IEEE Access
practical innovations : open solutions

Received April 6, 2014, accepted May 16, 2014, date of publication June 24, 2014, date of current version July 8, 2014.

Digital Object Identifier 10.1109/ACCESS.2014.2332817

Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-Based Diversionary Routing in Wireless Sensor Networks

JUN LONG[1], MIANXIONG DONG[2], KAORU OTA[3], AND ANFENG LIU[1]

[1]School of Information Science and Engineering, Central South University, Changsha 410083, China
[2]National Institute of Information and Communications Technology, Tokyo 619-0289, Japan
[3]Muroran Institute of Technology, Muroran 050-0071, Japan

Corresponding author: A. Liu (afengliu@mail.csu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61272150 and Grant 61379110, in part by the National High Technology Research and Development Program of China (863 Program) under Grant 2012AA010105, in part by the Open Research Project, State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou, China, under Grant ICT1407, in part by the Grants-in-Aid for Scientific Research, Japan Society for the Promotion of Science (JSPS), under Grant 25880002 and Grant 26730056, and in part by the JSPS A3 Foresight Program.

ABSTRACT Wireless sensor networks (WSNs) have been proliferating due to their wide applications in both military and commercial use. However, one critical challenge to WSNs implementation is source location privacy. In this paper, we propose a novel tree-based diversionary routing scheme for preserving source location privacy using hide and seek strategy to create diversionary or decoy routes along the path to the sink from the real source, where the end of each diversionary route is a decoy (fake source node), which periodically emits fake events. Meanwhile, the proposed scheme is able to maximize the network lifetime of WSNs. The main idea is that the lifetime of WSNs depends on the nodes with high energy consumption or hotspot, and then the proposed scheme minimizes energy consumption in hotspot and creates redundancy diversionary routes in nonhotspot regions with abundant energy. Hence, it achieves not only privacy preservation, but also network lifetime maximization. Furthermore, we systematically analyze the energy consumption in WSNs, and provide guidance on the number of diversionary routes, which can be created in different regions away from the sink. In addition, we identify a novel attack against phantom routing, which is widely used for source location privacy preservation, namely, direction-oriented attack. We also perform a comprehensive analysis on how the direction-oriented attack can be defeated by the proposed scheme. Theoretical and experimental results show that our scheme is very effective to improve the privacy protection while maximizing the network lifetime.

INDEX TERMS Wireless sensor networks, source location privacy, network lifetime, tree based routing, performance optimization.

I. INTRODUCTION

Wireless Sensor networks (WSNs) rely on wireless communication, which is a kind of broadcasting media and vulnerable to be eavesdropped [1]–[3]. The adversaries may use expensive radio transceivers to interact with the networks and to detect the message flow, and then trace back to the message source by moving along the reversed path [4], [5], even if strong data encryption is utilized. The object, e.g., the endangered animal species, or a vehicle of military aides, may have to be protected for safety reasons and the related location information should not be disclosed. This concern will become even more serious for future sensor network prevalence in pervasive computing applications, as the ubiquitous information collections doubtlessly encroaches on the privacy of the people involved [3]–[5].

Many techniques to address the source location privacy issue have been proposed, see [4], [5], [7], [8], where phantom routing is one of the popular approaches for preserving privacy [6]. The source location privacy preservation is to hide the physical location of the message source and makes it more difficult for an adversary to trace messages back to the source location [3], [6]. In phantom routing, instead of source node's directly sending its data to the sink, the source first forwards the data to a phantom node which is located away from it, and then the phantom node acts as a decoy relaying the data in a shortest path to the sink [6]. Due to the fact that the currently existing phantom routing scheme always has the phantom node routed to the sink directly, it allows the adversary trace back along the route to phantom nodes, which could result in that the target can be found at last. Obviously, an enhancement routing scheme is to make it difficult for the adversary to trace back to the phantom node, and as a result, the source location cannot be traced and then is protected. A straight-forward solution is to have several diversionary routes to the sink. It is difficult for the adversary to determine which route is the actual data in. So the source location privacy is improved. Unfortunately, another critical issue arises due to the fact that the energy consumption of establishing n diversionary routes can be n times of a single phantom routing. Despite an improvement in source location privacy, the network lifetime could be only $1/n$ of the single phantom routing.

In this paper, we propose a novel tree-based diversionary routing scheme for preserving source location privacy and maximizing network lifetime in Wireless Sensor Networks (referred to as the tree route, **TR**). TR is different from current studies in which TR creates more diversionary routes than the traditional phantom routing schemes, which greatly improves source location privacy, and at the same time, the network lifetime does not deteriorate with the increase of the number of diversionary routes compared with the traditional routing protocol for privacy preservation. The major contributions of this paper are as follows:

(1) To the best of our knowledge, this is one of the first attempts of network lifetime-conserved source location privacy preservation. Previous study shows that the applications concern about network lifetime and there is no direct relationship between network lifetime and network total energy consumption. This is due to the fact that there exists a special phenomenon called energy hole in WSNs [7]. In WSNs, nodes near the sink have to burden the data forwarding for nodes away from the sink and the region with high energy consumption near the sink is called as hotspot. Since nodes in hotspots consume more energy than other nodes, they die early and a dead ring around the sink can be formed. If the width of this dead ring exceeds the nodal transmission radius r, then data of the entire perimeter of the network area cannot be sent to the sink, and thus it results in complete death of the entire network. Therefore, the network lifetime of WSNs depends on the energy consumption of the hotspot. In other words, if the increased energy consumption is not in hotspot, the network lifetime will not be affected. Based on the above observations, the main contribution of this work is to better preserve source location privacy while at the same time keeping network lifetime unaffected by minimizing the energy consumption in hotspots and fully using residual energy of light-load regions to establish diversionary routes as much as possible. Furthermore, we analyze the energy consumption in different regions in details and provide guidance on the number of diversionary routes which can be created in different regions. The analysis and experimental results show that the network lifetime with TR is not inferior to the best currently known source-privacy preservation routing protocol.

(2) TR achieves strong privacy preservation. We first analyze possible attack methods in-depth against existing phantom single-path routing schemes and identify a novel attack called direction-oriented attack, which is based on historical statistics of routing path. Then we evaluate the proposed TR scheme in terms of privacy preservation, including defense against the direction-oriented attack. It is show that from the perspective of privacy preservation, the proposed scheme outperforms currently existing works.

(3) We conduct extensive simulations with Omnet++ to evaluate the proposed scheme. The experimental results confirm the effectiveness of the proposed scheme. Compared with some existing schemes, our results show that the proposed scheme has longer network lifetime and better privacy.

The remainder of this paper is organized as follows: In Section 2, the related works are reviewed. In Section 3, we discuss the system model as well as problem statement. In Section 4, we propose a novel tree-based diversionary routing scheme, followed by security analysis and performance analysis in Section 5. In Section 6, we present the experiment results. Finally, we conclude our work in Section 7.

II. RELATED WORK

The privacy threats that exist in wireless sensor networks can be broadly classified along two dimensions, namely (i) content-based privacy threats and (ii) context-based privacy threats [4]. While content-based threats are well understood [1], with cryptographic techniques often being used to address these problems [9], cryptographic techniques do not address context based threats and context-based privacy has greater challenge [10]. One important aspect of context based privacy in several applications is source location privacy.

There have been many studies of source location privacy preservation in wireless sensor networks [4]–[6], [12]–[19], [21], [24], and the existing research works can be divided into two categories based on attacker's ability, namely, source location privacy preservation protocol against local attacks [6], [12]–[14] and source location privacy preservation protocol against global attacks [15]–[17]. In order to defense the global attacker who has global flow monitoring capability, Ref. [18] proposed ConstRate protocol, namely, no matter whether the actual data packet is received, all nodes in the whole network send data packets with a constant rate. This protocol effectively defends against the global traffic analysis attacks, but the introduction of more pseudo-packets leads to a sharp decline in the network lifetime, and the transport delay of actual data packet is larger. As an enhancement, a proxy-based filtering protocol is proposed in [19], where some sensor node as proxy can filter out fake data packets, thereby reducing network traffic to some extent. Ref. [17] proposed FitProbRate protocol. By adjusting the nodal data transmission rate, the source location privacy can be preserved and the transport delay can be also reduced. Bicakci, Kemal et al. [15] introduced a filtering scheme called OFS (Optimal Filtering Scheme) to maximize the network lifetime and preserve event-unobservability against global eavesdroppers. However, for the global eavesdroppers, the existing works [15], and [17]–[19] have certain limitations. Since all nodes are sending a large number of fake packets, which will not only greatly increase the energy consumption of nodes and reduce the network lifetime, but also increase the probability of packet collisions and reduce the efficiency of packet transmission. It still remains as an open problem.

For local eavesdroppers, Ref. [6] introduced the Panda-Hunter game model for source location privacy. In this model, a large number of sensor nodes are deployed to monitor the wild habits of Panda. Once the behavior of Panda is monitored, the node nearest to the Panda will report to the base station. The hunter watch near the sink can locate the source node by tracing in the reverse direction hop-by-hop and try to capture the Panda. C. Ozturk, et al. proposed a more well-known phantom routing protocol [12] to against eavesdropping attacks to the source location. However, the phantom node by the first proposed routing is closer to the source node, and as a result the source location may still be easily found by the attacker. Both theoretical and simulation results demonstrate that if the message is routed randomly for h hops, then the message will be largely within $h/5$ hops away from the actual source. Ref. [6], [12] designed directed walk through either sector-based approach or hop-based approach to ensure the phantom node away from the actual source as far as possible, thereby reducing the threat to source node when the attacker traced the phantom node. There is much privacy preservation research based on phantom routing [5].

Recent work is the cloud-based scheme proposed by M. E. Mahmoud and X. Shen [20], that is, by generating multiple fake source nodes around real source node and data of source nodes (including both the real source node and fake source nodes) are routed in a limit region which is called cloud. The adversaries can be trapped in the cloud and can't determine where the real source node is.

Another type of research is different from the above approaches which confuse the adversary near the Sink node. They generate some confusing routes on the way from the source node to sink node for the attacker. For example, the strategy proposed in Ref. [5], [13] transmits the source data packet to the randomly selected intermediate node in the first routing phase. In the second routing phase, the data packet will be mixed with other packets through a network mixing ring (NMR). Research which is similar to this can be found in Ref. [21]. Another analogous research such as: Yi Ouyang et al. [22] introdcued a concept, the cyclic entrapment method (CEM), to preserve the performance advantage of shortest path routing while also protecting the location of a source. In this approach, several loops are generated after the deployment of the sensor network before sources send any messages to the sink. When a real route encounters one of these pre-configured loops, the encountered loop will be activated and begin cycling fake messages in the loop. The attacker will be trapped in these loops.

The most similar research compared with this paper is Ref. [23]. Ref. [23] proposed four location privacy protection schemes are called forward random walk (FRW), bidirectional tree (BT), dynamic bidirectional tree (DBT) and zigzag bidirectional tree (ZBT) respectively. Among them, both DBT scheme and ZBT scheme build some branch routes in the route from the real source node to Sink node to improve the privacy protection performance. In the DBT scheme, real messages are delivered along the shortest path, making it possible for the eavesdropper to infer the location of the source or sink by extending the line of the shortest path. So, a proxy source and a proxy sink are adopted in the ZBT scheme, which prevents the adversary from inferring the location of the source or sink easily.

The fake source idea is proposed to make the sensor network have more sources which generate fake messages that have the same size of the real messages and encrypted as well so that an adversary cannot differentiate between the real message and the fake one. In this scenario, it is expected that an adversary could be directed to a fake source [4], so as to achieve privacy preservation. Ref. [24] proposes a hybrid source location privacy technique. In their approach, temporary and permanent fake sources are modelled as fake sources with varied duration. So, the problem of selecting temporary and permanent fake sources is then directly addressed [24].

Although many approaches have been proposed to preserve source location privacy, but they also cause extra energy consumption to sensor nodes, which could shorten the network lifetime [4]–[6], [12]–[24]. Further, in existing phantom single-path routing, the phantom nodes are at risk of being traced, which could result in revealing the location of the source. In this paper, we take advantages of the unique properties of WSNs, and propose a novel tree based diversionary routing scheme, which not only better preserves source location privacy, but also maximizes network lifetime.

III. SYSTEM MODEL AND PROBLEM STATEMENT

A. SYSTEM MODEL

1) NETWORK MODEL

We make the following general assumptions about our network model:

1) Our network model is similar to the explanatory Panda-Hunter Game that was introduced in [5], [6], [23], and [26]. In this Panda-Hunter Game, a sensor network is deployed with nodal density ρ to continuously monitor activities and locations of the animals in a wild animal habitat. As soon as a Panda is discovered [5], [6],

the corresponding source node in the nearby area will observe and report data periodically to the sink node [6], [14];

2) The positions of the target in the network are randomly distributed, i.e., the probability of each sensor node to monitor the target is equal, and then the probability of generating data to the sink is equal [27], [28];
3) The sensor nodes know their relative locations and the sink node location. Each sensor node has the knowledge of its adjacent neighboring nodes. The information about the relative location of the sensor domain may also be broadcasted through this network for routing information update [29]–[31]; and
4) A security infrastructure, secure communication, has already been in place. In other words, no information carried in the message (e.g., packet head) will be disclosed. The key management, including key generation, key distribution and key update, is beyond the scope of this paper. However, the interested readers are referred to references such as [10] and [25].

2) ADVERSARIES MODEL

Because of the high profits related to Panda hunting, the adversaries would try their best to equip themselves with advanced equipments, which means they would have some technical advantages over the sensor nodes [5], [6]. The adversaries are assumed to have the following capabilities:

1) The adversaries are capable of having sufficient energy resource, adequate computation capability and enough memory for data storage [5], [6]. The adversaries observe the wireless communication within a certain detection range. On detecting an event, they could determine the immediate sender by analyzing the strength and direction of the signal they received. They can move to this sender's location without any delay. We assume that the adversaries will never miss any event when they are close to the event;
2) The adversaries are able to adopt the direction-oriented attack strategy: the adversaries estimate the direction of the source node, and traces along the estimated direction rather than reversely traces hop by hop; and
3) The adversaries will not interfere with the proper functioning of the network, such as modifying packets, altering the routing path, or destroying sensor devices, since such activities can be easily detected and could put the adversaries at risk of being caught. However, the adversaries may carry out passive attacks, such as eavesdropping the communications [5], [13].

B. ENERGY CONSUMPTION MODEL AND RELATED DEFINITIONS

In this paper, we adopt the topical energy consumption model in [7], where the transmission energy consumption E_t follows eq. 1 and energy consumption E_r for receiving follows eq. 2.

$$\begin{cases} E_t = lE_{elec} + l\varepsilon_{fs}d^2, & if\ d < d_0; \\ E_t = lE_{elec} + l\varepsilon_{amp}d^4, & if\ d > d_0. \end{cases} \tag{1}$$

$$E_r = lE_{elec} \tag{2}$$

Where E_{elec} represents transmitting circuit loss. Both the free space (d^2 power loss) and the multi-path fading (d^4power loss) channel models are used, If the transmission distance is less than the threshold d_0, the power amplifier loss is based on free-space model; if the transmission distance is larger than or equal to the threshold d_0, respectively. The multi-path attenuation model is used. ε_{fs} and ε_{amp} are the energy required by power amplification in the two models. l is the number of bits in a packet. The above parameter settings are given in *Table 1*, as adopted from [7].

TABLE 1. Network parameters.

Parameter	Value
Threshold distance (d_0) (m)	87
E_{elec} (nJ/bit)	50
e_{fs} (pJ/bit/m^2)	10
e_{amp} (pJ/bit/m^4)	0.0013
Initial energy (J)	0.5

C. PROBLEM STATEMENT

In this paper, we focus on designing routing protocols to protect source location privacy, while maximize the lifetime of WSNs. Thus, our objective function consists of two parts: preserving source location privacy and maximizing network lifetime.

The preserving source location privacy of a WSN can be characterized by the performance indicators as explained below:

1) trace time(denoted as T): the same as Ref. [3], [23], trace time is defined as the safety period begins from the moment the adversary initiates the tracing procedure (i.e., eavesdrops on the first packet) and ends at the moment when the adversary captures the source. Because the frequency source node generates a data packet frequency, so the attacker can only be in one data cycle reverse trace jump, so trace time can also mean path length by reverse tracking [3], [6], [23]. The objective of preserving source location privacy can be expressed as

$$\max(T) = \max(tracetime)$$

2) Lifetime (denoted as ℓ). Since the outage of sensor nodes may have significant impacts on network coverage and communications, we denote the network lifetime ℓ as the period from the starting of network operation until the first power outage occurs in WSNs [7], [23], [29], [32], [33]. Let E_i denote the energy consumption of node i [28]. The objective of maximizing

network lifetime can be expressed as

$$\max(\ell) = \min \max_{0<i\leq n} (E_i)$$

Obviously, the main goal of TR scheme can be stated as follows:

$$\begin{cases} \max(\ell) = \min \max\limits_{0<i\leq n} (E_i) \\ \max(T) = \max(tracetime) \end{cases} \quad (3)$$

IV. PROPOSED TREE-BASED DIVERSIONARY SCHEME

We propose a novel tree-based diversionary routing scheme for preserving source location privacy and maximizing network lifetime. The proposed scheme satisfies the following principles: (1) The routing trees established are homogeneous, and adversary cannot infer the source location based on the shape of the tree and the historical trajectory of the routing path; (2) The energy consumption of the node in hotspots is not increased and the network lifetime is not decreased; and (3) The abundant energy in the region away from the sink is utilized to build redundancy diversionary routes, so that it is difficult for the adversary to trace to phantom node.

The implementation of TR is divided into two phases to meet the design principles: (1) Establish the backbone route path direct to the network edge based on the existing phantom routes, and improve the historical trajectory in order to avoid direction-oriented attacks which will be discussed in detail later, so as to establish homogeneous trees according to principle 1; and (2) Establish redundancy diversionary routes as many as possible in regions with abundant energy to meet principle 2 and principle 3.

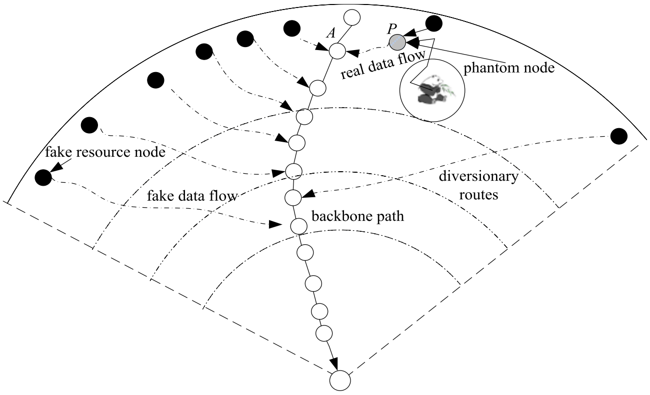

FIGURE 1. Illustrate of the tree-based diversionary routing.

A. OVERVIEW OF THE PROPOSED SCHEME

Tree-based diversionary routing aims at preserving source node privacy and maximizing network lifetime shown in Fig.1. The main idea is that we establish the phantom node away from the source node and then establish tree routing path towards the sink with strategically created diversionary routes as its branches, also known as diversionary routes. The ends of these diversionary routes are fake source nodes, namely decoy. Our goal is to improve its performance in terms of the following two aspects.

1) PRIVACY

In phantom routes, data of phantom node is sent to the sink according to the shortest routing protocol, therefore the adversaries can trace back to the phantom node. Prievious studies have shown that, adversaries can still trace to the source node with a relatively high possibility [5]. Therefore, one possible solution is to make it difficult for adversaries to trace to the phantom node, so that will be impossible to trace the source node. The proposed scheme first establishes a backbone route direct to the network border with diversionary routes as its branches. Then, it establishes diversionary routes as many as possible with each diversionary route directing to the network border, forming a tree based routing path. The data packet length and the data generating possibility are the same in each diversionary route. By doing so, we can achieve relatively high privacy. (A) Firstly, since all routes generated by the source node are the same tree routing paths, so adversaries cannot speculate the source location based on the routing path. In most current phantom routes, routes generated by different source nodes are not homogeneous. For source node near the sink, its routing path is relatively short, while for that away from the sink, its routing path is relatively long. Therefore, adversaries can still speculate the approximate location of source node from the length of routing path. (B) Secondly, since there are many branches in tree routing paths, when adversaries reverse trace, they confront two branches each time, and the probability of right choice is only 1/2. Therefore, for tree routing path with n branches, the possibility of adversaries trace to the phantom is very low. The privacy is greatly improved compared with the traditional protocol [6].

2) NETWORK LIFETIME

In many existing studies [3]–[6], the privacy and energy consumption are contradictory. More diversionary routes require extra energy consumption, thus affecting the network lifetime. Generally, after the first nodal death, the network cannot completely and effectively monitor the monitoring area. Therefore, the network lifetime is usually defined as the first node death time [7], [27], [28]. Obviously, to maximize the network lifetime, the key is to reduce the energy consumption in hotspot. Therefore, we minimize the energy consumption in the hotspots and at the same time. Establish diversionary routes by fully using of abundant energy in non-hotspot regions in order to improve the network lifetime.

B. TREE-BASED DIVERSIONARY ROUTING

Based on the network model discussed above, tree based route scheme includes three stages: (1) Tree-based diversionary routing establishment; (2) Stable operation stage of the tree-based routing; and (3) Destruction of tree-based diversionary routing. It is worth noting that we adopt the same method of creating a phantom node from [3], [4], [6]. The requirement

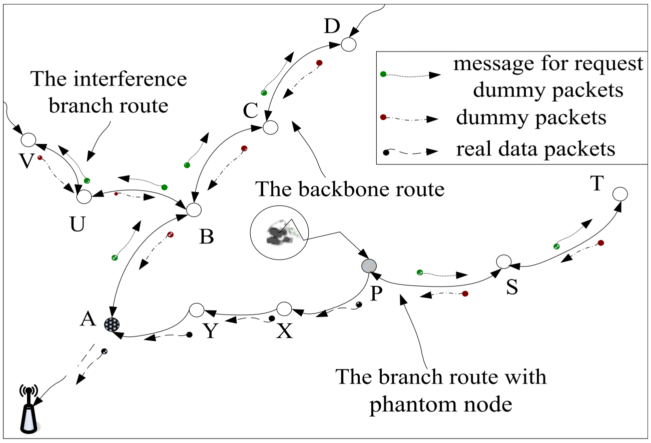
D
The interference branch route
C
V
U
B
The backbone route
T
S
P
A
Y
X
The branch route with phantom node
message for request dummy packets
dummy packets
real data packets

FIGURE 2. **The establishing process of tree route.**

of choosing a phantom node is that the phantom node is as far away from the source node. In the following, we will describe the proposed tree-based diversionary routing in details.

1) TREE-BASED DIVERSIONARY ROUTING ESTABLISHMENT

(i) Establish Tree-based diversionary route with phantom node. First, establish the branch with phantom node, and then establish the tree trunk and other branches. Generally, phantom node cannot be the node on the backbone routing path, because the backbone route is relatively easy to identify, and therefore the phantom node is more vulnerable to be traced. If the phantom node is not on the backbone path, it can be on any existing branches, therefore it is difficult for adversaries to trace. The establishing process of branch with phantom node is as the following two directions (see Fig. 2).

(A) The left-down direction according to the left-hand rule (or the right-hand rule): The phantom node P selects node X from its neighbour nodes, which is the node closest to the sink and on the left (right) of P according to the left-hand rule (or the right-hand rule). Then, X selects node Z which is on the most right of X and with the same hops as X to the sink according to the left-hand rule, then selects the most left node closest to the sink, i. e., alternately selects the node closest to the sink and the node with same hops, until the transmission distance reaches the specified hops Φ, namely, node A in Fig.2, we call it the intermediate node.

(B) The upper right direction of phantom node P. P sends request packet containing information of "request sending dummy packets" to the most right node S according to the right hand rule, and the sending frequency of dummy packets is included in the request packet, which indicates node S should send dummy data packets to P in a fixed time. Similarly node S sends request packet to node T for dummy data packets, then T sends dummy packets to S, and so on, until reaching the network border, then the branch route with phantom node is established.

(ii) Establish backbone route with intermediate node. Assume it starts from intermediate node A, then there are also two directions:

(A) The direction from intermediate node A to the sink. Similar with the traditional shortest route protocol, node A chooses the neighbour closest to the sink each time, until the packet is sent to the sink.

(B) The opposite direction from node A to the sink: Node A selects the neighbour farthest from the sink as the next hop and sends the request packet node A to select the furthest neighbour to the sink as the next hop, and sends request packet containing information of "request sending dummy packets," node B sends dummy packets to A in a fixed time after B receives the request packet, and the B determine whether it has neighbour to the sink farther than itself, if so, node B sends the request packet to the furthest neighbour to the sink and so on, until to the network border.

(iii) Establish the diversionary routes. If node B on the backbone route is required to establish the diversionary route, node B will send request packet containing information of "request sending dummy packets" to node U which has the closest number of hops to the sink with B, then node U sends dummy packets to B. Similarly, node U sends request packet to node V, and so on, until to the network border, then a branch of diversionary route on 45^0at the backbone route is established.

2) STABLE OPERATION STAGE OF TREE-BASED DIVERSIONARY ROUTING

In the stable operation stage of the tree route, once all nodes are included in the routes, they operate as the following principle: (a) If the real data packet is received, then the node sends the real data packet when it comes to the transmission time, if not, dummy message is generated in a fixed time and sent when it comes to the transmission time.

3) DESTRUCTION OF TREE-BASED DIVERSIONARY ROUTING

The destruction of tree route is relatively simple, which depends on the phantom node P, and intermediate node A. If node P and node A have not received the real data packets within the timeout interval, this routing path will be discarded. Node P and node A will send message to nodes involved in the route to stop, and once they receive the stop information, they will no longer send any message. Thus, the entire route stops sending message. The algorithm of tree based routing scheme is shown in the Table 2.

We can get the following Conclusion 1 from the establishing process of tree route.

Conclusion 1: The tree which is created by diversionary tree based route scheme is a homogeneous tree from the adversary's view.

Proof: Consider the adversary is within the transmission radius of any node C in the routing path (any node as shown in Fig.2, such as C). The adversary begins to trace node C. In the worst case, the route from D to C has not been established. Then node C sends request packet for dummy packets to D, although the adversary can confirm that C is the sender and trace it, the adversary cannot know who receives the packet and the adversary will know D is the previous node of C only

TABLE 2. Pseudo-code of algorithm 1 for tree based routing.

```
Algorithm 1: Tree based Routing
Phase Ⅰ: Creating tree
1: create phantom node P use the same algorithm as reference [6]
2: $\sigma$ =random(0,1)
3: If $\sigma \geq \frac{1}{2}+\frac{1}{h}$ then $\vartheta$="right" Else $\vartheta$="left"
4:P(claim) ← <ID$_p$,type, $\Phi$ ,branch_loactions, $\tau$ , $\vartheta$ , padding_data>
5:p(sign_claim) ← $k_p^x$ (<ID$_p$,type, $\Phi$ , branch_loactions, $\tau$ , $\vartheta$ , padding_data>)
6: next_node=$P$
6.1:while (next_node(sign_claim). $\Phi$ >0)
    Alternately select the next_node as the next hop based on
        the following two strategies
    next_node = GetNextOnLeastHop(current_location, $\vartheta$ );
    next_node = GetNextOnEqualPath(current_location, $\vartheta$ );
    $\Phi = \Phi$ -1
  End
6.2: A= next_node
6.3: next_node=$P$
6.4: while (next_node has not reached network border)
    Alternately select the following next_node as the next hop
     next_node = GetNextOnMaxHop(current_location, $\vartheta$ );
    next_node = GetNextOnEqualPath(current_location, $\vartheta$ );
  End
7: for node A respectively runs 7.1 and 7.2
    7.1: while (GetNodeOnMinHop(A) is not sink)
        $A$= GetNextOnMinHop(A)
    End
    7.2 while (GetNextOnMaxHop(A) not reach network border)
        $A$= GetNextOnMaxHop(A)
    End
  End
8:for each node $B$ in the backboneroute
    If B.hop is in branch_loactions
      next_node=$B$
      while (next_node have not reach network border)
        Alternately select the following next_node as the next hop
         next_node = GetNextOnMaxHop(current_location, $\vartheta$ );
         next_node = GetNextOnEqualPath(current_location, $\vartheta$ );
      End while
    End if
End for
Phase Ⅱ: Tree routing
9: for each node C on the tree route
    when the fixed time $\tau$ comes, do the following
        if $C$ receives the real data packet
          Send the real data packet to GetNextOnMinHop(C);
        else
          Send dummy packets to GetNextOnMinHop(C);
        End if
End for
Phase Ⅲ: Destroying tree
10: If a node receives a "stop" packets
      Send packets to all neighbors in the tree route
      Stop transmitting any packets
End if
```

when D sends dummy packets to C until the transmission time comes, and then the adversary traces D. Therefore, the adversary confronts a previously created homogeneous complete tree. In fact, the speed of adversary is constrained by the speed of nodes transmiting data packets. If the attack range is only one hop, the adversary can forward one hop only when it receives one data packet, and thus its trace speed cannot be faster than the tree establishing. Therefore, the tree established will be a previously created homogeneous complete tree for the adversary's view. ■

C. DISCUSSIONS

The establishing process of tree-based diversionary routing has been presented, while the number of diversionary routes has not been calculated. Since the diversionary routes consume energy, the location and the number of diversionary routes should be carefully planned, so as to achieve the network security as well as the network lifetime maximization. Therefore, in this section, we give guidance on how to strategically select the diversionary routes. Also, we discuss the establishment of the backbone route path. we first analyze the energy consumption of the network and determine the number and location of diversionary routes to maximize network lifetime.

1) THE LOCATION AND NUMBER OF DIVERSIONARY ROUTES

The network energy consumption mainly contains the following two parts: (1) Energy consumption for creating phantom nodes: Since we consider that events are randomly uniform, therefore the possibility of sensing event is the same for all nodes in the network. Meanwhile, phantom nodes are created equally with the same algorithm, so the energy consumption of phantom node is uniformly distributed, namely, the nodal energy is reduced by the same amount for nodes in the network. Obviously, their effect on the network lifetime is the same. Even this part of energy consumption is not taken into consideration, it will not have any impact on the following analysis. (2) Energy consumption for establishing tree route. It is the main part of network energy consumption. Therefore, in this section, we mainly focus on the analysis of this part.

First, we consider the backbone route establishment to the network border with length R, when there is no diversionary route, the following theorem can be obtained from the network lifetime time comparison after phantom node creation between this work and the traditional shortest route algorithm [6].

Theorem 1: When there is only one backbone route, the network lifetime of this work is the same as that of the shortest route algorithm.

Proof: The network lifetime is determined by the node that consumes the highest energy, and therefore, we can prove that in these two algorithms, the energy consumption of node that consumes highest energy is the same.

(i) The highest energy consumption in the shortest route strategy.

Similarly to [6], we divide the network into concentric rings in unit r, $r \ll R$, and let $R = mr$. With the shortest route strategy, since the creation method of phantom node is the same, so the energy consumption is the same, which will not affect the comparison of network lifetime. Hence, we don't consider it in our comparison. Therefore, we only consider the energy consumption for phantom node to the sink with the shortest route. Under this condition, the energy consumption of ring i is:

For nodes in ring i, the routing path of nodes above ring i must route through the i_{th} ring, therefore, nodes in ring i burden the energy consumption of all routes above ring i. There are $\pi m^2 r^2 \rho - \pi i^2 r^2 \rho$ nodes above ring i and denote the event probability as λ, then the number of routes undertaken by ring i is $\pi m^2 r^2 \rho\lambda - \pi i^2 r^2 \rho\lambda = \pi r^2 \rho\lambda(m^2 - i^2)$.

Denote the path energy consumption of unit length as e_u, since the shortest routes strategy is adopted, the path length in each ring can be considered as r. As a result, the path energy consumption within a ring is re_u. Thus, the total energy consumption required at ring i is $\pi r^2 \rho\lambda(m^2 - i^2)re_u$.

Since the number of nodes in ring i is $\pi i^2 r^2 \rho - \pi (i-1)^2 r^2 \rho = \pi(2i-1)r^2\rho$

Then, we have the energy consumption of nodes in ring i is $\frac{\pi r^2 \rho\lambda(m^2-i^2)re_u}{\pi(2i-1)r^2\rho} = \frac{(m^2-i^2)}{(2i-1)}\lambda re_u$

Meanwhile, ring i will consume energy for sending data of nodes in ring i, each node transmits its data by distance r, so the energy consumption for each node is $re_u\lambda$.

Therefore, the total energy consumption of nodes in ring i is: $re_u\lambda + \frac{(m^2-i^2)}{(2i-1)}\lambda re_u$.

Obviously, when $i = 1$, the nodes energy consumption is the highest, that is, $m^2\lambda re_u$.

(ii) Energy consumption for establishing route direct to the network border

Since $R = mr$, the number of total nodes in the network is $n = \pi R^2\rho = \pi m^2 r^2 \rho$, the even probability is λ, therefore, the number of event is $\pi m^2 r^2 \rho\lambda$, each event will generate one backbone route, so the number of routes is $\pi m^2 r^2 \rho\lambda$.

Since each route is directly routed to the network border from the sink, so its path length is R. Therefore, the total energy consumption is $\pi m^2 r^2 \rho\lambda Re_u$.

With this strategy, each node burdens the same number of routes, that is, $\pi m^2 r^2 \rho\lambda$, the path length in each ring is r, so the total energy consumption in each ring is $\pi m^2 r^2 \rho\lambda re_u$. Since the number of nodes in ring i is $\{\pi(ir)^2 - \pi((i-1)r)^2\}\rho = \pi(2i-1)r^2\rho|i \in \{1...m\})$.

The energy consumption of nodes in ring i is $\frac{\pi m^2 r^2 \rho\lambda re_u}{\pi(2i-1)r^2\rho} = \frac{m^2}{(2i-1)}\lambda re_u|i \in \{1...m\}|i \in \{1...m\}$

Obviously, when $i = 1$, the nodes energy consumption is the highest, that is, $m^2\lambda re_u$.

As can be seen, when only one route to the network border is established, although the path length is increased, the highest energy consumption is still $m^2\lambda re_u$, so their network lifetime keeps unchanged. ■

Besides, when each event generates only one backbone route, the energy consumption in each ring differs, and the difference is quite large, for example, when $m = 10$, the energy consumption in ring 1 is above 10 times than the outermost ring. Therefore, we can fully use such energy to establish diversionary routes as many as possible, to better preserve privacy.

Different with previous research which aims at minimizing total energy consumption, the purpose of this work is to maximize network lifetime as well as better preserving privacy. Therefore, we next discuss about how to establish as many diversionary routes as possible by fully using energy in non-hotspot area, without affecting network lifetime. Since each ring above ring i will add one route when ring i creates one branch route, so we should carefully plan the number of routes that will be established. The best situation is that except for ring 1, the number of route created by ring $i > 1$ is k_i, and the network energy consumption rate equals. Then, all remaining energy can be fully utilized and all possible diversionary routes are created.

Theorem 2: If the network achieves the balanced energy depletion, then k_i (the number of diversionary routes created by ring i) meets the following. $\frac{m^2}{(2\times2-1)} + \sum_{i=2}^{2}\frac{(2i-1)\varphi k_i}{(2\times2-1)} = \frac{m^2}{(2\times3-1)} + \sum_{i=2}^{3}\frac{(2i-1)\varphi k_i}{(2\times3-1)} = \ldots = \frac{m^2}{(2\times m-1)} + \sum_{i=2}^{m}\frac{(2i-1)\varphi k_i}{(2\times m-1)} st. \frac{m^2}{(2y-1)}\lambda re_u + \varphi re_u\lambda + \sum_{i=2}^{y}\frac{(2i-1)\lambda\varphi re_u k_i}{(2y-1)} \leq m^2\lambda re_u|y \in \{2...m\}$

Proof: As can be seen from the theorem 1, the energy consumption in ring 1 is the highest, that is:

$$E(\max) = \frac{m^2}{(2i-1)}\lambda re_u = m^2\lambda re_u \tag{4}$$

Therefore, compared to ring 1, energy consumption in other rings is smaller. So the diversionary route can be created from ring 2. Denote the number of newly created routes by ring i (denote as C_i) by k_i, since the diversionary route will reach as far as the border, these k_i routes will consume extra energy for nodes $\geq i$ and the energy consumption for each ring $\geq i$ is calculated as follows.

Consider the length of diversionary route in each ring is $\hbar = \varphi r$. Since the shortest route strategy is not adopted, φ is a coefficient bigger than 1. The energy consumption is e_1 for unit length, then the extra energy consumption for each ring above i is $\hbar\ e_u\ k_i$. There are $\pi(2i-1)r^2\rho$ nodes in ring i, and the number of events is $\pi(2i-1)r^2\rho\lambda$, Each event creates k_i routes, so the total energy consumption is $\pi(2i-1)r^2\rho\lambda\ \hbar\ e_u\ k_i$. Then the additional energy consumption for nodes in ring j is

$$\frac{\pi(2i-1)r^2\rho\lambda\hbar e_u k_i}{(\pi j^2 r^2 - \pi(j-1)^2 r^2)\rho} = \frac{(2i-1)\lambda\varphi re_u k_i}{(2j-1)} \tag{5}$$

Then, additional energy consumption for ring i is $\varphi re_u\lambda$.

For ring y, the energy consumption is as the following:

$$\varphi re_u\lambda + \sum_{i=2}^{y}\frac{(2i-1)\lambda\varphi re_u k_i}{(2y-1)} \tag{6}$$

To balance the energy consumption of these rings, it is required that $\frac{m^2}{(2y-1)} + \sum_{i=2}^{y}\frac{(2i-1)\varphi k_i}{(2y-1)}$ is a certain constant with respect to any values of y.

If the above holds, the network lifetime is maximized, and to create as many diversionary routes as possible, we should meet the following $\frac{m^2}{(2\times2-1)} + \sum_{i=2}^{2}\frac{(2i-1)\varphi k_i}{(2\times2-1)} = \frac{m^2}{(2\times3-1)} + \sum_{i=2}^{3}\frac{(2i-1)\varphi k_i}{(2\times3-1)} = \ldots = \frac{m^2}{(2\times m-1)} + \sum_{i=2}^{m}\frac{(2i-1)\varphi k_i}{(2\times m-1)} st. \frac{m^2}{(2y-1)}\lambda re_u + \varphi re_u\lambda + \sum_{i=2}^{y}\frac{(2i-1)\lambda\varphi re_u k_i}{(2y-1)} \leq m^2\lambda re_u | y \in \{2\ldots m\}$ ■

According to Theorem 2, each ring should create different number of diversionary routes. However, in terms of privacy, that which ring creates the diversionary route has little effect on network privacy. Therefore, we can consider the number of diversionary routes created by each ring is the same and each ring creates the same number of diversionary routes. Then, we can easily obtain the number of diversionary routes required in each ring in the backbone route.

Theorem 3: Consider each ring creates the same number of diversionary routes. Then, the number is:

$$k = \min(\frac{2(y-1)m^2 - (2y-1)\varphi}{\sum_{i=2}^{y}(2i-1)}) | y \in \{2\ldots m-1\} \quad (7)$$

Proof: Denote the number of diversionary routes by each ring as k_i. According to Theorem 2, it should meet the following.

$$\frac{m^2}{(2y-1)}\lambda re_u + \varphi re_u\lambda + \sum_{i=2}^{y}\frac{(2i-1)\lambda\varphi re_u k_i}{(2y-1)} \leq m^2\lambda re_u \quad (8)$$

That is to say, for ring y, it should meet the following.

$$\frac{m^2}{(2y-1)} + \varphi + \sum_{i=2}^{y}\frac{(2i-1)k_i}{(2y-1)} \leq m^2 \quad (9)$$

If the number of newly created diversionary routes by each ring is k, the k should meet the following, note that $y \in \{2\ldots m-1\}$:

$$\frac{m^2}{(2y-1)} + \varphi + k\sum_{i=2}^{y}\frac{(2i-1)}{(2y-1)} \leq m^2 \quad (10)$$

Then, k should meet the following:

$$k \leq \frac{m^2 - \frac{m^2}{(2y-1)} - \varphi}{\sum_{i=2}^{m}\frac{(2i-1)}{(2y-1)}} = \frac{2(y-1)m^2 - (2y-1)\varphi}{\sum_{i=2}^{y}(2i-1)} | y \in \{2\ldots m-1\} \quad (11)$$

Since the created branches should meet the energy consumption constraint, thus:

$$k = \min(\frac{2(y-1)m^2 - (2y-1)\varphi}{\sum_{i=2}^{y}(2i-1)}) | y \in \{2\ldots m-1\}$$

■

Inference 1: The network lifetime in this work, where $(m-1)k$ extra routes are created, is the same as that of phantom single-path route.

Proof: If the energy consumptions of other rings are not greater than the first ring, the network lifetime is determined by ring 1 which has the highest energy consumption. If the energy consumption of ring 1 in these two strategies is the same, then the network lifetime is the same. As can be seen from previous discussion, the energy consumption can be divided into two parts, one is the energy consumption of creating phantom node, and the other is energy consumption of creating route to the sink. (i) Since the strategy of creating phantom node is the same, the energy consumption of creating phantom node is the same. (ii) In phantom route strategy, only one route to the sink is created, with the strategy in this work, a tree is created, but there is also only one route in ring 1 which has the highest energy consumption. Besides, although diversionary routes are created in other rings, according to Theorem 2 and Theorem 3, the energy consumption of other rings will not be greater than ring 1, so the energy network lifetime of these two strategies remains the same. ■

2) ESTABLISHMENT OF THE BACKBONE ROUTE PATH

The previous section has given the number of branches through the analysis of relationship between energy consumption and network lifetime. In this section, we will discuss the location of the backbone route to achieve security. With phantom route strategy, there is only one route path, which is the shortest path from phantom node to the sink, so the route path depends on the phantom node. Most researchers think that phantom node should be selected randomly [6], and further studies propose that the route path should avoid visible area [7]. However, we identify a novel attack method called direction-oriented attack, which has good attack performance and can effectively attack the privacy preserving strategies based on phantom routing, and it shows that there is still potential security hazard by randomly selecting phantom node. Therefore, in this work, we propose a new strategy to avoid direction-oriented attack in tree based diversionary routing.

With phantom route strategy, in order to preserve the source location privacy, the phantom node should be away from the source node as far as possible, for example, h hops away from the sink. Since the phantom node is dynamic randomly selected, it is difficult for the adversary to trace to the source node. The adversary is supposed to reverse traces in this assumption. However, we think the adversary can adopt a more effective way to trace to the source node, which is called direction-oriented attack. The core idea of this kind of attack is: Since the distance from phantom route to the sink is no more than h hops, and the phantom path is to the sink in the shortest path. Obviously, the source node of the phantom route must be sent from h hops from the source node. If the phantom node is uniformly and randomly generated [6], then the phantom node is generated randomly at the distance ±h hops from the source node. Therefore, if the adversary collects a certain amount of the route path trajectory and then calculates the average direction, from the statistics knowledge, this average direction is the real direction of the source node. It is highly possible that the adversary traces to the source node.

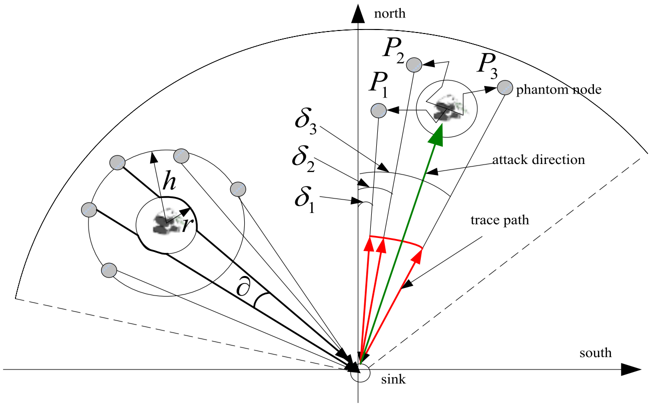

FIGURE 3. Direction-oriented traces the phantom route.

Fig. 3 shows the implementation process of direction-oriented attack. Denote p_1, p_2, p_3 are 3 different phantom nodes in the route strategy. To increase the tracing difficulty, these three phantom node use shorter periods of time, making the route cessation before the adversary can trace to the phantom nodes. Therefore, the adversary can only trace to a short part of the route, such as the red path shown in the Fig. 3. However, the adversary can figure out that the real source node must be close to these three tracing directions (shorter than h hops). Denote the angles between these three paths and Y coordinate respectively are $\delta_1, \delta_2, \delta_3$. If the adversary chooses the average $\delta = \frac{\delta_1+\delta_2+\delta_3}{3}$ direction to trace, then it is very likely for the adversary to succeed by tracing along the presumed direction, for the statistical perspective. The more directions the adversary has known, the higher possibility the adversary traces to the real source node by using the average direction. If the number of trace paths $n \to \infty$, the adversary will succeed. Therefore, the key of direction-oriented attack lies in whether the sample route is enough. The following Theorem 4 shows the relationship between the number of trace paths and the success probability. As can be seen, the adversary can have a high success rate with a smaller number of the trace paths.

Theorem 4: In phantom routing, assume the phantom node is generated randomly and the route is dynamically chosen, the longest distance from the phantom node to the source node is h hops. The adversary trace with direction-oriented attack. If the number of trace path is n, then the success probability $F_Y(y; n)$ is the following.

$$\begin{cases} F_Y(y;n) = \int_{\frac{n(h-1)}{2h}}^{\frac{n(h+1)}{2h}} f_Y(y;n)dy \\ f_Y(y;n) = \frac{1}{2(n-1)!}\sum\limits_{k=0}^{n}(-1)^k \binom{n}{k}(y-k)^{n-1}\text{sgn}(y-k) \\ \text{sgn}(y-k) = \begin{cases} -1 & y<k \\ 0 & y=k \\ 1 & y>k \end{cases} \end{cases}. \tag{12}$$

Proof: Since the distance from the phantom node to the source node is at most h hops. Then, the phantom node is within $[-h, h]$ from the source node. Due to the fact that the shortest path routing has been adopted from the phantom node to the sink. Denote the angle between phantom node at $-h$ and the standard axis as a, and the angle between phantom node at h and the standard axis b. If the adversary's trace direction is within one hop from the source location, then the trace succeeds. The problem can be transformed into: the adversary averages the values of phantom node, if it falls into $[-1, 1]$, then succeed. That is because phantom node has responding value in $[a, b]$ for values in $[-h, h]$. If the average value of direction falls into $[-1, 1]$, then the tracing direction must go through within one hop from the source node and then it will succeed.

Then the problem is transformed into: calculate the probability of the x average value all falls into $[h-1, h+1]$ when taken n times. Denote the positions as X_i, $i = 1, \ldots n$, which are independent and identically distributed uniform random variables and meet $X_i \sim U(0, 2h)$, $i = 1, \ldots n$.

Then $Y_i = \frac{1}{2h}X_i \sim U(0, 1)$, denoted by $\tilde{X} = \frac{1}{n}\sum_{i=1}^{n} X_i$, and the problem is transformed into calculating the probability of $P(h-1 \le \tilde{X} \le h+1)$. From [31] the distribution density function of $Y = \sum_{i=1}^{n} Y_i$ is:

$$f_Y(y;n) = \frac{1}{2(n-1)!}\sum_{k=0}^{n}(-1)^k \binom{n}{k}(y-k)^{n-1}\text{sgn}(y-k) \tag{13}$$

Where sgn$(y-k)$ denotes the sign function:

$$\text{sgn}(y-k) = \begin{cases} -1 & y<k \\ 0 & y=k \\ 1 & y>k \end{cases}$$

Therefore,

$$\begin{aligned} P(h-1 \le \tilde{X} &\le h+1) \\ &= P\{n(h-1) \le \sum_{i=1}^{n} X_i \le n(h+1)\} \\ &= P\{\frac{n(h-1)}{2h} \le \sum_{i=1}^{n} Y_i \le \frac{n(h+1)}{2h}\} \\ &= P\{\frac{n(h-1)}{2h} \le Y \le \frac{n(h+1)}{2h}\} \end{aligned} \tag{14}$$

According to [23]:

$$P\{\frac{n(h-1)}{2h} \le Y \le \frac{n(h+1)}{2h}\} = \int_{\frac{n(h-1)}{2h}}^{\frac{n(h+1)}{2h}} f_Y(y;n)dy.$$

■

In fact, as can be seen from Theorem 4, the direction-oriented attack is very effective on phantom routing strategy, the following gives a specific example to illustrate the above problem, and explains the function use in Theorem 4. When the number of tracing path in Theorem 4 is 5, $f_Y(y; n)$ is the

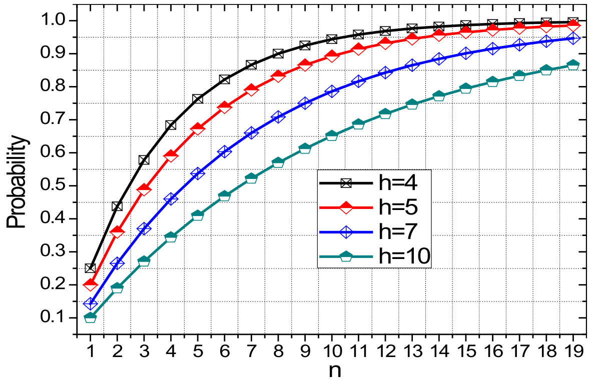

FIGURE 4. The relationship between the trace route number and success probability.

following function.

$$f_X x=\begin{cases}\frac{1}{24}x^4 & 0\le x\le 1\\ \frac{1}{24}\left(-4x^4+20x^3-30x^2+20x-5\right) & 1\le x\le 2\\ \frac{1}{24}\left(6x^4-60x^3+210x^2-300x+155\right) & 2\le x\le 3\\ \frac{1}{24}\left(-4x^4+60x^3-330x^2+780x-655\right) & 3\le x\le 4\\ \frac{1}{24}\left(x^4-20x^3+30x^2-500x+625\right) & 4\le x\le 5\end{cases}$$

Assume $h = 2$, $n = 5$, then the integration interval is $[\frac{n(h-1)}{2h},\frac{n(h+1)}{2h}]=[\frac{5}{4},\frac{15}{4}]$, and then the success probability is

$$\begin{aligned}F_Y(y;n) &= \int_{\frac{5}{4}}^{\frac{15}{4}} f_x(x)\\ &= \int_{\frac{5}{4}}^{2} f_x(x)+\int_{2}^{3} f_x(x)+\int_{3}^{\frac{15}{4}} f_x(x)=96.875\%\end{aligned}$$

Fig. 4 shows success probability under different trace paths number n and different hops h from the phantom node to the source node. As can be seen, the success rate is lower when h is bigger, and the success rate is higher when n is bigger. If $h = 4$, the success rate can be 68.359% when $n = 4$, and the success rate can be 94.369% when n =10. Meanwhile, when the distance from the phantom node to the source node is more than 4 hops, both theoretical and practical results have demonstrated that if the message is routed randomly for h hops, then the message will be largely within $h/5$ hops away from the actual source node [6]. Therefore, to meet $h = 4$, the message needs to be routed randomly for 16 hops, which is already a big number, but even in this situation, the adversary only needs 4 tracing routes, the success probability can be 68.359%. Obviously, the direction-oriented attack is a bit threat to source location privacy.

As can be seen from the above analysis, direction-oriented attack is a strong threat to source location privacy, although the strategy in paper has extended the spatial distribution to a very broad range, increasing the difficulty of attack, if the backbone route is evenly distributed around the source node and the adversary attacks along the tree trunk with direction-oriented strategy, the attack can still get a certain success rate, as Inference 2 shows.

Inference 2: Denote the cover range of tree route in this paper as κ times of that in phantom route, if the backbone route of tree route is uniformly distributed, then the success probability with direction-oriented method is only $(\kappa^z h^z - (\kappa h-1)^z/\kappa^z(h^z-(h-1)^z))$ of phantom route.

Proof: Assume the phantom node is selected within h hops from the source node, then the routing path must be in range $[-h, h]$, then the selection range of routing path in tree route is κ times of phantom route, that is, within $[-\kappa h, \kappa h]$. According to Theorem 4, the success probability with direction-oriented attack in phantom route is $1-\frac{(h-1)^z}{h^z}$, and in tree route it is $1-\frac{(\kappa h-1)^z}{\kappa^z h^z}$. Divide these two,

$$\frac{\kappa^z h^z-(\kappa h-1)^z}{\kappa^z h^z}\frac{h^z}{h^z-(h-1)^z}=\frac{\kappa^z h^z-(\kappa h-1)^z}{\kappa^z(h^z-(h-1)^z)}$$

■

Obviously, to avoid direction-oriented attack, the average angle of all backbone route angle cannot fall in the visible area [7], if not so, the adversary may succeed with statistical theory, so we choose to create more routes in once direction and less in the other. Then the average angle must be deviate from the visible area. In this work, we use a simple way to achieve this. After the creation of phantom node, the phantom node can decide to create the first branch with the left hand rule or the right hand rule. Obviously, the backbone route will focus on the left side of source node when left hand rule is used, and vice versa. If we make the probability of rule selection not equal, then the average angle must be deviate from the visible area, and when the probability is as what shown in eq. 15, the average angle is not in the visible area.

Denote the probability of choosing left hand rule as θ, the maximum distance from the backbone route to the source node is h, then the average angle is $\overline{X} = -\frac{h}{2}\theta + \frac{h}{2}(1-\theta)$, to make $\overline{X}$ not in 1 hop range of the source node (the visible range is 1 hop), then we can get

$$-\frac{h}{2}\theta+\frac{h}{2}(1-\theta)>1\Rightarrow\theta<\frac{1}{2}-\frac{1}{h},\text{ or }\theta\ge\frac{1}{2}+\frac{1}{h}\tag{15}$$

In fact, an extreme case is $\theta = 0(\theta = 1)$, in which case, the backbone route is always on one side of the source node. As long as eq. 15 is satisfied, the average angle is not in the visible range and then the direction-oriented attack can bed avoided.

By now, we have discussed about all aspects of tree based routing scheme, the tree creation process, the number of branch routes and the choice of backbone route, the following will give the performance analysis.

V. ANALYSIS OF SECURITY AND ENERGY EFFICIENCY

A. ANALYSIS OF TRACE TIME

We explore the optimal routing strategies under two different performance metrics: average trace time and minimal trace time.

The frequency of source node generates data is denote by f, then the time interval of data generation is $Tc = 1/f$. This indicates that one data packet will be generated during Tc.

We consider the transmission radius of adversary is the same as that of sensor nodes [14]. Therefore, only data packets within one hop can be detected, and when the data packet is detected, we assume the adversary has strong ability to move and can move to the data source node right away, then the adversary can trace back to the node within Tc, which means the trace distance within Tc is r. In this case, we can consider the trace time is proportional to the trace distance, and then we get Theorem 5.

Theorem 5: The average total route length in tree based routing scheme is $R + k(\sum_{i=2}^{m}(m-i)\varphi r + \frac{(m-1)r}{2})$, and that of traditional phantom protocol is $\frac{2}{3}R|R = mr$.

Proof: First, in traditional phantom protocols, there is only one route path, and the length can be considered as the distance from the sink to source node. However, the location of source node differs, take a small section of fan ring with angle $d\theta$ from any location in the network, whose distance from the sink is $x|x \in \{0..R\}$ and the width is dx, such as Q. Then the number of nodes in this region is $xd\theta dx\rho$, and the distance from this region to the sink is $xd\theta dx\rho \times x$, the number of event is $xd\theta dx\rho \times x\lambda$. Therefore, the distance from source node of this region to the sink can be obtained, that is,

$$\iint_{s} \rho\lambda x^2 d\theta dx = \rho\lambda \int_0^R \int_0^{2\pi} x^2 d\theta dx = \frac{2}{3}\rho\lambda\pi R^3$$

The total number of nodes is $\pi R^2\rho\lambda$, and the average distance from the node to the sink is

$$R_1 = \frac{2}{3}\rho\lambda\pi R^3/(\pi R^2\rho\lambda) = \frac{2}{3}R.$$

In the proposed tree-based diversionary routing scheme, the backbone route length is R, k diversionary routes are created starting from the second ring, and there are total $(m-1)k$ diversionary routes,.

The distance between route path in i_{th} ring and the network border is $(m-i)\varphi r$, the route path length within the ring is $r/2$.

Then the total length of a diversionary route is $k(\sum_{i=2}^{m}(m-i)\varphi r + \frac{(m-1)r}{2})$.

Therefore, the total route length in tree based routing scheme is $R + k(\sum_{i=2}^{m}(m-i)\varphi r + \frac{(m-1)r}{2}))$ ■

Then the average trace time with the proposed scheme can be obtained, as shown in Theorem 6.

Theorem 6: With the proposed scheme, the average trace time is $\frac{\{R+k(\sum_{i=2}^{m}(m-i)\varphi r+\frac{(m-1)r}{2}\}}{2}\frac{Tc}{r}$; and the average trace time in traditional phantom protocol is $\frac{2}{3}R\frac{Tc}{r}$. In the worst case, the minimal trace time in both scheme is $\frac{2}{3}R\frac{Tc}{r}$, while the probability of the worst case with this scheme is only $\frac{1}{(m-1)k+1}$, and is 1 in traditional phantom protocol.

Proof: With the proposed scheme, there are $(m-1)k$ branch routes and 1 backbone route, so there are total $(m-1)k+1$ routes, the probability of the adversary chooses any path is equal, it is $\frac{1}{(m-1)k+1}$. Then, we can get the average search length is half of the total routing path length, i. e., $\frac{\{R+k(\sum_{i=2}^{m}(m-i)\varphi r+\frac{(m-1)r}{2}\}}{2}$, and the trace time is $\frac{\{R+k(\sum_{i=2}^{m}(m-i)\varphi r+\frac{(m-1)r}{2}\}}{2}\frac{Tc}{r}$.

While with traditional phantom routing protocol, there is only one route and the trace probability is 1, and the trace length is $\frac{2}{3}R$, so the trace time is $\frac{2}{3}R\frac{Tc}{r}$.

The worst case with the proposed scheme is that the adversary traces the phantom node in the right direction at the first time, which is the same as that in traditional phantom protocol, therefore, in the worst case, the trace time is $\frac{2}{3}R\frac{Tc}{r}$ and the probability of worst case in the proposed scheme is $\frac{1}{(m-1)k+1}$. ■

Although many studies proposed a dynamic routing approach to improve network security [5], to the best of our knowledge, there is no research which can provide the duration time of path after it is created and then to select the next route dynamically. After we calculate the trace time, and we can easily get that if the duration time of a route is shorter than the trace time, it can be very difficult for the adversary to trace to the phantom node.

Theorem 7: If k tree routes are created at the same time, time for an adversary to trace single tree route is increased by k times, the total route trace length is also increased by k times, then the total time is k^2 times of the single tree route.

Proof: As mentioned above, if the data generation frequency of the source node is f, then the time interval of data generation is $Tc = 1/f$. When there is one tree route, then within Tc, there is only one data packet generated in this route. While if k tree routes are created, the probability of data sent to each tree route is equal, then the data generation frequency is $1/k$ of the original, i. e., f/k. Then the data generation interval is $k\,Tc$. Relativly to a single tree path, the time for an adversary to trace one hop is k times of the single tree route, so the time for tracing one tree is k times of the single tree route. Obviously, the length of k tree route path is k times of the single tree route. Therefore, the total route trace length is k times of the single tree route. Then, time for tracing one tree route is increased by k times, and time for tracing k tree routes is k^2 times of the single tree route. ■

As can be seen from Theorem 7, if k tree routes are created at the same time, the trace difficulty is increased greatly. The adversary has to spent k times of trace route length and k^2 times of trace time to achieve the same attack effect under single tree route path. Obviously, creating k routes can greatly improve the network security, and now, the question is, whether the additional k tree routes affect on the network lifetime. Theorem 8 gives the conclusion.

Theorem 8: Even if k tree routes are created at the same time, the network lifetime is not affected, namely, the same as that with only single tree route.

Proof: Obviously, the amount of data in each route is only $1/k$ of the single tree route. Although k tree routes are created, the total energy consumption is the same. In addition,

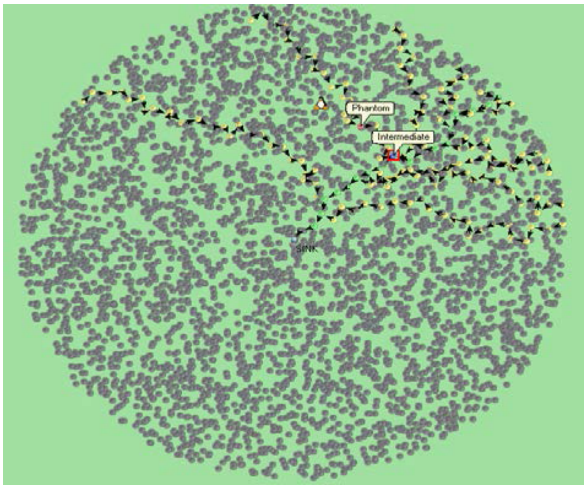

FIGURE 5. Experimental screenshot.

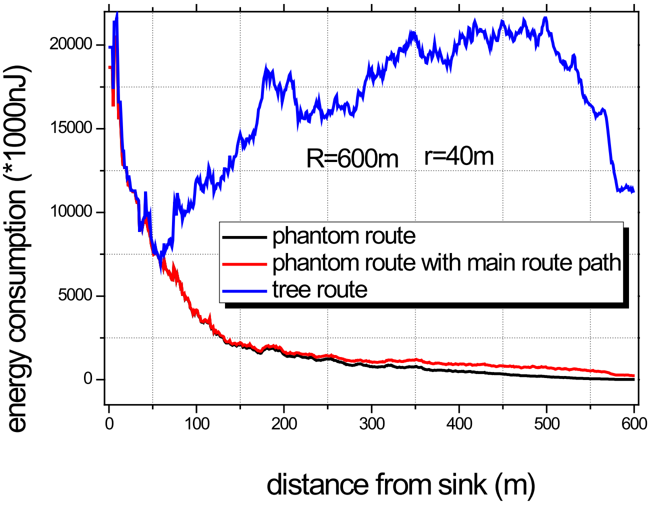

FIGURE 6. Energy consumption under different route protocols.

according to Theorem 2, the created tree can guarantee the energy balance in different regions of the network. Therefore, we can conclude that the network lifetime is not affected. ■

VI. EXPERIMENTAL RESULTS

In this section, we evaluate the performance of proposed scheme with OMNET++, which is an open network simulation platform for large network [35].

A. EXPERIMENTAL RESULTS OF ENERGY CONSUMPTION AND NETWORK LIFETIME

First, we calculate the location and number of diversionary routes according to network parameters, then establish the tree route according to algorithm 1 in section 4. As shown in Fig.5, "phantom" refers to the phantom node at the source node, "Intermediate node" refers to the node to which the phantom node routes Φ hops according to the right hand rule. The backbone route path is created from the intermediate node to the sink and reverse extends to the network border, and then create branch routes in the backbone route path (the number of branch routes see Theorem 3). As can be seen from Fig.5, the experimental result implements the tree route scheme and creates 9 branch routes besides the backbone route, among which the length of some branch routes is longer than the phantom node path. In addition, the created tree is completely homogenous, which reaches the goal of scheme in this paper. It is very difficult for the adversary to trace back to the phantom node, with high security performance.

Fig. 6 shows the energy consumption in different regions under phantom route and tree route. The experimental scene is that we randomly choose 200 source nodes in the network, and then do experiments on each node as the following. (A) First create a phantom node, and then create a tree according to algorithm 1, as shown in Fig. 5, for each created tree, revoke it when 10 rounds data collection are finished. (B) Then create another phantom node, repeat step (A). Go on like this until 10 phantom nodes are created. After doing this, get the energy consumption of the network, as shown in Fig. 6. In Fig. 6, the phantom route refers to the route from phantom node created near the source node to the sink, additionally, if the route is extended to the network border, it is called the phantom route with backbone route path, which is equivalent of the tree route with only backbone route path. As can be seen from Fig. 6, under phantom route protocol, the energy consumption near the sink is quite large, and small for regions away from the sink, so its energy efficiency is not high. While under the tree route scheme in this paper, the energy consumption is also high for regions away from the sink, as long as the energy consumption does not exceeds the energy consumption in hotspots, the network lifetime will not be affected. Therefore, we create diversionary routes as many as possible by fully using energy in regions away from the sink, since there is only one route path in hotspots near the sink, the energy consumption in hotspot is the same with that under phantom route protocol, thus the lifetime is the same. The experimental results in Fig. 6 show the route scheme in this paper greatly improves the network security by creating more diversionary routes without affecting the network lifetime.

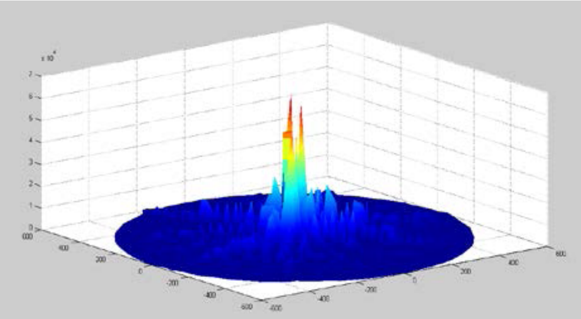

FIGURE 7. Energy consumption under phantom route protocol.

Fig. 7 and Fig. 8 respectively show the 3D map of energy consumption under phantom routing protocol and tree based

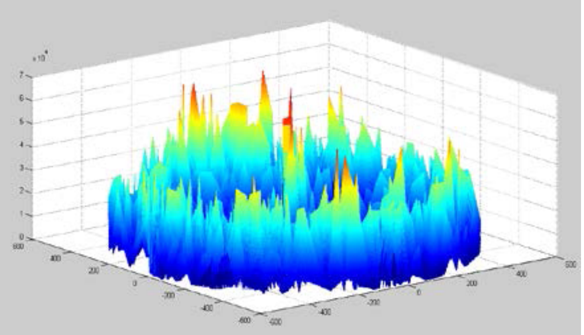

FIGURE 8. Energy consumption under tree route scheme.

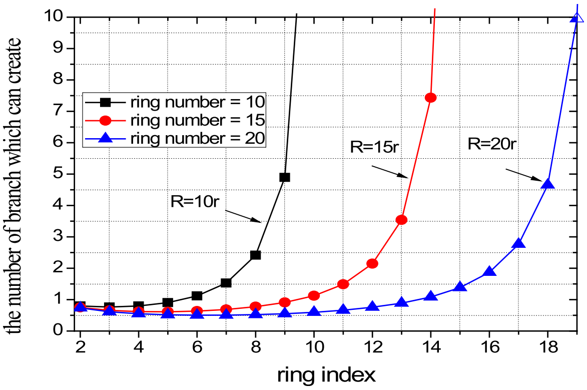

FIGURE 9. The number of branch routes in each ring.

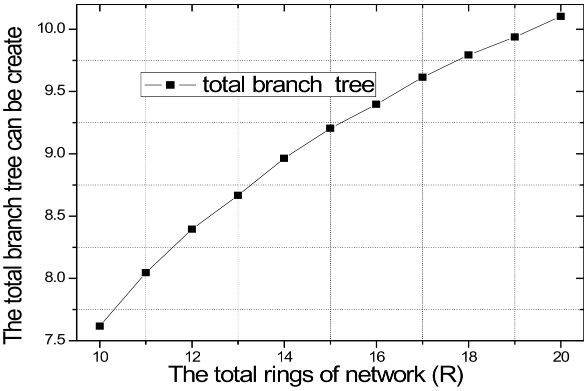

FIGURE 10. Total number of diversionary routes under different *R*.

routing scheme. As can be seen from Fig. 7, the energy consumption is high for regions near the sink under phantom route and it is low for regions away from the sink([9] points out the remaining energy is up to 90%), while under tree route scheme, energy consumption in different regions is balanced, achieving high energy efficiency.

In previous discussion, the number of diversionary routes in tree route scheme is calculated according to Theorem 3, Fig. 9 and Fig. 10 show the calculation results of diversionary routes number in different regions. Fig.9 refers to the diversionary routes number in each ring when the network radius R is 10, 15, 20 times of the nodal transmission radius r. As can be seen from Fig. 9, the bigger R, the smaller diversionary routes number(this does not mean the total number of diversionary routes is also smaller). Generally, farther from the sink, more branches can be created. Fig. 10 shows the number of branches can be created according to Theorem 3 without affecting network lifetime. Fig.11 shows the number of diversionary routes can be created under different R, as can be seen, the bigger R, the more diversionary routes can be created.

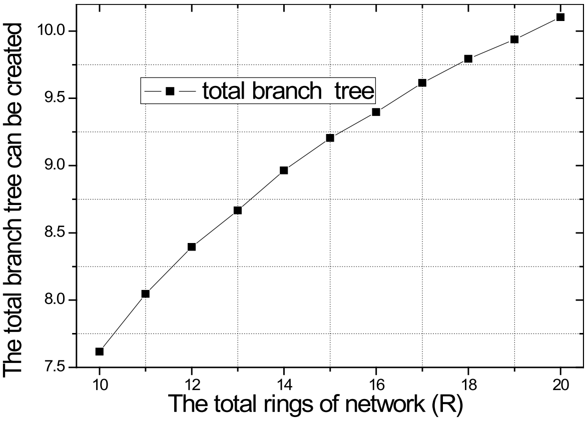

FIGURE 11. Total number of branches under different *R*.

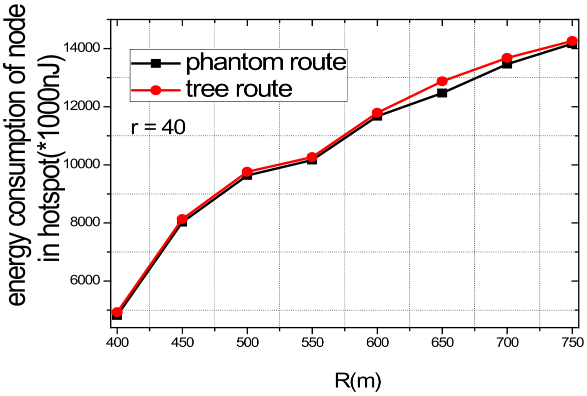

FIGURE 12. Maximum energy consumption under different *R*.

Fig. 12 shows the maximum energy consumption under different R with tree based routing scheme and phantom route protocol (actually the maximum energy consumption determines the network lifetime). As can be seen from Fig.12, the maximum energy consumption (network lifetime) under these two protocols is basically the same, indicating that the scheme in this paper can improve the network security without affecting network lifetime.

Fig. 13 shows the total energy consumption under tree based route and phantom route. As can be seen from Fig. 13, the energy consumption with tree route is 5.7 times to 22.7 times of the energy consumption with phantom route, this is because the tree based route scheme creates many diversionary routes, and then the energy consumption is increased by times, since this increased energy consumption is in the outside region, so this has no effect on the network lifetime. Meanwhile, the route path length in tree route scheme is

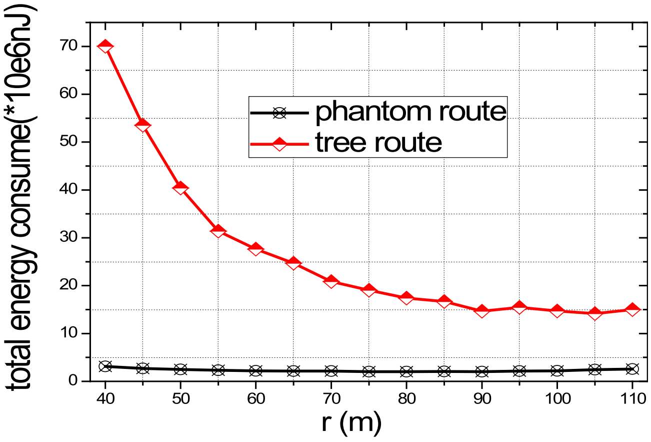

FIGURE 13. Total energy consumption under different *r*.

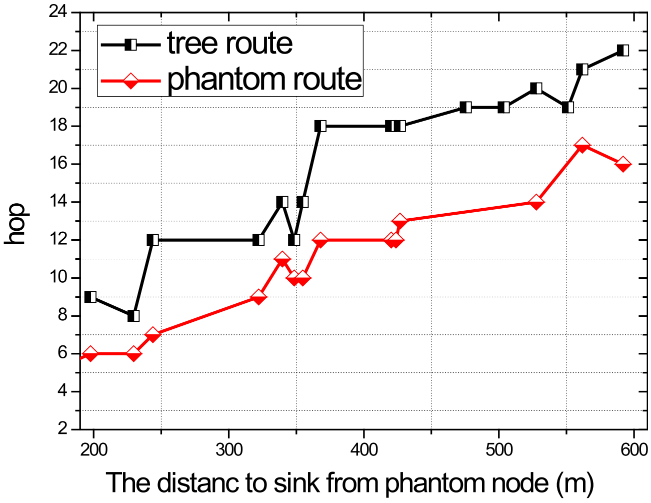

FIGURE 14. Delay comparison between phantom route and tree route.

*m*times of that in phantom route, this means the network security is improved greatly by tree route.

In this work, we assume that the adversary has the capability of figuring out the sender based on the signal received without any delay. Therefore, for simplicity, we define the delay by using the hops from the phantom node to the sink. Fig. 14 shows the delay under these two protocols, and, as can be seen, the delay under tree based routing protocol is longer than phantom route, this is because, for the sake of security, the tree based routing scheme does not deploy the shortest path route protocol, nor the phantom node is created on the backbone route path, so the data of phantom node is sent to the backbone route via diversionary routes, and then the backbone route deploys the shortest path. Since the maximum delay is no more than 10 hops, it is very small compared with the tree route which is up to hundreds of hops (see Fig. 9), this shows the cost for security is very small.

Fig. 15 shows the relationship between the source node data transmission frequency and network lifetime. As can be seen, the network lifetime is inversely proportional to the frequency, namely, the high frequency, the more energy consumption per unit time, so the network lifetime is lower. Fig. 16 gives the relationship between network lifetime and number of tree created under certain data transmission frequency. As can be seen from Fig. 16, to create more trees on the same source node has little effect on the network lifetime. The main reason is as the following. When *m*trees are created, the data transmission frequency is only $1/m$ of the original, so the energy consumption is only $1/m$ of the original, since there are *m*trees, the total energy consumption remain the same, this shows more routes do not affect network lifetime. And through more trees, the network security is improved, relevant theoretical analysis can be found in Theorem 7 and Theorem 8.

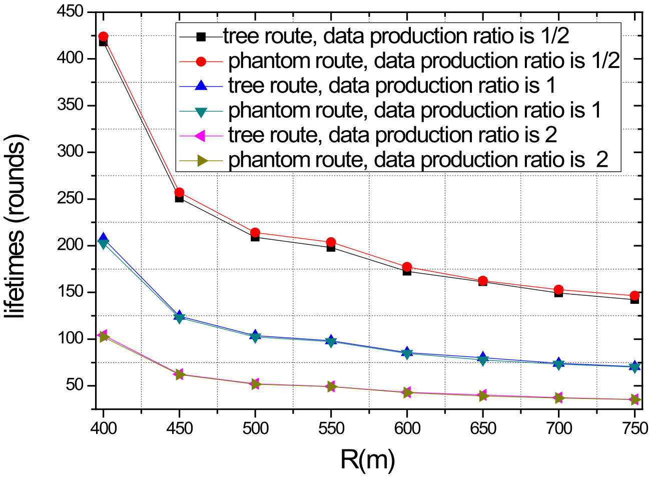

FIGURE 15. Relationship between the source node data transmission frequency and network lifetime.

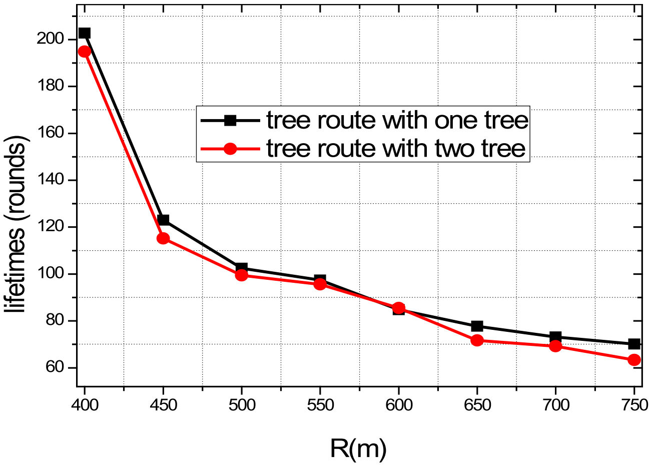

FIGURE 16. Network lifetime comparison under multiple trees.

B. EXPERIMENTAL RESULTS OF THE SECURITY PERFORMANCE

1) THE ABILITY TO AGAINST DIRECTION-ORIENTED ATTACK

Fig.17 shows the performance comparison between tree based route and phantom node when the probability of choosing diversionary route according to the left hand rule is $\theta = 0.2$. In the experiment, the angle range of phantom

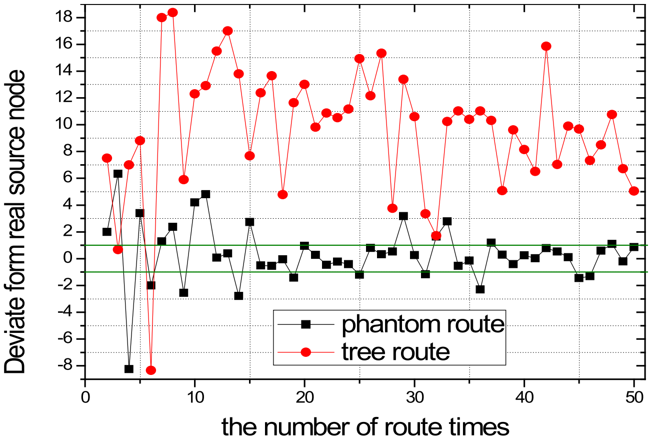

FIGURE 17. Attack direction deviate from real direction between tree route and phantom route under direction-oriented attack. ($\theta = 0.2$).

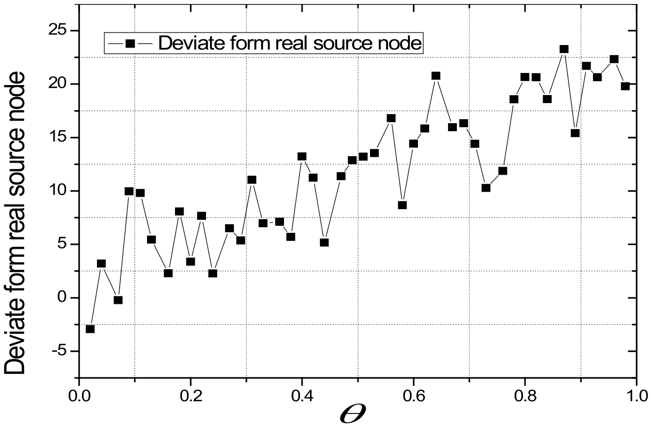

FIGURE 18. Attack direction deviate from real direction under different θin tree route.

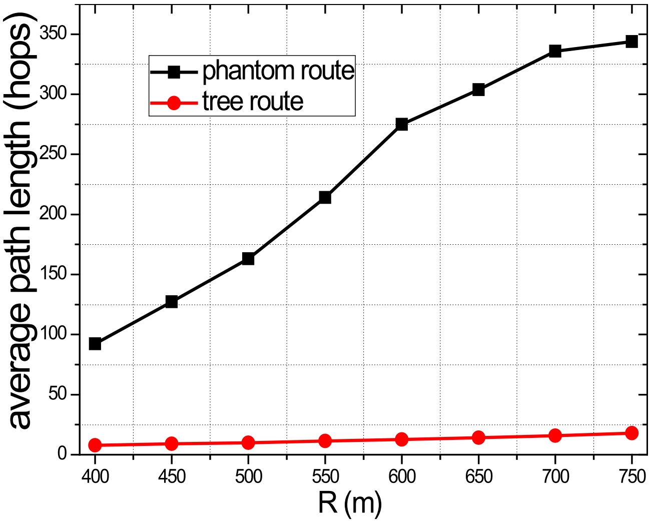

FIGURE 19. Route length comparison under different *R*.

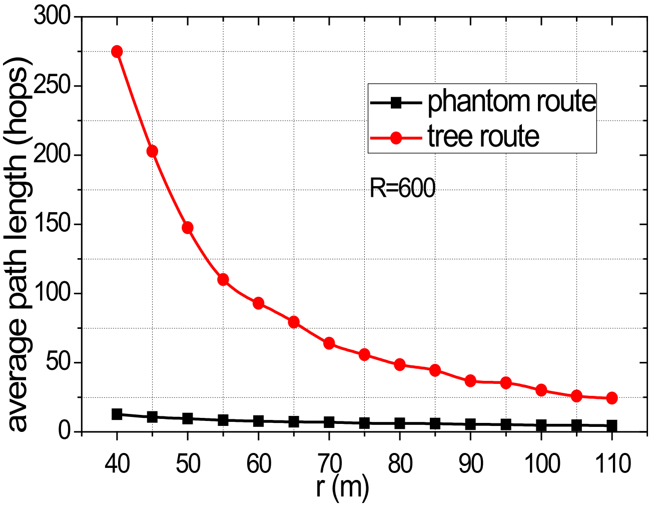

FIGURE 20. Route length comparison under different *r*.

route is [0,30°], the angle range of tree route path is [0,90°]. We then calculate the deviation between the attack direction and the real source node direction according to direction-oriented attack method. If the deviation <1°, then the adversary succeeds. As can be seen, with the proposed scheme, only once can succeed, while with phantom route, as the trace times increases, the success probability >90%. Obviously, our scheme has a better performance against the direction-oriented attack.

Fig.18 shows the deviation between the attack direction and the real source node direction when routed 30 times with θ changing. As can be seen, with the proposed scheme, as θ grows, the attack direction deviates farther from the real direction, indicating the success rate is very low.

2) COMPARISON OF TRACE TIME

Fig. 19 and Fig. 20 shown the route length comparison under different network scale *R*and nodal transmission radius *r*. From Fig.18, under different *R*, the total route length of tree route is 11.9 to 19.23 times of phantom route. While in Fig. 20, under different *r*, the total route length of tree route is 5.44 to 21.66 times of phantom route. Due to the homogeneity of tree, the adversary cannot speculate the location of source node, and can only attack through exhaustive search, so the security is proportional to its route length, indicating that the security of tree route is relatively higher.

Table 3 gives the number of hops to the sink and the number of nodes for each diversionary route in Fig. 9, where the real source node is located in the 8th diversionary route. The following experiment shows the performance of tree based route against adversary.

The experimental scene in Fig. 21 is as shown in Fig. 5, 9 diversionary routes and one backbone route are created in the tree, the detail is as shown in table 3. since the adversary cannot speculate the location of source node from the tree shape, so the adversary will choose one branch to trace randomly, if not succeed, then choose another branch until reach the preset number of trace time. Besides, we assume the adversary is very intelligent, the next trace can be processed without time cost, namely, the cost of rollback from the previous route is not considered. The experiment is repeated

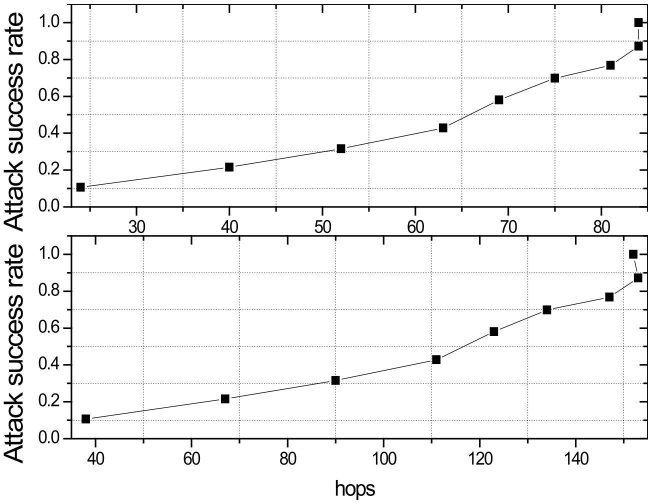

FIGURE 21. Success rate under different trace length.

TABLE 3. The Number of nodes in each diversionary and hops to the sink.

Diver-sionary **index**	**Hops to the sink**	**Number of nodes**	**Branch index**	**Hops to the sink**	**Number of nodes**
1	3	42	**6**	13	18
2	4	41	**7**	14	28
3	6	36	**8**	17	12
4	8	34	**9**	18	18
5	12	25	**10**	0	20

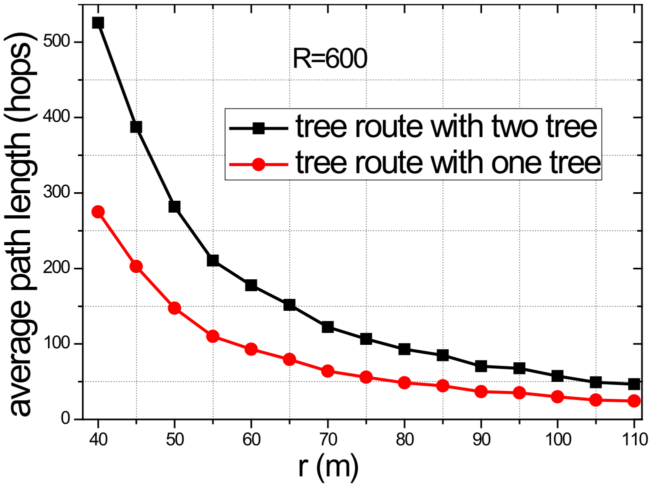

FIGURE 22. Route length comparison under different number of trees.

by 500 times, and an average success rate then is calculated. The bottom figure of Fig. 21 shows the success rate under certain trace times. As can be seen, when the adversary attacks with 38 hops trace length, the success rate (success means the phantom node is traced) is only 10.6%, while if it is phantom route, the success rate can be up to 100% under this condition. Moreover, when the trace length is 111 hops, the success rate is less than 50%, namely, only 42.8%. Obviously, the tree based routing scheme greatly improves the ability against the attack.

Fig. 22 shows the route length under different number of trees, as can be seen, when more trees are created, the route length is approximately increased by corresponding times, and then it is safer. The conclusion can be seen in Theorem 7 and Fig. 21.

VII. CONCLUSION

Source location privacy preservation is becoming more and more important in pervasive computing, and its research is of great significance.

(1) First: The TR scheme has the following advantages over the traditional phantom routing protocol: (A) The route structure is homogeneous, so the adversary cannot speculate the phantom node and source of data, while in previous research, there is only one path in phantom route, and many improved algorithms based on phantom node aim at creating phantom node far away from the source node, so their preservation of the phantom node is weak. (B) This paper analyzes possible adversary models and we identify a new attack called direction-oriented attack, which is a great threat to traditional phantom route protocol, and to the best of our knowledge, previous research all ignored this threat, meanwhile, our scheme can avoid this threat by creating the tree backbone route with left hand rule at probability θ. (C) The proposed scheme fully uses remaining energy in remote regions to create diversionary routes as many as possible, and with only one route in regions near the sink. This strategy improves the security without affecting network lifetime.

(2) Second, extensive performance analysis of the proposed tree based route scheme shows that tree based route scheme is better than existing privacy preservation protocols. (A) Tree based route scheme has a strong resistance to reverse trace of the adversary , the theoretical and experimental results show that the route length in this paper is more than 10 times of traditional phantom route, which indicts that the adversary has to spend more than 10 times of time to achieve the same effect with phantom route. (B) Tree based route has strong resistance to direction-oriented attack. (C) The proposed scheme has high network lifetime, although the total energy consumption of this scheme is more than 10 times of other protocols, since it maximumly reduce the energy consumption in hotspot, the theoretical and experimental results show that the lifetime is the same with phantom route with one route.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, Apr. 2002.

[2] S. He, J. Chen, Y. Sun, D. K. Y. Yau, and N. K. Yip, "On optimal information capture by energy-constrained mobile sensor," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2472–2484, Jun. 2010.

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

[4] A. Jhumka, M. Leeke, and S. Shrestha, ''On the use of fake sources for source location privacy: Trade-offs between energy and privacy,'' *Comput. J.*, vol. 54, no. 6, pp. 860–874, 2011.

[5] Y. Li, J. Ren, and J. Wu, ''Quantitative measurement and design of source-location privacy schemes for wireless sensor networks,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 7, pp. 1302–1311, Jul. 2012.

[6] 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.*, Columbus, OH, USA, Nov. 2005, pp. 599–608.

[7] A.-F. Liu, P.-H. Zhang, and Z.-G. Chen, ''Theoretical analysis of the lifetime and energy hole in cluster based wireless sensor networks,'' *J. Parallel Distrib. Comput.*, vol. 71, no. 10, pp. 1327–1355, 2011.

[8] A. Jarry, P. Leone, S. Nikoletseas, and J. Rolim, ''Optimal data gathering paths and energy-balance mechanisms in wireless networks,'' *Ad Hoc Netw.*, vol. 9, no. 6, pp. 1036–1048, 2011.

[9] L. Lamport, R. Shostak, and M. Pease, ''The Byzantine generals problem,'' *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.

[10] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, ''SAGE: A strong privacy-preserving scheme against global eavesdropping for ehealth systems,'' *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 365–378, May 2009.

[11] K. Pongaliur and X. Li, ''Maintaining source privacy under eavesdropping and node compromise attacks,'' in *Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011, pp. 1656–1664.

[12] C. Ozturk, Y. Zhang, and W. Trappe, ''Source-location privacy in energy-constrained sensor network routing,'' in *Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw. (SASN)*, vol. 4. 2004, pp. 88–93.

[13] Y. Li and J. Ren, ''Preserving source-location privacy in wireless sensor networks,'' in *Proc. 6th Annu. IEEE Commun. Soc. Conf. Sens. Mesh Ad Hoc Commun. Netw.*, Jun. 2009, pp. 1–9.

[14] H. Wang, B. Sheng, and Q. Li, ''Privacy-aware routing in sensor networks,'' *Comput. Netw.*, vol. 53, no. 9, pp. 1512–1529, 2009.

[15] K. Bicakci, H. Gultekin, B. Tavli, and I. E. Bagci, ''Maximizing lifetime of event-unobservable wireless sensor networks,'' *Comput. Standards Interf.*, vol. 33, no. 4, pp. 401–410, 2011.

[16] K. Bicakci, I. E. Bagci, and B. Tavli, ''Lifetime bounds of wireless sensor networks preserving perfect sink unobservability,'' *IEEE Commun. Lett.*, vol. 15, no. 2, pp. 205–207, Feb. 2011.

[17] M. Shao, Y. Yang, S. Zhu, and G. Cao, ''Towards statistically strong source anonymity for sensor networks,'' in *Proc. 27th Conf. Comput. Commun. IEEE INFOCOM*, Phoenix, AZ, USA, Apr. 2008, pp. 51–55.

[18] K. Mehta, D. Liu, and M. Wright, ''Location privacy in sensor networks against a global eavesdropper,'' in *Proc. IEEE Int. Conf. Netw. Protocols (ICNP)*, Oct. 2007, pp. 314–323.

[19] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, ''Towards event source unobservability with minimum network traffic,'' in *Proc. ACM Conf. Wireless Netw. Security*, 2008, pp. 77–88.

[20] M. M. E. A. Mahmoud and X. Shen, ''A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 10, pp. 1805–1818, Oct. 2012.

[21] G. Tan, W. Li, and J. Song, ''Enhancing source location privacy in energy-constrained wireless sensor networks,'' in *Proc. Int. Conf. Comput. Sci. Inf. Technol.*, 2014, pp. 279–289.

[22] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, ''Entrapping adversaries for source protection in sensor networks,'' in *Proc. Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Buffalo-Niagara Falls, NY, USA, 2006.

[23] H. Chen and W. Lou. (2014). On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks. *Pervas. Mobile Comput.* [Online]. Available: http://dx.doi.org/10.1016/j.pmcj.2014.01.006

[24] A. Jhumka, M. Bradbury, and M. Leeke. (2014). Fake source-based source location privacy in wireless sensor networks. *Concurrency Comput., Pract. Experience* [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/cpe.3242/pdf

[25] A. Sgora, D. D. Vergados, and P. Chatzimisios. A survey on security and privacy issues in wireless mesh networks. *Security Commun. Netw.* [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/sec.846/

[26] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, ''A novel scheme for protecting receiver's location privacy in wireless sensor networks,'' *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 3769–3779, Oct. 2008.

[27] M. Dong, K. Ota, Z. Tang, M. Lin, S. Du, and H. Zhu. UAV assisted data gathering in wireless sensor networks. *J. Supercomput.* [Online]. Available: http://link.springer.com/article/10.1007%2Fs11227-014-1161-6

[28] M. Dong, K. Ota, H. Li, S. Du, H. Zhu, and S. Guo. RENDEZVOUS: Towards fast event detecting in wireless sensor and actor networks. *Computing* [Online]. Available: http://link.springer.com/article/10.1007%2Fs00607-013-0364-7

[29] Y. Zhang, W. Liu, Y. Fang, and D. Wu, ''Secure localization and authentication in ultra-wideband sensor networks,'' *IEEE J. Sel. Areas Commun.*, vol. 24, no. 4, pp. 829–835, Apr. 2006.

[30] A. E. A. A. Abdulla, H. Nishiyama, J. Yang, N. Ansari, and N. Kato, ''HYMN: A novel hybrid multi-hop routing algorithm to improve the longevity of WSNs,'' *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2531–2541, Jul. 2012.

[31] A. Liu, D. Zhang, P. Zhang, G. Cui, and Z. Chen, ''On mitigating hotspots to maximize network lifetime in multi-hop wireless sensor network with guaranteed transport delay and reliability,'' *Peer-to-Peer Netw. Appl.*, vol. 7, no. 3, pp. 255–273, Mar. 2014.

[32] J. Pan, L. Cai, Y. T. Hou, Y. Shi, and S. X. Shen, ''Optimal base-station locations in two-tiered wireless sensor networks,'' *IEEE Trans. Mobile Comput.*, vol. 4, no. 5, pp. 458–473, Sep./Oct. 2005.

[33] K. Ota, M. Dong, Z. Cheng, J. Wang, X. Li, and X. Shen, ''ORACLE: Mobility control in wireless sensor and actor networks,'' *Comput. Commun.*, vol. 35, no. 9, pp. 1029–1037, 2012.

[34] H. Philip, ''The distribution of means for samples of size n drawn from a population in which the variety takes values between 0 and 1, all such values being equally probable,'' *Biometrika*, vol. 19, no. 3, pp. 240–245, 1927.

[35] (2013, Mar.). *OMNet++ Network Simulation Framework* [Online]. Available: http://www.omnetpp.org/

JUN LONG is a Professor with the School of Information Science and Engineering, Central South University, Changsha, China. His major research interest is wireless sensor network.

MIANXIONG DONG received the B.S., M.S., and Ph.D. degrees in computer science and engineering from the University of Aizu, Aizuwakamatsu, Japan. He is currently a Researcher with the National Institute of Information and Communications Technology, Tokyo, Japan. He was the prestigious Japan Society for the Promotion of Sciences (JSPS) Research Fellow with the School of Computer Science and Engineering, University of Aizu, and a Visiting Scholar with the BBCR Group, University of Waterloo, Waterloo, ON, Canada, supported by the JSPS Excellent Young Researcher Overseas Visit Program from 2010 to 2011. He was selected as a Foreigner Research Fellow (a total of three recipients all over Japan) by the NEC C&C Foundation in 2011. He was a recipient of the Best Paper Award at the IEEE International Conference on High Performance and Communications in 2008 and the IEEE International Conference on Embedded Software and Systems in 2008. He is currently a Research Scientist with the A3 Foresight Program (2011–2014) funded by the JSPS, the National Natural Science Foundation of China, and the National Research Foundation of Korea. His research interests include wireless sensor networks, vehicular ad hoc networks, and wireless security.

KAORU OTA received the M.S. degree in computer science from Oklahoma State University, Stillwater, OK, USA in 2008, and the Ph.D. degree in computer science and engineering from the University of Aizu, Aizuwakamatsu, Japan, in 2012. She is currently an Assistant Professor with the Department of Information and Electronic Engineering, Muroran Institute of Technology, Muroran, Japan. From 2010 to 2011, she was a Visiting Scholar with the BBCR Group, University of Waterloo, Waterloo, ON, Canada. She was also a prestigious Japan Society of the Promotion of Science (JSPS) Research Fellow with the Graduate School of Information Sciences, Tohoku University, Sendai, Japan, from 2012 to 2013. Her research interests include wireless sensor networks, vehicular ad hoc networks, and ubiquitous computing. She joined the JSPS A3 Foresight Program as a Primary Researcher in 2011, which is supported by the Japanese, Chinese, and Korean government. She serves as the Guest Editor of the 2014 *IEICE Transactions on Information and Systems, Special Section on Frontiers of Internet of Things*, and an Editorial Board Member of *Peer-to-Peer Networking and Applications* (Springer), *Ad Hoc & Sensor Wireless Networks*, *Journal of Cyber-Physical Systems*, and *International Journal of Embedded Systems*.

ANFENG LIU is a Professor with the School of Information Science and Engineering, Central South University, Changsha, China. He received the M.Sc. and Ph.D. degrees in computer science from Central South University in 2002 and 2005, respectively. His major research interest is wireless sensor network.