Accepted Manuscript

A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things

Guangjie Han, Lina Zhou, Hao Wang, Wenbo Zhang, Sammy Chan

PII: S0167-739X(17)31034-8
DOI: http://dx.doi.org/10.1016/j.future.2017.08.044
Reference: FUTURE 3639

To appear in: *Future Generation Computer Systems*

Received date : 18 May 2017
Revised date : 7 July 2017
Accepted date : 23 August 2017

Please cite this article as: G. Han, L. Zhou, H. Wang, W. Zhang, S. Chan, A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.08.044

A Source Location Protection Protocol Based on Dynamic routing in WSNs for the Social Internet of Things

Guangjie Han[a], Lina Zhou[a], Hao Wang[a], Wenbo Zhang[b], Sammy Chan[c]

[a]*Department of Information and Communication Systems, Hohai University, 200 North Jinling Road, Changzhou 213022, China; hanguangjie@gmail.com, zhouln1993@gmail.com, wanghaohhu@outlook.com*
[b]*School of Information Science and Engineering, Shenyang Ligong University, China; E-mail:zhangwenbo@yeah.net.*
[c]*Department of Electronic Engineering, City University of Hong Kong, Kowloon Tong, Hong Kong; E-mail:eeschan@cityu.edu.hk.*

Abstract

With the development of the Internet of Things (IoT), a more humanity-related network called the Social Internet of Things (SIoT) is now evolving. WSNs are also part of the Social Internet of Things (SIoT), a new application of the Internet of Things (IoT). Considering the characteristics of sensor nodes, including limited resource, limited communication capability, and an uncontrollable environment, location privacy protection is a challenging problem for WSNs. In this paper, we propose a source location protection protocol based on dynamic routing to address the source location privacy problem. We introduce a dynamic routing scheme that aims at maximizing paths for data transmission. The proposed scheme first randomly chooses an initial node from the boundary of the network. Every package will travel a greedy route and a subsequent directed route before reaching the sink. Theoretical and experimental results show that our scheme can preserve source location privacy and defeat various privacy disclosure attacks (eavesdropping attack, hop-by-hop trace back attack, and direction-oriented attack) without affecting the network lifetime.

Keywords: source location privacy, Social Internet of Things, wireless sensor networks, cyber attacks

1. Introduction

The Internet of Things (IoT) has developed a lot in recent years [1-2], and the Social Internet of Things (SIoT), a new application of IoT, is now evolving. The SIoT is a larger social network, connecting people and people, people and objects, and objects and objects. Using the perceptual monitoring technology of IoT, every building, car, or shopping mall can post a message automatically, realizing the interaction of people and a specific object. One part of SIoT can be a wireless sensor network (WSN), sensing the state of an object or monitoring an event in the network. Since SIoT enables interaction of an object with people or another object, there will be wireless communication between objects and people. In that case, The use of wireless communication media means that anyone with powerful radio transceivers can attack the network. Because of this vulnerability, SIOT faces security threats such as information eavesdropping, data fabricating, node compromising, and route disrupting. These network attacks threaten either content privacy, the confidential data of a message, or contextual privacy, information about the surrounding network. All these problems make privacy protection of the SIoT becomes essential.

Wireless sensor networks (WSNs) show great application value for national security, military monitoring, health care, and environmental monitoring [3-5]. However, wireless network privacy issues have become the main bottlenecks for its further development. In this paper, we focus on protecting source location in a WSN related to SIoT.

Location privacy is a typical context privacy issue. Particularly, an adversary can detect the message flow to determine the source node location and then attack the target of interest. This problem of source location privacy (SLP) has not been addressed effectively because it cannot be easily solved by encryption or authentication. Wireless sensor nodes have limited storage space, energy supply, and computing capacity. In order to preserve the location of the sensitive source node, we must develop a feasible and energy-efficient protocol to hide the source from being detected by adversaries.

To clearly illustrate the SLP issue, we consider the classical "panda-hunter" model in Figure 1. A WSN can be deployed in a wildlife habitat to monitor pandas' habits and behavior. Once a node detects a panda in its communication range, it becomes a source node and periodically sends report packets to the base station (Sink in Figure 1) by multi-hop wireless communications. Obviously, this scenario is unsafe for the source since the communication signal is exposed to the air. The hunters and poachers (Adversary in Figure 1) can use expensive devices to eavesdrop on the network, following the flow of packets, speculating the routing pattern and finally tracing back hop-by-hop to find the panda. Thus, hiding the location of a source node is a critical issue for WSNs.

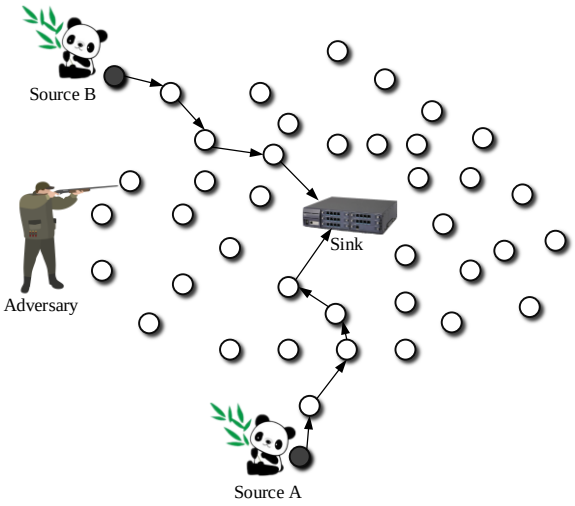


Figure 1: The panda hunter model as a source location privacy-sensitive scenario.

SLP issues have been extensively studied in the past years, but the balance of package delay and source safety time, energy consumption, and network lifetime, have yet to be explored. In this paper, we propose a source location protection protocol based on dynamic routing (SLPDR) to protect against a local eavesdropper in wireless sensor networks. The major contributions are as follows:

(1) To the best of our knowledge, this is the first report that considers two pairs of relationships, package delay and source safety time, and energy consumption and network lifetime. Previous studies mostly focused on maximizing the safety time of the source node and cannot provide

trade-offs between source safety time and data transmission latency. In SLPDR, the lengths of routing paths tend to be consistent and do not need to go through intermediate nodes from a remote area. SLPDR is also an energy-efficient protocol, since there are enough dummy packets to confuse the adversary, without significantly shortening the network lifetime.

(2) SLPDR can withstand different types of attacks. A common attack is a traffic hop-by-hop-trace attack. In SLPDR, the dynamic route changes periodically and the varying traffic pattern makes it difficult to be traced. The flow of message in SLPDR will not reveal the location of source. Another common attack is a direction-oriented attack strategy. A powerful adversary can save useful information and conduct historical statistics of routing path to estimate the possible direction of source. Here, the proposed routing protocol can resist this kind of attack because the boundary node is chosen periodically from all directions from the outermost ring.

(3) Extensive simulations were performed on MATLAB to demonstrate the effectiveness of SLPDR. The performance of SLPDR was analyzed and compared against several existing algorithms. The results demonstrate the effectiveness and superiority of our proposed protocol in source location protection.

The rest of this paper is organized as follows. Section 2 provides a review of related work about source location privacy routing techniques. In Section 3, we introduce the system model and assumptions. Section 4 presents the details of the proposed privacy routing scheme, SLPDR. Our simulation results and comparisons of different schemes are presented in Section 5. Conclusions and future research directions are presented in Section 6.

2. Related work

Network privacy protection is a critical and challenging topic. Privacy problems of WSNs can be categorized as content-oriented and contextual-oriented problems. Content-oriented issues usually can be addressed through message encryption or authentication, and these problems are not discussed in detail here. Contextual-oriented problems are more intractability because of the exposure of the network communication signal. Location privacy is a kind of contextual problem requiring hiding the location of a specific node. Since Ozturk *et al.* originally described the panda-hunter model, SLP problems have been widely studied [6]. Kamat *et al.* formalized the problem in [7]. Subsequently, the panda-hunter game became a classical monitoring-based application scenario in studies of SLP. Several source security performance metrics have been proposed [8-9]. One of these is the security time of source, namely, the total number of packets that the source can successfully send out before being caught by the adversary. Another metric is the possibility that the adversary can locate the source node in a set amount of time.

Before the SLP was developed, some studies used anonymity and pseudonyms to hide a subject among a set of anonymities [10-13]. Solutions based on the k-anonymization technique were proposed in [10]. There are k phantom nodes around the real source which makes the adversary confused. However, these techniques are far from sufficient to protect the source location.

Ozturk *et al.* first proposed a random walk approach to deal with SLP [9]. When a source node detects a subject or event, it generates an event message and randomly sends it to one of its neighbors and the neighbor passes the message in a similar fashion. The message is unicasted (single sender and single receiver) in a random fashion for h hops. Then, the message is forwarded in a broadcast fashion to multiple receivers until it reaches the sink node or the base station. The

algorithm can make it difficult for an adversary to trace hop-by-hop back to the source since the packets route looks completely random in the random walk phase. However, a purely random walk may cause loops when a node receives the same packet two times or more. In that case, there is redundant energy consumption and the direction information may be revealed to the adversary. Subsequent studies proposed solutions derived from a random walk approach. Tan *et al.* [14] proposed a directed random walk approach, EDROW. In this scheme, packets are forwarded by nodes called parent nodes, located closer to the base station. Different packets generate different paths. The more parent nodes there are in a path, the better the provided SLP. Luo *et al.* [15] proposed a phantom single-path routing. There is a path initialed from the phantom node simulating the real event packages' routing. Xi *et al.* [16] introduced a greedy random walk, GROW. In this approach, the sink firstly initiates a random walk. Next, the source node generates and forwards the event packets through a random walk in the same pattern, with an intersection node connecting the two paths. Then, packets are transmitted along the sinks path in the reverse order. A Bloom filter is used in GROW to avoid repeating cycles.

Using dummy data sources is also a common strategy to provide SLP. Dummy data sources obfuscate real traffic and make it difficult for adversaries to perform traffic analysis. Lightfoot *et al.* [17] put forward the concept of an intermediary node. The proposed algorithm STaR does not leak any directional information. However, the achieved location protection level depends greatly on the distance between the intermediary node and the source. Kumar *et al.* [18] introduced a multiple-phantom approach. The proposed protocol can keep the adversary confused as every source node has two phantom nodes. Chen *et al.* [19] proposed a dynamic bidirectional tree scheme to provide end-to-end location privacy. To withstand attacks under a specific eavesdropper model, other schemes related to dummy sources or a technique that results in a similar pattern were presented in [20-23]. Solutions in this category make it difficult for an adversary to differentiate the real traffic from the fake traffic.

Another kind of solution that aims at providing a better SLP is cyclic entrapment [24-27]. Long *et al.* proposed a Ring-Based Routing (RBR) scheme [28]. In the algorithm, ring routes are generated away from the hot areas to confuse the adversaries. The RBR-based scheme can balance the energy consumption in the network without affecting the network lifetime. However, RBR will cause data transmission latency and is not suitable for most applications with an urgent need for rapid network transmission.

Most protocols described above can provide some level of SLP. Nevertheless, trade-offs between package delay and source safety time, energy consumption, and network lifetime are difficult to balance. In this work, we proposed a SLPDR scheme to address the source location privacy problem. In SLPDR, an initial node is randomly chosen from the boundary of the network. Every package will travel a greedy route and a subsequent directed route before reaching the sink. The network is divided into different grids and rings. Dummy traffic is generated on the outer rings without significantly deteriorating the network lifetime. The real event packets are transmitted forward in a one-hop flooding pattern and only the node on the greedy path will replace the dummy packet with the real packet. SLPDR can keep the adversary confused since data packets that initiate from the same source take different paths.

3. The system model and assumptions

3.1. Network model

We defined the source location problem based on the panda-hunter game model [29]. In this set-up, the WSN is deployed to continuously detect and monitor the activity and habits of pandas. Once a node detects a panda in its administrative area, it becomes the source node and periodically generates encrypted event packets about the panda and sends it to the sink hop-by-hop. The goal of this protocol is to conceal the traffic flow of the real packets and therefore keep the pandas location unknown to an adversary. In this design, we make the following assumptions of the monitor-based network model.

(1) Sensor nodes are uniformly and randomly deployed with density ρ in the network. Once the sensors are deployed in the wild habitat, their position is set permanently. Each sensor node has limited energy and computing capacity. The whole network is fully connected through multi-hop communications.
(2) There is a single static sink node that acts as the controller and is deployed in the center of the network. The location information of the sink node is public since it is the destination of the event packets.
(3) The network is divided into grids and rings. In each grid, the node with the highest energy acts as a cluster header that can occasionally communicate with other nearby grids. The energy information of the grids is updated periodically.
(4) Each event packet is encrypted using a secret key shared between sensor nodes and the sink node. This method focuses on location privacy protection, and data (packet) privacy is beyond the scope of this work and should be considered elsewhere.
(5) Each node knows its location (x, y) and the shortest path to the sink. Additionally, nodes are assumed to know the knowledge of its immediate adjacent neighbors.

3.2. Adversary model

The adversaries usually try their best to equip themselves with some advanced equipment to locate the source node such as a panda to get high profits. In this paper, the adversaries are assumed to have the following characteristics:

(1) Well-equipped. The adversaries are equipped with advanced devices such as spectrum analyzers and antenna. The attackers have sufficient energy resources and therefore the energy consumption of adversaries is not taken into consideration. They also have sufficient storage capacity and computation capability. An adversary resides at the spectrum analyzer and eavesdrops somewhere in the network. It can hear the transmission information in its transmission range and measure the angle as well as the strength of the received signal and accurately locate the immediate sender. After detection, the adversary can move to the senders location without delay. A well-equipped adversary usually starts its back-tracing attack from the sink, since the process of packet transmission always ends at the sink. The overhearing radius is assumed to be larger than that of common nodes.
(2) Passive. The adversaries can only carry out passive attacks, such as eavesdropping on communications, and will not interfere with the normal operation of the network. Active attacks, including packet falsification, a compromised node, or communication destruction, can be easily discovered by a self-adaptive network, but passive attacks are more dangerous as they are harder to detect.

(3) Local vision. The adversaries will not miss any event packets in the monitored area. Several adversaries can reside in the network at the same time and gather periodically to share information. However, we presume that the adversaries cannot hear and collect all the occurrence of the packets throughout the whole network. Note that the event detection devices must be customized and therefore are often costly. Additionally, expensive devices cannot be recycled due to environmental effects. If the attackers can monitor the entire network, they can directly analyze the monitored information. Here, to simplify the model, we assume there is only one attack in the network.

(4) Backtracking. Adversaries can trace back hop-by-hop according to the received transmission signal. The scenario in Figure 2 is used as an example, where an adversary resides somewhere in the network and eavesdrops on the transmission signal. If the adversary hears that a packet is transmitted forward near D, it can find the immediate sender C and move to it, waiting for the next packet. However, it cannot locate the destination D since the packets are broadcasted to all the neighbors in a single hop. In that situation, the adversary can identify the transmission sequence A $\rightarrow$ B $\rightarrow$ C through tracking back hop-by-hop.

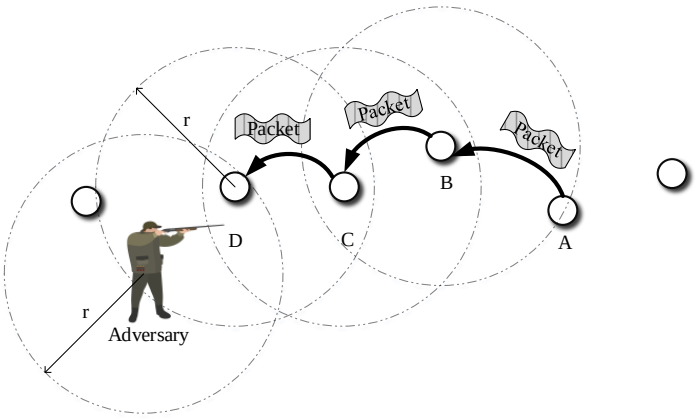


Figure 2: A local adversary can use a backtracking model by packet eavesdropping.

(5) Direction-oriented analysis. A more powerful adversary can save useful information such as the location of observed nodes and the traffic flow in a specific area to analyze the historical statistics of routing paths and estimate the possible directions of the source. In this way, the adversary can filter out some dummy packets and accelerate the backtracking process.

3.3. Energy consumption model

Energy consumption is an essential metric to evaluate the performance of a protocol. The amount of energy consumed in hot areas has a direct impact on the lifetime of the whole network, since nodes near the sink must act as intersections to relay all the data packets. Sensor nodes consume energy when receiving or transmitting packets. Here, we adopt the typical energy consumption model described previously in [30-31]. The energy consumption for transmitting uses formula (1) and the energy consumption for receiving can be represented by formula (2)

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

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

where E_{elec} represents the transmitting circuit loss and l is the length of the packet in bits. Free space (d^2 power loss) as well as the multi-path fading (d^4 power loss) channel models are considered. The value of E_{elec} depends on the distance between the transmitter and the receiver. If the transmission distance is less than d_0, the power amplifier loss follows the free space model. If the transmission distance is more than d_0, the power amplifier is based on the multi-path fading model. ε_{fs} and ε_{amp} represent the energy required by power amplification for the two models. The values of these parameters are presented in Table 1 [32].

Table 1: Network parameters

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

3.4. Design goals

Our design goals are as follows.

(1) The proposed protocol should conserve source location privacy and be secure enough to defend the attacks of a powerful adversary. Thus, an adversary cannot easily find the source by traffic analysis or backtracking. To better evaluate the safety performance of the scheme, we define the metric safety time(T) as

$$max(T) = max(tracetime) = max(tracelength) \tag{3}$$

The safety time is defined as the safety period from the time that an adversary starts to eavesdrops on the first packet in the network to the moment when the adversary successfully captures the real source. Since the interval of the packet is consistent, the safety time also reflects the path length an adversary must traverse in a duty cycle.

(2) The lifetime of the network should be little affected by injecting a dummy message and utilizing diverse paths. We define the network lifetime as the period from the start of the WSN to the moment when the first node is out of power. After deployment, the sensor nodes are left unattended and it is infeasible to replace the batteries or re-charge them. Since all the event packets are transmitted via nodes near the sink, these nodes consume more energy than nodes far from the sink, thus causing the hotspot area in the network. The goal of our proposed scheme is to take advantage of the redundant energy in locations that are distal to the sink and maximize the lifetime of nodes in the hotspot area.

(3) A SLP scheme allows correspondence of the safety time and packet delay relationship, and the network lifetime and energy consumption relationship. We also propose a fit between these relationships.

4. The proposed SLPDR routing protocol

4.1. Three routing patterns

In this section, we describe our SLPDR dynamic routing scheme in detail. The routing scheme includes an initial stage and can undergo three kinds of routing patterns, cyclic routing, greedy routing, and directed routing. Switching between different routing modes can be performed as required by the conditions.

(1) Cyclic routing.

To confuse the adversary about the details of the traffic pattern and increase the amount of time required to trace the traffic flow, we propose a cyclic routing technique. During the forwarding process, a cluster head will first check whether or not the packet holds the real event data when it receives the packet. It then passes forward the packet in two opposite directions, clockwise and anti-clockwise. Next, the cluster head stores the real data in its cache and just releases a dummy packet. In this case, every packet will take a round trip in a cyclic route. Figure 3 shows the cyclic routing with a real event.

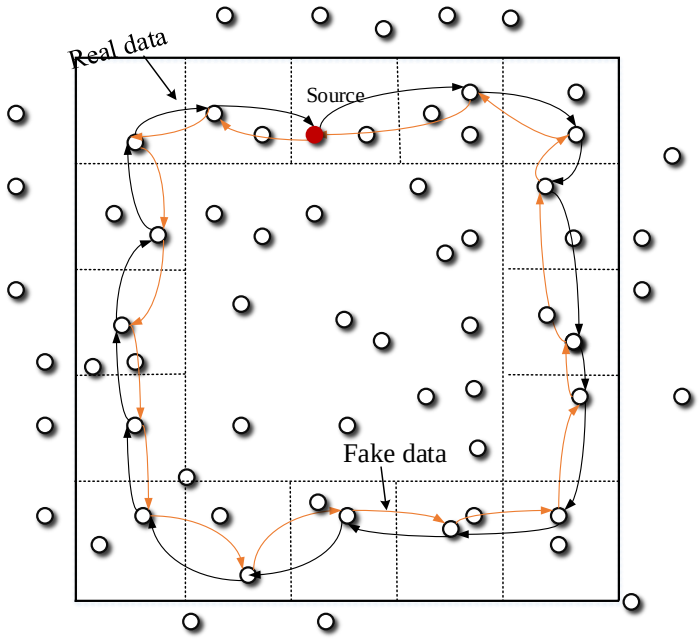


Figure 3: Illustration of cyclic routing.

(2) Greedy routing.

In a sensor networks, greedy routing is one of the most popular routing techniques, and is typically used in networks with limited energy. Unlike flooding, the greedy routing needs a pre-configuration phase to set up the hop count between each node and the sink node. In the initial configuration phase, the sink initials a flood with an initial hop count of zero. Making sure that any immediate node only passes the packet from neighbors forward once. Every time a node receives a packet, it increases the hop and records the hop number. After the initial process, each node chooses the minimum hop value as the final number of hops to the sink, and then broadcasts that value to its neighbors. In greedy routing, nodes pass forward packets to the neighbor with the minimum number of hops to the sink.

(3) Directed routing.

Directed routing is adopted between grids, and aims at realizing the diversity of paths. Once a node receives a packet, the packet is transferred, based on unicasting, to the cluster head in the neighboring grid in the direction of the sink. The immediate cluster head forwards the received packet to one of the neighboring grids in the same manner. Directed routing creates a large number of paths from a node to the destination. An adversary may be attracted to a path that may not be used for packet transmission. In this way, routing can resist the backtracking attack of the adversaries.

Figure 4 shows the process of the directed routing. If there are n grids between a specific node A and the sink, the number of paths from A to the sink is H. The value of H is defined as formula (4):

$$\begin{cases} H_{min} = 1 \\ H_{max} = \dfrac{n(n-1)(n-2)\cdots(n-\lceil n/2\rceil+1)}{(\lceil n/2\rceil)!} = C_n^{\lceil n/2\rceil} \end{cases} \tag{4}$$

As shown in Figure 4, we can draw two different routes for packets to travel from node A to the sink. In this scenario, there can be no more than 70 paths between node A and sink. Supposing that the angle between node A and the horizontal line according to the sink node is α. When the angle α is closer to 45°, there are more paths between node A and the sink. However, if node A and the sink are scattered around a straight line, there are not enough paths.

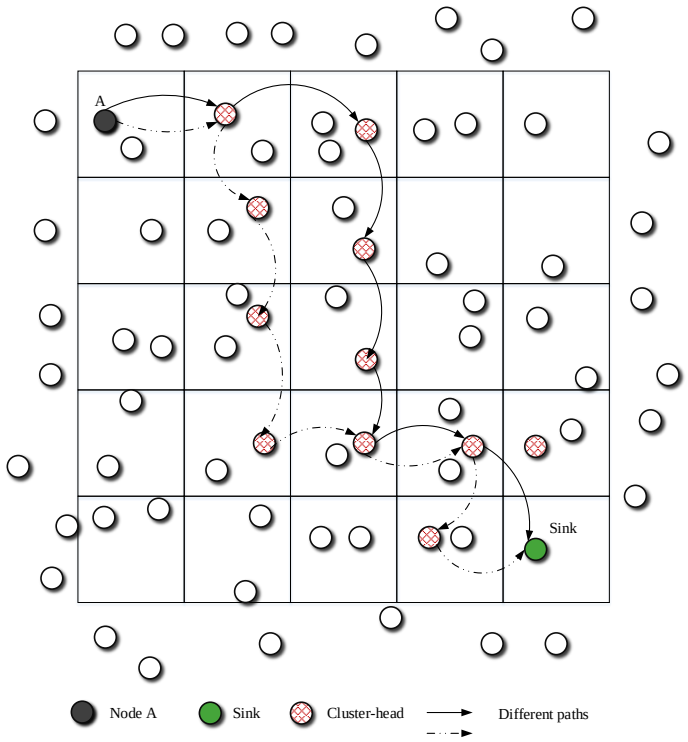


Figure 4: Directed routing process.

4.2. Description of the SLPDR protocol

To describe our protocol in more detail, we separately consider the grid and ring partitioning phase and the route establishment phase.

(1) Grids and rings partitioning.

In our scheme, selecting the origin as the sink node, the entire network is evenly divided into grids after deployment. Each grid selects a node with the highest energy to be a cluster node in a transmission round. Packets are transmitted through cluster nodes. The cluster node can be changed whenever a node has more remaining energy than the present cluster node. Sensor nodes calculate and store their grid coordinate values. Rings are generated in areas other than the hotspot area depending on the distance to the sink. We use these rings to create diversionary cyclic routes. After the partitioning of rings, each node knows its ring number i. Nodes broadcast their grid coordinate values and ring numbers to neighboring nodes. Each sensor node can classify its neighboring nodes as: (a) Nodes with a smaller hop to the sink (parent node), (b) Nodes with a larger hop to the sink (child node), (c-f) nodes in the up, down, left, or right grid direction. Because the WSNs have wireless media characteristics, to guarantee the link of the paths, the communication range of nodes is set to $r = \sqrt{5}a$, where a represents the length of the grids.

(2) Route establishment.

At the start, we select a node in the outmost ring as a starting node of the route. The selection process can be realized by a token scheme [27]. The rule of the token scheme is that when a node belongs to a ring, it waits for token in the idle state and passes to Have token state if it has data to send. The starting node first holds a token for predefined intervals T and then passes it to another node. The selected starting node generates a dummy packet and starts the data forwarding process. The dummy packet is passed forward in the greedy routing manner.

During the greedy routing process, once a sensor node finds a panda in its monitored area, it becomes a source. The ring where the source exists is called the event ring. The source generates and passes forward the event packet around the event ring in the clockwise (or anti-clockwise) direction. At the same time, the source generates a dummy packet and transmits it in the opposite direction. Cluster heads in the event ring keep the real data in their cache and just discard the dummy packets. In this case, real event can be successfully stored in all the cluster heads on the event ring. In order to further confuse the adversary, we randomly select part of the rings to generate interference ring routes with a certain probability p_i for a fixed time d_u. To ensure that the energy consumption in these rings will not affect the lifetime of the network, we can theoretically calculate the value of p_i. The average energy consumption of the ith interferential ring should meet the following constraints:

$$E_i^{avg} \leq E_1^{avg}, i \in \{2, 3 \cdots k\} \tag{5}$$

$$E_1^{avg} = \frac{2(E_t^{l,r} + E_r^l)}{4S_0\rho} = \frac{E_t^{l,r} + E_r^l}{2S_0\rho} \tag{6}$$

$$E_i^{avg} = \frac{2(E_t^{l,r} + E_r^l)P_i}{S_0\rho} \tag{7}$$

where k represents the number of the rings in the network, l represents the number of bits in a packet, r denotes the transmission range of nodes, ρ is the node density of the network, S_0 refers to the area of a grid.

When the dummy packet on the greedy route reaches the intersection node on the event ring, the stored event message replaces the empty packet and then the packet will be transmitted forward hop-by-hop to the sink through directed routing. Figure 5 shows a schematic illustration of the whole process of SLPDR.

5. Performance evaluation

We implemented our proposed SLPDR protocol in MATLAB to compare the performance of SLPDR scheme with GR [11] and CDR [22]. The GR scheme is a routing protocol without protection of the source node, in which the source sends the event packet to the sink along the shortest path upon detection of an object. The CDR scheme uses cyclic entrapment to confuse the adversary. We evaluate our protocol based on the four metrics of safety time, latency, lifetime, and energy consumption.

5.1. Simulation settings

In this simulation, sensors are deployed in a square area and the sink is located at the center of the network. For unspecified conditions, the relevant simulation parameters are outlined in table 2.

Table 2: Simulation parameters

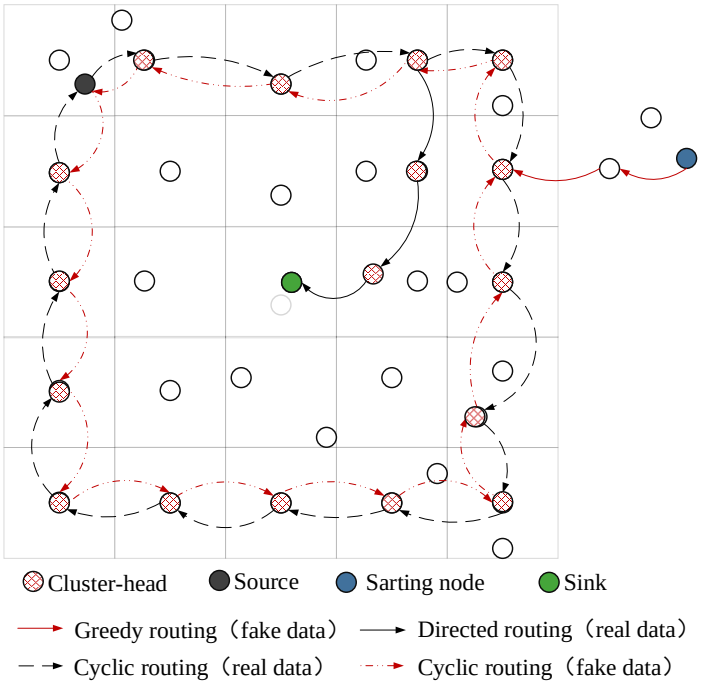
Parameter	Value
Node density (ρ)	0.003
Network radius (L)	$500m$
Transmission range (r)	$45m$
Date bits in a message (l)	1000bits
Interferential ring probability (P_i)	0.2

5.2. Simulation results

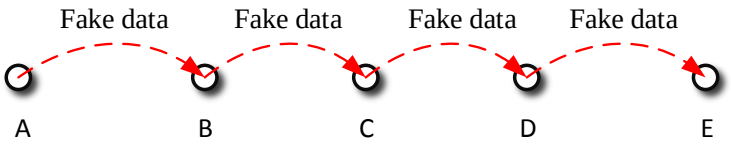
(1) Energy consumption.

Figure 6 depicts the relationship between nodal energy consumption and the distance from source to sink. As shown in this figure, we can see that the GR scheme consumes little energy since it does not inject any dummy packets into the network and it does not protect the source node. We can also see that the nodal energy consumption in SLPDR is larger than CDR. We create more fake messages in the outer areas to confuse the adversaries and increase the network security. Cluster nodes on the event ring transmit the packet hop-by-hop in SLPDR, but only some nodes on the event ring send dummy packets in CDR. As the distance from source to sink increases, the nodal energy consumption increases in both SLPDR and CDR since there are more nodes in the event ring that are forwarding packets.

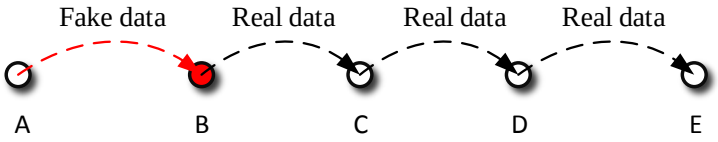
Figure 7 gives the detailed comparison of total energy consumption of the network in the three protocols in one data aggregation period. Similar to what was seen for nodal energy consumption, the GR scheme consumes the least energy and the CDR uses more energy than



(a) Process of SLPDR.



(b) Route lacking a real event.



(c) Route with a real event.

Figure 5: Illustration of SLPDR.

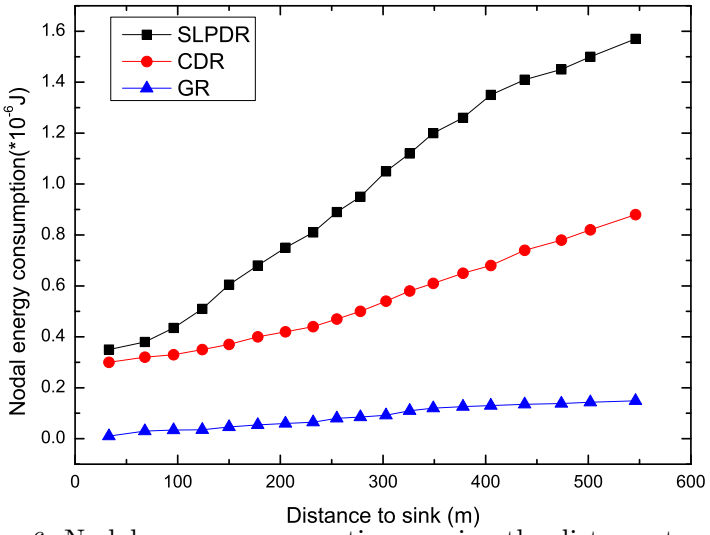


Figure 6: Nodal energy consumption varying the distance to sink.

GR, but less than SLPDR. As we can see in the figure, when there are about 6 rings in the network, the total energy consumption is the lowest. When there are less than 6 rings, the transmission range of node is large and the energy consumption for packet transmission is also large.

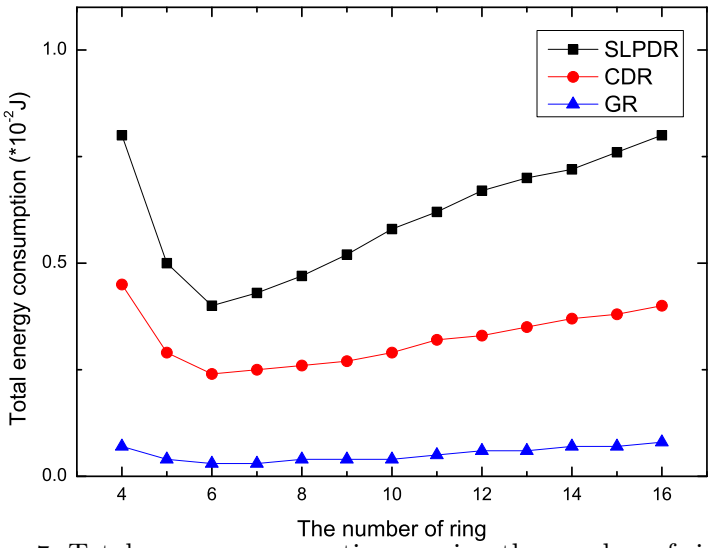


Figure 7: Total energy consumption varying the number of rings.

(2) Network lifetime.

The network lifetime of the three protocols are shown in Figure 8. We consider the data production period as T. As described in the figure, the network lifetimes are basically the same regardless of the change of side length L. This result is reasonable since the three schemes do not generate dummy packets in the hotspot area, so the lifetime depends only on the energy consumption in the hotspot area near the sink. Thus, the energy consumption in the outer areas is lower than the hotspot area in SLPDR, and although the SLPDR consumes a little more energy than GR and CDR, the network lifetime is not affected.

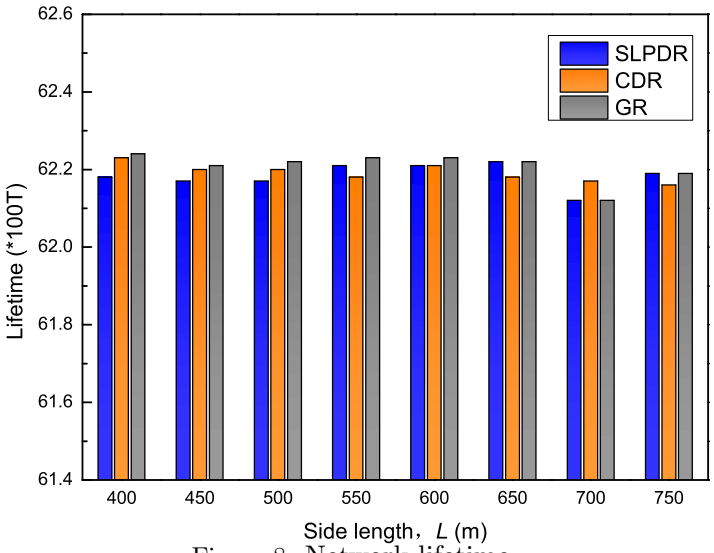


Figure 8: Network lifetime.

(3) Transmission delay.

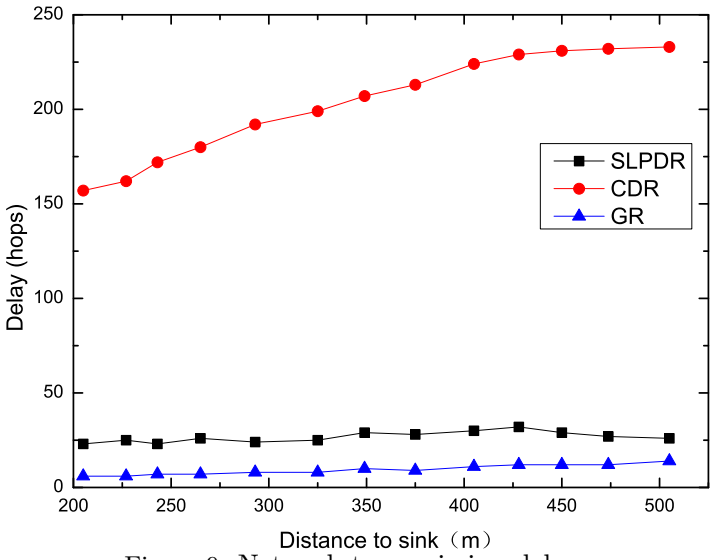


Figure 9: Network transmission delay.

The network transmission delay of SLPDR, CDR, and GR are shown in Figure 9 as a function of the distance between the source and sink. As we can see in the figure, the packet latency of CDR is greater than for SLPDR and GR. In CDR, intercluster communication and the cyclic route both contribute to a huge transmission delay of the network. However, in the SLPDR scheme, the network transmission delay does not fluctuate much despite the change of the source location because the packets do not go through cyclic routes. Therefore, SLPDR is suitable for applications where low data latency is required.

Figure 10 depicts the data latency in SLPDR as a function of the transmission range of nodes. As the transmission range increases, the transmission delay drops accordingly. Additionally, the network scale has a direct impact on transmission delay.

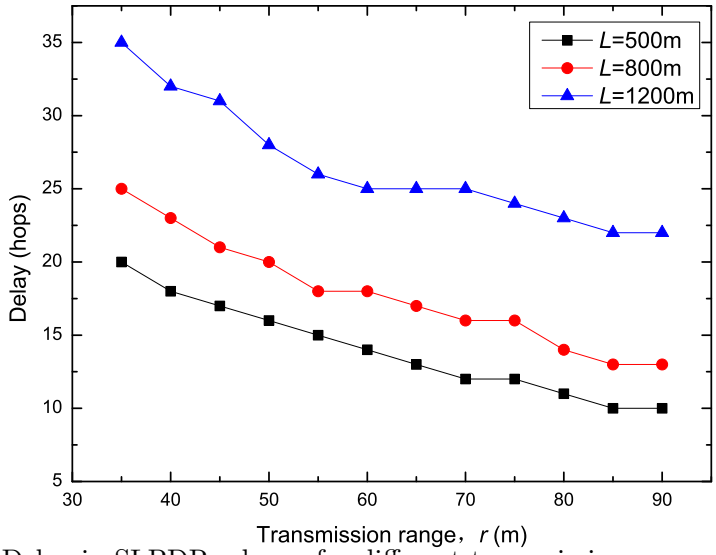


Figure 10: Delay in SLPDR scheme for different transmission range values (r).

(4) Network security.

Figure 11 describes the different network security level of the three protocols. In our model, we represent the safety time by the path length that an adversary has to traverse in a data cycle. The safety time is proportional to the network scale. As shown in the figure, the proposed SLPDR scheme is obviously superior to the other two models in protecting the source location. In the panda-hunter model, it is possible that a panda stays in one area for a relatively long period. In this case, a powerful adversary can find the event ring quickly since the backbone route in CDR is the shortest path from the trigger node to the sink. However, in our protocol, the starting node changes regularly and the direct route changes every time, making it difficult for an adversary to deduce the real location of the object.

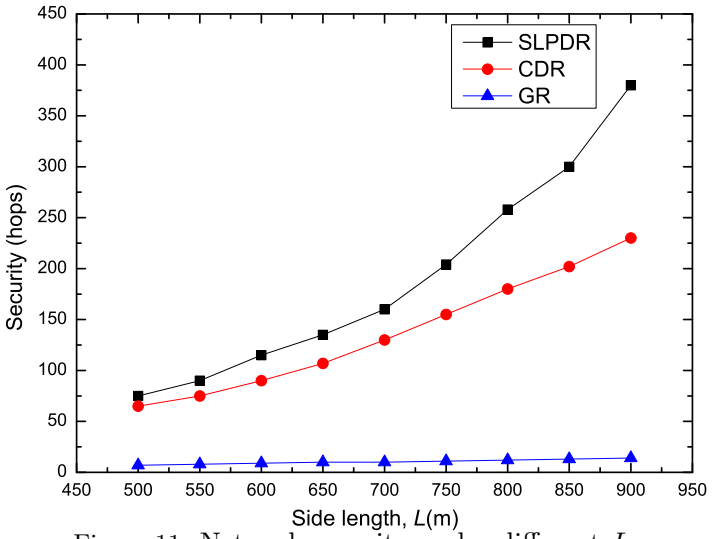


Figure 11: Network security under different L.

Figure 12 shows the relationship between source location security and the transmission range of the proposed protocol. The security level is inversely proportional to the transmis-

sion range of sensor nodes. With a certain transmission range, the safety time of the source continues to increase with the growing side length.

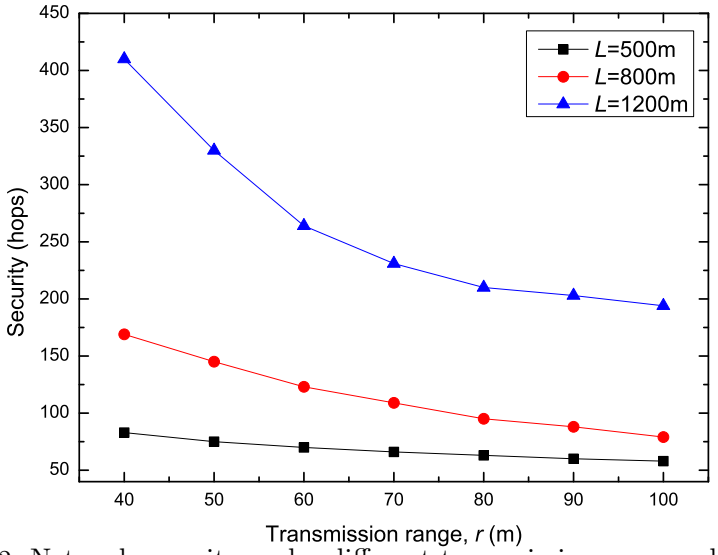


Figure 12: Network security under different transmission range values (r).

6. Conclusions and future research direction

Here, we proposed a source location protection protocol based on dynamic routing (SLPDR) to address the source location privacy problem. Packet forwarding is triggered by a boundary node, and then a dummy packet is transmitted through GR. In the proposed scheme, packages on the backbone will experience a greedy route and a subsequent directed route. Additionally, we also take full use of the redundant energy in outer regions to generate cyclic routes on several rings to confuse the adversary. Through this mechanism, the real source is hidden, and we can achieve a significant enhancement in network security without sacrificing the lifetime of the network. MATLAB simulation showed that SLPDR outperforms the existing protocols.

Despite the fact that SLPDR can provide strong SLP, a more capable attack model has yet to be considered. During the exploration of future source location protection algorithms, attention should be given to a more powerful adversary (such as global attackers or more cautious attackers). Future work will include greater exploitation of the utility of surplus energy outside the hotspot area and the development of a more effective protocol to protect the source location.

Acknowledgements

The work is supported by “the National Natural Science Foundation of China under Grant No.61572172” and supported by “the Fundamental Research Funds for the Central Universities, No.2016B10714” and supported by “Changzhou Sciences and Technology Program, No.CE20165023 and No.CE20160014” and “Six talent peaks project in Jiangsu Province, No.XYDXXJS-007” and sponsored by Liaoning Fourth Batch of Distinguished Professor Project (2014), Liaoning BaiQian-Wan Talents Program(2016) and Liaoning Province Natural Science Foundation (20170540793).

References

[1] T. Qiu, RX. Qiao, DO. Wu, "EABS: An Event-Aware Backpressure Scheduling Scheme for Emergency Internet of Things," *IEEE Transactions on Mobile Computing,* 2017, DOI: 10.1109/TMC.2017.2702670.

[2] T. Qiu, AY. Zhao, RX. Ma, V. Chang, FB. Liu, ZJ. Fu. "A Task-Efficient Sink Node Based on Embedded Multi-core SoC for Internet of Things," *Future Generation Computer Systems,* 2017, DOI: 10.1016/j.future.2016.12.024.

[3] Guangjie Han, Xuan Yang, Li Liu, Wenbo Zhang, Mohsen Guizani, "A Disaster Management-Oriented Path Planning for Mobile Anchor-Based Localization in Wireless Sensor Networks," *IEEE Transactions on Emerging Topics in Computing,* 2017, DOI: 10.1109/TETC.2017.2687319.

[4] Guangjie Han, Li Liu, Sammy Chan, Ruiyu Yu, Yu Yang, "HySense: A Hybrid Mobile Crowd-Sensing Framework for Sensing Opportunities Compensation under Dynamic Coverage Constraint," *IEEE Communications Magazine,* 2017, DOI: 10.1109/TNET.2017.2713530.

[5] Tie Qiu, Aoyang Zhao, Feng Xia, Weisheng Si, Dapeng Oliver Wu. "ROSE: Robustness Strategy for Scale-Free Wireless Sensor Networks," *IEEE/ACM Transactions on Networking,* 2017, DOI: 10.1109/TNET.2017.2713530

[6] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," *ACM Workshop on Security of Ad Hoc and Sensor Networks,* 2004, pp. 88-93.

[7] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," *IEEE International Conference on Distributed Computing Systems IEEE Computer Society,* 2005, pp. 599-608.

[8] WP. Wang, L. Chen, and JX. Wang, "A Source-Location Privacy Protocol in WSN Based on Locational Angle," *IEEE International Conference on Communications IEEE,* 2008, pp. 1630-1634.

[9] H. Bahsi and A. Levi, "Energy efficient privacy preserved data gathering in wireless sensor networks having multiple sinks," *International Conference on Computer Science and ITS Applications IEEE,* 2009, pp. 1-8.

[10] J. Jiang, J. Sheu, C. Tu, and J. Wu, "An anonymous path routing (apr) protocol for wireless sensor networks," *information science and engineering,* 2011, vol. 27, no. 2, pp. 657C680.

[11] J. Chen, X. Du, and B. Fang, "An efficient anonymous communication protocol for wireless sensor networks," *Wireless Communications and Mobile Computing,* 2011, vol. 12, no. 14, pp. 1302C1312.

[12] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Towards a statistical framework for source anonymity in sensor networks," *IEEE Trans. Mobile Computing,* 2011, vol. 10, no. 12, pp. 1C1.

[13] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Statistical framework for source anonymity in sensor networks," *IEEE Global Telecommunications Conference,* 2010, pp. 1-6.

[14] G. Tan, W. Li, and J. Song, "Enhancing Source Location Privacy in Energy-Constrained Wireless Sensor Networks," *Proceedings of International Conference on Computer Science and Information Technology,* 2014, Vol. 255, pp. 279-289.

[15] X. Luo, X. Ji, and M. Park, "Location privacy against traffic analysis attacks in wireless sensor networks," *International Conference on Information Science and Applications,* 2010, pp: 1-6.

[16] Y. Xi, L. Schwiebert, and W. Shi, "Privacy preserving shortest path routing with an application to navigation," *Pervasive & Mobile Computing,* 2014, Vol. 13, No. 4, pp: 142-149.

[17] L. Lightfoot, Y. Li, and J. Ren "Preserving source-location privacy in wireless sensor network using star routing," *IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE GLOBECOM,* 2010, pp: 1-5.

[18] P. Kumar, JP. Singh, P. Vishnoi, and MP. Singh, "Source location privacy using multiple-phantom nodes in WSN," *TENCON,* 2015, pp: 1-6.

[19] H. Chen and W. Lou, "From nowhere to somewhere: protecting end to-end location privacy in wireless sensor networks," *PERFORMANCE Computing and Communications Conference,* 2010, pp: 1-8.

[20] L. Chen, H. Shen, "Consolidating complementary VMs with spatial/temporal-awareness in cloud datacenters," *IEEE INFOCOM 2014-IEEE Conference on Computer Communications,* 2014, pp: 1033-1041.

[21] S. Kki, G Dek, A. Lvai, and M. Zsuga, "The quality of source location protection in globally attacked sensor networks," *IEEE International Conference on Pervasive Computing and Communications Workshops,* 2011, pp: 44-49.

[22] A. Jhumka, M. Leeke, and S. Shrestha, "On the use of fake sources for source location privacy: trade-offs between energy and privacy," *Computer Journal,* 2011, Vol. 54, No. 6, pp: 860-874.

[23] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Towards a statistical framework for source anonymity in sensor networks," *IEEE Transactions on Mobile Computing,* 2013, Vol. 12, No. 2, pp: 248-260.

[24] Y. Li, J. Ren, and J. Wu, "Quantitative Measurement and Design of Source-Location Privacy Schemes for Wireless Sensor Networks," *IEEE Transactions on Parallel & Distributed Systems,* 2012, Vol. 23, No. 1, pp: 1302-1311.

[25] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *Mobile Computing,* 2011, Vol. 11, No. 2, pp: 320-336.

[26] M. Raj, N. Li, D. Liu, M. Wright, and SK. Das, "Using data mules to preserve source location privacy in Wireless Sensor Networks," *Pervasive & Mobile Computing,* 2014, Vol. 11, No. 2, pp: 244-260.

[27] J. Ren, Y. Zhang, K. Liu, "An Energy-Efficient Cyclic Diversionary Routing Strategy against Global Eavesdroppers in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks,* 2014, pp: 94-100.

[28] J. Long, A. Liu, "An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing," *Journal of Parallel & Distributed Computing ,* 2015, pp: 47-65.

[29] N. Li, N. Zhang, S. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey," *Ad Hoc Networks,* 2009, Vol. 7, No. 8, pp: 1501-1514.

[30] A. Liu, D. Zhang, P. Zhang, G. Cui, and Z. Chen, "On mitigating hotspots to maximize network lifetime in multi-hop wireless sensor network with guaranteed transport delay and reliability," *Software: Practice and Experience,* 2014, Vol. 7, No. 3, pp: 255-273.

[31] H. Wang, B. Sheng, and Q. Li, "Privacy-aware routing in sensor networks, *Computer Networks* 2009, Vol. 53, No. 9, pp: 1512-1529.

[32] F. Wei, X. Zhang, H. Xiao, and A. Men, "A modified wireless token ring protocol for wireless sensor network, *International Conference on Consumer Electronics* 2012, pp: 795-799.

Guangjie Han is currently a Professor with the Department of Information and Communication System, Hohai University, Changzhou, China. He received the Ph.D. degree from Northeastern University, Shenyang, China, in 2004. From 2004 to 2006, he was a Product Manager for the ZTE Company. In February 2008, he finished his work as a Postdoctoral Researcher with the Department of Computer Science, Chonnam National University, Gwangju, Korea. From October 2010 to 2011, he was a Visiting Research Scholar with Osaka University, Suita, Japan. He is the author of over 220 papers published in related international conference proceedings and journals, and is the holder of 90 patents.

His current research interests include sensor networks, computer communications, mobile cloud computing, and multimedia communication and security. Dr. Han has served as a Co-chair for more than 50 international conferences/workshops and as a Technical Program Committee member of more than 150 conferences. He has served on the Editorial Boards of up to 14 international journals, including the IEEE ACCESS, Telecommunication Systems, International Journal of Ad Hoc and Ubiquitous Computing, Journal of Internet Technology and KSII Transactions on Internet and Information Systems. He guest edited a number of special issues in IEEE Journals and Magazines. He has served as a Reviewer of more than 50 journals. He had been awarded the ComManTel 2014, ComComAP 2014, Chinacom 2014 and Qshine 2016 Best Paper Awards. He is a member of IEEE and ACM.

Lina Zhou received the B.S. degree from Hohai University, Changzhou, China, in 2015, where she is currently pursuing the M.S. degree with the College of Internet of Things Engineering. Her research interests include localization for wireless sensor networks.

Hao Wang received the B.S. degree from Nanjing Agriculture University, Nanjing, China, in 2015, where he is currently pursuing the M.S. degree with College of Internet of Things Engineering. His research interests include Protection of location privacy in wireless sensor networks.

Wenbo Zhang is currently a professor of School of Information Science \& Engineering, Shenyang Ligong University, China. He received his Ph.D. in Computer science at Northeastern University, China, in March 2006. He has

published over 100 papers in related international conferences and journals. He has served in the editorial board of up to 10 journals, including Chinese Journal of Electronics and Journal of Astronautics. He had been awarded the ICINIS 2011 Best Paper Awards and up to 9 Science and Technology Awards including the National Science and Technology Progress Award and Youth Science and Technology Awards from China Ordnance Society. His current research interests are Ad hoc networks, Sensor Networks, Satellite networks, Embedded systems.

Sammy Chan received the BE and MEngSc degrees in electrical engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and the PhD degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. From 1989 to 1994, he was with Telecom Australia Research Laboratories, first as a research engineer, and between 1992 and 1994 as a senior research engineer and project leader. Since December 1994, he has been with the Department of Electronic Engineering, City University of Hong Kong, where he is currently an associate professor.

Highlights for this paper are listed as follows:

Source location privacy issues have been extensively studied in the past years, but the balance of package delay and source safety time, energy consumption and network lifetime have yet to be explored. We therefore propose a source location protection protocol based on dynamic routing, taking both two pairs of relationship into account. The proposed protocol SLPDR can withstand hop-by-hop-trace attack and direction-oriented attack. We contribute to interchangeably use three categories of routing patterns: cyclic routing, greedy routing and directed routing. These three kinds of routing can be switched from one to another circumstantially. The simulation results demonstrate the effectiveness of our proposed protocol in source location protection and it outperforms other schemes.