From Nowhere to Somewhere: Protecting End-to-End Location Privacy in Wireless Sensor Networks

Honglong Chen and Wei Lou
Department of Computing, The Hong Kong Polytechnic University, Hong Kong
Email: {cshlchen, csweilou}@comp.polyu.edu.hk

Abstract

Wireless sensor networks (WSNs) are often deployed in hostile environments for specific applications from mobile objects monitoring to data collecting. By eavesdropping the sensor nodes' transmissions and tracing the packets' trajectories in the WSNs, an adversary can capture the location of a source or sink eventually. Thus, the location privacy of both source and sink becomes a significant issue in WSNs. Previous research only focuses on the location privacy of the source or sink independently. In this paper, we address the importance of location privacy of both source and sink and propose four schemes to protect them simultaneously. Simulation results illustrate the effectiveness of our proposed schemes.

Keywords: Location Privacy; Secure Routing; Wireless Sensor Networks.

1 Introduction

Wireless sensor networks (WSNs) are made up of a number of sensor nodes that are self-organized to carry out tasks such as mobile objects monitoring and environmental sensing. Because they use wireless communications, which can be accessed by anyone who wishes, it is not difficult to attack wireless networks with the goal of either obtaining confidential data or simply disrupting the normal operation of the WSNs [1]. In either case, they may involve threats to one of two types of WSN privacy, *content* privacy and *contextual* privacy [2]. The content privacy refers to the confidentiality of the content of the packets passing between the nodes in the network. This is usually guaranteed by using methods of encryption and authentication [3]. The contextual privacy refers to the confidentiality of information about traffic patterns in the network, which attackers may use to disrupt the network. The location privacy, which is the confidentiality of the location of either source or sink nodes, is a kind of the contextual privacy.

This work is supported in part by grants PolyU 5236/06E, PolyU 5243/08E, PolyU 5253/09E, 1-ZV5N, ZJU-SKL ICT0903.

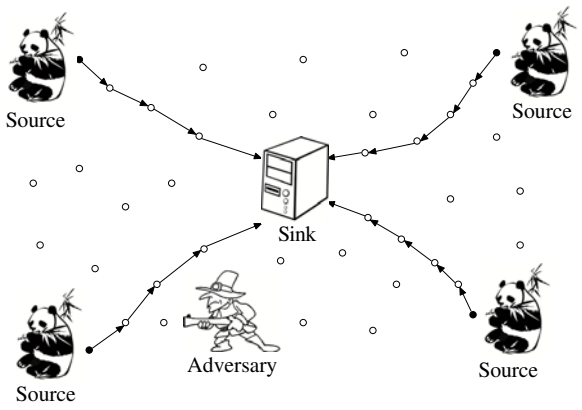

Figure 1. Location privacy sensitive scenario.

To illustrate how information about traffic patterns in a network might be exploited by an adversary, consider the scenario of "panda-hunter" [2] in Figure 1, which shows a typical WSN where sensor nodes monitor the pandas in the environment and then send report packets to a sink by multi-hop wireless communications. There is a central controller (sink in Figure 1) and several pandas in the monitoring field. The sensor nodes which monitor the pandas will act as the source nodes and they will report the monitored information to the central controller via WSN periodically. The scenario is obvious unsafe as the hunter (adversary in Figure 1) is easily able to either locate a source by back tracing hop-by-hop to capture the panda or locate a receiver by following the flow of packets in the network to destroy the central controller, which will make the whole system crash. The challenge in the scenario is essentially to protect the end-to-end location privacy rather than merely the source or sink location privacy. Thus, the end-to-end location privacy protection becomes one of the most important contextual privacy problems in the WSNs.

Lots of location privacy routing techniques in WSNs

978-1-4244-9328-9/10/$26.00 ©2010 IEEE

have been developed in the past decade. However, these proposed techniques can only protect the source location privacy or the sink location privacy independently. In this paper we propose four end-to-end location privacy protection techniques to protect against a local eavesdropper who might breach the location privacy of a source or sink, that is, end-to-end location privacy. The four schemes are forward random walk, bidirectional tree, dynamic bidirectional tree and zigzag bidirectional tree. In the forward random walk approach, every node relays a received packet to a node randomly chosen from its forward neighbors whose hop-count to the sink is no larger than its own. This procedure is repeated at each node until the packet arrives at the sink. To increase the location anonymity, tree topology is employed at the two ends of the routing path respectively in the bidirectional tree scheme. In the dynamic bidirectional tree scheme, branches of the trees are generated dynamically which can improve the performance. However, in the bidirectional tree scheme, real messages routed along a shortest path, which makes it possible for an eavesdropper to infer the location of the source and sink by extending the line of the shortest path. To solve this potential threat, a proxy source and a proxy sink are devised in the zigzag bidirectional tree scheme, making it more difficult for the adversary to obtain the location of the source and sink.

The main contributions of this paper can be summarized as follows:

- We address the importance of simultaneously protecting the location privacy of both source and sink;
- We propose four privacy routing schemes to preserve the end-to-end location privacy against a local eavesdropper;
- We demonstrate the effectiveness of our proposed schemes with simulations.

The rest of this paper is organized as follows. Section II reviews the existing privacy routing techniques. Section III describes the system scenario and the adversary model. Section IV describes our proposed four privacy routing schemes. Section V evaluates the performance of the proposed schemes under the TOSSIM platform. Finally, Section VI concludes this paper and puts forward the future work.

2 Related Work

Many techniques have been proposed for the protection of the source location privacy in WSNs. [2] and [4] have proposed a source location privacy scheme that makes use of the *Panda-Hunter* problem as an application scenario for monitoring-oriented sensor networks where the location privacy is important. The *Phantom routing* protocol makes use of a random walk to prevent attackers from identifying the source. Xi *et al.* [5] have proposed a two-way random walk routing protocol (from both source and sink) called greedy random walk which can reduce the opportunity for an eavesdropper to collect the location information. PRLA [6] protects the source location privacy by using so-called inclination angles to ensure that every random walk gets away from the region close to the source, which enhances the source location privacy. In [7], loops are generated in the network. The adversary has to go around these loops, thereby being led away from the real path, which guarantees high privacy. A suboptimal privacy routing scheme called WRS has been proposed in [8] to protect the source location privacy by distributing message flows to different disjoint routes. It also formulates the performance bound for any routing scheme. Jian *et al.* [9] protect the source location privacy through a two-phase routing process. In the first phase, the packet travels randomly through the intermediate nodes before it is routed to a ring node. Then the packet is mixed with other packets through a network mixing ring (NMR). In [10] two techniques called *periodic collection* and *source simulation* are proposed. In the periodic collection, every node sends messages periodically, making the network n-anonymous. In the source simulation, it provides trade-offs between privacy, communication cost and latency. Four schemes named *naive*, *global*, *greedy* and *probabilistic* are proposed in [11] to provide location privacy against a laptop-class attack. Yang *et al.* [12] propose to use proxies to protect the source location of an event. A prototype of the scheme is implemented on Mica2 motes. In [13] FitProbRate is proposed, which first adopts the statistically strong source anonymity to reduce the latency efficiently.

Sink location privacy has also been well studied. In [14], Deng *et al.* have proposed a base station privacy scheme against the traffic-rate analysis attack that randomly delays the transmission time of each packet. They have also proposed in [15] to defend against the traffic analysis attacks by using multi-path routing and fake message injection to hide the location of the base station. LPR [16] provides the receiver location privacy against the packet tracing attacks. In LPR, the message flows incoming from and outgoing to a sensor node are uniformly distributed, which makes it difficult for an adversary to ascertain the direction of the sink. Moreover, LPR injects fake messages into the network to get a longer safety period.

However, the common drawback of all these approaches is that they only consider the location privacy of the source or sink independently, while it is particular important to protect the location privacy of both simultaneously for some application scenarios such as the one illustrated in Fig-

ure 1. In this paper, we aim to combine the protection of the source location privacy and the sink location privacy together. Thus, four end-to-end location privacy protection techniques against the local eavesdropper are proposed in this paper.

3 Problem Statement

In this section, we will describe a generic scenario in which a WSN is potentially threatened by a particular adversary, where the adversary seeks to breach the location privacy of a source or sink in the network. After that we will introduce the adversary model in detail.

We consider a scenario where a WSN is deployed for pandas monitoring. The WSN is comprised of a sink node and many sensor nodes among which the packets flow from certain source nodes to the sink. As the WSN is potentially threatened by a particular adversary, where the adversary seeks to breach the location privacy of a source or sink in the network, it is equally important to protect the location privacy of the sources and sink simultaneously. We use the arrangement illustrated in Figure 1, the sensor nodes which monitor the pandas (stationary or nomadic), will act as sources and periodically send reports of their surveillance to a static central controller. Routing strategies are demanded to protect the location privacy of the pandas and the central controller, i.e., the sources and the sink.

We assume that all the sensor nodes are identically configured, thus, they have the same capability and communication range r. Two sensor nodes can communicate with each other when their distance is less than r. The sink is assumed to have greater capabilities than the sensor nodes. During the initialization phase of the network, the sink originates a flooding, which provides each sensor node three kinds of information: 1) the least hop count from itself to the sink; 2) its neighboring nodes; 3) the least hop count from each neighboring node to the sink. During the report period T_r, each source sends a packet to the sink periodically with an interval of T_S using certain routing strategies. The location privacy of sources and sink are regarded as intact if none of them can be identified by the adversary within T_r.

We assume attackers to be equipped with some powerful devices that can be used to locate the sender of a transmitted packet. Attackers can also move freely in the network. Typically, attackers against the contextual privacy are of two classes: *local* (or *mote-class*) attackers and *global* (or *laptop-class*) attackers [17]. Local attackers are assumed to have a local view of the network traffic, which means that they can only eavesdrop on the packets within the transmission range. Global attackers acquire a global view of the network traffic, based on which they can intercept every packet in the network. The global attackers have serious effects on the network but they are very difficult to implement, especially in a large scale wireless sensor network. In this paper, we focus on the location privacy protection of both source and sink against the local adversary.

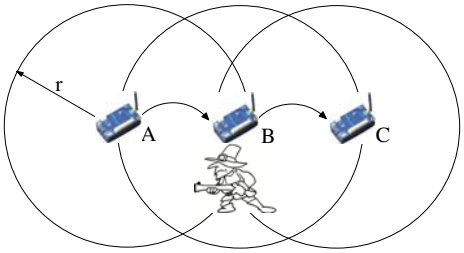

Figure 2. The adversary eavesdrops on packets in the network.

We assume that each message transmitted in the network is encrypted and the adversary cannot access the content. Thus, a local adversary is reduced to identifying either source (or sink) by analyzing the traffic flow and tracing back (or forth) hop-by-hop. We define the characteristics of a local adversary as follows, some of which are borrowed from the "panda-hunter" model [2]: 1) The adversary randomly walks in the network until it eavesdrops a packet transmitted by some sensor node. The adversary then randomly decides whether to trace the source (capture the pandas) or sink (destroy the whole system). 2) The adversary is equipped with powerful devices, such as antenna and spectrum analyzer, which can be used to measure the arriving angle and the received signal strength of a message. Based on the above two measurements, the adversary can identify the location of the immediate sender. 3) The adversary is able to detect the target (the source or sink) when it is close enough. 4) The movement of the adversary is far slower than the transmitting speed of a packet in the network. Therefore, the adversary can only trace the flow by one hop for one packet transmission. 5) The adversary will not actively interfere with the packet transmission in the network as there may exist intrusion detection mechanisms. 6) The adversary has enough memory space to save the trace information, and if it receives no more packets for some time, it may retreat to a previous location. 7) According to Kerckhoff's Principle, the adversary is aware of the routing strategies of the network.

An adversary can initially move around and wait for eavesdropping a message. As soon as it detects a new packet, it can determine the location of the immediate sender for tracing the source. It can then move to that location and wait there for the next packet. To trace the sink, the adversary needs to identify the direction of the packet and then moves to the receiver of the packet. In Figure 2 for example, the adversary stays at node B. If the adversary

wants to trace the source, it will move to node A as soon as node A transmits a packet to node B. On the other hand, if the adversary wants to trace the sink, it can identify the direction of the packet as follows: It detects a packet transmitted from node A when node A sends a packet to node B. Shortly after that, node B transmits a packet and soon again after node C transmits a packet. The adversary identifies the transmission sequence A→B→C and node C is the last receiver. The adversary then moves to node C.

In this paper we assume that the adversary behaves according to one of two models: the patient adversary model and the cautious adversary model. In both models, the adversary first randomly walks and detects packets in the network. As soon as it detects a packet, it triggers a hop-by-hop tracing procedure to capture either the source or the sink. In the patient adversary model, the adversary will use the above technique patiently until it captures its target, i.e., the source or sink. In the cautious adversary model, the adversary will trace back if it waits for a given period at some location. We define the path that the adversary visited as $V = \{v_1, v_2, ..., v_{l-1}, v_l\}$, where v_l is the current location of the adversary. When the adversary has not received any new packet within a specific interval at v_l, it will trace back along V to v_{l-1}, delete v_l in V and then wait there for new packet. We define the set of locations that the adversary has visited and traced back as F. To avoid invalid tracing, when the adversary traces back from v_l to v_{l-1}, it will add v_l into F, and ignore packets coming from any location in F. Also, the adversary can avoid getting lost in a loop with loop detection techniques.

4 Location Privacy Protection Techniques

The location privacy is vulnerable when the packets travel from source to sink since the adversary can trace the source or sink by monitoring the packets flow in the network. Thus, the primary purpose of privacy routing protocols is to protect the location privacy of both the source and sink during the report period T_r. This section describes our proposed four routing schemes for protecting the end-to-end location privacy: forward random walk, bidirectional tree, dynamic bidirectional tree and zigzag bidirectional tree schemes.

4.1 Forward Random Walk Scheme

In the sample network in Figure 1, the source periodically sends packets to the sink by multi-hop wireless communications during the report period T_r. If the packets always travel from the source to the sink along a fixed route, it will be easy for an adversary to capture either the source or the sink via hop-by-hop tracing. Therefore, a solution to achieve end-to-end location privacy is to randomize the routing path, based on which we propose the *forward random walk* scheme (FRW).

The FRW requires all the nodes in the network to obtain their hop counts to the sink, which can be achieved using a sink-based flooding. At the end of the flooding, each node can get both its own and its neighbors' hop counts to the sink. Let the hop count of node i be H_i, then it satisfies $|H_i - H_j| \leq 1$, where node j is a neighbor of node i and H_j is the hop count of node j.

In the FRW scheme, every node divides its neighbors into three lists, *further list*, *equivalent list* and *closer list*. Each neighbor in the further list has a larger hop count than the sender, while each neighbor in the closer list has a smaller hop count than itself. The node' equivalent list consists of neighbors that have the same hop count with itself. The combination of the equivalent list and closer list forms the *forward list*. When forwarding a packet, the node will randomly select a neighbor from its forward list as the next hop. Neighbors in the further list will not be considered as the candidates for the next hop since they will remarkably increase the latency. Consequently, the packet will be randomly forwarded from source to sink.

The FRW scheme protects the end-to-end location privacy by randomizing the routing path. However, its latency will be large since the forward random walk lengthens the routing path. Furthermore, the FRW scheme relays packets only to the neighbors in the forward list, resulting in that it can not obtain a high location privacy. A method to achieve a high location privacy is to inject *dummy messages* into the network. We define the *real messages* as the report packets transmitted from the source to sink and the *dummy messages* are the packets with no useful content and they are generated to draw the adversary away from the actual path.

4.2 Bidirectional Tree Scheme

In the hostile network, as the adversary can threaten the location privacy of the source or sink by monitoring the packets flow, an effective idea to defend against the threat is to let the source and sink hide in the branches of a tree topology, which requires the adversary to consume more time on discovering them. Therefore, we employ the tree topology in the BT scheme to protect the end-to-end location privacy. Figure 3 shows the main idea of the BT scheme. The real messages travel along the shortest path from the source to the sink. To protect the source location privacy, branches are designed along the shortest path in the source side, in which the dummy messages travel from the leaf nodes to the stalk nodes. As the adversary would trace the source by moving backward the direction of the packets, it makes the adversary deviate from the real path, which can protect the source location privacy. Similarly, the branches along the shortest path in the sink side are designed to protect the

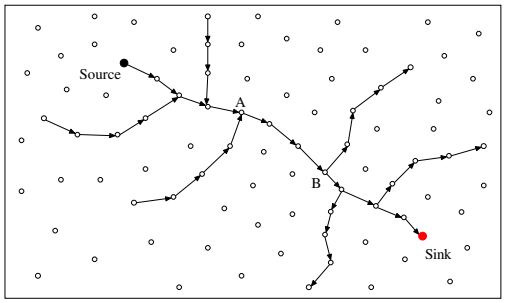

Figure 3. The scenario for the bidirectional tree scheme.

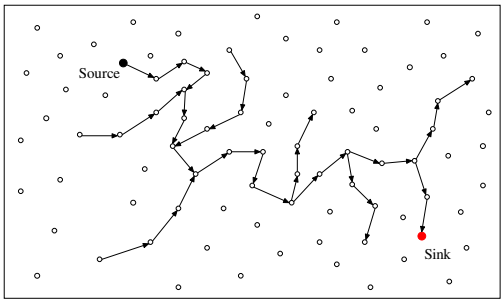

Figure 4. The scenario for the dynamic bidirectional tree scheme.

sink location privacy. The dummy messages in the branches travel from the stalk nodes to the leaf nodes, which can draw the adversary away from the real path to protect the sink location privacy since the adversary would trace the sink by moving forward the direction of the packets.

Initially, the sink originates a flooding such that each node can obtain the hop count to the sink. Before sending report messages to the sink, the source generates a routing request message including its hop count H_s and sends it to the sink along the shortest path. For each node who receives the routing request message, if its hop count to the sink is larger than $(1 - \frac{\alpha}{2})H_s$, it will randomly select a neighbor with probability P to generate a branch, where α is the percentage of the nodes on the shortest path that generate the tree branches to protect the location privacy of the source or sink. Meanwhile, for each node who receives the routing request message and its hop count is less than $\frac{\alpha}{2}H_s$, it will randomly select a neighbor with probability P to generate a branch, which can protect the sink location privacy.

For instance, if $\alpha = 2/3$, each node on the shortest path with a hop count larger than $\frac{2}{3}H_s$ will originate a branch with probability P to protect the source location privacy. Each node on the shortest path with a hop count less than $\frac{1}{3}H_s$ will also originate a branch with probability P to protect the sink location privacy. The nodes in-between just relay the routing request message along the shortest path to the sink.

The dummy messages in the branches can entice the adversary to get away from the real path. Thus, the BT scheme can obtain a high location privacy against a local eavesdropper. However, there is still a potential threat in the BT scheme. As shown in Figure 3, the adversary may be misled, getting lost in the path between A and the source or in the path between B and the sink. However, a powerful adversary may infer the direction of the target based on its visited path V (as mentioned in the adversary model). If the adversary is searching for the source when it is near to B. As the real messages travel along the shortest path, the adversary can trace hop-by-hop from B to A. Then the adversary can infer that the source should be on the extending line of $\overline{BA}$. Thus, the adversary can move directly along $\overline{BA}$ from A and it can identify the source as soon as it gets close enough with a high probability. The adversary can also use the same strategy to infer the direction of the sink.

4.3 Dynamic Bidirectional Tree Scheme

To prevent the adversary from inferring the direction of the source or sink as mentioned above, the dynamic bidirectional tree (DBT) scheme combines the FRW scheme and the BT scheme. Figure 4 shows the main idea of the DBT scheme. The paths for the real message vary over time, which greatly increases the tracing difficulty for the adversary as it prevents the adversary from inferring the direction of the target.

Initially, the sink triggers a flooding such that each node can get its hop count to the sink. During the report period T_r in which the source periodically sends reporting packets to the sink by multi-hop wireless communications, each node who receives the reporting packet will randomly select a neighbor from its *forward* list to forward the received reporting packet. Therefore, the real messages travel with a forward random walk mode from source to sink.

To protect the source location privacy, a dynamic tree topology will be adopted. Assume that the hop count of the source is H_s. When a node i receives a real message from its neighbor j, it will forward the real message to the next hop, which is randomly selected from its *forward list*. Also, if its hop count is larger than $H_s/2$ but smaller than H_j, it will generate a source side's branch with probability P using a method similar to that in the BT scheme. The essential difference is that each fake source will only send L dummy messages. Otherwise, if its hop count is smaller than both $H_s/2$ and H_j, it will generate a sink side's branch with probability P using a method similar to that in the BT scheme. The difference is that when a node receives a dummy mes-

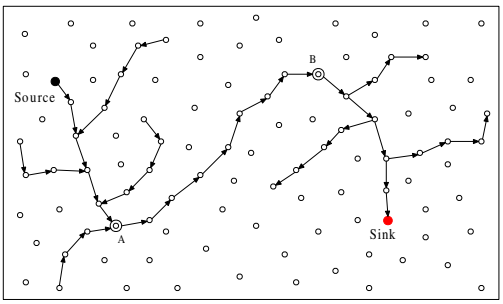

Figure 5. The scenario for the zigzag bidirectional tree scheme. Concentric circle A represents a proxy source and B represents a proxy sink.

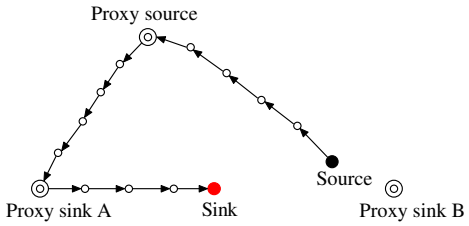

Figure 6. Proxy sink and proxy source selection for zigzag bidirectional tree scheme.

sage, it will reselect a child node to relay this dummy message.

4.4 Zigzag Bidirectional Tree Scheme

The zigzag bidirectional tree scheme (ZBT) is another location privacy protection scheme we propose to prevent the adversary from inferring the direction of the source or sink. In the ZBT, the proxy source and the proxy sink are employed. The real messages travel along three segments: from the source to the proxy source, from the proxy source to the proxy sink and from the proxy sink to the real sink. As shown in Figure 5, concentric circle A represents a proxy source and B represents a proxy sink. In the path from source to A, there will be tree branches to lead the adversary away from the real path. From A to B, the packets will travel along the shortest path. And in the path from B to the sink, there will also be tree branches to protect the sink location privacy.

To guarantee the effectiveness of the ZBT scheme, two proxy sink candidates are generated, which are deployed at the two opposite sides of the sink. Otherwise, if only one proxy sink candidate exists and the source is very close to this proxy sink, then the branches on the source side will be invalid in protecting the source location privacy. As shown in Figure 6, if the source is close to proxy sink B and proxy sink B is selected as the proxy sink, then the path from the source to proxy source and the path from proxy source to proxy sink B will be very close to each other, it will be vulnerable if the adversary traces from proxy sink B to capture the source as the source is close to proxy sink B. Thus, we can generate two candidates on the two opposite sides of the sink as the proxy sink nodes. We can make the distances between the sink and the proxies approximate to hr, which makes the hop count from each proxy sink to the sink proximate to h. The sink and the two proxy sink nodes initiate flooding so that the hop counts to each of them can be obtained by every node in the network. As the zigzag routing will be invalid if the proxy sink is close to the source, the source will always select the candidate further away from itself as the proxy sink (Proxy sink A is selected in Figure. 6). To determine the source proxy, the source can initiate a h-hops flooding. Before delivering the report packets to the sink, the source will select a node which is h hops away from itself as the source proxy. Note that the proxy source should be carefully selected to make the path from the source to proxy source away from the sink, making the sink safe when the adversary traces along this path.

Similar to the BT scheme, as shown in Figure 5, when the reporting packet travels between the source and proxy source, each node in the path will generate a branch with probability P and TTL of L. When the report packet travels from proxy sink to the sink, it will also generate a branch with probability P and TTL of L. The real packet will travel along the shortest path from the proxy source to the proxy sink and no branch will be generated on this path.

5 Performance Evaluation

We implement our proposed end-to-end location privacy protection schemes on TOSSIM platform to illustrate their effectiveness. The topology of the network is generated by uniformly deploying 3000 sensor nodes within a rectangular area of 30×100. The communication range of each sensor node is 1.67. The average number of neighbor for a node is 8.76. We evaluate our proposed schemes in term of *safety period* which begins from the moment the adversary triggers the tracing procedure (i.e., detects the first packet) and ends at the moment when the adversary identifies the source or sink. It is measured using the ratio of the time period before the adversary identifies the source or sink to the length of interval T_s. Two different adversary models, i.e., the patient adversary model and the cautious adversary model are considered in the simulations.

The parameter settings are as follows: Each node who relays the real packet has the probability $P = 0.8$ to generate a branch, the length of each branch is $L = 10$. α is set as 1

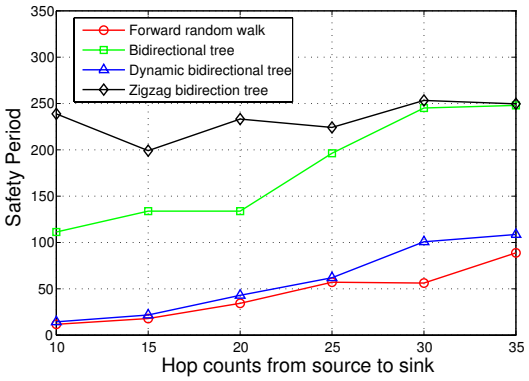

Figure 7. Safety period of the source location privacy under patient adversary model.

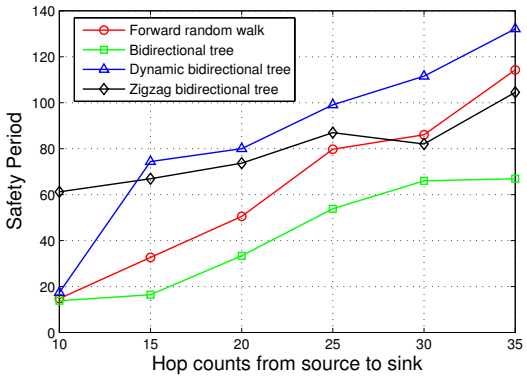

Figure 9. Safety period of the source location privacy under cautious adversary model.

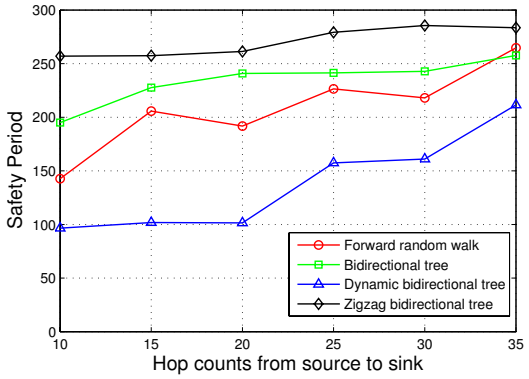

Figure 8. Safety period of the sink location privacy under patient adversary model.

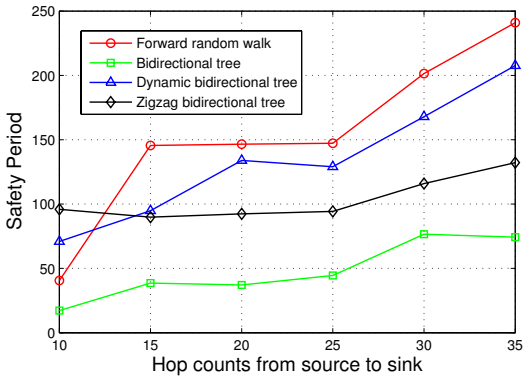

Figure 10. Safety period of the sink location privacy under cautious adversary model.

for the BT scheme, and in the ZBT scheme, the hop count of the proxy source to the source is $h = 15$.

Figure 7 shows the safety period of the source location privacy under the patient adversary model. It is obvious that the ZBT scheme achieves the highest safety period. The safety period of the BT scheme increases rapidly as the hop count increases. When the hop count is larger than 30, the safety period of the BT scheme gets close to that of the ZBT scheme. The safety period of the FRW and DBT schemes are relatively low, and the DBT scheme slightly outperforms the FRW scheme.

In Figure 8, the safety period of the sink location privacy under the patient adversary model is shown. As the adversary has to determine the direction of the packet before it moves to the receiver, which is more time-consuming for the adversary, under the patient adversary model, the safety period of sink location privacy is larger than that of source location privacy. We can find that the ZBT scheme outperforms other schemes. When the hop count is larger than 15, the safety period of the ZBT, BT and FRW scheme tends to be larger than 200, indicating a high sink location privacy. Figure 7 and Figure 8 illustrate that under the patient adversary model, the DBT scheme cannot achieve a high location privacy.

Under the cautious adversary model, the safety period of the source location privacy of our proposed schemes is shown in Figure 9. The safety period of source location privacy under the cautious adversary is lower than that under the patient adversary model. The reason is that the cautious adversary is smarter and when it waits for a long time at some location, it is able to trace back to avoid being drawn away by some dummy messages. When the hop count equals to 10, the ZBT scheme obtains the highest safety period. However, the DBT scheme outperforms other schemes when the hop count is larger than 15. The safety period of all the schemes increases with the increase of hop count. However, the increase ratio of the ZBT scheme is the least. Thus, when the hop is larger than 30, the FRW

scheme outperforms the ZBT scheme. The performance of the BT scheme is always the worst.

Figure 10 illustrates the safety period of the sink location privacy under the cautious adversary model. Compared to the sink location privacy under the patient adversary model, the safety period is lower under the cautious adversary model as the adversary has higher capacity. The FRW scheme achieves the highest performance while the BT scheme has the lowest safety period. As it is more time-consuming for the adversary to capture the sink than the source, when under the cautious adversary model, the safety period of the sink location privacy is also larger than that of the source location privacy.

6 Conclusion and Future Work

The end-to-end location privacy is an important issue in WSNs. In this paper, we address the necessity of simultaneously protecting the location privacy of both the source and sink for a typical application. We propose four privacy routing schemes, forward random walk, bidirectional tree, dynamic bidirectional tree and zigzag bidirectional tree, against a local eavesdropper, to obtain the end-to-end location privacy. We also implement the proposed privacy routing schemes on the TOSSIM platform, and evaluate the performance in term of safety period. The simulation results illustrate that our proposed location privacy protection schemes can obtain satisfied performance.

Since each of our proposed schemes obtains different performance on protecting the source location privacy or sink location privacy, we, as the future work, plan to decompose our proposed schemes and deeply analyze the effects of each one on the source location privacy and sink location privacy respectively. We will then design an optimal combination from these decomposed schemes to achieve a highest location privacy protection for both ends.

References

[1] A. Perrig, R. Szewczyk, V. Wen, and D. Culler, "SPINS: Security Protocols for Sensor Networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[2] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," in *IEEE ICDCS*, 2005.

[3] L. Eschenaur and V. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," in *ACM CCS*, 2002.

[4] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privay in Energy Constrained Sensor Network Routing," in *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, 2004.

[5] Y. Xi, L. Schwiebert, and W. Shi, "Preserving Source Location Privacy in Monitoring-based Wireless Sensor Networks," in *the 2nd International Workshop on Security in Systems and Networks (SSN)*, 2006.

[6] W. Wang, L. Chen, and J. Wang, "A source-location privacy protocol in wsn based on locational angle," in *IEEE ICC*, 2008.

[7] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "Entrapping Adversaries for Source Protection in Sensor Networks," in *IEEE WoWMoM*, 2006.

[8] H. Wang, B. Sheng, and Q. Li, "Privacy-aware Routing in Sensor Networks," *Computer Networks*, vol. 53, no. 9, pp. 1512–1529, 2009.

[9] Y. Li and J. Ren, "Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks," in *IEEE INFOCOM*, 2010.

[10] K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks Against a Global Eavesdropper," in *IEEE ICNP*, 2007.

[11] Y. Ouyang, Z. Le, D. Liu, J. Ford, and F. Makedon, "Source Location Privacy against Laptop-Class Attacks in Sensor Networks," in *ICST SecureComm*, 2008.

[12] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks," in *ACM WiSec*, 2008.

[13] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," in *IEEE INFOCOM*, 2008.

[14] J. Deng, R. Han, and S. Mishra, "Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Netowrks," in *IEEE DSN*, 2004.

[15] J. Deng, R. Han, and S. Mishra, "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks," in *ICST SecureComm*, 2005.

[16] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting Receiver-Location Privacy in Wireless Sensor Networks," in *IEEE INFOCOM*, 2007.

[17] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, vol. 1, no. 2-3, pp. 293–315, 2003.