Received August 22, 2020, accepted September 7, 2020, date of publication September 10, 2020,
date of current version September 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3023260

A Ring-Based Routing Scheme for Distributed Energy Resources Management in IIoT

ZHIWEN XIONG[1,2], HUIBIN WANG[1], LILI ZHANG[1], TANGHUAI FAN[2], AND JIE SHEN[1]
[1]College of Computer and Information Engineering, Hohai University, Nanjing 211100, China
[2]School of Information Engineering, Nanchang Institute of Technology, Nanchang 330029, China

Corresponding author: Huibin Wang (hbwang@hhu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61671201 and Grant 61903124.

ABSTRACT Recently, Distributed Energy Resources (DERs) have been utilized with increasing frequency in Industrial Internet of Things (IIoT) to deal with energy and environmental challenges. IIoT with wireless communication technology, which is easy to be intercepted, often facing various attack. For the safety of the network, more complex algorithms need to be run on IIoT, but the action need more energy. In addition, in some application scenarios, the location where the packets were generated indicates that an event occurred. An attacker can find the sensor node through a backtracking attack, which is equivalent to reaching the place where the event occurred. In order to hide the location information of the event, it is necessary to protect source location privacy (SLP), which will also increase the energy consumption of IIoT. If only the traditional battery is used to power the nodes in IIoT, the lifetime of the system will be limited. When IIoT is deployed outdoors, it is often difficult to replace the battery. The existence of lakes make IIoT have coverage holes during deployment. In order to implement SLP and make the system work for a long time in the environment with deployment holes, we use DERs. Herein, we propose an SLP protection scheme based on phantom nodes, rings, and fake paths (PRFs) for IIoT. To increase the safety time of the network, the PRFs dynamically selects the phantom nodes. To adapt to a complex deployment environment, the ring can be flexibly deployed according to the terrain. The PRFs uses fake paths to confuse attackers. We integrate DERs technology into PRFs, such as using solar power modules, looking forward to extending the lifetime of the system. The experimental results proved that the PRFs could efficiently reduce backtracking attacks while maintaining a balance between security and network energy consumption of IIoT.

INDEX TERMS Source location privacy, distributed energy resources, IIoT, coverage hole, phantom node, fake path.

I. INTRODUCTION

With the rapid development in wireless communication technology, the application of wireless sensor networks (WSNs) has rapidly increased, such as those in wildlife protection [1], environmental monitoring [2], traffic management [3], disaster management [4], and medical care [5]. Owing to the wireless medium and constrained nature of resources [6] of the sensors used in WSNs, source location privacy (SLP) faces more severe challenges compared to traditional networks. The resource limitations of sensor nodes and unreliable communication medium in harsh environments render it difficult to directly employ the existing security approaches owing to the complexity of the algorithms involved. Increasing the complexity of SLP routing schemes can effectively prevent attackers from implementing backtracking attacks, so more and more routing schemes use ring routing paths. But the sensor nodes that make up the loop usually consume a lot of energy, which shortens the life cycle of the network. The motivation of this paper is how to make the SLP with loop routing path be deployed efficiently in complex environment and not shorten the network lifetime because of the high energy consumption of the ring routing path. Therefore, we integrate Distributed Energy Resources (DERs) [7], [8] into the solution. When the deployment position of the ring node is relatively fixed, we add the solar module to the node, so that Industrial Internet of Things (IIoT) [9], [10] has a more flexible energy management. DERs are reshaping the operation of the electric power system. New technologies and lower costs increase deployment opportunities for DERs,

The associate editor coordinating the review of this manuscript and approving it for publication was Jiayong Li.

such as photovoltaic, electric vehicles, energy storage, and promote the energy transition from fossil fuels to renewable.

Herein, we focus on the protection of SLP for IIoT. We propose a routing scheme based on phantom nodes, rings, and fake paths (PRFs). PRFs can be deployed in IIoT, where multiple source nodes or multiple sink nodes [11], [12] exist. In RPFs, each node must acquire and store less network topology information to ensure that the network is operating, which reduces the storage space for sensor nodes and further strengthens the security of WSNs. In PRFs, data packets transmitted in the network are primarily divided into two categories: real and fake packets [13]. The real packets contain data collected by the source node, while the fake packets are used to imitate the behavior of real packets to confuse attackers. In PRFs, the transmission of a real packet comprises four phases. Architecture of the PRFs is shown in Figure 1:

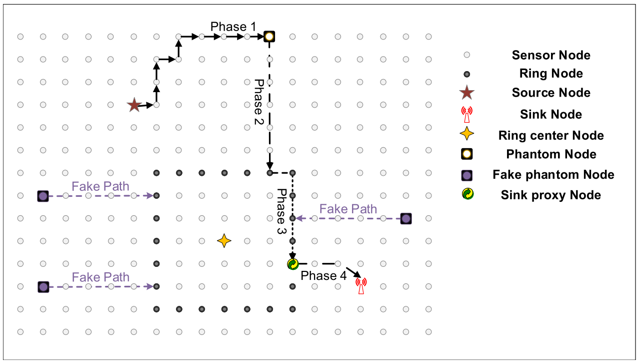

FIGURE 1. Architecture of the PRFs.

Phase 1. The source node detects the monitoring target and generates the real packet, and the source node transmits the real packet to the phantom node by the method described in Algorithm 1;

Phase 2. the phantom node transmits the real packet to the ring by the method described in Algorithm 2;

Phase 3. the real packet is transmitted clockwise in the ring and arrives at the sink proxy node;

Phase 4. the sink proxy node transmits the real packet to the sink node through the shortest path. If the sink node is in the ring, the phase 4 does not exist because the sink proxy node in stage 3 is the sink node itself.

Fake paths are generated by the method described in Algorithm 5. The node of the beginning of a fake path is in the ring, and the last node of a fake path is called a fake phantom node. A fake phantom node generates many fake packets and sends them to the ring, mimicking the behavior of a real phantom node. The lifetime of a fake packet is measured in hops. A fake packet is transmitted in the network during its lifetime to confuse the attacker such that the attacker cannot distinguish real packets from all packets traveling in the network.

The main contributions of this paper as follows:

1) This paper presents the PRFs scheme based on phantom nodes, rings, and fake paths. The scheme can protect the source location privacy of IIoT and support the multiple sources or multiple sink scenario. If some areas exist in the deployment environment where sensors are not allowed to be deployed, the PRFs can still perform efficiently;
2) In this study, many intuitive, simple, and efficient algorithms are used to realize the PRFs scheme; these algorithms require little computational power and is suitable for WSNs;
3) We integrate DERs technology into PRFs to improve the lifetime of the IIoT.
4) We perform simulations using OMNET++ to prove the efficiency of our scheme.

The remainder of this paper is organized as follows. In section II, we provide a review of related studies. Section III introduces the assumptions and system model. Section IV describes our proposed scheme in detail. The experimental results and analysis are presented in Section V. In Section VI, conclusions and future studies are presented.

II. RELATED STUDIES

The variety of sensors are increasing and hence the reliability of sensors [14], which promotes the accurate acquisition of environmental information by high-precision data fusion [15]. Based on accurate access to environmental information, location-based services are increasing as well [16], and a large amount of private data is used for analysis [17], which poses a threat to SLP. This paper focuses on the protection of SLP, which is aimed at WSNs deployed on land, to strengthen the context privacy of transmission and realize the protection of SLP.

The existing works rarely consider the problem of deployment holes, such as the existence of lakes in the environment. We solve the problem by integrating DERS with ring. SLP schemes can be divided into two categories: using or without using ring. Let's first review SLP schemes without using ring.

A. SLP SCHEMES WITHOUT USING RING

Ozturk first proposed the concept of SLP and the panda-hunter model, and used a phantom routing (PR) and phantom single-path routing (PSPR) [18] to protect SLP. Both schemes divide the transmission process of a real packet into two phases. In the first phase, the packet is transferred from the source node to the phantom node, and vice versa in the second phase. The algorithms adopted by the PR and PSPR are different in the two phases. In the first phase, the PR separates the neighbors into two groups such that those nodes whose directions are opposite to each other do not belong to the same group. The PSPR divides neighbor nodes into two groups according to their number of hops from the sink: one group of nodes with more hops than themselves from the sink node, and the remaining nodes into one group. In the second phase, the PR uses flooding routing to transmit packets, while the PSPR uses single-path routing to transmit packets. To select the optimal next-hop node among the neighboring nodes, some new factors are often introduced to assist judgment. In the Identity, Route and Location privacy algorithm (IRL) [19], the routing method is similar to that of the PR, but in addition to grouping neighbor nodes, it calculates the trust degree for each neighbor node and selects the next hop from the neighbor nodes by combining grouping and trust degree.

The scheme in [20] takes sink nodes as the center, divides the network into four quadrants, and constructs x-y coordinates. An arbitrary factor named AF is generated by the algorithm. Convert the AF factor to an angle in the x-y coordinates and find the path node along this angle, then the data packet generated by the source can be transmitted to the sink node through the relay of the path node. In [21], dynamic shortest path (DSP) algorithm is proposed, which divides the whole WSN into equally sized square grid, and each grid has a cluster head(CH) and an equal number of nodes. Data packets can be transmitted between CHs, and according to the cluster head list(CHL), each CH knows the next CH with the shortest path to sink node. When the source node detects an event, it sends data to the CH of the grid, and the CH transmits the data to the sink node through the shortest path. Every once in a while, the CHs are reselected and the CHL is updated to prevent backtracking attacks.

Wang defines the concept of hatched circle [22], which is the visible area of the source node. The radius of a hatched circle, called the visible distance, is the maximal distance that an attacker can detect, as shown in Figure 4. In the Phantom Routing with Locational Angle scheme, every data packet will first be transmitted using random walk according to the inclination angle. Subsequently, it will be transmitted along the shortest path to the sink node.

Some schemes will actively monitor whether attackers exist in the network and take corresponding measures to protect the location privacy of the source nodes. In the light-weight and distributed protocol against adversarial localization scheme [23], the network is divided into multiple grids. If an attacker is found in a grid, all sensor nodes in that grid become silent. When the grid boundary node discovers that the attacker has left the grid, it will send a warning message to the adjacent grid and broadcast the activation packet in its own grid. In the Context-Aware Location privacy scheme [24], the node that detects the attacker sends the attacker's location information to the surrounding nodes through the MAC layer, and the transmission path of all packets is the farthest possible from the attacker. Y. Wang [25] proposed an efficient algorithm based on circular trap (CT), which integrates the routing layer and MAC layer protocol to provide SLP protection for WSNs. In the proposed scheme, a CT route is formed to induce an attacker to first detect the packets from the nodes on the circular route, thereby moving away from the real route and protecting the SLP.

Some algorithms that are widely used in other research fields are also used in SLP. An energy efficient scheme [26] based on the ant colony optimization scheme, which is a flexible routing strategy, provides a natural and intrinsic method to explore the search space for preserving a sensor's location privacy. The Source-location privacy full protection scheme [27] considers a practical adversarial model, which is a combination of global and local models. The source node constructs a cloud around itself based on shares and dummy packages to hide its location. In [28], Kirton presented a multiobjective optimization problem where SLP, schedule latency, and final attacker distance were the criteria, and genetic algorithms were employed to generate Pareto-optimal schedules using two fitness criteria. In [29], Bradbury modeled the SLP problem as an integer linear programming optimization problem using the optimizer to obtain an optimal solution to provide SLP. In [30], Gu proposed a methodology where SLP protocols were first profiled to capture their performances under various protocol configurations. Subsequently, a novel decision theoretic procedure was presented for selecting the most appropriate SLP routing algorithm for the application and network under investigation.

B. SLP SCHEMES USING RING

Increasing the complexity of the routing path is a typical approach to confuse the attackers, Let's review SLP schemes using ring. In [31], the destination node is placed in the center of a square area called destination area. The shortest path between the source node and the different parts of the square edge constructs many disjoint routing paths. Data packets are transmitted to destination area by the source node through several paths, and then reaches the destination. The tree-based scheme [32] builds a backbone path from an edge node to sink node, and then generates numerous branch paths along this backbone path, resembling a tree. Branch paths generate fake packets, and if they are close to the source node, real packets are collected and transmitted. All packets are transmitted to the sink node through the backbone path. In the tree-based scheme, several branch paths increase the difficulty of the attack. The path extension scheme [33] uses the backbone path; however, unlike the tree-based scheme, its backbone path is the shortest path from the source node to the sink node, which can reduce the delay of real packets. To render the path more deceptive to attackers, the path in Multi rings scheme (Multirings) [34] comprises multiple rings, where all rings have the same sink node as their center. If a source node is created in the ath ring, the scheme selects the bth and cth rings and angles a and b. Subsequently, the packets travel outward from the source node to the bth ring. It travels counterclockwise for an a angle and then to the cth ring and transmits at a b angle. Subsequently, the packets transmit along the shortest path to the sink node.

The ring has been adopted in many schemes [35], where fog appeared. In the Redundant Fog Loop-based scheme (RFL) [36], a fog is composed of a ring and nodes within the ring. The fog's center node has many branches connected with the fog's ring, the fog's center node generates fake packets and routes them to the fog's ring via these branches. The branch near the source node collects and transmits the real packets to the ring. The real packet is sent to the ring by a nearby branch and, after several hops within the ring, travels to the sink node. In [37], with sink as the center, using two concentric circles to build a two-level phantom routing strategy. The packets start from the source and arrive at the sink through a first level phantom node and a second level phantom node.

In other words, many routing protocols have been proposed to protect SLP, all of which exhibited a tradeoff between safety time and energy while considering the adaptation of the routing scheme to the deployment environment. This provided the motivation for this study.

III. SYSTEM MODEL AND ASSUMPTIONS

A. NETWORK MODEL

The network model in this study resembles the panda-hunter model [18], in that the wireless sensor network continuously monitors and locates pandas. When a sensor node detects a panda, it becomes a source node, packages the collected data, and sends the data to the sink node hop by hop. The purpose of SLP protection is to prevent an attacker from discovering the panda's location. Therefore, the following assumptions were made:

1) The nodes of the wireless sensor network can be divided into two types in terms of hardware: a sensor node and a sink node. A network contains multiple sensor nodes, including one or more sink nodes. Each sensor node has the same hardware resources, initial energy, communication capability, storage capacity, and computing power;
2) The sensor nodes, which are responsible for monitoring the pandas and collecting information, are deployed randomly and evenly; the position remains unchanged once the nodes are deployed. The sink node assigns different roles to different sensor nodes;
3) A network has one or more sink nodes that can be deployed anywhere in the network, and the position remains unchanged once they are deployed. The sink node is responsible for initializing the network topology and adjusting the network topology when necessary. The sink node is also the transmission terminal of the packets. The sink node will assign different roles to different sensor nodes. As shown in Figure 1, these roles involve the sensor, ring, source, ring center, phantom, fake phantom, and sink proxy nodes;
4) All the packets are encrypted [38]. This aspect is beyond the scope of this paper;
5) Each node knows its location and relevant information pertaining to their neighboring nodes. Communication is realized by hop-by-hop packet transmission between nodes.

B. ADVERSARY MODEL

The main purpose of the attacker is to find the pandas, that is, to locate the source node. The equipment used by the attacker will surpass the sensor and sink nodes in terms of performance. In this study, the characteristics of the attacker are assumed as follows:

1) The device adopted by the attacker has strong computing power, sufficient energy, and storage space. When intercepting a packet, the attacker can determine the location of the node that sent the packet, and the attacker can quickly move to the node. Because the attacker's equipment is sophisticated, it is assumed that the attacker can eavesdrop on all nearby packets and will therefore not miss these packets;
2) The attacker adopts a passive attack mode. The attacker can eavesdrop on the packets and monitor the network traffic. However, the attacker does not actively attack the node, damage the network topology, and serialize the contents of the packets;
3) We assumed that the attacker only adopts the local attack. The attacker can move quickly as required to monitor the different network areas of the WSNs, which means that the attacker can hop-by-hop trace back to the source sensor's location.

IV. OUR PROPOSED PRFS SCHEME

A. OVERVIEW OF PRFs

In PRFs, except the control commands packets, the remaining packets are primarily of two types: real and fake data packets. As shown in Figure 1, the source node sends real packets to the sink node, and the real packets are transmitted to the sink node along the path of phase 1–4. Fake packets are primarily used to confuse attackers; these fake packets are born from fake phantom nodes that travel to the ring along the fake path, and simulate the behavior of real packets until the end of their lifetime.

In a wireless sensor network (WSN), sink nodes are responsible for aggregating the packets in the network and initializing and adjusting the network topology. When the sink node initializes the WSN, some of the sensor nodes are defined as ring nodes, and all the ring nodes are connected to form a ring. In addition, a ring center is defined. In general, the ring center is a sensor node inside the ring. The selection strategy for the ring center will be discussed later.

The real packets are born at the source node, and the destination is the sink node. The transmission process is primarily composed of four phases. Using Figure 1 as an example, in phase 1, the real packets travel to the phantom node from the source node; subsequently, the real packets are sent to the ring in phase 2. In phase 3, the real packets travel clockwise inside the ring; finally, in phase 4, all the real packets travel to the sink node. If the sink node is one of the ring nodes, then phase 4 is not required.

To protect the security of the source node, after the source node transmits $K(K >= 1)$ packets with a phantom node, a new phantom node is generated and the old one is invalidated. Simultaneously, several fake phantom nodes will be generated in the network to imitate the behavior of real phantom nodes, and each fake phantom node will send K fake packets to the ring to confuse the attacker.

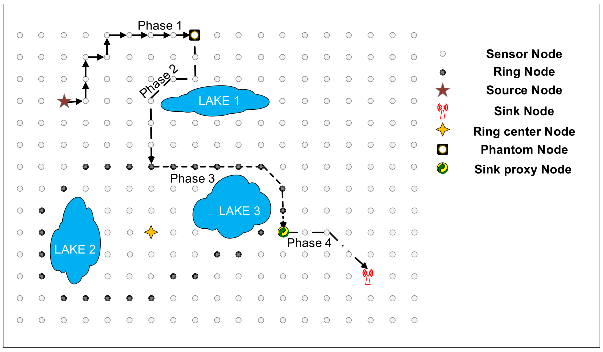

FIGURE 2. The ring center is a sensor node inside the ring.

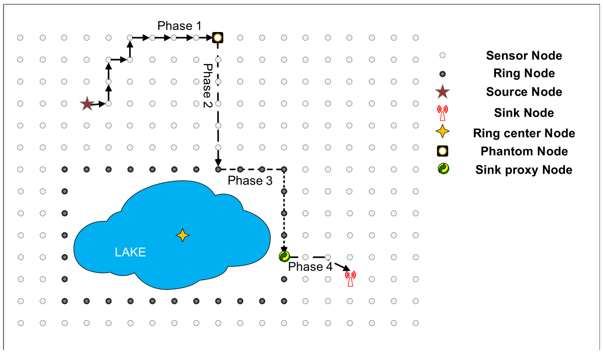

FIGURE 3. The ring center is a logically existing node.

Each node in the wireless network classifies its neighbor nodes based on the number of hops they require to reach the ring center. Each sensor node does require information regarding the ring nodes and can transmit the packets outside the ring to the ring. Each node transmits the packets to a neighbor node closer to the ring than itself, and the packet will finally reach the ring because the path of the packets to the ring center will intersect with the ring. Similarly, when sending packets from inside the ring to the ring, each node must send the packet to a neighbor node far away from the ring center.

The distance between the ring and the ring center can be calculated by hops, which is the information required by all sensor nodes. For the network to adapt better to the complex deployment environment and terrain, the selection of ring and ring center in PRFs is highly flexible and independent of the source and sink nodes' location. The method for all sensor nodes to obtain the number of hops is as follows:

1) In the deployment environment shown in Figure 1, sensor nodes can be deployed in all areas. When initializing the network, the sink node will specify a sensor node as the ring center, which broadcasts beacons [34]. The beacons contain the number of hops to the ring center. As the beacons spread, all nodes in the network will know their number of hops from the ring center;
2) As shown in Figure 2, sensor nodes cannot be deployed in some areas owing to the presence of three lakes. The ring is formed flexibly according to the terrain. The ring center is a sensor node. By broadcasting a beacon, all nodes in the network will know their number of hops from the ring center;
3) In Figure 3, the ring is formed around the lake, and sensor nodes cannot be deployed inside the ring. In this case, the ring center is only a logical node. In the initial network, the base station will specify that the distance between the ring nodes and ring center is 1 hop. The ring nodes continue to broadcast beacons, and all nodes in the network will know their number of hops from the ring center, as if the ring center is a sensor node.

If in the application scenario, the ring nodes are mainly deployed in a fixed location, for example, the ring nodes are mainly deployed around the lake, then these nodes can be equipped with solar modules to extend the lifetime. If the deployment location of the ring node already supports the DERs, for example, there are street lights supporting the DERs around the lake, then the ring nodes equipped with solar modules can join the existing DERs.

B. DETAILS OF THE PROPOSED SCHEME

1) PHASE 1: REAL PACKETS TRAVEL TO THE PHANTOM NODE

In phase 1, the source node sends real packets to the phantom node. The following factors should be considered when selecting the phantom node:

1) The phantom node should be farther from the ring center than the source node;
2) The number of hops from the source node to the phantom node is appropriate;
3) The shortest path from the phantom node to the ring center does not pass through the visible area [22] of the source node;
4) The phantom node changes dynamically and randomly to prevent the phantom node from being exposed;
5) The amount of computation for generating phantom nodes is small.

As shown in Figure 4, nodes A, B, and C are phantom nodes that have the same number of hops to the source. Phantom node C is more suitable. Phantom node A is not an optimal choice because the shortest path to the ring center passes through the visible area. Additionally, phantom node B is not an optimal choice because its distance to the ring center is less than the distance from the source node to the ring center. In other words, the shaded portions denoted Area 1 and Area 2 in Figure 4 are suitable regions for the phantom nodes.

The PRFs select a small number of phantom nodes for calculation, and these nodes are distributed in Areas 1 or 2. For a clearer illustration, the new phantom nodes are born in Area 2, as shown in Figure 5. Algorithm 1 is the corresponding pseudo code running on the source node, and the sensor node receives the real packet. The meanings of the variables are detailed in Table 1.

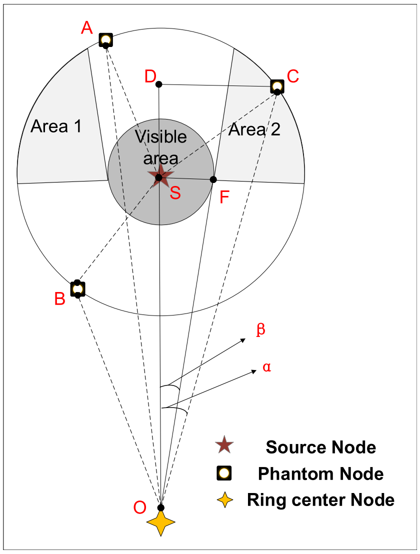

FIGURE 4. Suitable regions for the phantom nodes.

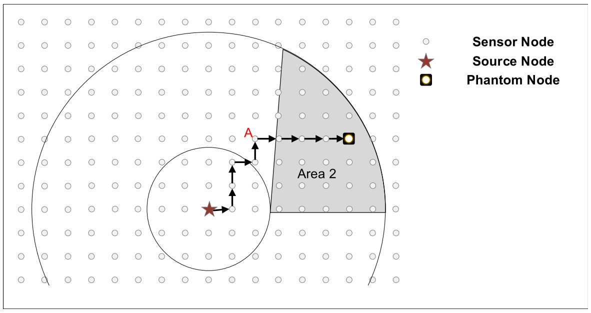

FIGURE 5. Process of generating a phantom node.

TABLE 1. Meanings of variables in Algorithm. 1.

Variables	Meaning of the variables
$SendMessage\ (Far)$	This node selects a node that is farther to the ring center from its neighbors and sends a packet to that node.
$SendMessage$ $(Clockwise)$	Filter out the group of neighbor nodes with the same number of hops from the center of the ring, and then select the last node in the clockwise direction as the next hop node in the group.
$Walk$	Record the total number of hops traveled by a packet.
$ProbabilityFar$	$0 < ProbabilityFar < 1$; adjust the possibility of executing $SendMessage\ (far)$.
M, N	M is the total number of hops from the source node to node A, and N is the path length from the source node to the phantom node.

Next, we provide an example of how the code works, the results of which are shown in Figure 5. We set *Walk* = 0, *M* = 5, and *N* = 9. The results obtained by executing code lines “1-8” are “*SendMessage(clockwise)*,” “*SendMessage(far)*,” “*Send Message(far)*,” “*SendMessage(clockwise)*,” and “*SendMessage(far)*”. The result of executing code lines “9-12” is the execution of “*SendMessage(clockwise)*” four times.

Algorithm 1 Real Packets Travel to the Phantom Node

```
1:  if ($Walk < M$) then
2:      $temp = random(0, 1)$;
3:      $Walk{+}{+}$;
4:      if ($temp < ProbabilityFar$) then
5:          $SendMessage(Far)$;
6:      else
7:          $SendMessage(Clockwise)$;
8:      end if
9:  else if ($Walk >= M$ and $Walk < N$) then
10:     $Walk{+}{+}$;
11:     $SendMessage(Clockwise)$;
12: else if ($Walk == N$) then
13:     $Walk{+}{+}$;
14:     This node is the phantom node; phase 1 is complete;
15: end if
```

To decide the numbers of M, N, and $ProbabilityFar$, the condition below is important:

$$\alpha > \beta. \tag{1}$$

To reduce the amount of calculation, Formula (1) is applied to obtain Formula (2):

$$\begin{cases} \frac{L_{CD}}{L_{OD}} > \frac{L_{SF}}{L_{OS}}, \\ L_{OD} = L_{OS} + M \times ProbabilityFar, \\ L_{CD} = L_{SF} + N + M \times (1 - ProbabilityFar), \end{cases} \tag{2}$$

where L_{CD}, L_{OD}, L_{SF}, and L_{OS} are the lengths of lines CD, OD, SF, and OS. L_{SF} is the number of hops of the radius of the visible area, L_{OS} is the number of hops from the source to the ring center node.

Equation (2) is applied to obtain Formula (3). M, N, and $ProbabilityFar$ must satisfy Formula (3).

$$(M + N) \times L_{OS} - M \times ProbabilityFar \times (L_{OS} + L_{SF}) > 0. \tag{3}$$

For more random values of M and N, random numbers “$Random1$” and “$Random2$” are used to perform the following operations: $M = M + Random1$, $N = N + Random2$. By using “$Random1$” and “$Random2$”, the phantom nodes can be distributed more randomly in the network.

When a phantom node is determined, a path from the source node to the phantom node can be determined. The phantom node and path will be used to transmit packets several times; subsequently, a new phantom node and path will be regenerated.

2) PHASE 2: REAL PACKETS TRAVEL TO THE RING

In phase 2, the phantom node sends the real data packet to the ring. As shown in Figure 1, the phantom node is outside the ring. The phantom node does not know which nodes are ring nodes. The phantom node sends the packet toward the ring center. All the sensor nodes that receive the packet perform the same operation, and the packet finally reaches the ring. Algorithm 2 is the corresponding pseudo code. The meaning of the variables is shown in Table 2.

Algorithm 2 Real Packets Travel to the Ring

```
if (The current node is not in the ring) then
    $Walk$++;
    $SendMessage(RingCenter)$;
else if (The current node is in the ring) then
    This node is a ring node; phase 2 is complete;
end if
```

TABLE 2. Meaning of variables in Algorithm 2.

Variables	Meaning of the variables
$SendMessage$ $(RingCenter)$	This node selects a node closer to the ring center from its neighbors and sends a packet to that node.

3) PHASE 3: REAL PACKETS TRAVEL IN THE RING

In phase 3, as shown in Figure 1, real packets are transmitted clockwise in the ring until they reach the sink proxy node; subsequently, they are transmitted to the sink node.

The ring node closest to the sink node is called the sink proxy node. To obtain the sink proxy node using the simplest algorithm, the shortest path between the base station and ring center intersects with the ring, and the node at the intersection is called the sink proxy node. In a special case where the sink node is in the ring and the base station is its own sink proxy node, the transmission of the real packet ends when it reaches the sink node. Algorithm 3 is the corresponding pseudo code.

Algorithm 3 Real Packets Travel in the Ring

```
if (The current node is sink) then
    The packet arrives at the sink node and the transmission is complete;
else if (The current node is a proxy for sink) then
    $Walk$++;
    This node is a sink proxy node; phase 3 is complete;
else
    $Walk$++;
    The packet is transmitted clockwise in the ring;
end if
```

4) PHASE 4: REAL PACKETS TRAVEL TO THE SINK NODE

If the sink node is in the ring, this phase is not required. Otherwise, the sink node is not in the ring; subsequently, the real packet is transmitted from the sink proxy node to the sink node through the shortest path. Algorithm 4 is the corresponding pseudo code and the meaning of the variables is shown in Table 3.

Algorithm 4 Real Packet Travel to the Sink Node

```
if (The current node is sink) then
    The packet arrives at the sink node and the transmission is complete;
else
    $Walk$++;
    SendMessage (Sink);
end if
```

TABLE 3. Meaning of the variables in Algorithm 4.

Variables	Meaning of the variables
$SendMessage$ $(Sink)$	This node selects a node closer to the sink node from its neighbors and sends a packet to that node.

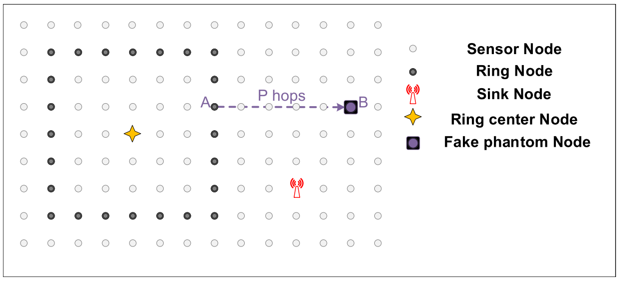

FIGURE 6. Process of generating a fake phantom node.

5) PROCESS OF GENERATING FAKE PHANTOM NODES

To prevent attackers from locating phantom nodes, fake phantom nodes in the network are used to simulate the behavior of the actual phantom nodes. These fake phantom nodes are distributed around the ring and send false data packets to the ring.

Each ring node triggers the birth of a false phantom node according to a preset probability. As shown in Figure 6, if a ring node decides to trigger the birth of a fake phantom node, which will generate a packet named "the seed of a fake phantom node," the node that a seed reaches after transmitting P hops is a fake phantom node. To reduce energy consumption, fake packets are assigned a lifetime. Algorithm 5 is the corresponding pseudo code.

Algorithm 5 Generating a Fake Phantom Node

```
if ($Walk < P$) then
    $Walk$++;
    SendMessage (Far);
else
    This node is a new fake phantom node, sending fake packets to the ring like a phantom node;
end if
```

6) UPDATE THE RING

If a panda is found near a ring node, the ring node near the panda must be updated, and new ring nodes should be far from the panda. All the operations are performed spontaneously by the ring node. Additionally, the sink node should be aware the operations and update the ring node again if necessary.

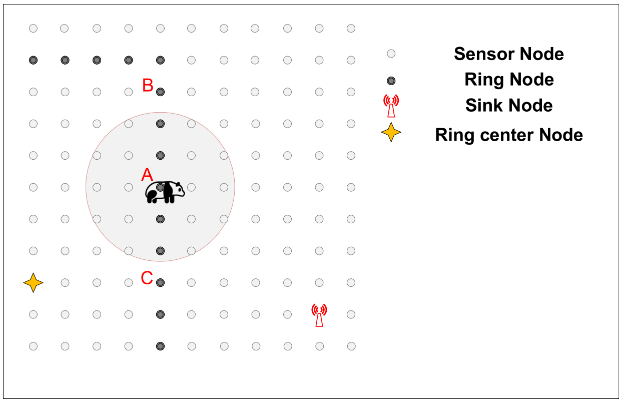

FIGURE 7. Ring node A becoming a source node.

As shown in Figure 7, the circle is the visible area of the panda. Ring node A detects the appearance of a panda nearby and subsequently sends a packet to ring node B, instructing B to start updating the ring. The purpose of updating the ring is to deter the ring from passing through the panda's visible area. Algorithm 6 is the corresponding pseudo code.

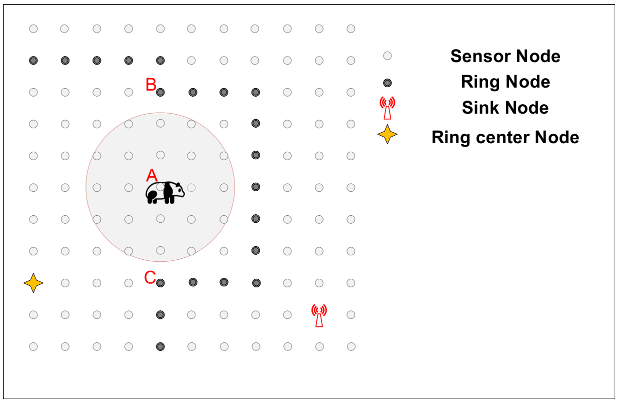

FIGURE 8. The ring updates itself.

After the ring updates itself, as shown in Figure 8, the sink node may update the ring again. A simple example is provided herein, as shown in Figure 9.

In our examples, all the source, phantom, fake phantom, and sink nodes are located outside the ring. In fact, they can remain inside the ring; the algorithms required are similar.

V. PERFORMANCE ANALYSIS

A. ENVIRONMENT SETTING AND PARAMETER CONFIGURATION

We tested our proposed PRFs scheme using OMNET++, which has gained widespread popularity as a network simulation platform in the scientific community. In the simulation, 10000 nodes were distributed over a 1000 m × 1000 m area. The area was divided into 10000 square grids measuring 10 m × 10 m, and only one sensor node was deployed in each grid.

Algorithm 6 Update the Ring

```
if ($Walk == 0$) then
    This node named "first node";
    $Walk{+}{+}$;
    $SendMessage(Far)$;
else if ($Walk > 0$ and $Walk < R$) then
    $Walk{+}{+}$;
    $SendMessage(Far)$;
else if ($Walk >= R$ and $Walk < 3R$) then
    $Walk{+}{+}$;
    $SendMessage(Clockwise)$;
else if ($Walk >= 3R$) then
    if (The current node is not in the ring) then
        $SendMessage(RingCenter)$;
    else if (The current node is in the ring) then
        This node named "last node";
        All the nodes between "first node" and "last node" in the old ring no longer play the role of ring node;
        This node sends the result to the sink node;
    end if
end if
```

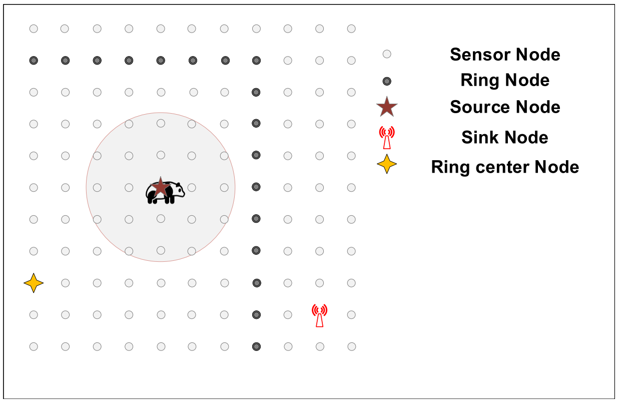

FIGURE 9. Sink node updates the ring.

TABLE 4. Parameter settings.

Test	1	2	3	4	5	6	7	8	9
K	1	4	4	1	1	1	1	1	1
$Source$	1	1	1	1	var	8	8	1	8
$Message$	32	32	248	var	32	8	8	32	8
$Sink$	1	1	1	1	1	1	2	1	1
M	10	10	10	10	10	10	10	var	var
N	10	10	10	10	10	10	10	var	var
$Radius$	var	var	var	14	14	var	var	14	14

Radius was defined as the hop distance from the ring center to the ring nodes. Attackers were initially deployed around the sink nodes.

We conducted 9 groups of experiments, and the main parameters are listed in Table 4. There are 1 or 2 variables in each group of experiments, which can determine the influence of different variables on the algorithm.

K, M and N are the parameters of the algorithm in PRFs, *Source* is the number of source nodes, *Message* is the total

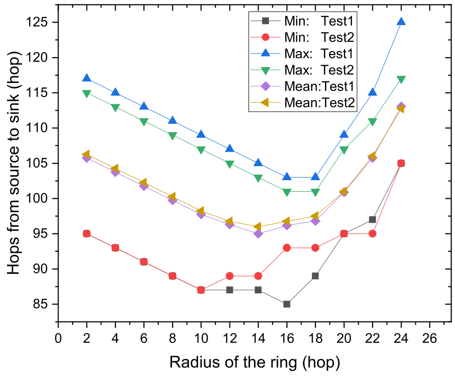

FIGURE 10. Comparison of the route length under different *K*.

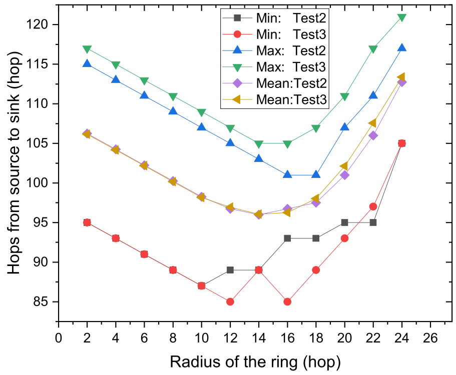

FIGURE 11. Comparison of the route length under different *Message*.

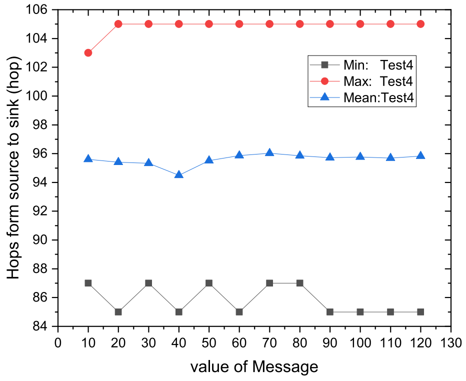

FIGURE 12. The route length under different *Message*.

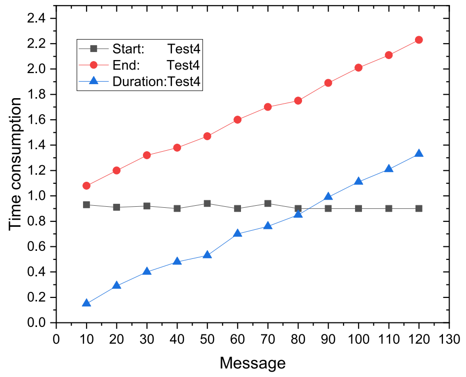

FIGURE 13. Time consumption under different *Message*.

number of data packets sent by each source node, *Sink* is the number of base stations, the radius of the ring in PRFs is *Radius*.

From the data of these tests, we can analyze the changing rules of the routing path, which is the basis for studying the delay, safety time and energy consumption of PRFs.

B. THE PERFORMANCE FOR OUR PRFs WITH DIFFERENT PARAMETERS

1) DIFFERENT VALUES OF *K*, *Message*

Except for K, Test1 and Test2 have the same parameters. We change the value of *Radius* and record the number of hops from the birth of each real data packet to the arrival of the sink node. The result is shown in Figure 10. For different *Radius*, *Min* and *Max* in the figure correspond to the minimum and maximum number of hops that arrive at the sink node after a single data packet is born. *Mean* is the average number of hops of all data packets.

Each phantom node sends K data packets during its lifetime, and these K data packets have the same routing path. When *Message* is fixed, the number of routing paths in one test is at least $Message/K$. The smaller K is, the more routing paths will be, which makes the interval between the *Min* and *Max* larger. But the value of K has little effect on the average number of hops of routing path length.

As shown in Figure 11, *Message* in Test3 is larger than Test, which is 248. In each test, the number of routing paths is at least $Message/K$, so the extreme values of *Min* and *Max* in Test3 exceed Test2, but the average routing path lengths of Test2 and Test3 are similar.

For a single test, as *Message* increases, the values of *Min*, *Max*, and *Mean* will tend to stabilize. In Test4, as shown in Figure 12, as *Message* increases from 10 to 120, *Min* and *Max* change from the beginning, and then become completely constant, the *Mean* curve becomes more and more linear.

The time when the first real data packet is born begins. The time when any real data packet arrives at the sink node is *Start*, and the time when all real data packets arrive at the sink node is *End*. $Duration = End - Start$. As shown in Figure 13, the linearity of these three values is obvious, especially after the *Message* increases to 90.

2) DIFFERENT VALUES OF *Source*

PRFs support multiple randomly distributed source nodes. Changes *Source* also affect the routing path. Increasing *Source* of Test5 from 1 to 3 in Figure 14, three parameters have changed significantly. After that, as the *Source* increases, the values of all parameters tend to stabilize. As long as the source node closest to and farthest from the base station is covered, the extreme values of *Min* and *Max* are covered. However, although *Mean* tends to stabilize eventually, the value is often different from that of a single source node. For example, *Mean* in Test5 finally stabilizes

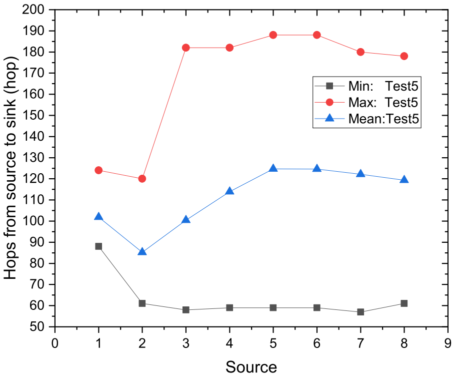

FIGURE 14. The route length under different *Source*.

at around 120, while in Test4 shown in Figure 12, *Mean* stabilizes at around 96.

In Test5, *Start*, *End*, and *Duration* also gradually stabilized with the increase of *Source*. As shown in Figure 15, when *Source* is less than 3, the value of the three parameters fluctuates greatly, and then quickly stabilizes.

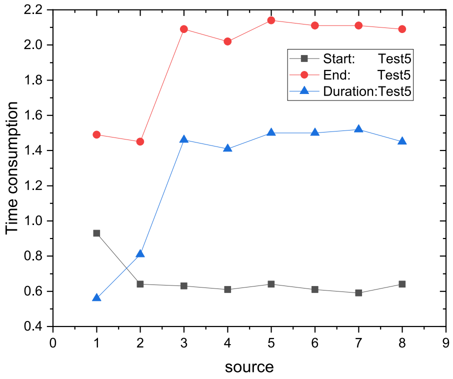

FIGURE 15. Time consumption under different *Source*.

The ring is an important part of PRFs, and *Radius* is an important parameter of rings. The number of sink node also significantly affects the routing path length. The data in Figure 16 comes from three experiments, of which Test7 has two sink nodes, which are represented by sink1 and sink2 in the chart. Test1 is the minimum value when $Radius = 14$, Test6 is the minimum value when $Radius = 10$, Test7 is the minimum value when $Radius = 18$.

With the increase of *Radius*, in Test1 of a single source node and a single sink node, the routing path length presents a "V-shaped distribution." This is because the length of the routing path is the sum of the number of hops experienced by real data packets in the four stages of PRFs and will be the smallest at a certain *Radius*. In Test6 with 8 source nodes and a single sink node, changing of the routing path length is greater than Test1. This is because Test6 have 8 source nodes, including the source node in Test1, so that *Min* in Test6 is smaller than Test1, and *Max* in Test6 is greater than Test1. In Test7 of two sink nodes, the routing path length smallest, because each source node can select the nearest sink node to transmit data packets.

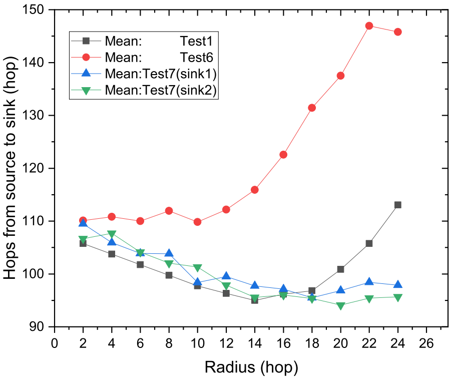

FIGURE 16. The route length under different *Source*.

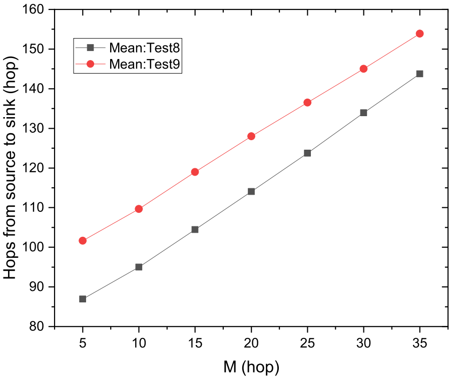

FIGURE 17. The route length under different *M*.

As *Sink* increases, the length of the routing path will decrease. $Sink = 1$ in Test6 and $Sink = 2$ in Test7, except that the two parameters are the same, but the routing path length of Test7 is obviously shorter than that of Test6.

3) DIFFERENT VALUES OF *M*, *N*

The variables *M* and *N* are important parameters in Algorithm 1, which determine the location distribution of phantom node. The data obtained when $ProbabilityFar = 2/3$ is shown in Figure 17, and it can be seen intuitively that the changes in *M* value and path length are relatively linear. As shown in Figure 18, as the *N* value increases, the average path length value also increases.

C. THE ENERGY PERFORMANCE ANALYSIS

We compared the PRFs scheme with the Multirings [34] and RFL schemes [36]. Both Multirings and RFL schemes adopt ring. In Multirings scheme, there are multiple Concentric rings, and in RFL scheme, ring is used to construct fog area. These two schemes have distinct characteristics in the use of ring and are representative. Therefore, the performance of proposed scheme and the above two algorithms are compared. Three parameters were used: safety time, energy consumption, and delay. In the Multirings scheme, multiple rings were

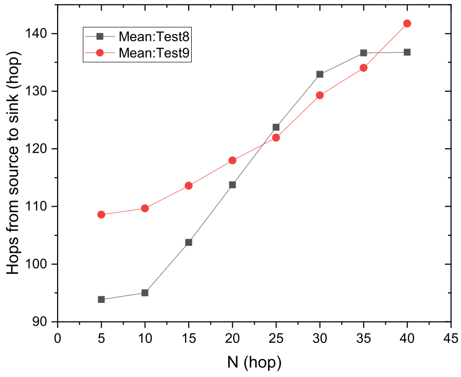

FIGURE 18. **The route length under different *N*.**

built around the sink node. In the RFL scheme, a ring was built around the source node. However, in the PRFs scheme, we could build a ring without considering the location of the source and sink nodes. The three schemes used rings differently; therefore, we compared the RPF with them.

A packet transmits from one node to another by travelling one hop. Safety time is the number of hops required by the adversary to locate the source node. Energy consumption refers to the number of hop counts per simulation run. Delay is the average number of hop counts for a real packet to complete its travel. The parameters used in the simulation are listed in Table 5.

TABLE 5. **Parameter settings.**

Parameters	Value
Network size	1000 m x 1000 m
Number of sensor nodes	10000
Communication radius of sensor nodes	15 m
Number of sink nodes	1
Number of source nodes	1
M, N	$M = 10, N = 10$
Birth rate of a fake packet within the interval of one hop	0.2

Herein, energy consumption refers to the number of hop counts per simulation run. Primarily, two types of packets travel in the network: real and fake packets. One sink was used in the test; each scheme builds a ring with the same radius, sends the same number of real packets, and generates the same number of fake packets within the same time interval. In PRFs, the time required and energy consumed are shown in Formula (4) and Formula (5), respectively.

$$T_{transmitalltherealpackets} = (n-1) \times T_{onehop} + T_{delay} \times T_{onehop}. \quad (4)$$

$T_{transmitalltherealpackets}$ is the time required to transmit all the real packets, and T_{onehop} is the time required for a packet to travel one hop; the source node transmits a real packet every other T_{onehop}, and the final real packet will travel in the network in T_{delay}.

$$E_{all} = T_{transmitalltherealpacket} \div T_{onehop} \times P_{fakepacket} \times H_{fakepacket} + T_{delay} \times n, \quad (5)$$

where E_{all} is the energy consumption; $P_{fakepacket}$ is the birth rate of a fake packet in every T_{onehop}, where a fake packet will result in $H_{fakepacket}$ hops of energy consumption to the network.

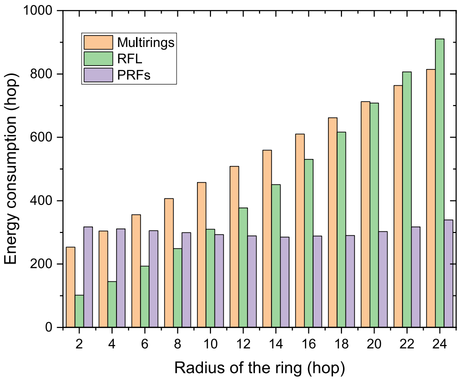

FIGURE 19. **Energy consumption with different *Radius*.**

Based on Figure 19, we can analyze the results based on two aspects. First, when the radius is smaller than 8, the RFL scheme performed better than our scheme. Next, if the radius is larger than 8, our scheme performed better than the Multirings or RFL scheme. The larger the delay, the more will energy be consumed. This is because with an increase in delay, more fake packets will travel in the network, and each real packet requires more hops to the sink node.

It should be emphasized that the RPF allows multiple sink nodes in the network. As presented in Figure 20 and Figure 21, one and two sink nodes exist, respectively. The energy consumption decreases with increasing number of sink nodes. In the Multirings scheme, the rings were built around the sink node; therefore, it is difficult to change the number of sink nodes. In the RFL scheme, the position of the fog centers is related to the position of the sink; therefore, it is difficult to change the number of sink nodes. In other words, if the number of sink nodes is likely to change, the PRFs scheme is superior to the other two schemes.

In PRFs, the ring node is the largest part of energy consumption. If the ring node is equipped with solar modules, it can supply the required energy by itself. If the ring node is connected to the DERs, it will have more flexible energy management.

D. THE TIME PERFORMANCE ANALYSIS

1) SAFETY TIME

In the PRFs, those nodes located far from the source node can be used as phantom nodes. The probability of a node becoming a phantom node twice in a short period is low. In addition, several fake phantom nodes mimic the actual phantom nodes, rendering it difficult for attackers to determine where to trace

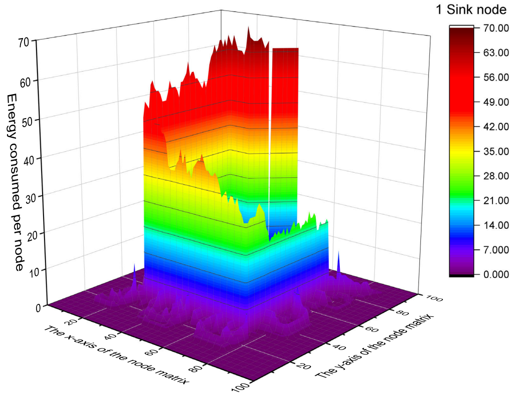

FIGURE 20. Distribution of energy consumption when one sink node exists in the network.

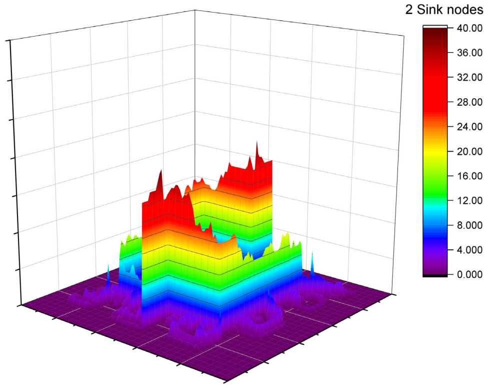

FIGURE 21. Distribution of energy consumption when two sink nodes exist in the network.

back to the source. As shown in Formula (6), $T_{safetytime}$ is the safety time and $T_{transmitalltherealpackets}$ is the time required to transmit all the real packets. The safety time is longer than the time required to transmit all the real packets.

$$T_{safetytime} > T_{transmitalltherealpackets}. \tag{6}$$

In the Multirings and RFL schemes, the safety time is related to the radius of the rings used by the schemes.

2) DELAY

In the PRF, the delay of the ith packet is T_i:

$$T_i = H_{phase1} + H_{phase2} + H_{phase3} + H_{phase4}, \tag{7}$$

where H_{phase1}, H_{phase2}, H_{phase3}, and H_{phase4} are the number of hops in $phases 1, 2, 3, 4$, respectively.

If a network transmits n real packets, the delay of the network is T_{delay}:

$$T_{delay} = (\sum_{i=1}^{n} T_i) \div n. \tag{8}$$

Figure 22 shows the delay under all three schemes. When the radius is smaller than 8, the delay of the PRFs is longer than that of the Multirings and RFL. This is because the PRFs routes a real packet from the source node to the phantom node first, whereas the other two algorithms do not require this step. When the radius is larger than 8, the delays of the PRFs and RFL are smaller than that of Multirings. This is because Multirings routes real packets in three rings; the larger the routing radius, the longer is the delay of the packet.

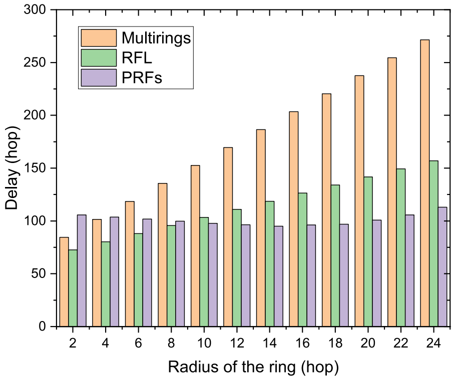

FIGURE 22. Transmission delay.

FIGURE 23. Lake surrounded by forest.

E. INDUSTRIAL APPLICATIONS

PRFs can be widely used in environmental protection, forest fire warning, wildlife protection, water regime automatic monitoring, traffic monitoring and other fields. If PRFs is deployed in an environment with water, it can show its advantages and make sure the entire network to work efficiently. As shown in Figure 23, the forest surrounds a large lake, and there is a road along the lake. In a similar environment, we can deploy ring nodes in the lamppost, and the remaining nodes are distributed in the forest.

Ring nodes are deployed in the lamppost, which can solve the energy problem and ensure the network to work for a long time. In addition, PRFs have more flexible energy management by connecting with the DERs system deployed on the lamp post. Ring nodes can provide support for traffic monitoring. At the same time, the ring node can also communicate with the water condition monitoring sensor near the shore to assist the automation of water condition monitoring. Sensors distributed in the forest transmit the collected environment, disaster and wildlife information to the ring nodes to realize data collection. PRFs provide privacy protection for the source node, collect and transmit data while preventing the source node from being backtracked by attackers.

VI. CONCLUSION AND FUTURE STUDIES

Recently, SLP has become an emerging research topic. We herein proposed a ring-based routing scheme to ensure SLP. The scheme was divided into four phases. In the first phase, the phantom node was selected based on the position of the source node, and real packets traveled from the source node to the phantom node. In the second phase, the real packets traveled to the ring. The real packets were transmitted within the ring until the sink proxy node was encountered in the third phase. In the fourth phase, the real packets were sent to the sink node from the sink proxy node via the shortest path. In addition, fake phantom nodes generated fake packets to propagate in the network to confuse attackers. With the integration of DERs, PRFs has longer lifetime and more flexible energy management. The experimental results demonstrated that our scheme provided efficient protection for SLP. For the future wrok, we plan to explore more energy-efficient solutions to address SLP based on mobile sink nodes. In addition, the proposed scheme will be deployed on the application of IIoT to increase the reliability of the scheme continuously.

REFERENCES

[1] F. H. El-Fouly, R. A. Ramadan, M. I. Mahmoud, and M. I. Dessouky, "REBTAM: Reliable energy balance traffic aware data reporting algorithm for object tracking in multi-sink wireless sensor networks," *Wireless Netw.*, vol. 24, no. 3, pp. 735–753, Apr. 2018. [Online]. Available: http://link.springer.com/10.1007/s11276-016-1365-1

[2] W. Wang, C. Feng, B. Zhang, and H. Gao, "Environmental monitoring based on fog computing paradigm and Internet of Things," *IEEE Access*, vol. 7, pp. 127154–127165, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8822720/

[3] K. Gao, D. Yan, F. Yang, J. Xie, L. Liu, R. Du, and N. Xiong, "Conditional artificial potential field-based autonomous vehicle safety control with interference of lane changing in mixed traffic scenario," *Sensors*, vol. 19, no. 19, p. 4199, Sep. 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/19/4199

[4] M. Biabani, H. Fotouhi, and N. Yazdani, "An energy-efficient evolutionary clustering technique for disaster management in IoT networks," *Sensors*, vol. 20, no. 9, p. 2647, May 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/9/2647

[5] A. El Attaoui, M. Hazmi, A. Jilbab, and A. Bourouhou, "Wearable wireless sensors network for ECG telemonitoring using neural network for features extraction," *Wireless Pers. Commun.*, vol. 111, no. 3, pp. 1955–1976, Apr. 2020, doi: 10.1007/s11277-019-06967-x.

[6] W. Fang, S. Ding, Y. Li, W. Zhou, and N. Xiong, "OKRA: Optimal task and resource allocation for energy minimization in mobile edge computing systems," *Wireless Netw.*, vol. 25, no. 5, pp. 2851–2867, Jul. 2019.

[7] A. Cherukuri and J. Cortes, "Distributed coordination of DERs with storage for dynamic economic dispatch," *IEEE Trans. Autom. Control*, vol. 63, no. 3, pp. 835–842, Mar. 2018. [Online]. Available: http://ieeexplore.ieee.org/document/7990564/

[8] W. Alharbi and K. Bhattacharya, "Flexibility provisions from a fast charging facility equipped with DERs for wind integrated grids," *IEEE Trans. Sustain. Energy*, vol. 10, no. 3, pp. 1006–1014, Jul. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8416779/

[9] W. Liu, P. Popovski, Y. Li, and B. Vucetic, "Wireless networked control systems with coding-free data transmission for industrial IoT," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1788–1801, Mar. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8922618/

[10] A. Seferagić, J. Famaey, E. De Poorter, and J. Hoebeke, "Survey on wireless technology trade-offs for the industrial Internet of Things," *Sensors*, vol. 20, no. 2, p. 488, Jan. 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/2/488

[11] Y. Liu, M. Ma, X. Liu, N. N. Xiong, A. Liu, and Y. Zhu, "Design and analysis of probing route to defense sink-hole attacks for Internet of Things security," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 356–372, Jan. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8533414/

[12] T. Li, Y. Liu, N. N. Xiong, A. Liu, Z. Cai, and H. Song, "Privacy-preserving protocol for sink node location in telemedicine networks," *IEEE Access*, vol. 6, pp. 42886–42903, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8417414/

[13] L. C. Mutalemwa and S. Shin, "Comprehensive performance analysis of privacy protection protocols utilizing fake packet injection techniques," *IEEE Access*, vol. 8, pp. 76935–76950, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9075992/

[14] P. Kassal, M. D. Steinberg, and I. M. Steinberg, "Wireless chemical sensors and biosensors: A review," *Sens. Actuators B, Chem.*, vol. 266, pp. 228–245, Aug. 2018.

[15] Y. Li and L. Jiang, "High accuracy data fusion algorithm for privacy preserving in wireless sensor networks," *J. Adv. Oxidation Technol.*, vol. 21, no. 2, pp. 4633–4638, Oct. 2018.

[16] T. Zhang, X. Li, and Q. Zhang, "Location privacy protection: A power allocation approach," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 748–761, Jan. 2019.

[17] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustain. Comput., Inform. Syst.*, vol. 19, pp. 174–184, Sep. 2018.

[18] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proc. 25th IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2005, pp. 599–608.

[19] R. A. Shaikh, H. Jameel, B. J. D'Auriol, H. Lee, S. Lee, and Y.-J. Song, "Achieving network level privacy in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 1447–1472, Feb. 2010.

[20] L. C. Mutalemwa and S. Shin, "Regulating the packet transmission cost of source location privacy routing schemes in event monitoring wireless networks," *IEEE Access*, vol. 7, pp. 140169–140181, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8848376/

[21] M. F. Al-Mistarihi, I. M. Tanash, F. S. Yaseen, and K. A. Darabkh, "Protecting source location privacy in a clustered wireless sensor networks against local eavesdroppers," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 42–54, Feb. 2020. [Online]. Available: http://link.springer.com/10.1007/s11036-018-1189-6

[22] W.-P. Wang, L. Chen, and J.-X. Wang, "A source-location privacy protocol in WSN based on locational angle," in *Proc. IEEE Int. Conf. Commun.*, 2008, pp. 1630–1634.

[23] N. Dutta, A. Saxena, and S. Chellappan, "Defending wireless sensor networks against adversarial localization," in *Proc. 11th Int. Conf. Mobile Data Manage.*, May 2010, pp. 336–341.

[24] R. Rios and J. Lopez, "Exploiting context-awareness to enhance source-location privacy in wireless sensor networks," *Comput. J.*, vol. 54, no. 10, pp. 1603–1615, Oct. 2011.

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

[26] L. Zhou and Q. Wen, "Energy efficient source location privacy protecting scheme in wireless sensor networks using ant colony optimization," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 3, Mar. 2014, Art. no. 920510.

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

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

[29] M. Bradbury and A. Jhumka, "A near-optimal source location privacy scheme for wireless sensor networks," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Aug. 2017, pp. 409–416.

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

[31] M. Kamarei, A. Patooghy, A. Alsharif, and V. Hakami, "SiMple: A unified single and multi-path routing algorithm for wireless sensor networks with source location privacy," *IEEE Access*, vol. 8, pp. 33818–33829, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8986664/

[32] 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.

[33] W. Tan, K. Xu, and D. Wang, "An anti-tracking source-location privacy protection protocol in WSNs based on path extension," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 461–471, Oct. 2014.

[34] L. Yao, L. Kang, F. Deng, J. Deng, and G. Wu, "Protecting source–location privacy based on multirings in wireless sensor networks," in *Concurrency Computation*, vol. 27, no. 15. Hoboken, NJ, USA: Wiley, Oct. 2015, pp. 3863–3876.

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

[36] M. Dong, K. Ota, and A. Liu, "Preserving source-location privacy through redundant fog loop for wireless sensor networks," in *Proc. IEEE Int. Conf. Comput. Inf. Technol.; Ubiquitous Comput. Commun.; Dependable, Autonomic Secure Comput.; Pervas. Intell. Comput.*, Oct. 2015, pp. 1835–1842.

[37] L. C. Mutalemwa and S. Shin, "Secure routing protocols for source node privacy protection in multi-hop communication wireless networks," *Energies*, vol. 13, no. 2, p. 292, Jan. 2020. [Online]. Available: https://www.mdpi.com/1996-1073/13/2/292

[38] L. Nemec, V. Matyas, R. Ostadal, P. Svenda, and P.-L. Palant, "Evaluating dynamic approaches to key (Re-)Establishment in wireless sensor networks," *Sensors*, vol. 19, no. 4, p. 914, Feb. 2019.

ZHIWEN XIONG received the M.S. degree in computer software and theory from Hangzhou Dianzi University, China, in 2009. He is currently pursuing the Ph.D. degree with the College of Computer and Information, Hohai University. His current research interests include wireless networks, information fusion, and video analysis.

HUIBIN WANG received the Ph.D. degree in information and communication engineering from the China University of Mining and Technology, Xuzhou, China. He is currently a Professor with the College of Computer and Information, Hohai University, Nanjing, China. His research interests include video analysis, information fusion, and wireless networks.

LILI ZHANG received the M.S. and Ph.D. degrees from the Department of Mathematics, Nanjing Normal University, in 2002 and 2008, respectively. She was ever visiting Virginia Tech in the Department of Electrical and Computer Engineering from June 2011 to June 2012. She is currently an Associate Professor with the College of Computer and Information Engineering, Hohai University, China. Her research interests include image processing and pattern recognition.

TANGHUAI FAN received the B.A. and M.A. degrees from Nanchang University, Nanchang, China, in 1983 and 1991, respectively, and the Ph.D. degree from Hohai University, Nanjing, China, in 2010. He received the Postgraduate Certificate. He has been a Professor with the School of Information Engineering, Nanchang Institute of Technology, since 2009. His research interests include wireless sensor networks, signal gathering and processing, telemetry and remote control, and information fusion.

JIE SHEN received the Ph.D. degree from Hohai University, in 2015. She is currently a Lecturer with the College of Computer and Information, Hohai University. Her main research interests include image processing, photoelectronic imaging, and bionic signal processing.