IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON INFORMATION SECURITY SOLUTIONS FOR TELEMEDICINE APPLICATIONS

Received May 15, 2018, accepted July 14, 2018, date of publication July 23, 2018, date of current version August 20, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2858274

Privacy-Preserving Protocol for Sink Node Location in Telemedicine Networks

TING LI[1], YUXIN LIU[1], NEAL N. XIONG[2], ANFENG LIU[1,3], ZHIPING CAI[4], (Member, IEEE), AND HOUBING SONG[5], (Senior Member, IEEE)

[1]School of Information Science and Engineering, Central South University, Changsha 410083, China
[2]Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, OK 74464, USA
[3]State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China
[4]Department of Network Engineering, School of Computer, National University of Defense Technology, Changsha 410073, China
[5]Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114, USA

Corresponding author: Yuxin Liu (yuxinliu@csu.edu.cn) and Neal N. Xiong (xiongnaixue@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61772554, Grant 61572528, and Grant 6157256, in part by the Open Research Project of the State Key Laboratory of Industrial Control Technology, Zhejiang University, China, under Grant ICT1800391, and in part by the National Basic Research Program of China (973 Program) under Grant 2014CB046345.

ABSTRACT Telemedicine is expected to play a significant role in previsioning better service and meeting various needs of patients, healthcare providers, and policy makers by exploiting advanced information and communication technologies. Because health data are highly sensitive, the security and privacy of telemedicine should be protected carefully to protect telemedicine from being potentially interrupted and attacked. In telemedicine networks, the sink node is the most vulnerable to attacks because it is where sensitive data will be collected. Thus, it is of great importance to protect the privacy of the sink node in telemedicine networks. To this end, this paper proposes an efficient privacy-preserving protocol for sink node location in telemedicine networks. Compared with the existing work, the scheme can improve the safe time of telemedicine networks by injecting request packets and reduce the delivery time by transmitting along the shortest route. In particular, the safe time can be improved by 28.57% to 52.70%, and the delivery time can be reduced by 22.86% to 27.61%.

INDEX TERMS Telemedicine networks, security, sink node privacy, safe, delivery time.

I. INTRODUCTION

A telemedicine network, as an essential part of a smart city, connects sensors, healthcare facilities, and organizations to meet the demands of patients, healthcare providers and policy makers [1]–[5]. Telemedicine networks can collect and process healthcare information by means of advanced information and communication technologies to improve services for people in all stages of life [6]–[8]. Telemedicine networks can be considered the infrastructure and are composed of tiny and power-efficient sensors over a broad area that transmit the healthcare data to the sink node, where collective data are analyzed through machine learning and data mining techniques [9]–[12]. Along with the benefits brought by telemedicine networks come many technical challenges, including energy consumption and energy control [13], [15], healthcare data collection [16], [17], the delivery process [18]–[20], delay issues [21], [22], data distribution methods [23]–[27], and privacy and security in telemedicine networks [23]–[28]. The security issue is a significant aspect that can influence the performance of telemedicine networks.

Due to the important role of the sink node, it is the most vulnerable part to potential attacks. Therefore, the location privacy of the sink node is of significance. Typically, telemedicine networks are deployed in environments without manual monitoring [29]–[33], and the sink node is responsible for healthcare data collection [34]–[36]. Therefore, if the location of the sink node is exposed to attackers, the entire network will break down [24]–[30]. Since the sink node is the destination of healthcare data collection in the network, all the data packets will be delivered to the sink node hop by hop. Therefore, without privacy measures, attackers can find the location of the sink node by tracing the direction of the data packet transmissions. They can then attack the sink node, which can dramatically affect the normal operation of the telemedicine network. Moreover, because the sink node is the destination of all the data packets in the network, it is very challenging to protect the location privacy of the sink node.

In telemedicine networks, the issue of location privacy of the sink node has attracted much research attention.

In the conventional data delivery model, the sink node is the only node to receive and collect data packets from all the sources in a telemedicine network. Because the sink node is different from other normal sensor nodes in the conventional data delivery model, the location of the sink node can be tracked easily. In this paper, in contrast to the former delivery model, the sink node can deliver information to other sensor nodes, which will confound adversaries and improve the security. Based on this observation, we propose a novel privacy-preserving data delivery model for telemedicine networks in this paper. The main contributions are summarized as follows.

(1) Firstly, we propose a novel privacy-preserving protocol for the sink node location by introducing fake sink nodes and fake data packets, which makes the system more complex and makes it harder to find the location of the real sink node.

(2) Secondly, the proposed scheme can reduce the delivery time while protecting the location privacy of the sink node.

(3) Thirdly, we compare our proposed scheme with previous schemes via extensive experiments and simulations. The experimental results show that our scheme can successfully improve the safe time and reduce the data delivery time. Specifically, the safe time of the sink node can be improved by 28.57% to 52.70%, and the delivery time can be reduced by 22.86% to 27.61%.

The rests of this paper are organized as follows. Section II reviews the related works. The system model and problem statements are described in Section III. Section IV elaborates the design of the PSNL-TNs scheme. Performance analysis and comparisons of the PSNL-TNs scheme are provided in Section V and Section VI, respectively. Section VII concludes the paper.

II. RELATED WORKS

In this section, related works are reviewed. Recently, telemedicine networks have begun to play an important role in providing equity and quality services by connecting healthcare facilities. This topic has gained significant research attention, and research efforts have been devoted to different issues, such as security [36], [37], [39], data collection [15], [40]–[44], data coverage [45] and storage [46]–[48]. Among these issues, security and privacy have attracted great attentions [35], [49]–[52]. Telemedicine networks should be secure and robust to resist malicious attacks [24]–[31], [34]. Extensive research has been performed on the topic of security of the sink node in a telemedicine network, and some of the developed methods have been applied to telemedicine networks. In telemedicine networks, the issue of privacy and security can be divided into three aspects: content privacy, source privacy and sink location privacy.

For the content privacy issue, [30] proposed a scheme that exploits homomorphic functions in the compressive data gathering process to hinder traffic flow tracking and preserve privacy. Via homomorphic encryption and aggregation in the encrypted domain, the security of the data packets can be guaranteed, as proposed by [16] . In wireless medical sensor networks (WMSNs), based on the existing scheme in WMSNs, [36] proposed an anonymous authentication scheme for health-care applications to ensure the security and privacy of the data information of patients.

In telemedicine networks, the privacy of the source location can also be jeopardized. Reference [27] improved the privacy of the source nodes via two clustering-based source privacy protection schemes: the dynamic path scheme and the dynamic tree scheme. Based on source-location privacy (SLP), [26] proposed a routing scheme called sink toroidal region (STaR scheme) to provide suitable SLP while maintaining low energy consumption.

For the sink node privacy issue in telemedicine networks, [28] proposed a scheme called ''homogenous injection for sink privacy with node compromise protection'' (HISP-NC) to protect the location of the sink node. In addition, [29] introduced a scheme to improve the safe time of the sink node by injecting fake data packets and random walks of the real data packets, which can protect the sink node location effectively. This paper also introduced direction attacks from adversaries in the telemedicine networks, with which the location of the sink node can be observed easily to some extent. Reference [24] proposed a random data collection scheme to protect the location privacy issue of the sink node in the networks, whereby the data packets are delivered along random routes to avoid tracking by adversaries. However, the energy consumption and delivery time of the data packets will increase because the data packets spend significant time performing the random walks.

III. THE SYSTEM MODEL AND PROBLEM STATEMENT

A. THE SYSTEM MODEL

There are four types of sensor nodes in telemedicine networks: the real sink node, fake sink nodes, ordinary sensor nodes and source sensor nodes. These four types of sensor nodes can be summarized as follows:

1. There is only one static sink node in a telemedicine network, and it can receive and analyze data packets.

2. Several fake sink nodes are distributed randomly in a telemedicine network, each of which can receive fake data packets to confound adversaries. Each fake sink node maintains a set of one-hop neighboring nodes. The actions of fake sink nodes are the same as the real sink node. The number of fake sink nodes is defined as N_f.

3. Source sensor nodes can generate real data packets, and the number of source nodes is defined as $\mathcal{N}_s$.

4. Ordinary sensor nodes can receive data packets. Meanwhile, if an ordinary sensor node receives a set of real data packets, it will generate a set of fake data packets to hide the real transmission routes of the real data packets. The number of ordinary sensor nodes is defined as N_o.

The adversary model is given as follows.

1. The adversaries follow a tracking scheme, which is defined as direction attacks in [24].

2. The adversaries are only interested in tracing the sink node and do not interfere with the normal communications of the sink node.

3. The adversaries trace the data packets hop by hop, and they can perform backtracking. The residence time of the adversaries at a sensor node is defined as $\wp$. If the residence time reaches a certain value and this sensor node is the real sink node, then the sink node is considered to succeed.

B. PROBLEM STATEMENT

(1) Enhancement of the security in telemedicine networks

The location privacy of the sink node should be protected to enhance the security. The period before the location of the sink node is found by attackers is defined as the safe time. Minimizing the probability of the sink node being found by adversaries is an efficient solution to enhance the network security. Assuming that there are N_f fake data packets generated in a sensor node, the number of hops in a transmitting route is N; the probability can be defined by equation (1):

$$MIN\ (\mathcal{P}) = \prod_1^N (\frac{1}{N_f + 1}) \tag{1}$$

(2) Reduction of delivery time in telemedicine networks

Delivery time is the total time spent in a data transmission process. With delivery time, a set of data packets can be delivered to the sink node after N hop transmissions. If, in a node, a set of data packets must wait for time $\hbar$, ideally, the equation of the delivery time reduction is as shown in equation (2).

$$MIN\ (\mathcal{W}) = (N - 2) \cdot (\hbar + d_t) \tag{2}$$

Where d_t represents the one-hop time when a node delivers a set of data packets to the next sensor node.

(3) Reduction of the energy consumption

In a transmission process of a data packet set, the total energy consumption is defined as $\mathcal{V}$. The energy consumption when generating a set of data packets is defined as C_1, and the energy consumption when delivering a set of data packets is defined as C_2 in a one-hop dissemination process. Then, the energy consumption in $\mathcal{V}$ can be expressed as:

$$MIN(\mathcal{V}) = C_1 \cdot \mathcal{N} + C_2 \cdot \mathcal{M} \tag{3}$$

where $\mathcal{N}$ is the number of data packet sets, including the number of real data packets, the fake data packets and the request packets of the sink node and fake sink node. $\mathcal{M}$ represents the total number of hops when transmitting a set of data packets.

In summary, the research objectives are as follows.

$$\begin{cases} MIN\ (\mathcal{P}) = \prod_1^N (\frac{1}{N_f+1}) \\ MIN\ (\mathcal{W}) = (N - 2) \cdot (\hbar + d_t) \\ MIN\ (\mathcal{V}) = C_1 \cdot \mathcal{N} + C_2 \cdot \mathcal{M} \end{cases} \tag{4}$$

Table 1 describes some basic notations used throughout this paper.

TABLE 1. Notations.

Symbols	Descriptions
ERQ_i	The request packets of fake sink node i
ERQ	The request packets of the real sink node
$\hbar$	The waiting time interval
f	The set of fake sink nodes
τ	The communication ranges
$\mathcal{P}ro_1$	The probability of the real sink node being traced in the first transmission period
$\mathcal{P}ro_2$	The probability of the real sink node being traced in the second transmission period
$\mathcal{P}ro$	The probability of the real sink node being traced in a data transmission process
$\mathcal{N}_\omega$	The number of sensor nodes that may be treated as the real sink node by adversaries
N	The total number of sensor nodes in a data transmission process
N_{source}	The number of source nodes
$\mathcal{J}_{eg}$	The energy consumption when generating a set of data packets hop by hop
$\mathcal{J}_{ef}$	The energy consumption when transmitting a set of data packets hop by hop
d_t	The one-hop time when a node transmits a set of data packets to the next node
$N_{\ell f}$	The number of fake data packets that a sensor node ℓ can generate
N_{rq}	The number of the request packets of the real sink node
N_{fq}	The number of the request packets of the fake sink nodes
$\aleph_{rh}$	The number of hops to the real sink node of the real data packets
$\aleph_{fh}$	The number of hops for all the fake data packets in a data transmission
T_d	The total delivery time

IV. THE DESIGN OF THE LRDC SCHEME

A. OVERVIEW

In telemedicine networks, the sink node can collect and analyze the data packets from other sensor nodes. In general, the privacy of the sink node includes two aspects: content privacy and contextual privacy. In this paper, we concentrate on the contextual privacy and do not consider the length or content of the data packets. In telemedicine networks, the sink node is traced by some of the adversaries, and those adversaries may perform attacks on the sink node or get the data packets from the sink node. Moreover, to attack the sink node location in telemedicine networks, some attackers may add additional nodes to the original network or compromise several original sensor nodes. Alternately, some of the adversaries may damage the data packets. This has become a serious issue for privacy in telemedicine networks. Therefore, it is necessary to protect the location privacy of the sink node to maintain the integrity and effectiveness of telemedicine networks. Many techniques and schemes have been proposed to protect the location information of the sink node in telemedicine networks.

However, several problems still exist, as follows:

1. The actions of the ordinary sensor nodes. In the previous schemes, if the data packets are transmitted to an ordinary sensor node, then those data packets are delivered to the next sensor node immediately. The adversaries can track the location of the sink nodes via the transmission routes of the data packets. Therefore, the location privacy of the sink node can be discovered easily to some extent.

2. The actions of the sink node. In the previous schemes, the sink node is the end destination of the data transmission processes, which differs from the actions of other sensor nodes. All the data packets will be delivered to the sink node. Because of this special characteristic, the location of the sink node will be exposed easily to some extent.

In a data transmission process, a set of data packets should be transmitted to the sink node. Therefore, the sink node is markedly set along the transmission route. In this paper, a scheme named "Privacy-Preserving Protocol of Sink Node Location in Telemedicine Networks" (the PSNL-TNs scheme) is proposed to protect and hide the location privacy of the sink node in telemedicine networks. Fake sink nodes and fake data packets can increase the complexity of the entire network. Therefore, the PSNL-TNs scheme can confuse the tracking processes of adversaries. In general, with the PSNL-TNs scheme, the probability of the sink node being traced can be decreased to a large extent.

To be specific, to protect the location privacy of the real sink node, the two main contributions in this paper are as follows.

1. When data packets are transmitted to an ordinary sensor node, this ordinary sensor node will hold the real data packets for a small time. Meanwhile, this ordinary sensor node will generate a random number of fake data packets and deliver those fake data packets to other sensor nodes.

2. Both the real sink node and fake sink nodes can generate a set of data packets. The set of data packets generated by the sink node is empty, and its function is to require the ordinary sensor nodes, whether they have data packets or not. The actions of the sink node are shown in Figure 1. This will confuse the tracking routes of adversaries and protect the location privacy of the real sink node to a large extent.

In the PSNL-TNs scheme, there are four types of sensor nodes: the source nodes, the real sink node, the fake sink nodes and the ordinary sensor nodes. By injecting the fake sink nodes, the fake data packets and the request packets, the telemedicine networks will become more complex. Both the real and fake data packets are transmitted along the shortest routes. In a data transmission process, there exist four types of sensor nodes, including the sink node, the ordinary sensor nodes, the fake sink nodes and a source node.

The locations of the sink node and the fake sink nodes are set statically in telemedicine networks. In the data transmission processes of previous schemes, the sink node is only responsible for receiving the data packets; it is the end of a data transmission process. In the PSNL-TNs scheme, the sink node needs to generate and transmit a set of data packets that

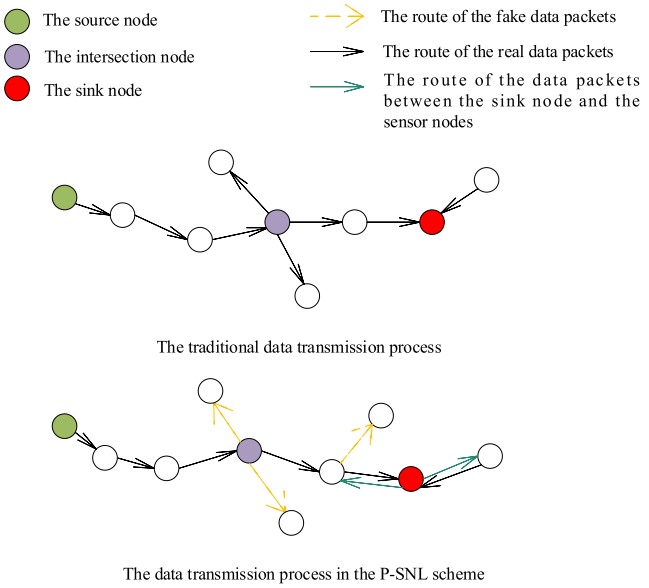

FIGURE 1. The actions of the sink node.

is a set of requirements for data packets to the sensor node in the set of one-hop neighboring nodes of the sink node. This process can help confuse adversaries because they cannot figure precisely determine which node is the end of a data transmission process. Thus, the location privacy of the sink node can be protected to some extent.

At first, the sink node broadcasts a beacon packet, which carriers a number to count the hops, and the initial value of this packet is zero. The beacon packet, which is defined as $\mathcal{B}eacon$, can record the hop count and increase the hop count if it is received by a sensor node. Via the value of the beacon packet, the set of one-hop neighboring nodes of the sink node and the fake sink nodes can be obtained. This beacon packet is delivered to the next sensor node until the value of $\mathcal{B}eacon$ reaches $\mathcal{B}$. In a network, each sensor node holds a transmission range, defined as τ in this paper.

The fake sink nodes in the network should also broadcast a beacon packet to build the fake further lists. The actions of the fake sink nodes are the same as those of the real sink node.

In a data transmission process, the functions of those four node types are indicated below.

The source node can generate data packets.

The sink nodes (either the real sink node or the fake sink nodes) can require for the data packets generated by the source node. In the PSNL-TNs scheme, the data transmission process is bidirectional, which differs from the unidirectional characteristic in the traditional data transmission processes. Via this method, it is more complex for adversaries to find the location of the real sink node because every node in the network can be the start or end of a transmission process. The $\mathcal{B}eacon$ packet will be delivered by a random number of hops.

The actions of the fake sink nodes are the same as those of the real sink node. In a data transmission process, the only difference is that the data packets received by the fake sink

nodes are fake; those data packets are generated by the ordinary nodes in the data delivery routes. The set of fake sink nodes is defined as $f = (f_1, f_2, f_3, \ldots\ldots, f_n)$.

The ordinary nodes are the basis of a network. They coordinate with each other to transmit real data packets; meanwhile, the ordinary nodes will generate a random number of fake data packets when they deliver the real data packets to confuse the tracking route of adversaries. When an ordinary node receives a set of data packets, it will not deliver these data to other nodes immediately. This set of data packets will stay at the ordinary sensor node for a certain time k; during the waiting time k, if this sensor node does not receive the requirement data packets from the sink node, it will be delivered to the next ordinary node along the shortest path. If the ordinary node with data packets receives the request packets from the sink node within the waiting time k, then it will deliver the data packets to the next ordinary node along the shortest route.

The tracking routes of adversaries follow the direction attack scheme [24], which is called Direction Information Line (DIL). The DIL method is used to simulate the tracking processes of adversaries. For a sensor node n, the angle between this node and the DIL is defined as θ_n. Before a set of data packets reaches the real sink node, the set of angles is defined as $\theta = (\theta_1, \theta_2, \theta_3, \ldots\ldots, \theta_n)$. At each sensor node, the value of $Maximize(\theta, DIL)$ is utilized as the evaluation standard for adversaries. Therefore, the routes that are within $Maximize(\theta, DIL)$ may be the real route of a set of data packets. With the DIL scheme, the probability of tracking the real sink node is improved. This method makes our simulations and experiments more convincible.

The set of request packets from the sink node is defined as ERQ. The set of request packets from a fake sink node f_i is defined as ERQ_i. During this transmission period, the delay time for the entire telemedicine network may increase because the sensor node needs to keep the data packets for a short time, no more than k. The sensor node with data packets will transmit them to the sink node via the shortest path.

Based on the PSNL-TNs scheme, Figure 2 shows a concrete example of data delivery processes in a telemedicine network. In Figure 2, two source nodes generate data packets, and they transmit those data packets to the real sink node, routing in the shortest manner. When the data packets are delivered to an ordinary node, this ordinary node will generate a set of fake data packets. The N_f fake data packets will be delivered to a random number of sensor nodes when the ordinary node transmits the real data packets. In this paper, the value of N_f varies from 1 to 3, as shown in Figure 2.

An ordinary node with real data packets will wait for the request packets for a certain time k. If it receives the request packets within time k, then the real data packets will be delivered to the next hop immediately, along with N_f number of sets of fake data packets. This can help to hide the real transmission route. Based on the PSNL-TNs scheme, each node in the telemedicine network can be the sink node. It is

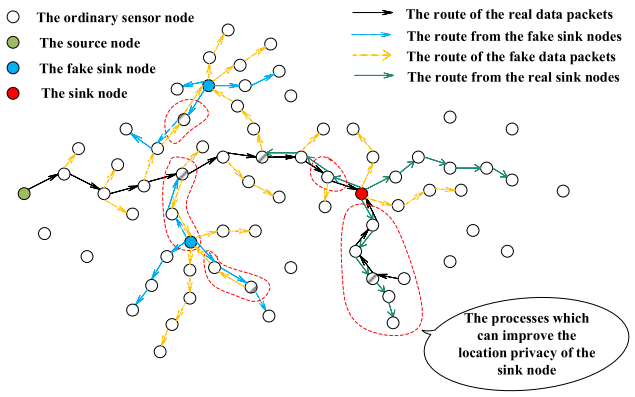

FIGURE 2. The processes of data transmission.

difficult to figure out which one is the end of a transmission process, which means that the location privacy of the sink node can be protected effectively. Moreover, in telemedicine networks, because of the existences of many fake sink nodes and fake data packets, the location privacy of the real sink node can be promised.

In the following subsections, the models in the PSNL-TNs scheme are introduced and formulated.

B. DATA DELIVERY MODEL

In the PSNL-TNs scheme, there are four types of data packets, i.e., the real data packets, the fake data packets, the request packets of the real sink node and the request packets of the fake sink node. In this subsection, the data delivery models of those four types are described.

1. The data delivery model of the real data packets. Obviously, a set of real data packets is generated by an ordinary node. The real data packet set will be delivered to the sink node eventually along the shortest route. By tracing the transmission routes of the real data packets, adversaries can track the location of the sink node. This is the most serious issue for the data transmission processes in telemedicine networks. Before the data packets reach the sink node, there is a probability that they are tracked by adversaries. During this period, the set of angles of each sensor node can be obtained, and we use $Maximize(\theta, DIL)$ as the selection standard. The route of the real packets is in $Maximize(\theta, DIL)$.

2. The data delivery model of the fake data packets. The set of fake data packets is utilized to confuse the tracking routes of adversaries. When a node needs to deliver real data packets to another node, it will generate a set of fake data packets and randomly deliver the fake data packets to other nodes. This can help confuse the tracking routes of adversaries. The fake data packets will eventually be transmitted to the fake sink nodes.

3. The data delivery model of the request packets of the real sink node. In the PSNL-TNs scheme, the sink node can not only receive real data packets but also generate the request packets and deliver this set of packets to other nodes. It will disseminate the request packets to a random number of nodes

to find if they have real data packets or not. The request packets will be delivered to several hops.

4. The data delivery model of the request packets of the fake sink nodes. To maintain consistency, the actions of the fake sink nodes should look the same as the actions of the real sink node. Therefore, the fake sink nodes are also required to generate the request packets. The request packets also need to be delivered to other sensor nodes.

With the injection of fake sink nodes and fake data packets, the location privacy of the sink node can be protected to some extent.

The pseudo-codes of the data delivery model are presented in algorithm 1.

Algorithm 1 Algorithm to Calculate the Data Delivery Model

Input: a source node, time interval ℓ, location of the sink node and number of fake sink nodes
Output: the hops in a data transmission process
1: initialize all the variables
2: the source node generates data packets in time φ
3: transmit the data packets to another node along the shortest route
4: **While** (the next hop is not the real sink node)
5: **For** (x. time = p; p<= ℓ; p = p+a)
// x is a sensor node
6: **If** (x receives the request packets of the sink node)
7: number++;
//record this node, which may be treated as the sink node
8: break;
9: **End if**;
10: **End for**;
11: generating n fake data packets;
12: deliver the real data packets and those fake data packets
13: hop ++;
14: **End while**
15: **output** the value of hop;
16: **output** the value of number;
17: **end**

The pseudocode of the actions of ordinary node is presented in algorithm 2.

Obviously, with the number of fake sink nodes N_f increasing, the routes of the fake data packets will markedly increase at the same time. Therefore, the data delivery time and the energy consumption will increase to some extent. At the same time, the safe time of the real sink node can be improved to a large extent. The experimental comparisons are shown in section 6.

C. SAFE TIME

In this paper, the PSNL-TNs scheme aims to protect the location privacy of the sink node by improving the safe time.

Algorithm 2 Algorithm of Actions of the Ordinary Nodes

Input: a set of real data packets, time interval ℓ, the request packets
Output: the hops in a data transmission process
1: initialize all the variables
2: receive the real data packets.
3: hop-received++;
// the number of received packets increases
4: select-routings to transmit data
//the methods to find the next destination node
5: **If** it finds the closest node in the neighboring nodes of ordinary node
6: **If** (it received the request data from sink node)
7: generate a random number of fake data packets fp
8: deliver real data to the next hop
9: deliver fp to the random sensor nodes
10: delete the real data packets
11: hop++
12: number++; //the number of node which //may be treated as the sink node //will increase
13: **Else**
14: wait for a variable ℓ time and deliver data
15: generate a random number of fake data packets fp
16: deliver fp to the random sensor nodes
17: delete the real data packets
18: hop++
19: **End if**
20: **End if**
21: **End select-routings**
22: **End**

Therefore, in this subsection, the safe time of the sink node in the PSNL-TNs scheme can be calculated by the following equations. In section 4.2, there are four types of data packets. There are four phases in a transmission process. Therefore, the calculation methods of the safe time of the sink node are separated into two parts. In this subsection, the safe time of the sink node in each period is calculated.

In the first period, the source node can generate a set of real data packets. Different from other sensor nodes in the transmission route, the source node will not transmit the set of fake data packets. Therefore, adversaries can track the route of the real data packets until the data packets are received by the first ordinary node. That is the first period. In the first period of data transmission, the probability of the real data packets being successfully traced by adversaries is defined as $\mathcal{P}ro_1$, and the value of $\mathcal{P}ro_1$ is 1.

In the second period of real data transmissions, the data packets are transmitted to the other ordinary sensor nodes

along the shortest routes. In the second period, the nodes can randomly generate fake data packets and deliver those fake packets to other nodes along the shortest routes. This can confuse the tracking routes of adversaries. Suppose that there are N number of nodes in a transmission process. Each ordinary sensor node can generate a set of fake data packets to hide the real transmission route. As is known, more fake data packets will lead to increased energy consumption, which is a side effect of the PSNL-TNs scheme.

In a data transmission process, the set of real data packets is transmitted along the shortest route hop by hop. The number of total hops in the route is defined as N. Obviously, the number of nodes that can generate and disseminate the fake data packets is $N-2$. In the second period, considering the influences of fake data packets only, the minimum probability of adversaries tracing the real route of a set of data packets in a node ℓ can be calculated by equation (5).

$$MIN(\mathcal{P}ro_\ell) = \frac{1}{N_f + 1} \tag{5}$$

Therefore, considering the number of fake data packets only, the minimum probability of the real transmission route for a set of data packets being traced in the second process can be obtained by equation (6).

$$MIN(\mathcal{P}ro_{fd}) = \mathcal{P}ro_\ell^{N-2} = (\frac{1}{N_f + 1})^{N-2} \tag{6}$$

When an ordinary sensor node generates two fake data packets, if the transmission routes are all located in the minimum probability $Maximize\ (\theta, DIL)$, then the probability can be calculated by equation (5). However, with the DIL scheme, the probability of tracing the location of the real sink node may increase. In general, with the PSNL-TNs scheme, the privacy of the real sink node will be improved.

In $\mathcal{P}ro_2$, to weaken the influences of direction attacks, the sink node will generate a set of request packets and transmit it along the shortest route, pretending it is an ordinary node or a source node. We then discuss the influences of the request packets. In this phase, for a data transmission process, any node can be treated as the sink node.

The ordinary node with real data packets needs to wait for the ERQ, and the ordinary node with fake data packets needs to wait for the ERQ_1 within time ℓ. The value of ℓ is limited and is fixed for each ordinary sensor node. In the PSNL-TNs scheme, the fake sink nodes and the real sink node need to deliver a set of request packets to other nodes to hide the location of the sink node. Each sensor node in the transmission route can be regarded as the sink node. In this paper, the fake sink node number N_f in each intersection node is defined as 1 or 3, and the transmission type of the fake data packets is the same as that of the real data packets.

There are two possible situations for the request packets. One is that the sensor node that the request packets are being delivered to does not have the real data packets. In this situation, the request packets will be transmitted to the next sensor node via the shortest route. Another situation is that the ordinary node that the request packets are being delivered to has the real data packets. In this situation, this sensor node will deliver the request packets to another node via the shortest route immediately. Specifically, in the traditional data transmission type, if sensor node A wants to transmit data packets to node B, it must first deliver a set of request packets to B; then, B will give a response message to A; and finally, A can deliver data packets to B. If the transmission process is ordinary node to sink node, then A is the ordinary node and B is the sink node. In the PSNL-TNs scheme, with the existence of request packets, the node B transmits data packets first, and A will deliver real data packets to B, which makes it seem like A is the sink node and B is the ordinary node. This will influence and confuse the tracking routes of adversaries. In a data transmission process ω, the number of sensor nodes in the second situation is defined as $\mathcal{N}_\omega$.

In the previous transmission protocol of data packets, the patterns of the sink node differ from the patterns of other sensor nodes. Therefore, the location of the sink node is easily found. In the PSNL-TNs scheme, the transmission patterns of telemedicine networks have changed. It is difficult to judge which one is the real sink node because of the existence of request packets. In a transmission process of a set of real data packets, considering both the request packets and the fake data packets, the minimum probability of an ordinary node ℓ being treated as the real sink node can be obtained by equation (7).

$$MIN\ (\mathcal{P}ro_\ell) = \frac{1}{N_f + 1} \cdot \frac{1}{\mathcal{N}_\omega} \tag{7}$$

In a data transmission process, considering both the influence factor of fake data packets and the request packets, the calculation methods of the minimum probability $\mathcal{P}ro_2$ can be defined by equation (8).

$$MIN\ (\mathcal{P}ro_2) = \prod_1^\omega (\frac{1}{N_f + 1} \cdot \frac{1}{\mathcal{N}_\omega}) \prod_1^{N-\omega-2} \frac{1}{N_f + 1} \tag{8}$$

According to the calculation methods of $\mathcal{P}ro_1$ and $\mathcal{P}ro_2$, the minimum probability of the location of the sink node being tracked by adversaries can be calculated by equation (9).

$$\mathcal{P}ro = \mathcal{P}ro_1 \cdot \mathcal{P}ro_2 \tag{9}$$

The value of $\mathcal{P}ro_1$ is 1. All the data packets are transmitted along the shortest routes to reduce the energy consumption and shorten the delivery time.

D. ENERGY CONSUMPTION

In telemedicine networks, the factor of energy consumption is a significant issue that can affect the overall network functions. Therefore, in this subsection, the calculation methods of energy consumption are discussed.

The calculation of the energy consumption in a transmission process ρ is shown in equation (10).

$$\mathfrak{E}_\rho = \mathfrak{J}_{eg} \cdot \left(N_{source} + \sum_1^{n-2} N_{\ell f} + N_{rq} + \sum_1^m N_{fq} \right) + \mathfrak{J}_{ef} \cdot (\aleph_{rh} + \aleph_{fh} + \aleph_{sh}) \tag{10}$$

where $\mathcal{J}_{eg}$ indicates the energy consumption when a sensor node generates the data packets or the fake data packets and N_{source} is the number of source nodes in this data transmission process; in a data transmission process, the value of $N_{source} = 1$. $N_{\ell f}$ indicates that a sensor node ℓ can generate $N_{\ell f}$ number of fake data packets, and $\sum_1^{n-2} N_{\ell f}$ is the total number of fake data packets in a data transmission process ρ. N_{rq} represents the number of request packets of the real sink node. N_{fq} indicates the number of request packets of the fake sink nodes. In the simulations, there are 4 fake sink nodes; therefore, the value of m is 4.

In equation (10), the first part is the calculation method of the energy consumption in generating the real data packets and fake data packets. In the second part of equation (10), the symbol $\mathcal{J}_{ef}$ indicates the energy consumption of the data transmission process ρ when a sensor node delivers the data packets, $\aleph_{rh}$ is the hops to the real sink node of the real data packets, $\aleph_{fh}$ is the hops for all the fake data packets in this data transmission, and $\aleph_{sh}$ indicates the hops of the request information ERQ_1 and ERQ generated by the real sink node and the fake sink nodes, respectively. The second part of equation (10) can calculate the energy consumption when a sensor node delivers the data packets.

In equation (10), obviously, the number of fake sink nodes, the number of fake data packets and the number of hops of the request information are three important factors when considering the energy consumption issue of the entire telemedicine network. Based on different values of m, the experiments in section 6 evaluate the results of the energy consumption.

Algorithm 3 Algorithm to Calculate the Value of Energy Consumptions

Input: values of $\mathcal{J}_{eg}$, $\mathcal{J}_{ef}$, N_{source}, $N_{\ell f}$, N_{rq}, and N_{fq}, obtain the value of hop, the value of number in algorithm 1.
Output: the value of energy consumption
1: initialize all the variables
2: $N_{\ell f} =$ hop – 2;
3: $N_{rq} =$ a;
// in the simulation, the value of N_{rq} is 3.
4: $N_{fq} = \sum_1^z N_{zq}$
// calculate the total number of request packets of
// the fake sink nodes
5: $\mathfrak{E}_\rho = \mathcal{J}_{eg} \cdot \left(N_{source} + \sum_1^{n-2} N_{\ell f} + N_{rq} + \sum_1^m N_{fq}\right) + \mathcal{J}_{ef} \cdot (\aleph_{rh} + \aleph_{fh} + \aleph_{sh})$
6: **output** the value of $\mathfrak{E}_\rho$ for process ρ
7: **end**

The pseudo-code of the energy consumptions is presented in algorithm 3.

E. DATA DELIVERY TIME

Data delivery time is the time consumption of the real data packets. In the PSNL-TNs scheme, the delivery time of a data transmission process is another important influence factor that can affect the functions of telemedicine networks. In a data transmission process, each sensor node in the transmission route needs to hold a time interval ℓ. Within the time interval ℓ, the sensor node with real data packets will wait for the request packets. If it receives the request packets, then the real data packets will be delivered to the next sensor node immediately along the shortest transmission route, along with N_f number of fake data packets. This type of data transmission process will improve the safe time of the sink node to a large extent but will result in an increase in the data delivery time because of the time interval ℓ.

We use hops as the measurement of the data delivery time. The one-hop time when a node delivers a set of data packets is defined as d_t. In a data transmission process, there are $\mathcal{N}_\omega$ number of sensor nodes that need not waits for time ℓ because those sensor nodes can receive request packets within time ℓ. In a data transmission process, the maximum delivery time can be calculated by equation (11).

$$MAX\ (T_d) = (N - 2) \cdot (\ell + d_t) \tag{11}$$

where N is the total number of sensor nodes in the real data transmission route. The calculation method of the minimum delivery time in the real transmission process is defined in equation (12).

$$MAX\ (T_d) = (N - 2) \cdot d_t = \mathcal{N}_\omega \cdot d_t \tag{12}$$

In equation (11), ideally, the minimum delivery time is that in the real data transmission route, except for the real sink node and the source node, all the other sensor nodes can receive the request packets of the real sink node. They do not need to wait for a time interval ℓ. Therefore, the number of $\mathcal{N}_\omega$ is $N - 2$.

The pseudocode of the actions of sink node is presented in algorithm 4.

Algorithm 4 Algorithm of the Actions of Sink Node

Input: data packets
Output: request packets
1: initialize all the variables
2: generate a random number of request packets rq
3: randomly generate destinations
4: send rq to these destinations
5: delete rq
6: **If** (sink node receives a set of data packets)
7: dp-received++; //the number of packets that the
//sink node received
will increase
8: generate a random number of request packets rq
9: randomly generate destinations
10: send rq to random neighboring nodes
11: delete rq;
12: **End if**
13: **ends**

F. COMPUTATIONAL COMPLEXITY

In this subsection, the computational complexity is discussed to evaluate the performances of the PSNL-TNs scheme. For a set of data packets, suppose there are N number of ordinary nodes will cooperate with each other to deliver it to the sink node in the telemedicine networks, then the computational complexity is $O(N)$.

V. EXPERIMENTAL ANALYSIS

In this section, we will demonstrate the effectiveness of the PSNL-TNs scheme by not only theoretical analysis but also simulation experiments. In section 5.2, the calculation methods of the safe time, energy consumption and data delivery time of the PSNL-TNs scheme are given to illustrate and compare the theoretical performances. In section 5.3, the performances of the PSNL-TNs scheme are analyzed by experiments and simulations, and we compare the experimental results of the PSNL-TNs scheme with those of the methods proposed in [24] to show the superiority and effectiveness.

All the simulation programs are implemented in C++. In the experiments, 420 nodes are distributed randomly in a cycle with a radius of 420. The communication range τ of each sensor node is defined as 15 in the networks. The locations of the real sink node are set randomly in the sensor networks. The fake sink nodes are distributed according to the distribution methods in [24]. Because of the delivery schemes in the PSNL-TNs networks, it is difficult for adversaries to trace the routes of real data packets. The safe time of the real sink node, the delivery time and the energy consumption of the entire networks are compared with those attained by the methods in [24]. Moreover, we take some influence factors into consideration, for example, the number of fake sink nodes has a great influence on the safe time and the energy consumption. The number of fake sink nodes and the number of fake data packets of a node ℓ can result in increasing safe time and energy consumption. However, because the real data packets are routed along the shortest routes, the number of fake sink nodes has no relationship with delivery time. We should balance those factors by comparing the experimental results to achieve the best performances of the entire sensor networks. In each ordinary node, the number of fake sink nodes is 2 or 3.

The performances of the PSNL-TNs scheme is analyzed for each index.

A. SAFE TIME ANAYSIS

In sensor networks, it is necessary to protect the location privacy of the sink node and improve the safe time of the entire network. Therefore, in this paper, the PSNL-TNs scheme mainly concentrates on improving the safe time of the real sink node, and several fake sink nodes are inserted into the networks to confuse the adversaries. The delivery actions of the sink node or the fake sink nodes are redefined in this paper to improve the location privacy. When adversaries trace the location of the sink node, it will stay at this node and return a "successful" message. Therefore, if adversaries stay at a sensor node for more than β, then this node is seen as the real sink node by the adversaries. Then, we need to judge if this node is the real sink node or not in the experiment. Based on different numbers of fake data packets and fake sink nodes, the safe time of the real sink node differs. Compared with the methods in [24]. The improvement percentage of safe time is defined as I_{stime}. the safe time can be improved.

B. DELIVERY TIME ANAYSIS

The delivery time is also an important factor in the sensor systems. In the PSNL-TNs scheme, because of the existence of fake sink nodes and the changes in the delivery model of the sink node, the delivery time of the PSNL-TNs scheme will increase. In this paper, we also use the hops to evaluate the delivery time of a data transmission process. d_t is the one-hop transmission time. Therefore, based on equations (11) and (12), the delivery time of the PSNL-TNs scheme is shown in equation (13).

$$\mathcal{N}_\omega \cdot t_h \leq T_d \leq (N-2) \cdot (\ell + d_t) \tag{13}$$

In the entire network, the delivery time is obtained as shown in equation (14).

$$\mathcal{T}_{PSNL-TNs} = \sum_{t=1}^{N_{source}} T_d \tag{14}$$

where N_{source} indicates the number of data transmission processes.

To reduce the probability of the real sink node being traced, the method in [24] takes a random walk for the real data packets. This will result in increasing the data delivery time markedly. In the PSNL-TNs scheme, the healthy information is delivered along the shortest route. Therefore, although it will take some time in each ordinary node of the shortest route, the delivery time can be reduced to some extents.

C. ENERGY CUNSUMPTION ANAYSIS

In the PSNL-TNs scheme, the real data packets are transmitted along the shortest route, and compared with the method in [24], the delivery time can be reduced to a large extent. The reduction of delivery time is defined as R_{dtime}.

The energy consumption of the PSNL-TNs scheme is compared with the consumption of the SP-DA schemes [24] in this subsection.

In [24], the fake data packets are generated in the intersection nodes, which is unreliable in real network systems. Each node in a network is an intersection node, as it can both transmit data packets and receive data packets.

D. EVALUATION METRIC

The energy consumptions in a data transmission process is divided into two parts: the energy consumption when generating a set of data packets and the consumption when delivering a set of data packets. Because of the existence of the fake data packets and the request packets, the energy consumption in

the PSNL-TNs scheme might increase to some extent compared with the schemes in [24]. The comparison of energy consumptions is defined as E_{ec}.

After computing I_{stime}, R_{dtime} and E_{ec} in the above three subsections, in this subsection, to comprehensively evaluate the performances of the PSNL-TNs scheme, the metric $\mathfrak{S}_{measure}$ is utilized set as a standard of those three-evaluation metrics. The calculation method of $\mathfrak{S}_{measure}$ can be derived by the following equation.

$$\mathfrak{S}_{measure} = \frac{|2 \cdot I_{stime} \cdot R_{dtime} + 2 \cdot I_{stime} \cdot E_{ec} + 2 \cdot R_{dtime} \cdot E_{ec}|}{|I_{stime}| + |R_{dtime}| + |E_{ec}|} \tag{15}$$

According to equation (15), the performance of the PSNL-TNs scheme can be evaluated comprehensively. Clearly, if the value of $\mathfrak{S}_{measure}$ is higher, the performance of the PSNL-TNs scheme is better.

VI. EXPERIMENTAL RESULTS OF THE PSNL-TNS SHCEME

In this section, the performance of the PSNL-TNs scheme is compared with those of the SP-DA schemes in [24]. The safe time of the real sink node, the delivery time and the energy consumption are compared with the SP-DA schemes, respectively. Moreover, we compare the performance of PSNL-TNs based on different numbers of fake sink nodes. The comparisons of safe time are illustrated in subsection 6.1, the delivery time of the PSNL-TNs scheme is compared with that of the SP-DA scheme in subsection 6.2, and the comparisons of energy consumption are presented in subsection 6.3.

A. COMPARISIONS OF SAFE TIME

In this subsection, we compare the safe time of the PSNL-TNs scheme with that of the SP-DA scheme. The number of fake sink nodes and the number of fake data packets have impacts on the safe time.

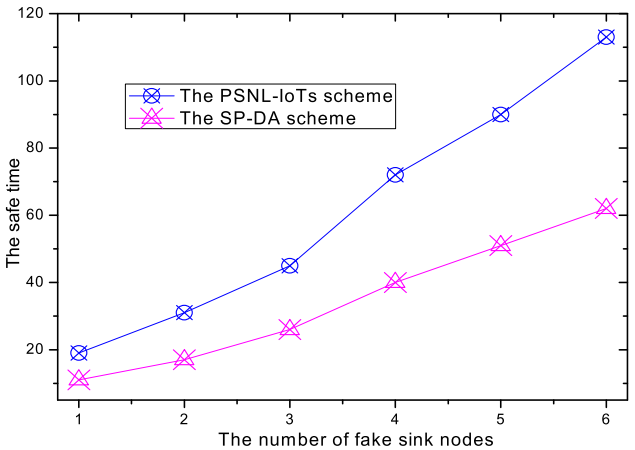

FIGURE 3. The comparisons of safe time based on the PSNL-TNs and the SP-DA schemes in [24] for different numbers of fake sink nodes.

Based on the PSNL-TNs scheme and the SP-DA scheme, under different numbers of fake sink nodes, the safe time of the entire sensor systems is compared in a data transmission process, as shown in Figure 3.

Figure 3 clearly shows that under different values of fake sink nodes, the safe time of the PSNL-TNs scheme can be improved to a large extent compared with that of the scheme in [24]. With an increasing number of fake sink nodes, the improved safe time increases. This is because, as the number of fake sink nodes increases, the number of request packets of the fake sink nodes will increase, which makes the location of the real sink node hard to find. The actions of a fake sink node are the same as those of the real sink node, and the actions of the request packets of the fake sink nodes are the same as those of the request packets of the real sink node. Thus, if the sensor node with fake data packets can receive the request packets of the fake sink nodes within the waiting interval ℓ, then this node may be treated as the sink node. Therefore, the probability of the real sink node being traced can be decreased, and the safe time can be improved. The methods in [24] do not have the requirement of fake sink nodes. It improves the safe time by only inserting the fake data packets and lengthening the transmission routes of a set of real data packets. As the number of fake sink nodes increases, the gap between the PSNL-TNs scheme and the methods in [24] becomes larger, which indicates that the PSNL-TNs scheme has better performance with larger number of fake sink nodes especially. The improvement percentage ranges from 43.11% to 51.11%.

With the improved percentages of safe time, when the number of fake sink nodes is 4, the performance of the PSNL-TNs scheme reaches its best. Then, with different numbers of source nodes, the performance of the PSNL-TNs scheme is compared with that of the methods in [24]. The comparisons are shown in Figure 4.

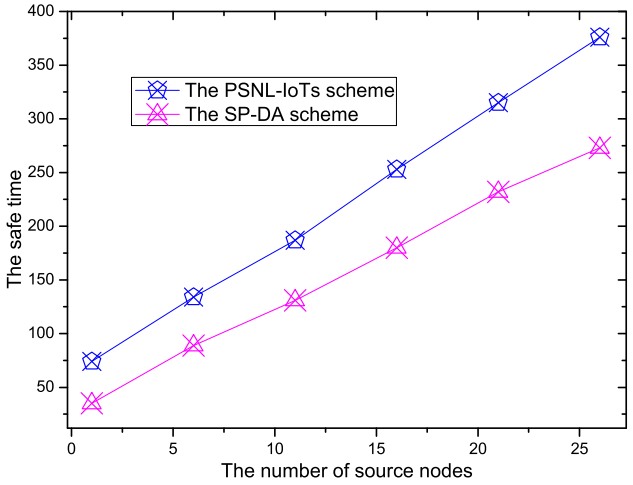

FIGURE 4. The comparisons of safe time based on the PSNL-TNs and the SP-DA schemes in [24] for different numbers of source nodes.

In Figure 4, with the number of source nodes increasing, the safe times of both the PSNL-TNs scheme and the SP-DA scheme are increasing, and the gap between those two schemes is becoming greater. This is because, as the number of source nodes increases, based on the same number of fake sink nodes, the number of ordinary sensor nodes in

the transmission routes will increase. Therefore, there are more ordinary nodes that could be treated as the sink node. Moreover, the number of fake data packets, fake request packets ERQ_i and real request packets ERQ will increase at the same time, which ensures that the location of the real sink node will be hard to find. According to the evaluation methods in sections 4 and 5, the probability of adversaries tracking the real sink node will be reduced compared with the SP-DA scheme. Thus, the safe time of the entire sensor system is improved. With different numbers of source nodes, the PSNL-TNs scheme shows the validity and advancement over the SP-DA schemes. The improvement percentage of the safe time ranges from 28.57% to 52.70%.

When the number of source nodes is 6, based on different numbers of fake data packets, the performance of the PSNL-TNs scheme is compared with that of the SP-DA scheme in [24]. In the simulations, the number of fake data packets of each sensor node is defined as 2 or 3. Based on different numbers of fake data packets, the comparisons are shown in Figure 5.

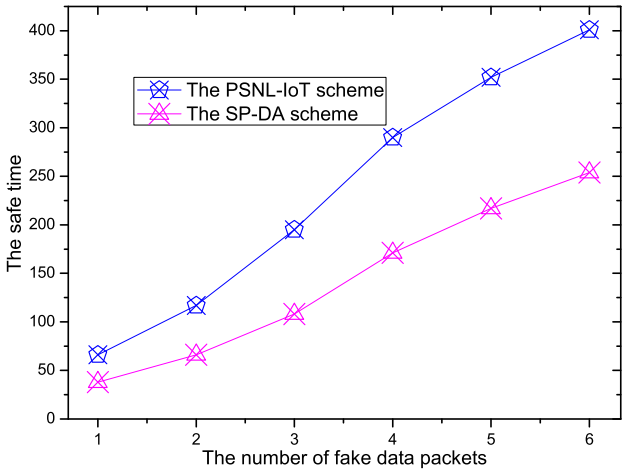

FIGURE 5. The comparisons of safe time based on the PSNL-TNs and the SP-DA schemes in [24] for different numbers of fake data packets.

In Figure 5, as the number of fake data packets increases, the safe times of both the PSNL-TNs scheme and the SP-DA scheme will increase. This is because more fake data packets will confuse the tracking routes of the adversaries. As the number of fake data packets increases, the gap between the PSNL-TNs scheme and the SP-DA scheme becomes greater. This is because more fake data packets can generate more ''sink nodes''. The number of sensor nodes with fake data packets increases, and the probability of those sensor nodes receiving the request packets of the fake sink nodes could increase. Therefore, those sensor nodes might be treated as the sink node. Moreover, in the methods in [24], the fake data packets are generated in the intersection nodes, which is not an option in real sensor systems, and this can reduce the energy consumption to some degree. However, the SP-DA scheme utilizes a random walk for the real data packets, which will markedly increase the energy consumption. In addition, with the number of fake data packets increasing, the safe time of the PSNL-TNs scheme will be improved more than that of the SP-DA schemes, which demonstrates the efficiency of the PSNL-TNs scheme. However, with the number of fake data packets increasing, the energy consumption will improve, which is a side effect of both schemes. The improvement percentage of the safe time ranges from 36.66% to 42.42%.

Based on different numbers of fake sink nodes, source nodes and fake data packets, respectively, simulations are made to compare the safe times of the PSNL-TNs scheme and the SP-DA schemes, which demonstrates the effectiveness and advancements of our scheme.

B. COMPARISIONS OF DELIVERY TIME

In this subsection, the delivery time of the PSNL-TNs scheme is compared with that of the SP-DA scheme. In the sensor systems, the delivery time is an important factor to consider and can influence the entire performance of a network. The PSNL-TNs scheme utilizes the shortest routes while delivering the real data packets. However, because of the existence of the waiting interval ℓ, the delivery time of the real data packets will increase compared to the shortest routes without waiting time in the traditional transmission protocols. However, compared with the methods of the SP-DA scheme in [24], the delivery time can be reduced. This is because the SP-DA scheme utilizes a random walk when delivering the real data packets. Meanwhile, in [24], the real data packets also need to wait a time interval at a sensor node. Those two factors lead to the delivery time of the SP-DA methods being greater than that of the PSNL-TNs scheme.

Once a data transmission process is decided, the ordinary sensor nodes in the transmission route are decided. Therefore, the hops in the real data transmission route can be obtained. Thus, the delivery time is related to the value of the waiting time interval ℓ in each sensor node. The numbers of fake sink nodes, fake data packets and request packets of the fake sink nodes have no relationship with the performance of the PSNL-TNs scheme. The delivery time of the PSNL-TNs scheme is compared with that of the SP-DA schemes based on different values of the waiting time interval ℓ. When the number of source nodes is 1 and the number of fake sink nodes is 4, the comparisons of delivery time are as shown in Figure 6.

In Figure 6, when the number of source nodes is 1, based on different values of ℓ, the comparisons of the two schemes are presented clearly. When the value of the time interval ℓ increases, the delivery times of both schemes will increase. This is because, as ℓ increases, more time will be spent waiting. In the PSNL-TNs scheme, the set of real data packets waits for the request packets, but in the SP-DA scheme, it waits for nothing and is intended to simply confuse the adversaries. With the value of time interval increasing, the gap between those two schemes is growing, which shows the efficiency of the PSNL-TNs scheme. With the PSNL-TNs scheme, the delivery time of the real data packets can be

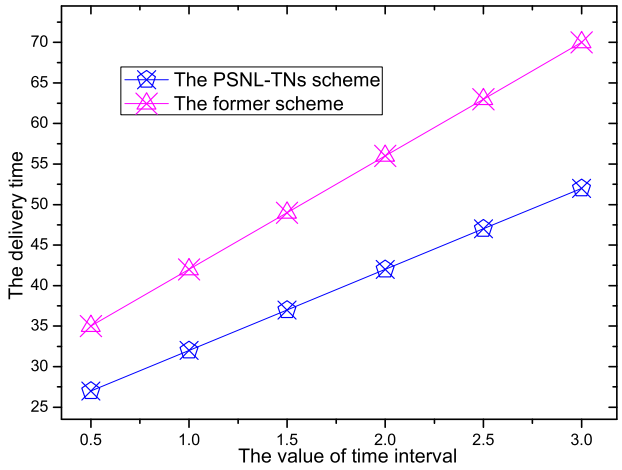

FIGURE 6. The comparisons of delivery time based on the PSNL-TNs and the SP-DA schemes in [24] for different values of k.

reduced to a large extent. In the simulations, we set the value of k to 0.5 to perform the experiments, aiming to reach the minimum delivery time while transmitting data packets. Moreover, in the simulations of the PSNL-TNs scheme, one sensor node in the transmission route can reach the request packets of the real sink node within the time interval k, and this will confuse the adversaries and improve the privacy of the real sink node. The PSNL-TNs scheme can reduce the delivery time and protect the location privacy of the sink node at the same time. When the number of source nodes is 1, based on different values of the time interval, the reduction percentage of the delivery time ranges from 22.86% to 25.71%.

With different values of k, the delivery time can be reduced by a large percentage, which is shown in Figure 7.

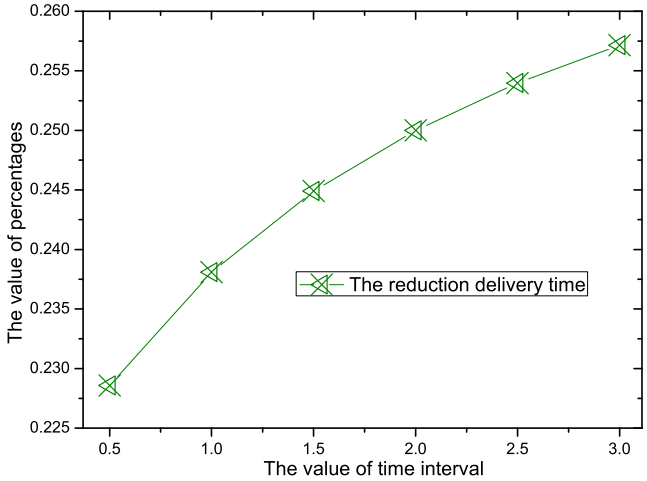

FIGURE 7. The comparisons of data delivery time in the PSNL-TNs scheme with different values of k.

In Figure 7, with the PSNL-TNs scheme, the delivery time can be reduced based on different values of k, which shows the efficiency of the PSNL-TNs scheme.

To further evaluate the performance of the PSNL-TNs scheme, based on different numbers of source nodes, the delivery time of the PSNL-TNs scheme is compared with that of the SP-DA schemes. The comparisons are shown in Figure 8.

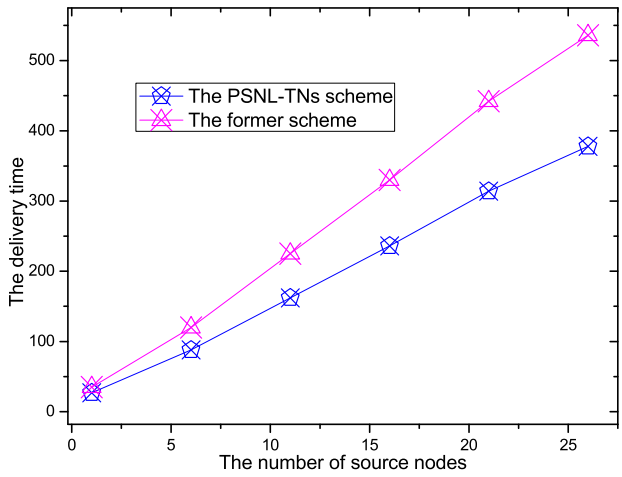

FIGURE 8. The comparisons of delivery time based on the PSNL-TNs and the SP-DA schemes in [24] for different numbers of source nodes.

In Figure 8, as the number of source nodes increases, the delivery times of both the PSNL-TNs scheme and the SP-DA scheme increase, and the gap between those two schemes is growing greater at the same time. This is because the transmission methods in the SP-DA schemes take a random route to transmit the real data packets, which will markedly result in increasing the delivery time, while in the PSNL-TNs scheme, the real data packets are transmitted along the shortest routes. The sensor nodes with data packets in both schemes need to hold for a time interval. If a sensor node with data packets in the PSNL-TNs scheme can receive the request packets within time interval, it can deliver the data packets to the next sensor node immediately. Therefore, the general waiting time of the PSNL-TNs scheme is either the same as that of the SP-DA scheme or shorter than that of the SP-DA scheme. In general, the delivery time of the PSNL-TNs scheme can be reduced to a great extent, based on different numbers of source nodes. The reduction percentage of the delivery time ranges from 22.86% to 27.61%.

The number of request packets of the sink node also has a relationship with the delivery time. In general, if the number of request packets is greater, the probability that the sensor nodes that are in the transmission route reach those requests is greater. Thus, that type of sensor nodes does not need to wait for the time interval k. The total delivery time will decrease. The influences of the time interval k are evaluated in this section to demonstrate the efficiency of the PSNL-TNs scheme. The evaluations are shown in Figure 9.

In Figure 9, clearly, as the number of source nodes increases, the number of sensor nodes that can receive the request packets of the real sink node increases. This can not only reduce the delivery time while transmitting data packets but also effectively improve the safe time of the entire system, which demonstrates the advancements of the

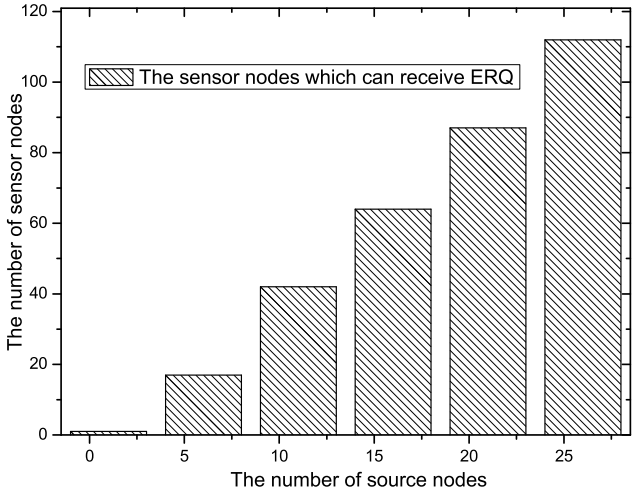

FIGURE 9. The number of sensor nodes that can receive the request packets within the time interval ℓ based on different numbers of source nodes.

PSNL-TNs scheme in this paper. Because of the request packets, the reduction proportion of delivery time in the PSNL-TNs scheme ranges from 3.70% to 29.63%.

The comparisons of delivery time of each data transmission process are shown in Figure 10.

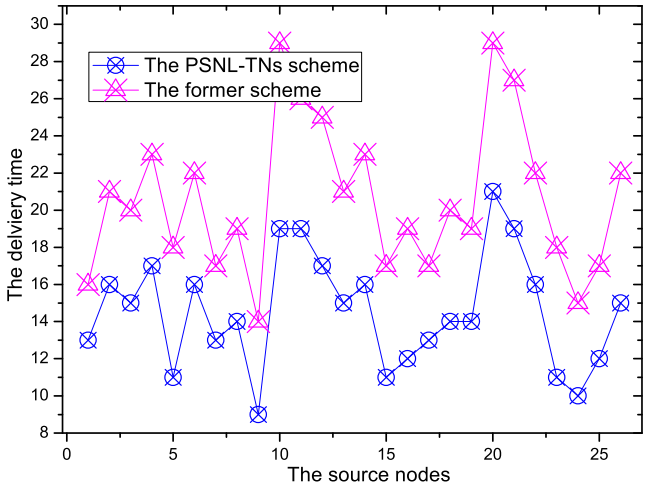

FIGURE 10. The comparisons of delivery time of each data delivery process.

Figure 10 shows that, based on different data transmission processes, the delivery time in the PSNL-TNs scheme is less than that in the SP-DA scheme, which demonstrates the efficiency of the PSNL-TNs scheme.

In this subsection, we evaluated the performance of the delivery time in the PSNL-TNs schemes. The value of the time interval ℓ and the number of source nodes have influences on the results of the delivery time. By comparing the simulation results with the SP-DA schemes, the PSNL-TNs scheme shows its superiority. The delivery time can be reduced to a large extent, and the sink node can be protected for a longer period.

C. COMPARISIONS OF ENERGY CONSUMPTIONS

In this subsection, the energy consumption of the PSNL-TNs scheme is compared with that of the SP-DA scheme. In the sensor systems, the energy consumption is an important issue that has a great influence on the entire system. In the PSNL-TNs scheme, because of the existence of the fake sink nodes, the fake data packets, and the request information of the sink nodes and the fake sink nodes, the energy consumption might increase compared with that of the SP-DA schemes. In this paper, we consider each sensor node in a data transmission hop to take the same energy consumption. Therefore, the energy consumption can be obtained by calculating the hops in the data delivery routes. The energy consumption when generating a set of data packets is the same. The number of fake sink nodes, the number of fake data packets and the number of request packets have influences on the evaluation results of energy consumption.

Based on different numbers of fake sink nodes, when the number of source nodes is 1, the energy consumption of the PSNL-TNs scheme is compared with that of the SP-DA scheme in [24]. The comparisons are shown in Figure 11.

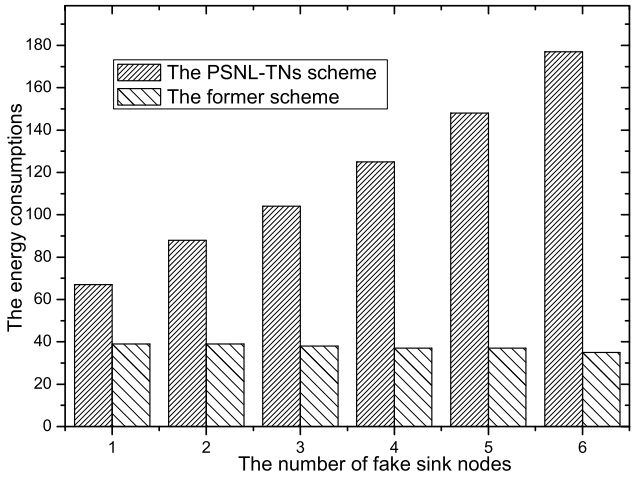

FIGURE 11. The value of energy consumption with different numbers of fake sink nodes.

In Figure 11, clearly, the number of fake sink nodes has a great influence on the energy consumption of the PSNL-TNs scheme. As the number of fake sink nodes increases, the value of the PSNL-TNs scheme increases. This is because the fake sink nodes must generate request packets (similar to the actions of the real sink node) and transmit those request packets to other sensor nodes. Those actions will involve a large amount of energy consumption, which is a side effect in the PSNL-TNs scheme.

Then, based on different numbers of source nodes, when the number of fake sink nodes is 1, the energy consumption of the PSNL-TNs scheme is compared with that of the SP-DA scheme, as shown in Figure 12.

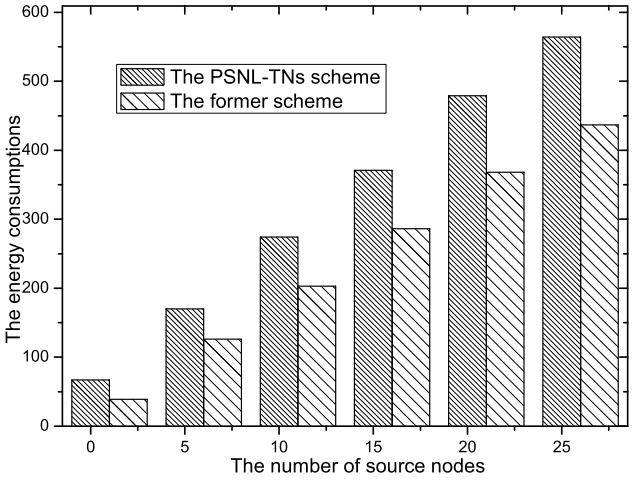

FIGURE 12. The value of energy consumption with different numbers of source nodes when the number of fake sink nodes is 1.

In Figure 12, as the number of source nodes increases, the energy consumptions of those two schemes increase at the same time. This is because the generation of more data packets and transmission of more data packets (whether they be real or fake data packets) will markedly lead to the consumption of more energy. The energy consumption of the PSNL-TNs scheme is greater than that of the SP-DA schemes, whatever the number of source nodes is. This is because, in the SP-DA scheme, the fake sink nodes need not generate the request packets and transmit them. The fake data packets are generated in the intersection nodes, which is unreliable in real systems. Although the PSNL-TNs scheme will require more energy consumption, the PSNL-TNs scheme is more practical and safer in real systems.

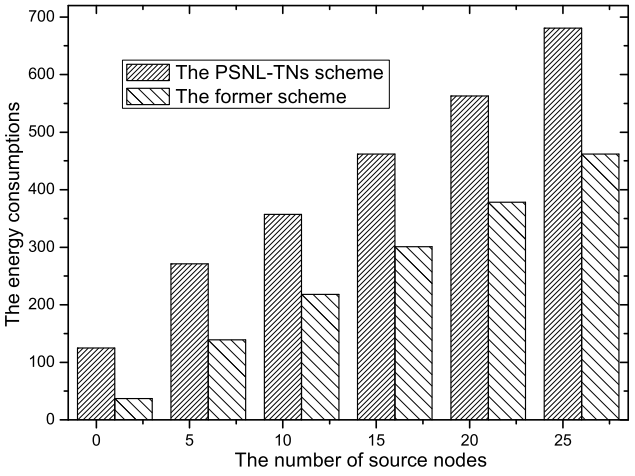

FIGURE 13. The value of energy consumption with different numbers of source nodes when the number of fake sink nodes is 4.

Then, to further evaluate the energy consumption of the PSNL-TNs scheme, when the number of fake sink nodes is 4, comparisons of the PSNL-TNs scheme and the SP-DA scheme are as shown in Figure 13.

The tendency in Figure 13 is the same as that in Figure 10. Based on the number of fake sink nodes being 4, compared with the energy consumption when the number of fake sink nodes is 1, the simulation results show that the energy consumptions of both schemes increase. With calculations, the gap in energy consumption between those two situations increases. The side effect of the PSNL-TNs scheme is that, with more fake sink nodes, the energy consumption will increase more than that of the SP-DA scheme. This is because the fake sink nodes in the PSNL-TNs scheme need to generate request packets and transmit them, which will cost energy. In future works, we will focus on reducing the energy consumption as well as protecting the privacy of the sink node.

The energy consumption is related to the number of fake data packets; in the above simulations, the number of fake data packets is either 2 or 3 in a sensor node. More fake data packets will lead to greater energy consumption. Although more fake data packets can improve the privacy level of the entire system, the energy consumption is a significant factor in the functioning of systems. In the PSNL-TNs scheme, we evaluated the energy consumption based on different numbers of fake data packets when the number of fake sink nodes is 4 and the number of source nodes is 1. The evaluation results are shown in Figure 14.

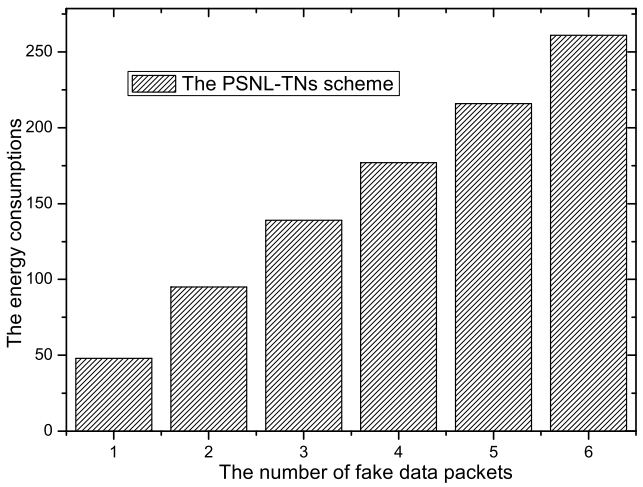

FIGURE 14. The value of energy consumption based on different numbers of fake data packets in the PSNL-TNs scheme.

In Figure 14, as the number of fake data packets increases, the value of energy consumption increases. More fake data packets will lead to more energy consumption because those fake data packets need to generate request packets and deliver them to confuse the tracking route of the adversaries. The energy consumption issue needs to be further researched to obtain better performance in sensor systems.

The number of request packets also has an impact on the performance of the energy consumption. More request packets of the sink node can result in more energy consumption. In the above simulations, the sink node (both the real sink

node and the fake sink nodes) generates three sets of data packets a period to confuse the adversaries and protect the location of the sink node. In the whole simulations and experiments, the number of request packets at one period is set as 3. To avoid repetition, it is not explored in this subsection.

D. THE VALUE OF THE EVALUATION METRIC $\mathfrak{S}_{measure}$

In this subsection, the performance of the PSNL-TNs scheme is evaluated comprehensively via equation (15). Based on different values, when the number of fake sink nodes is 1, 6, 11, 15, 21, and 26, respectively, the safe time, data delivery time and energy consumption are as shown in Figure 15. The comparison of the metric $\mathfrak{S}_{measure}$ is shown in Figure 16.

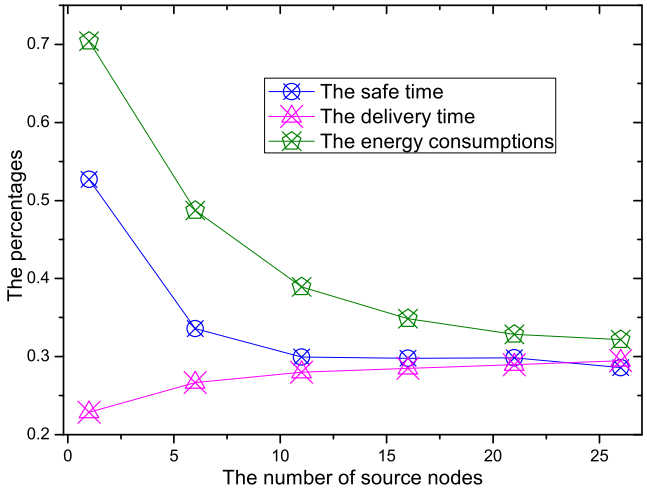

FIGURE 15. The performances of the safe time, delivery time and energy consumption.

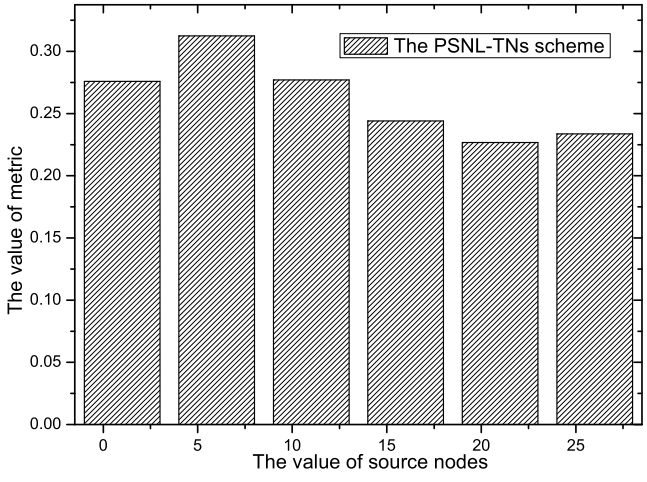

FIGURE 16. The value of the metric $\mathfrak{S}_{measure}$ based on different numbers of source nodes.

In the Figure 15, with the number of source nodes increases, the ratio of safe time and ratio of energy consumptions are decreased. And the ratio of delivery time will be increased. With simulations, those three evaluation factors will stay at a static level to some extents, which show the efficiency of the proposed scheme.

In Figure 16, based on different numbers of source nodes, the value of the metric $\mathfrak{S}_{measure}$ is evaluated. The improved percentage of the PSNL-TNs scheme ranges from 22.67% to 27.70%, which demonstrates the effectiveness of the PSNL-TNs scheme in this paper.

If we only consider the safe time and delivery time comprehensively, the performance of the PSNL-TNs scheme is as shown in Figure 17.

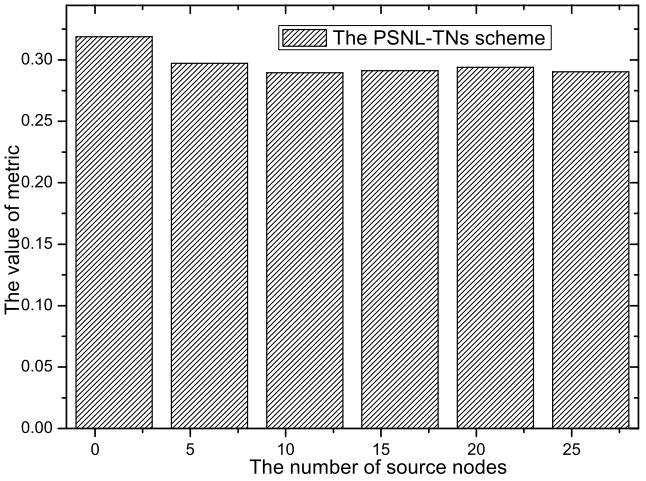

FIGURE 17. The value of evaluations based on the safe time and delivery time under different numbers of source nodes.

Figure 17 shows that after combining the safe time and delivery time comprehensively to evaluate the performance of the PSNL-TNs scheme, the improvement percentage ranges from 28.94% to 31.89%, which indicates that, with the PSNL-TNs scheme, the safe time can be improved and the delivery time can be reduced. The performances suit the original motivations of this research.

To further prove the performance, Table 2 provides experimental results.

TABLE 2. The experimental results of safe time, delivery time and $\mathfrak{S}_{measure}$.

Value	$source = 1$	$source = 6$	$source = 11$	$source = 16$	$source = 21$	$source = 26$
Safe time	0.527	0.336	0.30	0.298	0.298	0.285
Delivery	0.229	0.267	0.28	0.285	0.290	0.295
$\mathfrak{S}_{measure}$	0.276	0.312	0.277	0.244	0.227	0.234

The PSNL-TNs scheme can improve the security level of the telemedicine networks, as well as reducing the energy consumptions and delivery time to some extents. However, both the real sink node and the fake sink nodes require more energy compared with other schemes in the telemedicine networks, which is the demerits of the PSNL-TNs scheme. It is because that the sink node need to generate and deliver the empty data packets to confuse the adversaries. Based on different number of source nodes, when the number of fake

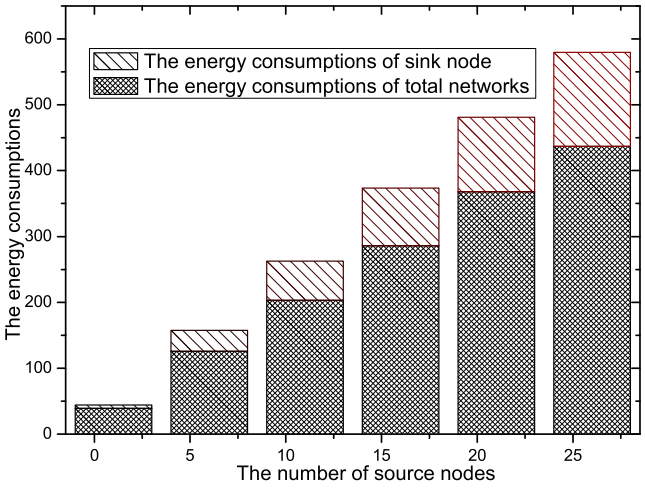

FIGURE 18. **The energy consumptions of the sink node based on different number of source nodes.**

sink node is 1, the energy consumptions of the real sink node are shown in the Figure 18.

VII. CONCLUSION

In this paper, we propose a "Privacy-Preserving Protocol of Sink Node Location in wireless sensor networks," called the PSNL-TNs scheme, which inserts fake sink nodes and the request information of the sink node and the fake sink nodes. Based on the PSNL-TNs scheme, the safe time of the networks will increase, which protects the location privacy of the sink node effectively. Meanwhile, the delivery time of the data packets will be reduced. In section 6, experiments and simulations demonstrate the effectiveness and advancements of the PSNL-TNs scheme in this paper.

With the advancement of telemedicine networks, adversaries in such networks are searching for the location of the sink node to seek more information, and moreover, some of the adversaries may attack the sink node and cause the entire network to crash. Therefore, the location privacy of the sink node is becoming a hot and significant issue. It is necessary to improve the safe time of the sink node. Security is a key requirement in telemedicine networks. The PSNL-TNs scheme gives a better solution to the security of the sink node, which make sense practically.

REFERENCES

[1] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 73–81, Apr. 2006.

[2] P. D. Jani *et al.*, "Evaluation of diabetic retinal screening and factors for ophthalmology referral in a telemedicine network," *JAMA Ophthalmol.*, vol. 135, no. 7, pp. 706–714, 2017.

[3] C. Huang, M. Ma, Y. Liu, and A. Liu, "Preserving source location privacy for energy harvesting WSNs," *Sensors*, vol. 17, no. 4, p. 724, 2017, doi: 10.3390/s17040724.

[4] S. Kumar, S. K. Singh, A. K. Singh, S. Tiwari, and R. S. Singh, "Privacy preserving security using biometrics in cloud computing," *Multimedia Tools Appl.*, vol. 77, no. 9, pp. 11017–11039, 2018, doi: 10.1007/s11042-017-4966-5.

[5] X. Liu, S. Zhao, A. Liu, N. Xiong, and A. V. Vasilakos, "Knowledge-aware proactive nodes selection approach for energy management in Internet of Things," *Future Gener. Comput. Syst.*, to be published, doi: 10.1016/j.future.2017.07.022.

[6] Y. Liu, A. Liu, S. Guo, Z. Li, Y.-J. Choi, and H. Sekiya, "Context-aware collect data with energy efficient in cyber–physical cloud systems," *Future Gener. Comput. Syst.*, to be published, doi: 10.1016/j.future.2017.05.029.

[7] B. Cao, J. Zhao, Z. Lv, and X. Liu, "3D terrain multiobjective deployment optimization of heterogeneous directional sensor networks in security monitoring," *IEEE Trans. Big Data*, to be published, doi: 10.1109/TBDATA.2017.2685581.

[8] A. Liu, M. Huang, M. Zhao, and T. Wang, "A smart high-speed backbone path construction approach for energy and delay optimization in WSNs," *IEEE Access*, vol. 6, no. 1, pp. 13836–13854, 2018, doi: 10.1109/ACCESS.2018.2809556.

[9] Y. Liu *et al.*, "QTSAC: An energy-efficient MAC protocol for delay minimization in wireless sensor networks," *IEEE Access*, vol. 6, no. 1, pp. 8273–8291, 2018

[10] J. Tang, A. Liu, J. Zhang, Z. Zeng, N. Xiong, and T. Wang, "A security routing scheme using traceback approach for energy harvesting sensor networks," *Sensors*, vol. 18, no. 3, p. 751, 2018, doi: 10.3390/s18034751.

[11] Z. Li, B. Chang, S. Wang, A. Liu, F. Zeng, and G. Luo, "Dynamic compressive wide-band spectrum sensing based on channel energy reconstruction in cognitive Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2598–2607, Jun. 2018, doi: 10.1109/TII.2018.2797096.

[12] A. Mehmood, Z. Lv, J. Lloret, and M. M. Umar, "ELDC: An artificial neural network based energy-efficient and robust routing scheme for pollution monitoring in WSNs," *IEEE Trans. Emerg. Topics Comput.*, to be published, doi: 10.1109/TETC.2017.2671847.

[13] A. Liu, X. Liu, T. Wei, L. T. Yang, S. Rho, and A. Paul, "Distributed multi-representative re-fusion approach for heterogeneous sensing data collection," *ACM Trans. Embedded Comput. Syst.*, vol. 16, no. 3, 2017, Art. no. 73, doi: 10.1145/2974021.

[14] X. Liu, M. Dong, Y. Liu, A. Liu, and N. N. Xiong, "Construction low complexity and low delay CDS for big data code dissemination," *Complexity*, vol. 2018, Jun. 2018, Art. no. 5429546, doi: 10.1155/2018/5429546.

[15] Q. Liu, Y. Guo, J. Wu, and G. Wang, "Effective query grouping strategy in clouds," *J. Comput. Sci. Technol.*, vol. 32, no. 6, pp. 1231–1249, Nov. 2017.

[16] M. Kumar, S. Verma, and K. Lata, "Secure data aggregation in wireless sensor networks using homomorphic encryption," *Int. J. Electron.*, vol. 102, no. 4, pp. 690–702, 2015.

[17] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," *IEEE Trans. Comput.*, vol. 65, no. 10, pp. 3184–3195, Oct. 2016.

[18] X. Liu, G. Li, S. Zhang, and A. Liu, "Big program code dissemination scheme for emergency software-define wireless sensor networks," *Peer-Peer Netw. Appl.*, vol. 11, no. 5, pp. 1038–1059, 2018.

[19] M. Huang, A. Liu, N. N. Xiong, T. Wang, and A. V. Vasilakos, "A low-latency communication scheme for mobile wireless sensor control systems," *IEEE Trans. Syst., Man, Cybern. Syst.*, to be published, doi: 10.1109/TSMC.2018.2833204.

[20] X. Xu *et al.*, "A cross-layer optimized opportunistic routing scheme for loss-and-delay sensitive WSNs," *Sensors*, vol. 18, no. 5, p. 1422, 2018, doi: 10.3390/s18051422.

[21] A. Liu, X. Liu, Z. Tang, L. T. Yang, and Z. Shao, "Preserving smart sink-location privacy with delay guaranteed routing scheme for WSNs," *ACM Trans. Embedded Comput. Syst.*, vol. 16, no. 3, 2017, Art. no. 68, doi: 10.1145/2990500.

[22] R. Wang, F. Nie, R. Hong, X. Chang, X. Yang, and W. Yu, "Fast and orthogonal locality preserving projections for dimensionality reduction," *IEEE Trans. Image Process.*, vol. 26, no. 10, pp. 5019–5030, Oct. 2017.

[23] M. Z. A. Bhuiyan, G. Wang, J. Wu, J. Cao, X. Liu, and T. Wang, "Dependable structural health monitoring using wireless sensor networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 14, no. 4, pp. 363–376, Jul./Aug. 2017.

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

[25] I. M. Tanash, F. Yaseen, M. F. Al-Mistarihi, B. Al-Duwairi, and M. Shurman, "Source location privacy in a cluster-based wireless sensor networks against local adversary," in *Proc. IEEE Int. Conf. Inf. Commun. Syst.*, Apr. 2017, pp. 348–351.

[26] L. Lightfoot, Y. Li, and J. Ren, *STaR: Design and Quantitative Measurement of Source-Location Privacy for Wireless Sensor Networks*. vol. 9. Hoboken, NJ, USA: Wiley, 2016, pp. 220–228.

[27] 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.
[28] R. Rios, J. Cuellar, and J. López, "Probabilistic receiver-location privacy protection in wireless sensor networks," *Inf. Sci.*, vol. 321, pp. 205–223, Nov. 2015.
[29] E. C.-H. Ngai and I. Rodhe, "On providing location privacy for mobile sinks in wireless sensor networks," *Wireless Netw.*, vol. 19, no. 1, pp. 115–134, 2013.
[30] K. Xie *et al.*, "An efficient privacy-preserving compressive data gathering scheme in WSNs," *Inf. Sci.*, vol. 180, no. 2, pp. 702–715, 2016.
[31] X. Liu, M. Dong, K. Ota, L. T. Yang, and A. Liu, "Trace malicious source to guarantee cyber security for mass monitor critical infrastructure," *J. Comput. Syst. Sci.*, to be published, doi: 10.1016/j.jcss.2016.09.008.
[32] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 7, no. 5, pp. 585–598, May 2015.
[33] Y. Guo, F. Liu, Z. Cai, N. Xiao, and Z. Zhao, "Edge-based efficient search over encrypted data mobile cloud storage," *Sensors*, vol. 18, no. 4, p. 1189, 2018, doi: 10.3390/s18041189.
[34] J. Gui, L. Hui, and N. Xiong, "Enhancing cellular coverage quality by virtual access point and wireless power transfer," *Wireless Commun. Mobile Comput.*, vol. 2018, Apr. 2018, Art. no. 9218239, doi: 10.1155/2018/9218239.
[35] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Comput. Secur.*, vol. 72, pp. 1–12, Jan. 2018.
[36] A. K. Singh, B. Kumar, S. K. Singh, S. P. Ghrera, and A. Mohan, "Multiple watermarking technique for securing online social network contents using back propagation neural network," *Future Gener. Comput. Syst.*, vol. 86, pp. 926–939, Sep. 2018, doi: 10.1016/j.future.2016.11.023.
[37] J. Li, Y. K. Li, X. Chen, P. P. C. Lee, and W. Lou, "A hybrid cloud approach for secure authorized deduplication," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1206–1216, May 2015.
[38] X. Liu, N. Xiong, N. Zhang, A. Liu, H. Shen, and C. Huang, "A trust with abstract information verified routing scheme for cyber-physical network," *IEEE Access*, vol. 6, pp. 3882–3898, 2018.
[39] W. Jiang, G. Wang, M. Z. A. Bhuiyan, and J. Wu, "Understanding graph-based trust evaluation in online social networks: Methodologies and challenges," *ACM Comput. Surv.*, vol. 49, no. 1, 2016, Art. no. 10.
[40] X. Chang, Z. Ma, Y. Yang, Z. Zeng, and A. G. Hauptmann, "Bi-level semantic representation analysis for multimedia event detection," *IEEE Trans. Cybern.*, vol. 47, no. 5, pp. 1180–1197, May 2017.
[41] J. Xu *et al.*, "Integrated collaborative filtering recommendation in social cyber-physical systems," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 12, 2017, Art. no. 1550147717749745.
[42] M. Huang *et al.*, "A services routing based caching scheme for cloud assisted CRNs," *IEEE Access*, vol. 6, no. 1, pp. 15787–15805, 2018.
[43] C. Han and J. Yang, "Multi-source cooperative data collection with a mobile sink for the wireless sensor network," *Sensors*, vol. 17, no. 11, p. 2493, 2017.
[44] M. Z. A. Bhuiyan, J. Wu, G. Wang, T. Wang, and M. M. Hassan, "e-sampling: Event-sensitive autonomous adaptive sensing and low-cost monitoring in networked sensing systems," *ACM Trans. Auton. Adapt. Syst.*, vol. 12, no. 1, 2017, Art. no. 1.
[45] M. Huang, A. Liu, M. Zhao, and T. Wang, "Multi working sets alternate covering scheme for continuous partial coverage in WSNs," *Peer-Peer Networking and Applications*, pp. 1–15, 2018, doi: 10.1007/s12083-018-0647-z.
[46] T. Wang *et al.*, "Fog-based storage technology to fight with cyber threat," *Future Gener. Comput. Syst.*, vol. 83, pp. 208–218, Jun. 2018.
[47] J. Wang, A. Liu, T. Yan, and Z. Zeng, "A resource allocation model based on double-sided combinational auctions for transparent computing," *Peer-Peer Netw. Appl.*, vol. 11, no. 4, pp. 679–696, 2018.
[48] J. Cui, Y. Zhang, Z. Cai, A. Liu, and Y. Li, "Securing display path for security-sensitive applications on mobile devices," *Comput., Mater. Continua*, vol. 55, no. 1, pp. 17–35, 2018.
[49] Q. Liu, G. Wang, X. Liu, T. Peng, and J. Wu, "Achieving reliable and secure services in cloud computing environments," *Comput. Elect. Eng.*, vol. 59, pp. 153–164, Apr. 2017.
[50] A. Liu and S. Zhao, "High performance target tracking scheme with low prediction precision requirement in WSNs," *Int. J. Ad Hoc Ubiquitous Comput.*, to be published.
[51] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," *IEEE Trans. Comput.*, vol. 64, no. 2, pp. 425–437, Feb. 2015.
[52] A. K. Das, A. K. Sutrala, V. Odelu, and A. Goswami, "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks," *Wireless Pers. Commun.*, vol. 94, no. 3, pp. 1899–1933, 2016.

TING LI is currently pursuing the master's degree with the School of Information Science and Engineering, Central South University, China. Her research interests include services-based network, crowd sensing networks, and wireless sensor networks.

YUXIN LIU is currently pursuing the degree with the School of Information Science and Engineering, Central South University, China. Her research interests are services-based networks, crowd sensing networks, and wireless sensor networks.

NEAL N. XIONG received the double Ph.D. degrees (about sensor system engineering) from Wuhan University and the Japan Advanced Institute of Science and Technology. He was with Georgia State University, Wentworth Technology Institution, and Colorado Technical University, about 10 years. He is currently an Associate Professor with the Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, OK, USA. His research interests include cloud computing, security and dependability, parallel and distributed computing, networks, and optimization theory.

He published over 200 international journal papers and over 100 international conference papers. Some of his works were published in the IEEE JSAC, the IEEE or ACM Transactions, the ACM Sigcomm workshop, the IEEE INFOCOM, ICDCS, and IPDPS. He is a Senior Member of the IEEE Computer Society. He has received the Best Paper Award in the 10th IEEE International Conference on High Performance Computing and Communications 2008 and the Best student Paper Award in the 28th North American Fuzzy Information Processing Society Annual Conference 2009. He has been the general chair, the program chair, the publicity chair, a PC member, and OC member of over 100 international conferences, and as a reviewer of about 100 international journals, including the IEEE JSAC, the IEEE SMC (Park: A/B/C), the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON MOBILE COMPUTING, the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS. He is serving as the Editor-in-Chief, an Associate editor, or Editor member for over 10 international journals, including an Associate Editor for the IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS and *Information Science* and the Editor-in-Chief for the *Journal of Internet Technology* and the *Journal of Parallel and Cloud Computing*, and a Guest Editor for over 10 international journals, including *Sensor Journal*, WINET, and MONET.

ANFENG LIU received the M.Sc. and Ph.D. degrees in computer science from Central South University, China, in 2002 and 2005, respectively. He is currently a Professor with the School of Information Science and Engineering, Central South University. He is also a member (E200012141M) of the China Computer Federation. His major research interest is wireless sensor networks.

ZHIPING CAI (M'08) received the B.Eng., M.A.Sc., and Ph.D. degrees in computer science and technology from the National University of Defense Technology (NUDT), China, in 1996, 2002, and 2005, respectively. He is a Full Professor with the College of Computer, NUDT. His current research interests include network security and big data. He is a Senior Member of CCF. His doctoral dissertation has been received with the Outstanding Dissertation Award of the Chinese PLA.

HOUBING SONG (M'12–SM'14) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in 2012. In 2007, he was an Engineering Research Associate with the Texas A&M Transportation Institute. He served on the Faculty of West Virginia University from 2012 to 2017. In 2017, he joined the Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL, USA, where he is currently an Assistant Professor and the Director of the Security and Optimization for Networked Globe Laboratory. He is the editor of four books, including *Smart Cities: Foundations, Principles and Applications* (Hoboken, NJ, USA: Wiley, 2017), *Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications* (Chichester, U.K.: Wiley–IEEE Press, 2017), *Cyber-Physical Systems: Foundations, Principles and Applications* (Boston, MA, USA: Academic Press, 2016), and the *Industrial Internet of Things: Cybermanufacturing Systems* (Cham, Switzerland: Springer, 2016). He has authored over 100 articles. His research interests include cyber-physical systems, cybersecurity and privacy, Internet of Things, edge computing, big data analytics, unmanned aircraft systems, connected vehicle, smart and connected health, and wireless communications and networking. He serves as an Associate Technical Editor for *IEEE Communications Magazine*.

Dr. Song is a Senior Member of ACM. He was the very first recipient of the Golden Bear Scholar Award, the highest campus-wide recognition for research excellence at the West Virginia University Institute of Technology in 2016.