes in WSNs called grid-based single phantom node source location privacy protection scheme (SPS) and grid-based dual phantom node source location privacy protection scheme (DPS) in this paper. Different from the idea of determining the phantom node by the source node in the existing schemes, we propose to use powerful sink node to help the source node to determine the phantom node candidate set (PNCS), from which the source node randomly selects a phantom node acting as a fake source node. We evaluate our schemes through theoretical analysis and experiments. Experimental results show that compared with other schemes, our proposed schemes are more efficient and achieves higher security, as well as keeping lower total energy consumption. Our proposed schemes can protect the location privacy of the source node even in resource-constrained wireless network environments.

Keywords: wireless sensor network; privacy preservation; phantom node; random routing

1. Introduction

As an important part of the Internet of Things (IoT), Wireless Sensor Networks (WSNs) are widely used in civilian and military applications. A WSN is composed of two kinds of nodes, namely, the sensor node and the sink node (SN). The sensor node acts as an information source, sensing the existence of objects and transmitting data packets to the SN by communicating with adjacent nodes wirelessly. The sink node is a powerful node with high performance, that is, it has unlimited computing capacity, storage capacity and energy resources. The SN is used to collect all the information sensed by the sensor nodes [1].

In the monitoring task-driven WSN, sensor nodes sense the existence of monitored objects in their sensing region, the node closest to the monitored target is called the source node (SoN). Anytime, any sensor node may become a SoN. Once the target is detected, the SoN will generate the encrypted data packets and transmit them to the SN in a multi hop fashion [2,3]. However, due to the open nature of the wireless transmission medium, the packet sender can easily be located by the adversary. Therefore, although the enemy cannot obtain the content of the encrypted data packets, he can reversely go to the actual source nodes via hop-by-hop tracking along the routing path of the packets [4]. If the adversary gets the location of the actual source node, he can capture the protected objects, which may lead to unpredictable consequences. For example, a very important application of WSN is monitoring valuable objects or personnel. When a large number of sensor nodes are deployed in the field to monitor precious animals (such as pandas, South China tigers, and golden monkeys), the locations of the animals should not be learned by poaching. Similarly, on the battlefield, the location of the soldier should not be tracked by the enemy. In the process of monitoring these objects or personnel, it is necessary to protect the safety of the target while obtaining valid information. Therefore, the physical location privacy protection of the source node in WSN becomes a critical problem worthy to be studied.

Source node location privacy protection is the process of keeping the location of a source node hidden from adversaries in a target monitoring network [5]. Celal Ozturk et al. first considered the source node location privacy problem of WSN in Reference [6], using Panda-Hunter game model, and based on this model they proposed to use a fake source called phantom node (PN) to entice the adversaries away from the actual source node [7]. In their Panda-Hunter model, shown in Figure 1, the monitored target is Panda, which is high-value and needs protection. In 2003, a single piece of panda fur was sold in Chongqing, China for \$66,500 [8]. In Figure 1, a large number of sensor nodes are deployed in the field by the Save-The-Panda Organization to monitor the habitats of the panda [9]. Once the panda pops up, the sensor node closest to the panda becomes the SoN. The SoN generates the data packets and transmits them to the SN periodically via multi-hop routing techniques. The hunter (also featured as the adversary or attacker) starts at the sink node. He waits until he hears a packet. Once he hears a data packet, he can determine the packet sender via wireless locating technology [10] and quickly move to its location. By this way, the attacker can backtrack the routing path hop-by-hop to the SoN where the Panda is and capture the panda. In Figure 1, no source node location privacy protection technology is adopted, so the panda can be easily tracked and captured by the hunter. Therefore, the source location privacy protection technology must be used to prevent the hunter from locating the SoN, while ensuring that the data packets can be transmitted to the sink node.



Figure 1. The Panda-Hunter model without privacy protection.

Existing source node location privacy protection schemes protect source location privacy by increasing path length or path complexity, such as cyclic entrapment [11], dummy data sources [6,7,12–16], phantom routing [6,7,16–22], etc. These technologies mainly improve security performance by sacrificing network performance (such as increased communication overhead and decreased network stability). However, the communication overhead is the largest energy consumption and is far greater than the computation overhead [23]. For example, the energy consumed to send 1-bit data by a sensor node can be used to perform 3000 calculation instructions [24]. Therefore, how to save energy in the process of network operation to maximize the network life cycle is critical in the design of security strategy. Worse, the sensor node is powered by a battery and its computational capability, storage capacity and energy resources are limited, so the existing schemes are not applicable to such resource-constrained application scenarios. How to save energy in the process of protecting the source location privacy is critical when designing the security strategy.

In addition, in order to make the real source node difficult to be traced by the attacker, the PN should be as far as possible from the real source node [18], and the PN should be replaced periodically for the sake of security. However, in the existing schemes, the selected PNs are mainly concentrated near the SoN and remain unchanged, and the location privacy of the source node cannot be well protected.

1.1. Related Works and Issues

Since the exposure of the source node location in WSN inevitably threatens the security of the monitored target, the source node location privacy protection becomes an urgent issue to be solved. However, since the computational capability, storage capacity and energy resources of sensor nodes are limited, the balance between security and network performance becomes an inevitable requirement.

The existing researches on source node location privacy protection are mainly based on cyclic entrapment [11], dummy data sources [6,7,12–16] and phantom routing [6,7,16–22]. Ouyang et al. [11] introduced the cyclic entrapment concept as a special case of dummy data source routing. In cyclic entrapment, multiple nodes act as dummy data sources, and interconnect to form a loop. The main aim of cyclic entrapment is to confuse adversary with these loops during a hop-by-hop-trace attack, thereby preventing the attacker from going back to the real source node. However, such a strategy needs to activate one or more loops to restrict the attacker, and the nodes in the loop which act as the dummy data source need to generate dummy data periodically, which causes a large amount of abnormal communication overhead, results in energy hole [19] and damages the network performance seriously. In addition, when the Panda-Hunter model was first proposed in Reference [6], it has been assumed that the hunter has the ability to cache the location information, and he can record the position of the nearest N nodes, so as to avoid falling into the loop, which invalidates the protection capability of the scheme. Although dummy data source routing can protect source location privacy to a certain extent, it needs to generate a lot of dummy data periodically, which not only causes a lot of waste of energy consumption, but also increases packet collision probability and reduces packet transmission efficiency. Moreover, the true path of packet transmission is included in all paths, and the source node location privacy protection capability is probabilistic.

Ozturk et al. first proposed the phantom routing scheme (PRS) in Reference [6] to protect the location privacy of source nodes using the Panda-Hunter model. They use the phantom node to entice the adversaries away from the actual source node. If the attacker cannot track the PN, it is impossible for him to trace the location of the true source node [2]. PRS involves two phases: The random walk phase and the subsequent flooding phase. In the random walk phase, the packet from the real source is randomly transmitted h hops to determine a PN. In the flooding phase, the PN transmits the data packets to the SN by the way of flooding. The main aim of this scheme is to ensure that the attacker can only trace back to the PN and cannot trace back to the real source node, thus ensuring the privacy of the source node location. However, the shortest path in the flooding phase is included in the flooding paths, and the first packet received by the attacker is the shortest path packet. The attacker can capture the SoN by tracing back along the shortest path. Kamat et al. proposed a phantom single-path routing

scheme (PSRS) in Reference [7], which is similar to the PRS scheme. In this scheme, the first phase is a directed random walk, and in the second phase, a single path routing algorithm is used to transmit data packets to the SN. This paper also provides a technique for classifying neighbors of nodes. In Reference [18], J. Chen et al. pointed out that the PNs in the existing source location privacy protection schemes are concentrated near the SoN, and once the attacker traces back to the PN, he can further trace to the SoN easily. In response to this problem, they proposed an enhanced source location privacy preservation protocol using source-based restricted flooding (EPUSBRF). Compared with the PSRS scheme, the EPUSBRF significantly improves the security of the source location privacy, and avoids the generation of the invalidate paths without increasing the energy consumption.

In recent years, the improvements for the source node location privacy protection of WSNs are mainly based on the idea of phantom routing. In Reference [19], Yi et al. proposed a trace time-constrained routing algorithm for preserving source-location in WSNs. Its main idea is that the routing path from the SoN to the SN is generated and distributed dynamically and randomly, and the lasting time of a routing path is shorter than the time for the adversary to trace to the PN. Hence, it is more difficult for the adversary to trace to the SoN, thus increasing the protection strength. In Reference [16], Ma et al. proposed a source location privacy preservation Routing Protocol Based on Multi-Path (RPBMP), which performs random routing based on multi-path selection and multiple PNs jump. This scheme greatly increases the number of routing path between the SoN and the SN, extends the safety period. The notion of the safety period is proposed in Reference [6] as a performance indicator of source location privacy protection in WSNs, and has been widely used in subsequent researches. In Reference [6], the safety period is measured by the number of packets the SoN has sent before it is caught by the attacker. To solve the problem of failure path in phantom routing protocols, in Reference [20], Chen et al. proposed an improved routing algorithm for WSN source node location privacy protection based on the minimum path routing. The improved routing algorithm has higher safety period and does better in protecting source location privacy in WSNs. In Reference [21], Kong et al. proposed a virtual ring-based routing protocol of source-location privacy protection, which avoids the generation of failure path and extends routing path to the annular region where SoN resided with the random virtual ring. This scheme greatly increases the diversity and randomness of the routing paths, and makes it harder for an attacker to deduce the SoN according to the routing path. In Reference [22], Wang et. al. proposed a location privacy protection strategy called PRABNS (Phantom Routing Based on Area and Brother Neighbor Selecting). The PNs selected by this strategy maintain a certain angle and distance, and the adjacent data packets have a certain angle space through the selection of partial region. This strategy increases the diversity for the path of the SoN to SN by selecting sibling nodes. However, the PNs determined by this strategy are still evenly distributed around the SoN, and the shielding nodes cannot guarantee the robustness of the network and the packet loss rate increases.

1.2. Our Motivations and Contributions

In this paper, we focus on the source node location privacy protection in WSNs, and our aim is to deal with the aforementioned problems, advance the existing researches and improve the security performance of source node. Different from the existing schemes which determine the PN by the SoN, in this paper, we propose to use powerful sink node to help the source node to determine the phantom node candidate set (PNCS) and propose two new grid-based source location privacy protection schemes in WSNs: The grid-based single phantom node source location privacy protection scheme (SPS) and the grid-based dual phantom node source location privacy protection scheme (SPS) and the grid-based dual phantom node source location privacy protection scheme (DPS). In our proposed schemes, the PNCS is firstly determined by the SN, and then the SoN randomly selects a PN from the PNCS with equal probability. After the source node transmits the data packets to the selected PN via multi-hop routing, the PN sends the data packets to the SN via the single path routing. As the energy of SN is unlimited, the method that the SN helps the SoN to select the PNCS, not only avoids a large amount of energy consumed by the ordinary sensor nodes when determining the PN, but also

distributes the PNs randomly throughout the network, thus greatly increases the security of the source node and provides better privacy preservation for them.

According to whether the PN is replaced, the above two schemes are further divided into two cases respectively: Not replacing the PN and replacing the PN. In the case of not replacing the PN, once the SoN chooses a PN from the PNCS, it will not be replaced. While in the case of replacing the PN, after a PN is used for a while, the SoN can replace the PN with another. When the PNCS is empty, that is, all the PNs selected by the SN are used up, the SoN sends a new request packet to the SN, requesting the SN to determine a new PNCS for it, which ensures that enough PNs can be used by the SoN during the panda's stay. Moreover, since the SN knows about the basic location information of each node in the entire network, the PNs selected in our schemes are not concentrated near the SoN, but distribute anywhere in the network, and therefore have stronger positional randomness compared with other existing schemes. At the same time, as our schemes select more PNs to ensure the diversification of routing paths, the security performance of privacy protection is further improved. Our proposed new method greatly increases the security of the source node and provides better privacy preservation for them.

In this paper, the SPS scheme in the case of replacing the PN is called the RSPS scheme, the SPS scheme in the case of not replacing the PN is called the NRSPS scheme, the DPS scheme in the case of replacing the PN is called the RDPS scheme, and the DPS scheme in the case of not replacing the PN is called the NRDPS scheme.

In the performance simulation of Section 5, we explore the impact of replacing PNs on security performance, and the impact of the number of PNs on security performance and total communication overhead. Simulation results verify the effectiveness of our proposed schemes. For example, compared with the shortest path algorithm, RPBMP [16] and EPUSBRF [18], the average safety period of our proposed NRSPS scheme, is increased by 6.08 times, 2.78 times and 3.57 times respectively; compared with RPBMP and EPUSBRF, the total communication overhead of our proposed NRSPS scheme is reduced by 88% and 95%, respectively.

We summarize our main contributions as follows:

(1) We proposed two new grid-based source location privacy protection schemes. In our proposed schemes, the sink node with high-computing power and high-energy is used to determine the phantom node candidate set, which avoids the disadvantage of excessive communication overhead caused by flooding to determine the phantom node in previous traditional schemes;

(2) The location of the phantom nodes is determined by our proposed schemes that are distributed throughout the network; which, in turn, improves the diversity of the phantom nodes in terms of location and the randomness of routing. In our proposed schemes, the routing path appears randomly across the entire network, which prevents the attackers from backtracking to the location of the source node via the routing path. Our proposed schemes avoid the defects that the phantom node locations in the traditional schemes are concentrated near the real source node and that the location privacy of the real source node cannot be well protected;

(3) Our proposed schemes do not require the node to be equipped with a positioning module, such as GPS, which reduces the node cost and energy consumption, hence the application scenario of our proposed schemes are universal, and the source location privacy can be effectively and stably protected even in resource-constrained wireless network environments;

(4) We conduct theoretical analysis and extensive experimental simulations to evaluate the performance of our proposed schemes. The simulation results further verify the effectiveness of our proposed schemes.

1.3. Organization of the Paper

The rest of this paper is organized as follows. The system model, including the network model, attack model, and security model used in our proposed schemes, is introduced in Section 2. Section 3 provides a detailed description of our proposed SPS scheme, and Section 4 introduces our proposed

DPS scheme. Section 5 presents the results and performance analysis. Finally, we conclude the paper in Section 6.

2. System Model

2.1. Network Model

Since the Panda-Hunter model was put forward in Reference [6] to study the source location privacy problem of WSNs, it has been widely used by researchers [6,7,11–20,25]. In this paper, similar to the existing researches, we also use the Panda-Hunter model as our network model, which is a deterministic deployment. For the sake of understanding, we make the following assumptions about the network model:

(1) There is only one sink node in the network, whose location is static and fixed in the network center. And the resources of the sink node, such as computing power, storage capacity and energy are not limited [26].

(2) The network is evenly divided into small grids. The sensor nodes in each grid are all fully connected. The whole network is fully connected through multi-hop communications [4].

(3) The sensor nodes in the network are deployed prior to the initialization phase. After being deployed, each node has the knowledge of its own basic information, such as node ID number, grid number, etc. The sink node knows about the basic information of each node in the entire network.

(4) When the panda appears, the node closest to the panda becomes the source node, that is, there is only one source node in the whole network. The source node will generate and send encrypted packets to the sink node through a multi-hop routing. The panda will stay for a period of time before leaving, and our schemes are applied during the panda's stay period.

(5) To facilitate latter theoretical analysis and simulation, we assume that all sensor nodes in the network are the same type and any two nodes can communicate via multi-hop fashion.

(6) In order to ensure the universality of the scheme, for example, the scheme can be applied even in the resource-constrained wireless networks, the node does not have the positioning and mobility capabilities. Therefore, it cannot obtain its own precise coordinates and cannot directly calculate the actual distance between two nodes. Therefore, the hop count is used as the index to measure the distance. The distance between two nodes within the communication radius of each other is called one hop.

2.2. Attack Model

Due to the rarity of panda, the attacker is driven by interest and tries to use advanced equipment to capture the panda. During the panda's stay period, the source node will continually send data packets, and the hunter may use this to his advantage to track and hunt the panda. Similar to most other pieces in the literature on source node location privacy protection [6,7,11–22], we mainly consider the local passive attackers with the ability to eavesdrop on local traffic of a WSN.

We make the following assumptions about the attack model:

(1) The attacker is equipped with wireless signal monitoring equipment, such as antenna and spectrum analyzers, and has sufficient computational capacity, storage capacity and energy resources. However, the attacker can only eavesdrop the network traffic in a local region; he cannot monitor the entire network. In fact, if the attacker can monitor the entire network, he can monitor the Panda directly without relying on the WSN [4]. Also, he cannot decrypt the packet and tamper with the packet content;

(2) The attacker just wants to get the location of the source node, in order to ensure his own concealment, the attacker only passively listens to the packets and hops back and forth. The attacker does not initiate an active attack on the network, that is, he does not interfere with the normal functioning of the network, and otherwise intrusion detection measures might detect the attacker's presence;

(3) The initial position of the attacker is at the sink node. He waits until he hears a packet. Once the attacker hears a data packet, he can determine the packet sender via wireless locating technology [10] and quickly move to its location. The monitoring radius of the attacker is the communication radius of sensor nodes. Although the attacker has strong mobility, he can sense only one hop transmission, and he moves only when he monitored a data packet, that is, the attack tracks a packet only via hop-by-hop;

(4) We emphasize that the attacker cannot learn the origin of a packet by merely observing a relayed version of it. If the attacker does not overhead the data packet within a certain period of time, he will roll back hop-by-hop along the tracking path until he returns to the sink node;

(5) The monitored object can be captured when the attacker appears in the visible area of the source node.

2.3. Security Model

We make the following assumptions about the security of the network:

(1) The network has basic security measures, such as encrypting the data packet. The attacker cannot decrypt the packet, and can only capture the panda in the visible area of the source node via hop-by-hop backtracking. We will not discuss specific encryption and decryption algorithms and key management mechanisms, since they are beyond the scope of this paper.

(2) We assume that the source node includes its ID in the encrypted packets, but only the sink node can identify the source location from its ID. Even if the hunter can break the encryption in a reasonably short time, he cannot tell the source node's location [4,8].

(3) The sink node is absolutely safe, and the attacker cannot break the sink node.

3. SPS: Grid-Based Single Phantom Node Source Location Privacy Protection Scheme

In this section, we first introduce the proposed grid-based single phantom node source location privacy protection scheme (SPS) in WSN. In our proposed schemes, the PNCS is firstly determined by the sink node, and then the source node randomly selects a PN from the PNCS. After the SoN transmits the data packets to the selected PN via multi-hop routing, the PN sends the data packets to the sink node via the single path routing. The method that the sink node helps the SoN to select the PNCS, not only avoids a large amount of energy consumed by the ordinary sensor nodes when determining the PN, but also distributes the PNs randomly throughout the network. Our proposed new method greatly increases the security of the SoN and provides better privacy preservation for them. In our latter description, the sensor node is simply referred to as nodes.

Specifically, our proposed scheme is divided into three phases: The initialization phase, the phantom node determination phase and the routing phase. For ease of understanding, the notations used herein are listed in Table 1.

Notations	Description
U	Node <i>u</i>
$Hop_{u,sink}$	Minimum hop count between node <i>u</i> and sink node
L*L	Network size
R	Node communication radius
i, j, m, n	Grid number index variable
$G_{i \times j}$	Grid number of the <i>i</i> -th row and the <i>j</i> -th column

Table 1. Notations.

3.1. The Initialization Phase

The specific process of the network initialization phase is as follows:

(1) As shown in Figure 2, the SN evenly divides the network into L^*L grids with the unit length of 2r (L is an even number). The SN is fixed at the center of the network, and its grid number is



represented as $G_{\frac{L}{2} \times \frac{L}{2}}$. The grid number of other grids is represented by the center point coordinates of the grid;

Figure 2. Network grid.

(2) The SN broadcasts a message Msg_b with the same power as the sensor nodes. Sink node's broadcast:

$$Msg_b = ID_{sink} \|Hop_{sink,sink}\| G_{\frac{1}{2} \times \frac{1}{2}}.$$
 (1)

Message Msg_b includes three parameters. The first one is the ID of the sending node, here is ID_{sink} . The second one is the hop count of the sending node from the SN, here is $Hop_{sink,sink} = 0$. The third one is the grid number of the sending node, here is $G_{\frac{1}{2} \times \frac{1}{2}}$;

(3) Suppose that node u is in grid $G_{i \times j}$. When node u receives the broadcast message Msg_b, it updates the minimum hop count of itself from the SN Hop_{u,sink'} and then continues to broadcast the message Msg_b to all of its neighbor nodes.

Node *u*'s broadcast:

$$Msg_b = ID_u ||Hop_{u,sink}||G_{i\times j};$$
(2)

(4) Suppose that the neighbor node v of node u is in the grid $G_{m \times n}$. When node v receives the broadcast message sent by node u, it adds the node ID of node u, the hop count of node u from the SN Hop_{$u,sink} and the grid number <math>G_{i \times j}$ of node u to its neighbor table, as shown in Table 2. Specifically, node v updates the minimum hop count of itself from the SN Hop_{v,sink} and then continues to broadcast messages Msg_b to all of its neighbors.</sub></sub>

Node v's broadcast:

$$Msg_b = ID_v ||Hop_{v,sink}||G_{m \times n}.$$
(3)

Similarly, node u can also receive the broadcast message of node v, and will add the node ID of node v, the hop count of node v from the SN Hop_{v,sink}, and the grid number of node <math>v to its own neighbor table;</sub>

(5) When all nodes receive the broadcast packet, the initialization phase ends. At this time, each node establishes its own neighbor table according to the received broadcast message. Then each node

classifies its neighbor nodes into three categories. Taking node u as an example, it classifies its neighbor node v according to Hop_{u,sink} and Hop_{v,sink}:</sub></sub>

- Near-hop neighbor node: Hop_{v,sink} < Hop_{u,sink};
- Same-hop neighbor node: Hop_{v,sink} = Hop_{u,sink};
- Far-hop neighbor node: Hop_{v,sink} > Hop_{u,sink}.

Node ID	Minimum Hop Count from Sink Node	Grid Number
и	$Hop_{u,sink}$	$G_{i \times j}$

3.2. The Phantom Node Determination Phase

(1) When the monitored target appears in the network, the node closest to the target becomes the source node. The SoN sends a request packet Msg_request to the SN, requesting the SN to help it determine the PNCS. The transmission mode of the request packet is: The SoN randomly selects a near-hop neighbor node from its neighbor table as the next hop node. The next hop node also randomly selects a near-hop neighbor node as its own next hop node. This process continues until the request packet reaches the SN;

(2) As shown in Figure 3, after the SN receives the request packet, it randomly selects M grids from the grids near the SoN while not in the visible area of the SoN (the grids outside the $P_1 \hat{O} P_2$ area). Then, the SN randomly selects one node in each of the selected M grids to form a PNCS;



Figure 3. The sink node helps select phantom node candidate set.

(3) The SN sends the PNCS and the grid number of each node in the PNCS to the SoN;

(4) The SoN randomly selects one node from the PNCS as the actually used PN with equal probability. All the nodes within the PNCS are chosen with equal probability.

3.3. The Routing Phase

The SoN periodically sends encrypted data packets containing the panda information to the SN through the PN via multi-hop routing. The data packets need to go through two transmission steps: The SoN sends the data packets to the PN, and the PN sends the data packets to the SN.

3.3.1. Step 1: The Source Node Sends Data Packets to The Phantom Node

In the process of sending data packets to the PN, the SoN only knows the ID of the PN and the grid number it is in. How to send data packets to the PN via multi-hop routing when no positioning capability is available is a question worth exploring. In this paper, we design the following strategies to solve this problem. Firstly, determine which grid will be passed through during the transmission process, and then find the node in the grid to forward the data packets by searching the neighbor table.

Taking the SoN as an example, the specific process is as follows:

(1) The SoN randomly selects a PN from the PNCS and removes the PN ID from the PNCS, which means that a PN can only be used once.

(2) Once selecting the PN, the SoN can simulate the grid diagram, as shown in Figure 4, and determine their positions in the grids according to the grid numbers of itself and the PN. The SoN simplifies Figure 4 to Figure 5 and builds a coordinate system. As shown in Figure 5, the SoN is in grid $G_{i\times j}$, and the PN is in grid $G_{m\times n}$.





(3) According to its grid number $G_{i\times j}$ and the PN's grid number $G_{m\times n}$, the SoN obtains the coordinates of the center point of the grids are (i, j) and (m, n), respectively. Then it calculates two-point straight line l, as shown in Equation (4),

$$\frac{x-i}{m-i} = \frac{y-j}{n-j}.$$
(4)

(4) The SoN determines whether the slope of the line l is 0. If the slope is 0, that is, the grids where the SoN and the PN belong to are in the same row, the SoN searches its neighbor table for the set of

neighbor nodes in the direction of the target grid, and randomly selects a node as the next hop node. The subsequent nodes do the same operation until the data packet reaches the PN.

(5) If the slope of the line *l* is not 0, the SoN calculates $x = i \pm 1$, $y = j \pm 1$, so that the distance from (x, y) to line *l* does not exceed $\sqrt{2}*r$. For example, as shown in Figure 5, if there are two possibilities (right grid and bottom right grid), the left and the right grids are determined first. The SoN makes x = i + 1, y = j, that is to say, the SoN determines the next grid through which the data packet passes is the right grid. Then it searches its neighbor table to find the neighbor node set in the right grid, and randomly selects one node as the next hop node.

The subsequent nodes repeat steps (4) and (5) until the data packet is transmitted to the PN.





The PN adopts the single-path routing method [27] to forward data packets to the SN. More specifically, after receiving the data packet, the PN randomly selects one node from the near-hop neighbor nodes as the next hop node, and forwards the packet to it. The next hop node repeats this process until the data packet reaches the SN.

Figure 6 shows the flowchart of our proposed SPS scheme.



Figure 6. The flowchart of our proposed SPS scheme.

In References [20,21], the PN distribution diversity and phantom routing path randomness are used as important indicators for security performance analysis. In this paper, it is the sink node that helps the source node choose the PNs randomly, and the phantom routing path is determined only after the packet transmission direction is determined through the PN. Moreover, the next hop node in the target grid is also randomly selected, so the PN distribution and the phantom routing path are maximally randomized and diversified.

4. DPS: Grid-Based Dual Phantom Node Source Location Privacy Protection Scheme

In order to explore the impact of the number of simultaneously used PNs on the performance of the scheme, we further propose a grid-based dual phantom node source location privacy protection scheme (DPS). Compared with the SPS scheme, DPS uses two types of PN simultaneously: The sending phantom node (SPN) and the receiving phantom node (RPN). The SPN is close to the SoN, and the RPN is far from the SoN, as shown in Figures 7 and 8.



Figure 7. The same side view of the phantom nodes.



Figure 8. The opposite side view of the phantom nodes.

The simulation results show that DPS can provide higher security performance for the network, but its communication overhead also increases. In practical applications, it is necessary to choose a suitable solution according to specific performance requirements.

4.1. The Initialization Phase

The network initialization phase of the DPS scheme is the same as that of the SPS scheme. After the initialization is completed, each node establishes its own neighbor table based on the received broadcast message.

4.2. The Phantom Node Determination Phase

(1) The first step in the PN determination phase is the same as that of the SPS scheme;

(2) After the SN receives the request packet from the SoN, it randomly selects 2*M* grids from the grids outside the visible region of the SoN, and randomly selects a node from each grid to form two PNCSs: The SPNCS and the RPNCS. The SPNCS is composed of nodes selected from *M* grids close to the SoN, and the RPNCS is composed of nodes selected from *M* grids far from the SoN;

(3) The SN sends the two PNCSs and the grid number of each node in them to the SoN;

(4) Once receiving the PNCSs, the SoN randomly selects a node from the SPNCS and a node from the RPNCS as the SPN and the RPN, respectively.

4.3. The Routing Phase

In the routing phase, the SoN sends the data packets to the SN periodically through the selected two PNs. The data packets need to go through three transmission steps: The SoN sends the data packets to the SPN, the SPN sends the data packets to the RPN, and the RPN sends the data packets to the SN.

(1) Step 1: The source node sends data packets to the sending phantom node:

The process that the SoN sends data packets to the SPN is the same as described in Section 3.3.1;

(2) Step 2: The sending phantom node sends data packets to the receiving phantom node:

Since the SPN and the RPN are randomly selected by the SoN, according to whether the SPN and the RPN are on the same side of the SN, there are two possibilities: The same side (as shown in Figure 7, the SPN and RPN are on the same side of the SN) and the opposite side (as shown in Figure 8, the SPN and RPN are on different sides of the SN). When it is the same side case, the transmission path is determined using the operations described in Section 3.3.1. When it is the opposite side case, the data packets may pass through the SN when they are transmitted from the SPN to the RPN, and the DPS scheme will degenerate to the SPS scheme. In order to avoid the above situation and ensure the privacy of the source location, we propose that the SPN first transmits the data packets to a transition node whose row (or column) is the same as that of the RPN, and then the transition node transmits the data packets to the RPN;

(3) Step 3: The receiving phantom node sends data packets to the sink node:

The RPN transmits the data packets to the SN using the single-path routing method described in Section 3.3.2.

Figure 9 shows the flowchart of our proposed DPS scheme.



Figure 9. The flowchart of our proposed DPS scheme.

5. Performance Analysis and Simulation

We compare our proposed schemes with RPBMP [16], EPUSBRF [18] and the shortest path algorithm from two aspects of security performance and communication overhead. According to References [16,18], EPUSBRF and RPBMP only include the PN determination phase, and they do not consider the lasting time of the PN and the number of PN. Therefore, we analyze the case of single PN based on the descriptions in References [16,18]. In order to prove the performance of our proposed schemes more intuitively, the shortest path algorithm with the lowest energy consumption is selected as one of the comparison schemes. Since the shortest path algorithm is locally optimal in terms of communication overhead, it does not consider security performance, so no further analysis is done below. For the convenience of description, in the following performance analysis, we assume that the source node visible area radius is the same as the node communication radius.

5.1. Security Performance Analysis

For an attacker, he needs to trace to the PN so as to find the real source node. More PNs can bring more diversities and uncertainties in routing which will increase the difficulty for the attacker to track back and provide longer safety period for the true source node. In this paper, the security performance indicator is also represented by the safety period. The safety period in our latter simulations is represented by the number of packets sent by the source node before the panda is captured.

5.1.1. Security Performance Analysis of EPUSBRF, RPBMP and Shortest Path Algorithms

Suppose that the time for the attacker to trace back one hop along the routing path is *T*. For the EPUSBRF scheme, let the hop count from the SoN to the PN be $Hop_{s,p}$ and the hop count from the PN to the SN be $Hop_{p,sink}$. For the RPBMP scheme, let the hop count from the SoN to the PN be $Hop'_{s,p}$ and the hop count from the PN to the SN be $Hop'_{p,sink}$. For the shortest path algorithm, let the hop count from the SoN to the SN be $Hop_{s,sink}$.

For EPUSBRF and RPBMP, the routing path hops are given by Equations (5) and (6), respectively:

$$Hop_{EPUSBRF} = Hop_{s,p} + Hop_{p,sink'}$$
(5)

$$Hop_{RPBMP} = Hop'_{s,p} + Hop'_{p,sink'}$$
(6)

For the shortest path algorithm, the routing path hops is:

$$Hop_{Shortest} = Hop_{s.sink}.$$
(7)

For EPUSBRF and RPBMP, the time required for the attacker to trace back to the SoN is given by Equations (8) and (9), respectively:

$$T_{EPUSBRF} = Hop_{EPUSBRF} * T = (Hop_{s,p} + Hop_{p,sink}) * T,$$
(8)

$$T_{\text{RPBMP}} = \text{Hop}_{\text{RPBMP}} * T = (\text{Hop'}_{s,p} + \text{Hop'}_{p,\text{sink}}) * T.$$
(9)

For the shortest path algorithm, the time required for the attacker to trace back to the SoN is shown in Equation (10):

$$T_{\text{Shortest}} = \text{Hop}_{\text{Shortest}} * T = \text{Hop}_{\text{s.sink}} * T.$$
(10)

5.1.2. Security Performance Analysis of our Proposed Schemes

The safety period is the number of packets the SoN has sent before it is caught by the attacker. In our proposed schemes, the safety period is mainly related to the PN usage time T_{pp} , the number of nodes *M* in the PNCS, and the number of routing path hops Hop_{sum}.

(1) Phantom Node Usage Time T_{pp}

In Reference [19], in order to prevent the attacker from tracing back to the SoN, it is proposed that the lasting time of each routing path should be less than the time used by the attacker to trace back to the SoN. In this paper, in order to ensure the location privacy of the source node and use the routing path efficiently, the PN usage time is determined according to the time required for the attacker to trace to trace to the PN.

Suppose that the SoN generates a data packet every time interval *T*. In the attack model, it is assumed that the attacker quickly moves to the sending node once it overhears a packet, that is, the time that the attacker traces back one hop along the routing path is *T*. Therefore, **Conclusion 1** can be drawn.

Conclusion 1. Suppose that in our proposed NRSPS scheme, the hop count from the source node to the phantom node is $Hop_{s,ps'}$ and the hop count from the phantom node to the sink node is $Hop_{ps,sink}$; in the NRDPS scheme, the hop count from the source node to the PN is the same as in the NRSPS scheme, also is $Hop_{s,ps'}$, the hop count from the SPN to the RPN is $Hop_{ps,pr'}$, the hop count from the SPN to the RPN is $Hop_{ps,pr'}$, the hop count from the data packet interval is *T*.

The time required for the attacker to trace to the PN in the NRSPS scheme is:

$$T_{\text{NRSPSp}} = T * (\text{Hop}_{\text{ps,sink}}).$$
(11)

The time required for the attacker to trace to the SoN in the NRSPS scheme is:

$$T_{NRSPSs} = T * (Hop_{s,ps} + Hop_{ps,sink}).$$
(12)

The time required for the attacker to trace to the SPN in the NRDPS scheme is:

$$T_{NRDPSp} = T * (Hop_{ps,pr} + Hop_{pr,sink}).$$
(13)

The time required for the attacker to trace to the SoN in the NRDPS scheme is:

$$T_{NRDPSs} = T * (Hop_{s,ps} + Hop_{ps,pr} + Hop_{pr,sink}).$$
(14)

Conclusion 2. Suppose that a phantom node usage time is T_{pp} . T_{pp} is represented as $T_{NRSPSpp}$ in the NRSPS scheme and $T_{NRDPSpp}$ in the NRDPS scheme. The NRSPS scheme and the NRDPS scheme only need to satisfy the Equations (15) and (16) respectively to ensure that the attacker cannot trace back to the phantom node, thus ensuring that the attacker cannot trace back to the source node. In very special cases, even if the attacker traces back to the phantom node, the attacker traces back to the phantom node, the source node.

$$T_{NRSPSpp} \le T_{NRSPSp} = (Hop_{ps,sink}) * T$$
(15)

$$T_{NRDPSpp} \le T_{NRDPSp} = (Hop_{ps,pr} + Hop_{pr,sink}) * T$$
(16)

(2) The Number of Nodes *M* in the Phantom Node Candidate Set

In the NRDPS scheme, the sink node randomly selects *M* grids from near source node side and *M* grids from away the source node side, respectively. Then the SN randomly selects one node from each grid to form the sending phantom node candidate set (SPNCS) and the receiving phantom node candidate set (RPNCS). Finally, the SoN randomly selects *i* pair node as the SPN and the RPN.

Conclusion 3. Suppose that the panda's stay time is T_1 , and the number of nodes in the phantom node candidate set is M, Equations (17) and (18) can be derived according to Equations (15) and (16).

$$T_{l} \le M * T_{NRSPSpp} \le M * T_{NRSPSp} = M * (Hop_{ps,sink}) * T$$
(17)

$$T_{l} \leq M * T_{NRDPSpp} \leq M * T_{NRDPSp} = M * (Hop_{ps,pr} + Hop_{pr,sink}) * T$$
(18)

From Equations (17) and (18), we can see that when $\frac{T_1}{T_{pp}} \le M$, the attacker cannot capture the SoN, where T_{pp} in the NRSPS scheme is shown in Equation (15), and T_{pp} in the NRDPS scheme is shown in Equation (16).

(3) Routing Path Hops Hop_{sum}

According to the assumption of 0, the hops of routing path Hop_{sum} of the NRSPS scheme and NRDPS scheme can be derived by Equations (19) and (20), respectively:

$$Hop_{NRSPSsum} = Hop_{s,ps} + Hop_{ps,sink}$$
(19)

$$Hop_{NRDPSsum} = Hop_{s,ps} + Hop_{ps,pr} + Hop_{pr,sink}$$
(20)

Since the attacker can only hop-by-hop backtrack, it takes time $T_s = T * Hop_{sum}$ to capture the SoN. According to Equations (15)–(20), the usage time of the PN $T_{pp} \leq$ the time for the attacker to trace to the PN $T_{ps} <$ the time for the attacker to trace to the SoN T_s . Therefore, before the attacker traces to the PN, the SoN has updated the PN and the attacker cannot continue backtracking.

5.1.3. Comparison of Security Performance

(1) The Case of Not Replacing the Phantom Node

Suppose that the NRSPS scheme, the NRDPS scheme, the EPUSBRF and the RPBMP use the same network topology. The PNs are all represented as p_c , and the path of the data packets transmitted from p_c to the SN does not pass through the visible area of the source node. The time that the attacker traces back one hop along the routing path is T. Since the purpose of using the PN is to hide the source node so that the attacker can only trace back to the PN while he cannot trace back to the real source node. Here, only the security performance is comparatively analyzed.

The time required for the attacker to trace to the PN in the EPUSBRF scheme is:

$$T_{EPUSBRFt} = (Hop_{pc,sink})$$
(21)

Suppose that the same-hop routing threshold in RPBMP is h_{RPBMP} , the time required for the attacker to trace to the PN is:

$$T_{\text{RPBMPt}} = (\text{Hop}_{\text{pc,sink}} + h_{\text{RPBMP}})$$
(22)

The time required for the attacker to trace to the PN in the NRSPS scheme is:

$$T_{\text{NRSPSt}} = (\text{Hop}_{\text{pc,sink}}) * T$$
(23)

The time required for the attacker to trace to the PN in the NRDPS scheme is:

$$T_{\text{NRDPSt}} = (\text{Hop'}_{\text{pc.sink}}) * T$$
(24)

where $\text{Hop'}_{pc,sink} = \text{Hop}_{ps,pr} + \text{Hop}_{pr,sink}$.

Therefore, in the above assumption, $T_{NRDPSt} > T_{RPBMPt} \ge T_{EPUSBRFt} = T_{NRSPSt}$, and the equal sign is established when $h_{RPBMP} = 0$.

(2) The Case of Replacing the Phantom Node

In this paper, *M* PNs are used in total. After the PN is replaced, the data packet transmission path will also change, and the attacker cannot eavesdrop the data packet and will return to the SN along the original path. The time required for the attacker to trace to the last PN in the RSPS scheme is:

$$T_{RSPSt} = (Hop_{pc,sink}) * T * M + T_{Esum},$$
(25)

where T_{Esum} represents the total time taken by the attacker to return to the SN when he cannot overhear the data packets. The time required for the attacker to trace to the last PN in the RDPS scheme is:

$$T_{RDPSt} = (Hop'_{pc,sink}) * T * M + T_{Esum'}$$
(26)

where $\text{Hop'}_{\text{pc,sink}} = \text{Hop}_{\text{ps,pr}} + \text{Hop}_{\text{pr,sink}}$.

In summary, we can obtain:

$$T_{RDPSt} > T_{RSPSt} > T_{NRDPSt} > T_{RPBMPt} \ge T_{EPUSBRFt} = T_{NRSPSst} \gg T_{Shortest}.$$
 (27)

Therefore, the security performance of our proposed RDPS scheme is superior to the RSPS scheme and better than the RPBMP, EPUSBRF and the shortest path algorithms.

5.2. Analysis of Communication Overhead

Because the energy of WSNs is limited and lower energy consumption means a higher lifetime of the WSNs, so energy consumption is another key factor in WSNs. In this paper, the energy consumption is represented by communication overhead.

Suppose that the communication overhead for each node to forward a data packet is the same. The communication overhead in this paper is represented by the number of nodes through which the data packets pass. Since the SN determines the PNCS in this paper, the SN is usually wired and has powerful hardware resources, the communication overhead of the SN is usually not considered in related researches. At the same time, there are initialization phases in all of the related researches and the costs are similar. Hence, we take the same approach as Reference [18], and do not analyze the communication overhead of the phases of determining PN and the routing.

5.2.1. Communication Overhead of the Phantom Node Determination Phase

In the existing source node location privacy protection schemes, the PN is determined by the SoN via flooding, which will consume a lot of communication overheads. We show the reason for the following mathematical analysis.

In the EPUSBRF scheme, the PN is determined by the SoN using *h*-hop flooding and the *h*-hop directed routing. According to the network environment described in Reference [18], the average neighbor numbers of each node is 8.64, so the communication overhead of determining PN in EPUSBRF scheme is Hop_{pEPUSBRF} = $8.64 + 8.64^2 + \cdots + 8.64^h + h$ where the communication overhead for *h*-hop flooding is $8.64+8.64^2 + \cdots + 8.64^h$, and the communication overhead for *h*-hop directed routing is *h*.

According to Reference [16], the communication overhead of determining PN in RPBMP scheme is $Hop_{pRPBMP} = 3 * h$. The shortest path algorithm does not need to determine PN, so the communication overhead of determining PN in it is $Hop_{pShortest} = 0$.

However, in our proposed schemes, we use the sink node to help the source node to determine the PN. As the energy of the sink node is unlimited, its communication overhead is not considered in related researches. Therefore, the communication overhead of determining PN in our proposed schemes is $Hop_{pSPS} = Hop_{pDPS} = 0$.

In summary, the following relationships are obtained:

$$0 = \text{Hop}_{pShortest} = \text{Hop}_{pSPS} = \text{Hop}_{pDPS} < \text{Hop}_{pRPBMP} < \text{Hop}_{pEPUSBRF}.$$
 (28)

Therefore, in the phase of determining PN, the communication overhead of our proposed schemes is the same as the shortest path algorithm, and both are lower than that of the RPBMP and EPUSBRF schemes.

5.2.2. Communication Overhead of the Routing Phase

Suppose that the SPS, EPUSBRF and RPBMP schemes use the same network topology, and the PNs are all represented as p_c , and the path of the data packets transmitted from p_c to the SN does not pass through the visible area of the source node.

The communication overhead of the EPUSBRF scheme in the routing phase is

$$Hop_{EPUSBRFc} = Hop_{pc,sink}.$$
 (29)

The communication overhead of the RPBMP scheme in the routing phase is

$$Hop_{RPBMPc} = 3 * Hop_{pc,sink}.$$
 (30)

The communication overhead of the NRSPS scheme in the routing phase is

$$Hop_{NRSPSc} = Hop_{pc,sink}.$$
(31)

The communication overhead of the RSPS scheme in the routing phase is

$$Hop_{RSPSc} = M * Hop_{pc,sink}.$$
(32)

The communication overhead of the NRDPS scheme in the routing phase is

$$Hop_{NRDPSc} = (Hop_{pc,pr} + Hop_{pr,sink}).$$
(33)

The communication overhead of the RDPS scheme in the routing phase is

$$Hop_{RDPSc} = M*(Hop_{pc,pr} + Hop_{pr,sink}).$$
(34)

In summary, the following relationships are obtained:

$$Hop_{RPBMPc} > Hop_{RDPSc} = Hop_{NRDPSc} > Hop_{EPUSBRFc} = Hop_{RSPSc} = Hop_{NRSPSc'}$$
 $M = 1$

 $Hop_{RPBMPc} > Hop_{RDPSc} > Hop_{RSPSc} > Hop_{NRDPSc} > Hop_{EPUSBRFc} = Hop_{NRSPSc'} \qquad M = 2$

$$Hop_{RDPSc} > Hop_{RSPSc} \ge Hop_{RPBMPc} > Hop_{NRDPSc} > Hop_{EPUSBRFc} = Hop_{NRSPSc}$$
. $M \ge 3$

Therefore, as the number of PNs actually used increases, the communication overheads of the RSPS scheme and the RDPS scheme increase accordingly.

5.2.3. Comparison of the Total Communication Overhead

The total communication overhead is the sum of the communication overheads consumed in the PN determination phase and the routing phase. The total communication overhead of each scheme is shown in Table 3. It can be seen from Table 3 that when M = 1,

 $Hop_{EPUSBRFsum} > Hop_{RPBMPsum} > Hop_{RDPSsum} = Hop_{NRDPSsum} > Hop_{RSPSsum} = Hop_{NRSPSsum}$ (35)

Scheme	Total Communication Overhead
EPUSBRF	$Hop_{EPUSBRFsum} = Hop_{pEPUSBRF} + Hop_{EPUSBRFc}$
RPBMP	Hop _{RPBMPsum} = Hop _{pRPBMP} + Hop _{RPBMPc}
Shortest path algorithm	$Hop_{Shortest} = Hop_{pShortest} + Hop_{s,sink}$
NRSPS	$Hop_{NRSPSsum} = Hop_{pSPS} + Hop_{NRSPSc}$
NRDPS	$Hop_{NRDPSsum} = Hop_{pDPS} + Hop_{NRDPSc}$
RSPS	$Hop_{RSPSsum} = Hop_{pSPS} + Hop_{RSPSc}$
RDPS	$Hop_{DPSsum} = Hop_{pDPS} + Hop_{RDPSc}$

Table 3. Comparison of the total communication overhead.

Therefore, our proposed RSPS and NRSPS schemes have the lowest total communication overhead among the seven schemes because no communication overhead is generated in the PN determination phase. The total communication overhead of our proposed NRDPS and RDPS schemes is higher than that of the RSPS and NCPSP schemes, due to the actual use of dual PNs. The EPUSBRF scheme has the largest total communication overhead because the communication overhead increases exponentially, due to the flooding in the PN determination phase. Therefore, it can be seen that the total communication overhead of our proposed schemes is lower than that of the EPUSBRF and RPBMP schemes.

5.3. Comparison of the Performance Simulation

In order to verify the performance of our proposed schemes, we perform simulations with Matlab platform on the safety period and communication overhead. We compare our proposed schemes with RPBMP [16], EPUSBRF [18] and the shortest path algorithm. In order to facilitate the comparison of the performance of each scheme, we follow the simulation scenario of [18].

Suppose that 10,000 nodes are randomly and evenly distributed in the area of 6000 m*6000 m, and the communication radius of each node is 110 m. The entire network is divided into 3600 grids, each with a unit length of 100 m. The SN is fixed at the center of the network, and the SoN is randomly selected from the nodes in the network which corresponds to the scenario that the panda pops up at a random location. The attacker's hearing radius is the same as the sensor node's communication radius, and the visible area radius is set to be 110 m. In the *h*-hop directed routing phase of EPUSBRF and RPBMP, *h* is set to be 10 hops, and the threshold of RPBMP in the same hop routing phase is also *h*.

5.3.1. Comparison of Safety Period

In each experiment, the network topology remains the same, and the SoN sends data packets to the SN at time interval T. The attacker traces back one hop every time he overhears a packet, and the simulation ends once the attacker captures the SoN. If the attacker does not overhead the data packet within the time interval T, he will roll back hop-by-hop along the tracking path until he returns to the

SN. If the attacker overhears a packet while returning to the SN, he moves to the packet sending node and continues listening and backtracking until the end of the experiment. It should be noted that the end condition of the experiment in this paper is that the attacker captures the SoN, that is, in a single experiment the panda does not disappear once it appears. If the safety period is greater than 1000, the scheme can ensure that the panda will not be captured by the attacker.

Experiment 1: Comparison of the safety period of NRSPS and other three schemes

According to the analysis in Section 5.1.3, the NRSPS scheme provides the shortest safety period among our proposed schemes. Therefore, in Experiment 1, we compare the safety period of the NRSPS scheme with that of the shortest path algorithm, EPUSBRF and RPBMP. The average safety period is obtained by repeating 100 experiments, as shown in Figure 10.



Figure 10. Comparison of the safety period of the NRSPS scheme with the other three schemes.

It can be seen from Figure 10 that compared with the shortest path algorithm, EPUSBRF, and RPBMP, the average safety period of our proposed NRSPS scheme increases by 6.08 times, 3.57 times and 2.78 times, respectively. As the hop count between the SoN and the SN increases, the safety period of the four schemes increases. This is because the hop count that the attacker needs to backtrack increases correspondingly with the increase of hop count between the SoN and the SN. However, the safety period of each scheme in the experiment is less than 200, indicating that the SoN only sent less than 200 packets before being captured by the attacker. Therefore, although the safety period of NRSPS scheme improves compared with the shortest path algorithm, EPUSBRF, and RPBMP, it still cannot prevent the SoN from being captured by the attacker.

Experiment 2: The effect of the number of phantom nodes on the safety period

Since the NRSPS scheme cannot prevent the source node from being captured by the attacker, in Experiment 2, we consider increasing the number of PNs, and compare the safety period of the NRSPS scheme with that of the NRDPS scheme. The average safety period is obtained by repeating the experiment 100 times, as shown in Figure 11.

It can be seen from Figure 11 that the safety period provided by our proposed NRDPS scheme is much larger than that of the NRSPS scheme. Compared with NRSPS, the average safety period of NRDPS increases by 7.62 times. This is because as the number of PNs increases, the hop count of the routing path increases accordingly, which leads to an increase in the hop count required by the attacker to backtrack. Moreover, when the hop count from the SoN to the SN is greater than 20, the average safety period of the NRDPS scheme is greater than 1000, that is, the attacker is never able to capture the source node.



Figure 11. Comparison of the safety period of NRSPS and NRDPS.

Experiment 3: Comparison of the safety period of the proposed four schemes

In order to further compare the security performance of our proposed four schemes, we compare the safety period of the four schemes of NRSPS, NRDPS, RSPS and RDPS. The average safety period is obtained by repeating the experiment 100 times, as shown in Figure 12.



Figure 12. Comparison of the safety period of NRSPS, RSPS, NRDPS and RDPS.

It can be seen from Figure 12 that the RDPS scheme has the highest safety period. When the hop count of the source node to the sink node is 5, the safety period of the RDPS scheme reaches 1000, that is, the attacker cannot trace back to the SoN. In practical applications, the SoN is far away from the SN, so the RDPS can ensure the privacy and security of the location of the source node in practical applications. Compared with NRSPS, RSPS and NRDPS schemes, the safety period of the RDPS scheme increases by 32.13 times, 1.33 times and 4.22 times, respectively. In Figure 12, the safety period of the NRSPS does not change much. This is because the safety period of the NRSPS is low, and the change is too small compared with other schemes. Its actual change trend is shown in Figure 10.

It can be seen from the above comparison results that replacing the PN can greatly improve the security performance of the scheme. This is because after the PN is replaced, the attacker loses the

interception target. During the process of the attacker returning to the SN, the SoN continues sending the collected data packets to the SN.

Experiment 4: The impact of when to replace the phantom node on the safety period

It can be seen from Experiment 3 that replacing the PN can improve the security performance of the scheme. Therefore, in Experiment 4, we further explore the influence of the timing of replacing the PN on security performance. Suppose that in the RDPS scheme, when the attacker backtracks $Hop_{ps,pr}+Hop_{pr,sink}/n$ hops, the SoN changes the SPN and the RPN. It can be known from Equations (12) and (13) that in the RDPS scheme, the attacker needs to backtrack $Hop_{sum} = Hop_{s,ps} + Hop_{pr,sink}$ hops to capture the SoN. In the RDPS scheme, $Hop_{s,ps}$ is used as the extra security hop count. Suppose that Hop_E is the hop count that the attacker backtracks, and when $Hop_E = Hop_{ps,pr} + Hop_{pr,sink}/n$, the SoN replaces the PN. If the attacker does not overhear the packet, he needs to jump back Hop_E hops to the SN. Except for Experiment 4, in other experiments, the value of *n* is 1.

In the case of different *n*, the average safety period is obtained by repeating the experiment 100 times, as shown in Figure 13.



Figure 13. Comparison of the safety period of RDPS scheme with different *n*.

From Figure 13, we can see that the average safety period of the three cases is increased. This is because as the distance between the SoN and the SN increases, the number of hops that the attacker needs to trace back increases accordingly. Meanwhile, it can be seen from Figure 13 that the larger the value of *n* is, the smaller the average safety period is. This is because in the simulation, in order to avoid the experiment falling into an infinite loop, the SoN no longer sends the request packet to the SN even when the PNCS is empty, and the experiment ends when the attacker traces back to the SoN. Therefore, when the number of PNs that can be used is fixed, prematurely changing the PNs will in advance lead to an insufficient of PNs that can be used. As described in Section 3.3.2, if the SoN continues requesting the SN to help determine the PNCS when there is no PN available in the PNCS, better security performance will be obtained.

Experiment 5: The impact of *M* on the safety period of the proposed schemes

In order to further study the impact of *M* on the safety period of the proposed schemes in the case of replacing the PN, we compare the safety period of the two schemes of RSPS and RDPS. The average safety period is obtained by repeating the experiment 100 times, as shown in Figure 14.



Figure 14. Comparison of the safety period of RSPS and RDPS with different M.

From Figure 14, we can see that the security performance of our proposed RDPS scheme is superior to the RSPS scheme, and the average safety period of the two schemes increases with *M*. This is because for an attacker, he needs to trace to the PN so as to find the SoN. In fact, the value of M determines the size of the PNCS. The larger the value of M, the more PNs are available for the SoN, and the higher the security is. On the other hand, no matter how big the value of *M* is, the SoN only select one PN from the PNCS for use at a time, after a PN is used for a while, the SoN can replace the PN with another one. The SoN does not use *M* PNs simultaneously. Moreover, after the PN is replaced, the data packet transmission path will also change, and the attacker can no longer overhear the data packets and will roll back to the SN along the previous path. More PNs can bring more diversities and uncertainties in routing which will increase the difficulty for the attacker to track back and provide longer safety period for the true source node.

5.3.2. Comparison of Communication Overhead

Experiment 6: Comparison of communication overhead between NRSPS and other three schemes

In Experiment 6, we compare the communication overheads of our proposed NRSPS scheme with the shortest path algorithm, EPUSBRF and RPBMP. Since each node consumes the same communication overhead when forwarding packets, the number of nodes through which each packet passes is used as the communication overhead of the routing phase. The total communication overhead is the sum of the communication overheads consumed in the PN phase determination phase and the routing phase. We perform Experiment 6 repeatedly for 100 times and compare its communication overhead with the other three schemes. The simulation results are shown in Figure 15.

It can be seen from Figure 15 that the total communication overhead of our proposed NRSPS scheme is only slightly higher than that of the shortest path algorithm. While compared with EPUSBRF and RPBMP, the total communication overhead of our proposed NRSPS is reduced by 95% and 88%, respectively. The higher communication overhead of EPUSBRF is due to the high communication overhead in the phase of determining PN. In the experiment, *h* is set to be 3 in the flooding phase of EPUSBRF, so the communication overhead for determining PN is 8.64 + 8.642 + 8.643 + 3 = 731.26 (see Section 5.2.1 for theoretical analysis). It can be seen that in the phase of determining PN, the SoN performs flooding to determine the PN which causes a large amount of communication overhead. While in this paper, the SN helps the SoN determine the PN, which saves a lot of communication overhead.



Figure 15. Comparison of communication overheads between NRSPS scheme and other three schemes.

Experiment 7: Comparison of communication overhead of our proposed four schemes

We further compare the communication overheads of our proposed four schemes of NRSPS, NRDPS, RSPS and RDPS. The average communication overhead is obtained by repeating the experiment 100 times, as shown in Figure 16.



Figure 16. Comparison of the communication overhead of NRSPS, RSPS, NRDPS and RDPS.

As can be seen from Figure 16, the communication overhead of the RDPS scheme is the largest, and compared with the NRSPS, RSPS and NRDPS, the communication overhead is increased by 53.1 times, 2.39 times, and 7.10 times, respectively. In Figure 16, the communication overhead of NRSPS does not change much. This is because the communication overhead of NRSPS is low, and the change is too small compared with other schemes. The actual change trend of NRSPS is shown in Figure 16. It can also be seen from Figure 16 that the communication overhead of RSPS and RDPS is greatly increased compared with that of NRSPS and NRDPS. This is because the number of nodes through which the packet passes after the PN is changed increases, resulting in an increase in communication overhead. Although changing the PN can improve the security performance of the scheme, it also causes large communication overhead.

In summary, the communication overhead of the PN determination phase (Overhead 1 for short), the communication overhead of the routing phase (Overhead 2 for short), the total communication overhead (Total overhead for short), and the total safety period are shown in Table 4.

		Overhead 1	Overhead 2	Total Overhead	Total Safety Period	SC Ratio
Shortest path		0	20.93	20.93	20.93	1
RPBMP		30	335.76	365.76	45.68	0.12
EPUSBRF		731.26	87.05	818.31	35.68	0.04
Proposed	NRSPS	0	43.18	43.18	127.21	0.34
	RSPS	0	959.62	959.62	3070	3.20
	NRDPS	0	323.04	323.04	969	3.00
	RDPS	0	2292.60	2292.60	4087	1.78

Table 4. Comparison of the performance.

In order to more clearly compare the cost performance of each scheme, we refer to the Safety Period/Communication Cost as the SC ratio. The higher the SC ratio is, the better the performance of the scheme is. It can be seen from Table 4 that the performance of RSPS is better than other schemes. Although the other three schemes proposed in this paper have lower communication overhead or higher safety period, the performance is not balanced. The average total safety period of NRSPS and NRDPS is less than 1000, so the SoN may be captured by the attacker. However, compared with the shortest path algorithm, RPBMP and EPUSBRF, the safety period of our proposed NRSPS and NRDPS are still greatly improved. The average total safety period of the RDPS is as high as 4087, but the average total communication overhead is as high as 2292.6, which means that it causes a lot of communication overhead while achieving high safety period. Therefore, we can choose the most suitable solution according to different requirements of different scenarios. For example, whether to use single PN or dual PNs, or whether to change the PN.

Experiment 8: The impact of *M* on the communication overhead of the proposed schemes

In order to further study the impact of *M* on the communication overheads of the proposed schemes in the case of replacing the PN, we compare the communication overheads of RSPS and RDPS. The average communication overhead is obtained by repeating the experiment 100 times, as shown in Figure 17.



Figure 17. Comparison of communication overhead of RSPS and RDPS with different *M*.

From Figure 17, we can see that the communication overhead of our proposed RDPS is higher than that of the RSPS, due to the actual use of dual PNs, and as *M* increases, the communication overheads of the RSPS scheme and the RDPS scheme increase accordingly.

Although Figure 14 shows that the average safety period of the two schemes increases with *M*, the communication overheads are also increased greatly. Considering the balance between security and network performance, it is necessary to select the most suitable solution according to different requirements of different scenarios.

6. Conclusions

Source node location privacy protection is an important issue in widely-used WSNs. In this paper, we propose two new grid-based source location privacy protection schemes in WSNs to ensure the location privacy of source nodes. The sink node with high power resource is used to determine the PNCS, which reduce the total communication overhead. The phantom nodes selected in our proposed schemes can be distributed anywhere in the network and thus have stronger positional randomness. As our proposed schemes ensure the diversification of the routing path by increasing the number of phantom nodes used, the security performance of the source location privacy protection is further improved. The simulation results show that compared with other schemes, our proposed schemes have higher safety period and less communication overhead, thus their application prospect can be expected. Our proposed schemes are especially suitable for resource-constrained scenarios. However, considering the balance of performance of the schemes, it is necessary to select the most suitable solution according to different requirements of different scenarios. For example, when the security requirement for the network is very high and the communication overhead is not a constraint, RDPS can be used. Instead, if the network's communication conditions are limited and the security requirement is not so high, NRSPS and NRDPS can be adopted.

In the future, we will continue to improve the performance of our schemes, and aim to adapt them to their practical environments. Further research should consider the following aspects:

(1) In this paper, in order to simplify the problem, referring to other relevant pieces in the literature, we evaluate our schemes in the deterministic network model. However, in some practical applications as described in Reference [28], the stochastic deployments should be paid attention too. Therefore, we will study the source node location privacy protection in the stochastic deployments in our subsequent research;

(2) In the network model of this paper, only one source node and one sink node are considered, but in practical applications, there may be multiple source nodes and multiple sink nodes. Hence, in future research, we will investigate the multiple objects tracking scenarios.

Author Contributions: The idea and primary algorithm were proposed by Q.W.; J.Z. carried out the simulations and wrote the draft of the manuscript, Q.W. and X.O. critically reviewed the algorithms, results and manuscript for important intellectual content, and gave constructive discussions; Q.W. revised the manuscript and Y.R. polished the paper. All authors read and approved the final manuscript.

Funding: This work was partially supported by Zhejiang Province Natural Science Foundation (No. LY19F020039, No. LY18F020017), National Natural Science Foundation of China (No. 61401128, No. 61872120) and Key technologies, system and application of Cyberspace Big Search, Major project of Zhejiang Lab (No.2019DH0ZX01).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

SPS	grid-based Single Phantom node source location privacy protection Scheme
DPS	grid-based Dual Phantom node source location privacy protection Scheme
WSNs	Wireless Sensor Networks
SN	Sink Node
PN	Phantom Node
PNCS	Phantom Node Candidate Set

IoT	Internet of Things
SoN	Source Node
PRS	Phantom Routing Scheme
PSRS	Phantom Single-path Routing Scheme
EPUSBRF	Enhanced source location privacy preservation Protocol Using Source-Based Restricted Flooding
RPBMP	source location privacy preservation Routing Protocol Based on Multi-Path
PRABNS	Phantom Routing based on Area and Brother Neighbor Selecting
RSPS	SPS scheme in the case of Replacing the phantom pode
ROIS	DPS scheme in the case of Replacing the phantom node
NDCDC	Di osciente in un case of Nat Benlaring une prantom note
NIDDDC	SI S science in the case of Not Replacing the phantom node
	Di siciente n'ule case of tor replacing the phanton node
5PIN DDNI	Senaing Prantom Node
KPN ODMCC	Receiving Phantom Node
SPNCS	Sending Phantom Node Candidate Set
RPNCS	Receiving Phantom Node Candidate Set
Hop _{s,p}	Hop count from the Source node to the Phantom node in the EPUSBRF scheme
Hop _{p,sink}	Hop count from the Phantom node to the Sink node in the EPUSBRF scheme
Hop′ _{s,p}	Hop count from the Source node to the Phantom node in the RPBMP scheme
Hop′ _{p,sink}	Hop count from the Phantom node to the Sink node in the RPBMP scheme
Hop _{s,sink}	Hop count from the Source node to the Sink node in the shortest path algorithm
Hop _{epusbrf}	routing path Hop in the EPUSBRF scheme
Hop _{RPBMP}	routing path Hop in the RPBMP scheme
Hop _{Shortest}	routing path Hop in the Shortest path algorithm
T _{EPUSBRF}	Time required for the attacker to trace back to the source node in the EPUSBRF scheme
T _{RPBMP}	Time required for the attacker to trace back to the source node in the RPBMP scheme
T _{Shortest}	Time required for the attacker to trace back to the source node in the Shortest path algorithm
T _{pp}	Phantom node usage Time
Hopsps	Hop count from the Source node to the Phantom node in the NRSPS and NRDPS scheme
Hop _{ne sink}	Hop count from the Phantom node to the Sink node in the NRSPS scheme
Hop _{pe pr}	Hop count from the Sending Phantom node to the Receiving Phantom node in the NRDPS scheme
Hop	Hon count from the Receiving Phantom node to the Sink node in the NRDPS scheme
Тырерс.	Time required for the attacker to trace to the Phantom node in the NRSPS scheme
Тырерс	Time required for the attacker to trace to the Source node in the NRSPS scheme
TNKSP5s	Time required for the attacker to trace to the Phantom node in the NDDPS scheme
T NRDPSp	Time required for the attacker to trace to the Source node in the NEDFS scheme
T NRDPSs	Dhantom node usage Time in the NIPSDS scheme
¹ NRSPSpp	Dhantom node usage Time in the NDDPC scheme
I NRDPSpp	Financia hode usage time in the NKDF5 scheme
nop _{NRSPSsum}	Hops of fouring pain in the NNSF5 scheme
Hop _{NRDPSsum}	Hops of routing path in the NKDP'S scheme
Hop _{pc,sink}	Hop count from the Phantom node to the Sink node in the NKSPS, NKDPS, EPUSBKF and KPBMP scheme
T _{EPUSBRFt}	lime required for the attacker to trace to the phantom node in the EPUSBKF scheme
T _{RPBMPt}	Time required for the attacker to trace to the phantom node in the RPBMP scheme
T _{NRSPSt}	Time required for the attacker to trace to the phantom node in the NRSPS scheme
T _{NRDPSt}	Time required for the attacker to trace to the phantom node in the NRDPS scheme
T _{RSPSt}	Time required for the attacker to trace to the last phantom node in the RSPS scheme
T _{RDPSt}	Time required for the attacker to trace to the last phantom node in the RDPS scheme
Hop _{pEPUSBRF}	communication overhead of determining Phantom node in the EPUSBRF scheme
Hop _{pRPBMP}	communication overhead of determining Phantom node in the RPBMP scheme
Hop _{pShortest}	communication overhead of determining Phantom node in the Shortest path algorithm
Hop _{pSPS}	communication overhead of determining Phantom node in the SPS scheme
Hop _{pDPS}	communication overhead of determining Phantom node in the DPS scheme
Hop _{EPUSBRFc}	Communication overhead of the EPUSBRF scheme in the routing phase
Hop _{RPBMPc}	Communication overhead of the RPBMP scheme in the routing phase
Hop _{NRSPSc}	Communication overhead of the NRSPS scheme in the routing phase
Hop _{RSPSc}	Communication overhead of the RSPS scheme in the routing phase
Hop _{NRDPSc}	Communication overhead of the NRDPS scheme in the routing phase
Hop _{RDPSc}	Communication overhead of the RDPS scheme in the routing phase
HopEDICERFEII	Sum of the communication overheads in the EPUSBRF scheme
HopRPBMPeum	Sum of the communication overheads in the RPBMP scheme
HopRDPSeum	Sum of the communication overheads in the RDPS scheme
HopNPDDC	Sum of the communication overheads in the NRDPS scheme
Hoppepeorem	Sum of the communication overheads in the RSPS scheme
HODNDODC	Sum of the communication overheads in the NRSPS scheme
~ r INKSF3Sum	

References

- 1. Wang, J.; Wang, F.; Cao, Z.; Lin, F.; Wu, J. Sink Location Privacy Protection under Direction Attack in Wireless Sensor Networks. *Wirel. Netw.* **2016**, *23*, 579–591. [CrossRef]
- Jia, Z.; Wei, X.; Guo, H.; Peng, W.; Song, C. A Privacy Protection Strategy for Source Location in WSN Based on Angle and Dynamical Adjustment of Node Emission Radius. *Chin. J. Electron.* 2017, 26, 1064–1072. [CrossRef]
- Mutalemwa, L.C.; Shin, S. A New Diversional Routing Scheme to Preserve Source Location Privacy in Wireless Sensor Networks. In Proceedings of the 3rd International Conference on Next Generation Computing (ICNGC2017b), Kaohsiung, Taiwan, 21–23 December 2017; pp. 260–262.
- Li, Y.; Lightfoot, L.; Ren, J. Routing-based Source-Location Privacy Protection in Wireless Sensor Networks. In Proceedings of the IEEE International Conference on Electro/Information Technology, Windsor, ON, Canada, 7–9 June 2009; pp. 29–34.
- Kirton, J.; Bradbury, M.S.; Jhumka, A. Source Location Privacy-Aware Data Aggregation Scheduling for Wireless Sensor Networks. In Proceedings of the 37th IEEE International Conference on Distributed Computing Systems, Atlanta, GA, USA, 5–8 June 2017; pp. 2200–2205.
- 6. Ozturk, C.; Zhang, Y.; Trappe, W.; Ott, M. Source-Location Privacy for Networks of Energy-Constrained Sensors. In Proceedings of the Second IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems, Vienna, Austria, 12 May 2004; pp. 68–72.
- Kamat, P.; Zhang, Y.; Trappe, W.; Ozturk, C. Enhancing Source-Location Privacy in Sensor Network Routing. In Proceedings of the IEEE international conference on distributed computing systems (ICDCS'05), Columbus, OH, USA, 6–10 June 2005; pp. 599–608.
- 8. Lilian, C.M.; Seokjoo, S. Strategic Location-Based Random Routing for Source Location Privacy in Wireless Sensor Networks. *Sensors* **2018**, *18*, 2291.
- 9. WWWF—The conservation organization. Available online: http://www.panda.org/ (accessed on 3 March 2019).
- 10. Wang, H.D.; Sheng, B.; Li, Q. Privacy-Aware Routing in Sensor Networks. *Comput. Networks* 2009, 53, 1512–1529. [CrossRef]
- Ouyang, Y.; Le, Z.; Chen, G.; James, F.; Fillia, M. Entrapping Adversaries for Source Protection in Sensor Networks. In Proceedings of the International Symposium on World of Wireless, Mobile and Multimedia Networks, Washington, DC, USA, 26–29 June 2006; pp. 23–34.
- 12. Tan, W.; Xu, K.; Wang, D. An anti-tracking source-location privacy protection protocol in WSNs based on path extension. *IEEE Internet Things J.* **2014**, *1*, 461–471. [CrossRef]
- 13. Yi, X.F.; Fan, X.P. Redundancy Branch Combine Spiral Routing to Preserve Source Location Privacy for WSNs. *J. Chin. Comput. Syst.* **2015**, *36*, 244–251. (In Chinese)
- 14. Roy, P.; Rimjhim; Singh, J.P.; Kumar, P. An efficient privacy preserving protocol for source location privacy in wireless sensor networks. In Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 23–25 March 2016; pp. 1093–1097.
- 15. Zhang, J.N.; Chu, C.L. A Scheme to Protect the Source Location Privacy in Wireless Sensor Networks. *Chin. J. Sens. Actuators* **2016**, *29*, 1405–1409. (In Chinese)
- 16. Ma, W.; Song, L. Source location privacy preservation routing protocol based on multi-path. *Comput. Eng. Appl.* **2018**, *54*, 81–85. (In Chinese)
- Ozturk, C.; Zhang, Y.; Trappe, W. Source-location privacy in energy-constrained sensor network routing. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington, DC, USA, 25–25 October 2004; pp. 88–93.
- Chen, J.; Fang, B.X.; Yin, L.H.; Su, S. A Source-Location Privacy Preservation Protocol in Wireless Sensor Networks Using Source-Based Restricted Flooding. *Chin. J. Comput.* 2010, 33, 1736–1747. (In Chinese) [CrossRef]
- 19. Yi, X.F.; Fan, X.P. Beyond Adversary Trace Time Routing Approach for Preserving Source-location in WSNs. *J. Chin. Comput. Syst.* **2014**, *35*, 311–318. (In Chinese)
- 20. Chen, Y.; Jiang, C.H.; Guo, C.; Xie, F.Y.; Wu, H.C. An Improved Routing Algorithm for Source Location Privacy Protection in Wireless Sensor Network. *Chin. J. Sens. Actuators* **2017**, *30*, 438–449. (In Chinese)
- 21. Kong, X.X.; Yuan, S.Q.; Chen, M. Routing Protocol of Source-Location Privacy Protection based on Virtual Ring. *Transducer Microsyst. Technol.* **2018**, *37*, 66–69. (In Chinese)

- 22. Wang, W.X.; Li, P.Z. A Privacy Protection Method of Source Location in Wireless Sensor Networks. *J. Chongqing Univ.* **2018**, *41*, 100–108. (In Chinese)
- Cerpa, A.; Estrin, D. ASCENT: Adaptive Self-Configuring Sensor Networks Topologies. *IEEE Trans. Mob. Comput.* 2004, 3, 272–285. [CrossRef]
- 24. Chai, R.; Zhang, Y. A Practical Supercapacitor Model for Power Management in Wireless Sensor Nodes. *IEEE Trans. Power Electron.* **2015**, *30*, 6720–6730. [CrossRef]
- 25. Jiang, J.; Han, G.; Wang, H.; Guizani, M. A survey on location privacy protection in Wireless Sensor Networks. *J. Networks Comput. Appl.* **2019**, 125, 93–114. [CrossRef]
- 26. Bradbury, M.; Jhumka, A.; Leeke, M. Hybrid Online Protocols for Source Location Privacy in Wireless Sensor Networks. *J. Parallel Distrib. Comput.* **2018**, *115*, 67–81. [CrossRef]
- 27. Intanagonwiwat, C.; Govindan, R.; Estrin, D. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks. In Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networks (MobiCOM), Boston, MA, USA, 6–11 August 2000; pp. 56–67.
- Olasupo, T.O.; Otero, C.E. The Impacts of Node Orientation on Radio Propagation Models for Airborne-Deployed Sensor Networks in Large-Scale Tree Vegetation Terrains. *IEEE Trans. Syst. Man Cybern. Part A Syst.* 2017, 1–14. [CrossRef]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).