

PTSLP: Position Tracking Based Source Location Privacy for Wireless Sensor Networks

Hao Wang¹, Guangjie Han^{1(✉)}, Chunsheng Zhu², and Sammy Chan³

¹ Department of Information and Communication Systems,
Hohai University, Changzhou 213022, China
wanghaohu@outlook.com, hanguangjie@gmail.com

² Department of Electrical and Computer Engineering,
The University of British Columbia, Vancouver, BC V6T 1Z4, Canada
cszhu@ece.ubc.ca

³ Department of Electronic Engineering,
City University of Hong Kong, Kowloon Tong, Hong Kong
eeschan@cityu.edu.hk

Abstract. Abundant experiments have shown that phantom source nodes cannot leave far away from the real source node. In this paper, we propose a novel position tracking based source location privacy (PTSLP) protection scheme for wireless sensor networks (WSNs). First, we construct a phantom area in order to make phantom source nodes being far from the real source node. Secondly, we combine shortest path routing and random routing to forward packets to sink node rather than deviating from sink node. Then, we make every packet pass through a special area called trace cost area which consists of many sensor nodes with different weights in different areas and finally reach the ring around sink node. Compared with SLP-E, which fails to take overlapping path into consideration, our proposed scheme can reduce overlapping path. Simulation results show that PTSLP can increase safety time and enhance source location privacy in WSNs.

Keywords: Wireless sensor networks · Source location privacy · Trace cost

1 Introduction

As an important part of the Internet of Things [1], wireless sensor networks (WSNs) [2–7] have played a vital role in military, healthcare, industry and many other fields to help people acquiring accurate and reliable information in any place any time, such as environment monitoring, disaster warning and traffic management. However, due to some common features of WSNs such as limited resources and simplified communication protocol, it is very easy for adversary to launch cyber attacks such as that which causes serious location privacy leakage problem [8]. For example, in animal-monitoring application, adversary can catch

animals' locations by monitoring traffic path [8]; in intelligent transportation, adversary can get users' privacy by analyzing users' trace and habit [9].

Nowadays, with the development of WSNs, source location privacy becomes a hot issue and raises a lot of attention. So far, privacy in WSNs can be categorized as data privacy and context privacy [10]. Data privacy aims to protect sensitive data collected by sensor nodes. For examples, methods like anonymous and recombination are used to protect data privacy. For context privacy, it mainly focuses on source location privacy (SLP) and sink location privacy. The main protections behind the context privacy (e.g., geographic routing [11], random walk [12], phantom source nodes [13], fake source nodes [14], etc.) are to prohibit adversaries from reaching the source node by analyzing data traffic and tracing back. In the classic Panda-Hunter model [8], when a sensor node detects the panda, it becomes the source node and sends message to the sink node periodically. Hunters can listen to the messages and trace back to the source node. In this model, location privacy is to prevent the adversary from finding panda while messages can be sent to sink node. As a solution, deploying phantom nodes can protect SLP to some extent. However, the scheme has a leakage that the adversary may find source node easily.

Considering the problems of phantom source node, in this paper, we propose a position tracking based source location privacy (PTSLP) protection mechanism for WSNs to prevent adversaries from reaching the source node and resist angle attack. We propose a new concept, trace cost, to formalize the difficulty that the adversary faces. Packets in a trace cost area are transmitted with random routing and thereby the safety time of the whole network is increased. In our scheme, steps can be summarized as follows.

- Establish a phantom area which is to decrease the probability of acquiring the real source node.
- Combine two routing strategies (i.e., shortest path routing and random routing) to make sure the packets can be transmitted to the sink node rather than deviating from sink node.
- Construct a trace cost area to further enhance SLP.
- Form a ring around the sink node to resist angle attack.

With these four steps, SLP is maintained and the safety time of network can be improved. In the first step, the phantom area is divided into several parts and all the phantom nodes are deployed in different parts. When a packet leaves the source node, it first starts a h -hop random walk to the phantom source node and is then routed to the sink node. In this way, the phantom source node can be far from the real source node. In the second step, by combining the shortest path routing and random routing, we make sure that the packet is routed toward the sink node rather than deviating from it. If we only use the random routing strategy, the packet has the probability that it cannot reach the sink node. In the third step, packets are routed with random routing in the trace cost area. For examples, the route may pass through mountains, plains or forests, which can slow down the adversary's tracking speed. In the fourth step, packets will be routed in a ring for several hops with different directions,

either in clockwise or anticlockwise, which can resist angle attack to some extent. Simulation results will show that PTSLP can increase safety time and improve source location privacy in WSNs, compared with SLP-E [15]. Even though SLP-E can make packets transmit in all directions, but it does not consider the situation that a phantom node can be selected as the source node's next hop for many times, which increases the energy consumption of nodes and overlapping degree of transmission path. When the overlapping degree of transmission path increases, the source location privacy decreases.

The rest of this paper is organized as follows. Section 2 presents the related work. Section 3 outlines the network model. Section 4 introduces the proposed PTSLP scheme. Section 5 shows the simulation results. Finally, Sect. 6 makes the conclusion.

2 Related Work

So far, many location privacy protection protocols have been proposed. Li *et al.* [10] summarized the traditional panda-hunter model. When a node detects the panda, it becomes a source node and sends packets to sink node periodically. He *et al.* [16] used flooding to send packets. However, this method sends packets to all the neighbor nodes and source location privacy mainly depends on the number of nodes between the source node and sink node. Moreover, flooding consumes too much energy and may not be suitable for large networks.

For the purpose of decreasing the negative effects of flooding, Lu *et al.* [17] presented a method using phantom source nodes to protect source location privacy. Each packet will first start a h -hop random walk. After the random walk finishes, the last node of the random walk becomes a phantom source node and then this phantom source node transmits packets to sink node by the shortest path routing or flooding. However, these phantom nodes cannot leave far away from the real source node. Thus, this approach may not provide enough privacy protection.

Yao *et al.* [18] used h -directed hop random walk to make phantom nodes far away from the real source node. In h -directed hop random walk, each packet is given a direction and neighbors of a node are divided into either the far or close list. Next hop is chosen in the far list which makes phantom source nodes far away from the real source node. However, these phantom nodes often gather close to each other.

In [15, 19] Chen *et al.* proposed a limited flooding protocol. First, the source node starts a limited flooding for h hops. After limited flooding finishes, a phantom area is formed and nodes within the phantom area become phantom source nodes. Second, each packet is transmitted in all directions to phantom source nodes. This method also takes visible area into consideration, which provides good source location privacy. But in each transmission, the real source node has to perform a limited flooding repeatedly, therefore consuming too much energy.

Moreover, in order to make phantom nodes to be deployed more uniformly and decrease overlapping transmitting paths, Zhao *et al.* [20] presented a protocol named RAPFPR based on angle and probability. First, a phantom area is

divided into several parts and packets are transmitted into different parts. Second, from a phantom source node to the sink node, RAPFPR takes probabilistic forwarding strategy that only some of the nodes take part in each transmission, which decreases overlapping paths. In [21] Zhang *et al.* presented EPURA and further addressed angle problem in phantom area. In [22] Liu *et al.* improved the energy consumption problem by choosing nodes with the minimum energy cost as next hop.

Wang *et al.* [23] presented a protocol named PRLA to protect source location privacy. In PRLA, a visible area is taken into consideration and a phantom area is formed by phantom nodes. First, when a packet leaves the source node, it will start a random walk for h hops and the last hop of the random walk becomes a phantom source node. Phantom source nodes work similarly as the real source node to confuse adversaries. After that, packets are routed from a phantom source node to sink node by the shortest path routing strategy.

3 Network Model

3.1 Scenario

We consider a scenario that all the sensor nodes are randomly deployed. Figure 1 shows our network model which is based on the model proposed in [15]. In our model, there are four kinds of nodes in the network: source node, sink node, ring nodes and common nodes. Once a sensor node detects the event, it becomes a source node. The source node will then generate encrypted event packets and send them to sink node periodically. However, an adversary, who tries to localize the source node, should be prevented from acquiring this kind of information. They usually try to locate the source node by hop by hop back tracking from the sink node. The purpose of our scheme is to protect the location of source node and increase the time that adversary takes to find the source.

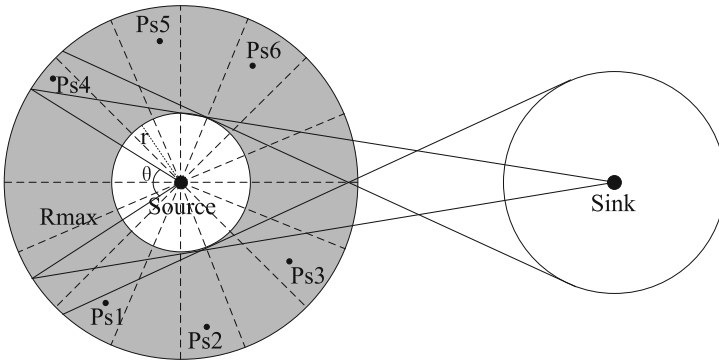


Fig. 1. Network model

3.2 Node Capability

We assume that nodes have the same capability of computing, communicating and storing. Each node only can have direct link with its one-hop neighbors. Moreover, all the sensor nodes in WSN are homogeneous, which means all the sensor nodes have the same initial energy levels and communication ranges. Each node is assigned a unique ID and a pair of public/private keys for encrypting and decrypting packets. Each node keeps a list of its neighbors which stores their IDs and communication information.

3.3 Adversary Model

Our adversary model is human, e.g., hunters. So, the adversary has to trace back on his own feet. The reason why we choose this restrictive model is that in the wild environment, the aim of hunters is to capture animals like panda, then hunters kill them or sell them. The more advanced equipment they use, the higher probability they will be found, because there are many monitoring systems in these rare animals shelter. In view of this, this adversary model is realistic. Commonly, an adversary has sufficient energy and enough memory for data storage, as well as equipment to monitor packets. The monitoring range of an adversary is equal to the communication radius of common nodes and the speed of an adversary can refer to speed of human. Moreover, in order not to be detected, the adversary only performs passive attacks such as traffic analysis and hop by hop back tracking.

4 Source Location Privacy Protection Based on Trace Cost

The proposed PTSLP is described in this section. Firstly, the sink node initializes the whole network by periodically broadcasting beacon messages. After the network initialization, every sensor node in the network knows their neighbors and parents. When a sensor node detects the event, it becomes a source node.

First, the source node will perform a h -hop random walk and thereby common nodes in h -hop random walk will get their distance to source node. Then, the source node will send packets for h -directed hops to phantom nodes. After a packet is routed to a phantom node, it will be routed to the sink node with the combined shortest path routing and random routing, then the packet will pass a sophisticated area which will increase the adversary's trace time. Finally, the packet will be routed to a ring node and then be routed to the sink node through the shortest path routing, which can resist angle attack to some extent. Detailed notations in our scheme are summarized in Table 1.

4.1 Network Initialization

The sink node broadcasts beacon messages periodically. When a node gets the broadcasted message, it first gets the hop information from the message and

Table 1. Parameter introduction

Parameter	Definition
h	The hop of random walk
H	The hop between source node and sink node
r	The radius of visible area
R	The communication radius of nodes
R_{max}	The max range of phantom area
r_s	The radius of ring around the sink node
α	The system constant
λ	The density of ring node
P_s	The Phantom source node
N	The number of sensor nodes

rebroadcasts the new message to its neighbors. Other nodes use the same method to get information about their hope distance to sink node. After all the nodes in network get the message, they will have the information of the hop counts to sink node. When a node detects an activity, it becomes the source node and then sends packets to sink node timely.

4.2 Phantom Area

When the network has been initialized, the source node will first calculate the range of the phantom area. As shown in Fig. 1, the shaded area is the phantom area and nodes such as Ps1, Ps2 are phantom source nodes. The phantom area is assumed to be a circle even though it is an uneven geographical environment. Nodes in phantom area will have a certain distance to source node. The distance to source node is obtained in the same way as the network initialization. The source node broadcasts beacon message periodically. When a node gets the message, it only records the minimum hop count. After these nodes get the hop counts to the source node, the phantom area is formed and is divided into several equal sectors. Each sector spans an angle θ , thereby we have $2\pi/\theta$ sectors.

Then the nodes in the visible area have to be removed. Because if nodes in these areas are chosen to be the next hop of the message, it is very easy for an adversary to trace back and finally catch source node since these nodes are extremely close to source node, and the adversary may monitor the communication among nodes and capture the packet, then reaches source node by tracing back hop by hop. So, in our scheme, we not only take visible area into consideration, but also expand the range of invalid region. By creating two tangents between visible area and the ring around sink node, then the overlapping area in phantom area is removed.

4.3 Combination of Two Routing Strategies

After a packet is routed to a phantom source node, then it will be transmitted to the ring nodes. Different from traditional routing strategy which uses only one routing method, in our scheme, we mix two routing strategies together: the shortest path routing and the random routing. Hence, when a node receives a packet, it will decide which routing strategy should be used.

In our scheme, we use a random number to make the two routing strategies work together. We first draw a random number between 0 and 1. If the number is larger than 0.7, the shortest path routing is selected, otherwise the random routing is selected.

The mixed routing strategy will work for a certain period. When choosing the next hop, our scheme first narrows the candidate region by using two tangents which is drawn from ring around the sink node to visible area. As shown in Fig. 2, the dotted lines between Ps1 and sink node are two tangents. Each node first draws two tangents and then next hop is selected in tangent area to make sure packets will be routed to the sink node instead of getting far away from sink node. Other sensor nodes work likewise.

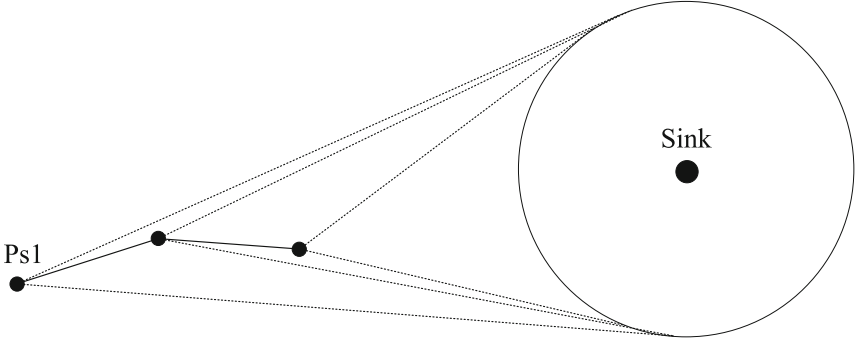


Fig. 2. Combination of two routing strategies

In the tangent area, our scheme increases the angle of invalid region of the phantom area. As shown in Fig. 1, for common visible area, the angle of invalid area can be calculated by the following equation:

$$\theta = \frac{\arcsin(\frac{r}{R_{max}}) + \arcsin(\frac{r}{H})}{\pi} \quad (1)$$

where H is the distance between the real source node and the sink node, r is the radius of the visible area, R_{max} is the radius of the phantom area.

When we take account of two tangents, this angle will get bigger. After combination of two routing strategy, packets will be transformed into the trace cost area and ring around the sink node. The trace cost area is a special area in which packets are routed by random routing and nodes in this area are mainly deployed in mountains, plains, and forests, which conforms to real environment.

4.4 Ring Routing Around Sink Node

Ring around the sink node is shown in Fig. 3. After a packet passes the trace cost area, it will be relayed to nodes in the ring around the sink node. In order to form the ring, some parts of the network are divided into small grids and several nodes will be placed in each grid. Ring nodes are randomly chosen from the nearby grid according to the residual energy of nodes, which means a node that has more residual energy has a higher likelihood to be arranged as a ring node.

Ring nodes will consume huge energy after several turns since all the packets are transmitted to ring nodes. Hence, ring nodes can be replaced by nodes in the corresponding grids. When a packet arrives at a ring node, it creates a random hop. This hop represents how long the packet can be transmitted. During each transmission, this random hop has two opposite directions: clockwise and anticlockwise. Transmitting in this way can prevent adversary from deducing the location of the source node by reverse extension cord of each packet. By the end of random hop, packets will be routed to sink node by shortest path routing.

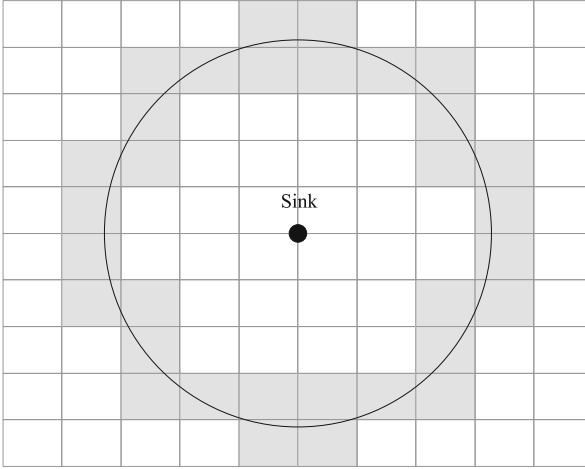


Fig. 3. Ring routing around the sink node

For reducing the energy consumption, we adapt the formula in [24] to calculate the radius of the ring around the sink node. We first set the sink node as center to establish axis and partition the ring into 8 parts. Energy consumption is proportional to the square of distance as the following equation:

$$\epsilon_{total} = 8\alpha\lambda \int_0^{\frac{\pi}{4}} \int_0^{\frac{s}{\cos\theta}} (r - e)^2 r dr d\theta \quad (2)$$

After derivation, we can evaluate the suitable ring radius.

5 Performance Evaluation

In this section, we evaluate our scheme through extensive simulations. We mainly consider two metrics: safety time and energy cost. Energy cost is the average energy consumed by nodes during one round data transmission. We use the number of hops to represent safety time and safety time is the number of packets that have been sent to sink node before the source node is captured by the adversary.

5.1 Simulation Environment

We have implemented the proposed PTSLP with MATLAB. In our simulation, 1000 nodes are deployed in a 600 m * 600 m square area. The communication radius of a node is 30 m. The radius of the ring and the visible area are 75 m and 50 m respectively and the maximum range of the phantom area is 150 m. For each transmission in network, there only exists a source node and a sink node. The simulation is performed for 400 times.

The performance of the PTSLP simulation is evaluated by two parameters, safety time and energy cost. We analyze the two parameters by varying the random walk hops from 2 to 10 and the hops between source node and sink node from 12 to 20. Then, safety time and energy cost of PTSLP and SLP-E [15] are compared.

5.2 Simulation Results of Safety Time

We evaluate the performance of our scheme by varying the hops of the random walk between 2 and 10 and the hops between source node and sink node from 12 to 20. The simulation results are shown in Figs. 4 and 5.

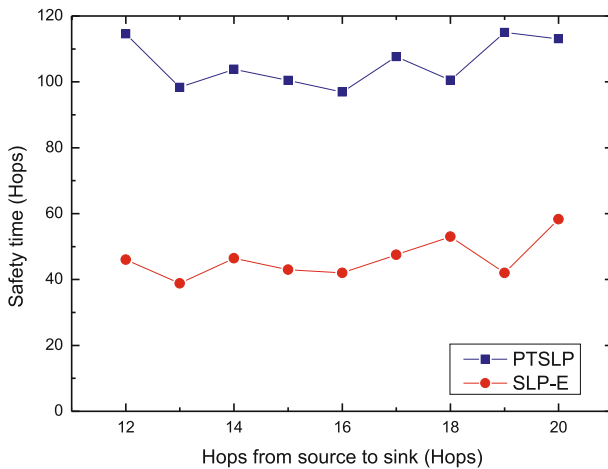


Fig. 4. Safety time under hops from source to sink

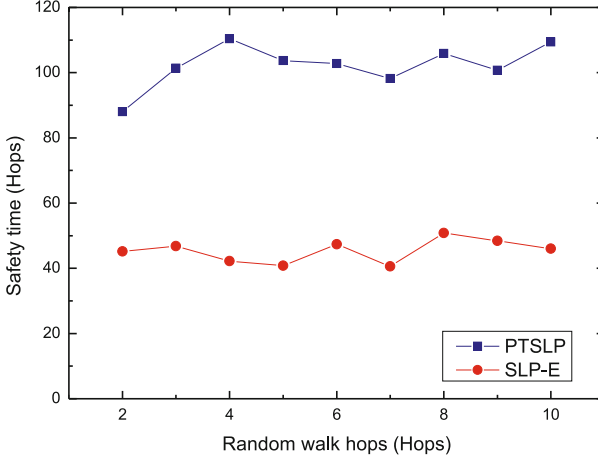


Fig. 5. Safety time under random walk hops

As presented in Fig. 4, safety time fluctuates when hops from source to sink varies. The reason that safety time is not linear is that each packet has to pass the trace cost area, and in this area, packets are routed in the random routing strategy. So the main determination of safety time depends on hops in the trace cost area while hops from source to sink play an auxiliary function in safety time. But when the number of hops increase, the safety time tends to increase and the safety time of our scheme is acceptable.

As shown in Fig. 5, when hops of the random walk varies, the overall performance of safety time is rising even though with some fluctuation. The reason is that these nodes are closer to sink node compared with other nodes at 4 to 6 random hops. Moreover, the transmission path of these nodes in the trace cost area are not long enough, so safety time decreases.

5.3 Simulation Results of Energy Cost

We compare the energy cost of PTSLP and SLP-E under two different variables: the random walk hops and the hops from source node to sink node.

As shown in Fig. 6, the overall trend of energy cost is ascendant. When the hops of the random walk increase progressively, energy cost increases steadily even in the middle of line chart declines for a little. It is because energy cost is proportional to hops while hops are composed of several parts. Energy cost will change when parts of hops change. The maximum energy cost stays in the trace cost area and it varies greatly. So, as explained in Sect. 4.2, the trend of energy cost mainly depends on hops in the trace cost area.

As shown in Fig. 7, the tendency of energy cost is steady. When we do not consider the first point, we can see energy cost enhances when hops from source node to sink node increases. The reason is that when hops from source node to sink node increase, each packet needs more hops to be relayed. The increased hops account for why energy cost grows.

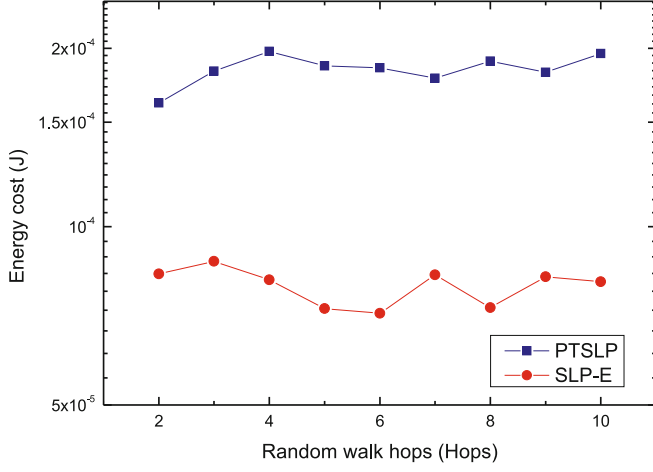


Fig. 6. Energy cost under random walk hops

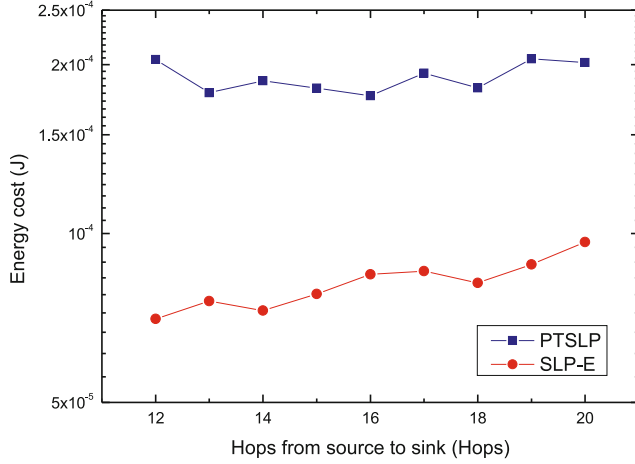


Fig. 7. Energy cost under hops from source to sink

6 Conclusion

In this paper, we have proposed the PTSLP protection mechanism for WSNs. Particularly, by utilizing the phantom source nodes and two routing strategies, source location privacy in WSNs can be maintained. In addition, the ring around the sink node can prevent the adversary from the angle attack in WSNs. Simulation results have shown that the proposed PTSLP mechanism is able to improve the safety time for WSNs, compared with SLP-E.

Acknowledgement. The work is supported by “Qing Lan Project” and “the National Natural Science Foundation of China under Grant No. 61572172 and No. 61602152” and supported by “the Fundamental Research Funds for the Central Universities, No. 2016B10714 and No. 2016B03114 and supported by “Changzhou Sciences and Technology Program, No. CE20165023 and No. CE20160014”.

References

1. Zhu, C., Leung, V.C.M., Shu, L., Ngai, E.C.-H.: Green Internet of Things for smart world. *IEEE Access*. **3**, 2151–2162 (2015)
2. Han, G., Jiang, J., Shu, L., Niu, J., Chao, H.C.: Managements and applications of trust in wireless sensor networks: a survey. *J. Comput. Syst. Sci.* **80**, 602–617 (2014)
3. Han, G., Jiang, J., Zhang, C., Duong, T.Q., Guizani, M., Karagiannis, G.K.: A survey on mobile anchor node assisted localization in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **18**, 2220–2243 (2016)
4. Wan, L., Han, G., Shu, L., Feng, N., Zhu, C., Lloret, J.: Distributed parameter estimation for mobile wireless sensor network based on cloud computing in battlefield surveillance system. *IEEE Access*. **3**, 1729–1739 (2015)
5. Zhu, C., Yang, L.T., Shu, L., Leung, V.C.M., Hara, T., Nishio, S.: Insights of top-k query in duty-cycled wireless sensor networks. *IEEE Trans. Ind. Electron.* **62**, 1317–1328 (2015)
6. Han, G., Liu, L., Jiang, J., Shu, L., Hancke, G.: Analysis of energy-efficient connected target coverage algorithms for industrial wireless sensor networks. *IEEE Trans. Ind. Inform.* **13**, 135–143 (2015)
7. Han, G., Dong, Y., Guo, H., Shu, L., Wu, D.: Cross-layer optimized routing in wireless sensor networks with duty-cycle and energy harvesting. *Wirel. Commun. Mob. Comput.* **15**, 1957–1981 (2015)
8. Peng, H., Chen, H., Hang, X., Fan, Y., Li, C.P., Li, D.: Location privacy preservation in wireless sensor networks. *J. Softw.* **26**, 617–639 (2015)
9. Chen, H., Wei, L.: On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks. *Pervasive Mob. Comput.* **16**, 36–50 (2014). Elsevier B.V
10. Li, N., Zhang, N., Das, S., Thuraishingham, B.: A state-of-the-art survey. *Ad Hoc Netw.* **7**, 1501–1514 (2009)
11. Zhu, C., Yang, L.T., Shu, L., Leung, V.C.M., Rodrigues, J., Wang, L.: Sleep scheduling for geographic routing in duty-cycled mobile sensor networks. *IEEE Trans. Ind. Electron.* **61**, 6346–6355 (2014)
12. Jia, D., Chi, Y.: REAL: a reciprocal protocol for location privacy in wireless sensor networks. *IEEE Trans. Dependable Secur. Comput.* **12**, 458–471 (2015)
13. Conti, M., Willemsen, J., Crispo, B.: Providing source location privacy in wireless sensor networks: a survey. *IEEE Commun. Surv. Tutor.* **15**, 1238–1280 (2013)
14. Jhumka, A., Bradbury, M., Leeke, M.: Fake source-based source location privacy in wireless sensor networks. *Concurr. Comput. Pract. Exp.* **27**, 189–203 (2014)
15. Chen, J., Lin, Z., Hu, Y., Wang, B.: Hiding the source based on limited flooding for sensor networks. *Sensors* **15**, 29129–29148 (2015)
16. He, W., Liu, X., Nguyen, H., Nahrstedt, K.: A cluster-based protocol to enforce integrity and preserve privacy in data aggregation. In: 29th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS Workshops 2009), pp. 14–19. IEEE, Los Alamitos. IEEE Computer Society (2009)

17. Lu, M., Zhao, Z., Tang, X., Zhou, J.: Research on phantom routing to provide source-location privacy in wireless sensor network. *Inf. Technol.* **10**, 72–79 (2012)
18. Yao, J., Hao, X., Wen, G.: Location privacy protecting in wireless sensor networks. *Chin. J. Sens. Actuators* **21**, 1437–1441 (2008)
19. Chen, J., Fang, B., Yin, L., Su, S.: A source-location privacy preservation protocol in wireless sensor networks using source-based restricted flooding. *Chin. J. Comput.* **33**, 1736–1749 (2010)
20. Zhao, Z., Liu, Y., Zhang, F., Zhou, J., Zhang, P.: Research on source location privacy routing based on angle and probability in wireless sensor networks. *J. Shandong Univ. (Nat. Sci.)* **48**, 1–9 (2013)
21. Zhang, Y., Xu, Y., Wu, X.: Enhanced source-location privacy preservation protocol using random angle. *Comput. Eng. Appl.* **52**, 1–8 (2015)
22. Liu, X., Li, J., Li, B.: Source-location privacy protocol based on the minimum cost routing. *Chin. J. Sens. Actuators* **27**, 394–400 (2014)
23. Wang, W., Chen, L., Wang, J.: A source-location privacy protocol in WSN based on locational angle. In: *Proceedings of the IEEE International Conference Communications*, pp. 1630–1634. IEEE Press, Beijing (2008)
24. Li, Y., Ren, J., Wu, J.: Quantitative measurement and design of source-location privacy schemes for wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **23**, 1302–1311 (2012)

Radio Frequency Identification and IoT Security
12th International Workshop, RFIDSec 2016, Hong
Kong, China, November 30 -- December 2, 2016,
Revised Selected Papers
Hancke, G.P.; Markantonakis, K. (Eds.)
2017, X, 205 p. 56 illus., Softcover
ISBN: 978-3-319-62023-7