This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks

Yun Li and Jian Ren
Department of Electrical and Computer Engineering
Michigan State University, East Lansing, MI 48824
Email: {liyun1, renjian}@egr.msu.edu

***Abstract*—Wireless sensor networks (WSNs) have the potential to be widely used in many areas for unattended event monitoring. Mainly due to lack of a protected physical boundary, wireless communications are vulnerable to unauthorized interception and detection. Privacy is becoming one of the major issues that jeopardize the successful deployment of wireless sensor networks. While confidentiality of the message can be ensured through content encryption, it is much more difficult to adequately address the source-location privacy. For WSNs, source-location privacy service is further complicated by the fact that the sensor nodes consist of low-cost and low-power radio devices, computationally intensive cryptographic algorithms and large scale broadcasting-based protocols are not suitable for WSNs. In this paper, we propose source-location privacy schemes through routing to randomly selected intermediate node(s) before the message is transmitted to the SINK node. We first describe routing through a single a single randomly selected intermediate node away from the source node. Our analysis shows that this scheme can provide great local source-location privacy. We also present routing through multiple randomly selected intermediate nodes based on angle and quadrant to further improve the global source location privacy. While providing source-location privacy for WSNs, our simulation results also demonstrate that the proposed schemes are very efficient in energy consumption, and have very low transmission latency and high message delivery ratio. Our protocols can be used for many practical applications.**

***Index Terms*—Source-location privacy, dynamic routing, intermediate node, simulation, wireless sensor networks (WSNs)**

I. Introduction

Wireless sensor networks have been envisioned as a technology that has a great potential to be widely used in both military and civilian applications. Sensor networks rely on wireless communication, which is by nature a broadcast medium that is more vulnerable to security attacks than its wired counterpart due to lack of a physical boundary. In the wireless sensor domain, anybody with an appropriate wireless receiver can monitor and intercept the sensor networks communications. The adversaries may use expensive radio transceivers and powerful workstations to interact with the networks from a distance since they are not restricted to using sensor networks hardware. It is possible for the adversaries to identify the message source or locate the source, even if strong data encryption is utilized.

Location privacy is an important security issue. Lack of location privacy can expose significant information about the traffic carried on the networks and the physical world entities. While confidentiality of the message can be ensured through content encryption, it is much more difficult to adequately address the source-location privacy. Privacy service in WSNs is further complicated since the sensor nodes consist of only low-cost and low-power radio devices. They are designed to operate unattended for long periods of time. Battery recharging or replacement may be infeasible or impossible. Therefore, computationally intensive cryptographic algorithms, such as public-key cryptosystems, and large scale broadcasting-based protocols, may not be quite suitable for WSNs. This makes privacy preserving communication in WSNs an extremely challenging research task. To optimize the sensor nodes for the limited capabilities and the application specific nature of the networks, traditionally, security requirements were largely ignored. This leaves the WSNs vulnerable to security attacks. In the worst case, the adversaries may be able to take control of some sensor nodes, compromise the cryptographic keys and reprogram the sensor nodes.

In this paper, we develop three two-phase dynamic routing based schemes to provide source-location privacy. In the first routing phase, the message source randomly selects an intermediate node, or multiple intermediate nodes, in the sensor domain, and then transmits the message to the randomly selected intermediate node(s) before it is transmitted to the SINK node. For single intermediate node case, the intermediate node is expected to be far away from the source node in the sensor domain. Our analysis shows that this scheme can provide great local source-location privacy, however, it may not be able to provide adequate global source location privacy. To further improve the performance of global security, we present two routing scheme that provide routing through multiple randomly selected intermediate nodes based on angle and quadrant. These two schemes can offer network-level (global) source-location privacy for WSNs. Our simulation results demonstrate that the proposed schemes are very efficient and can be used for many practical applications.

The major contributions of this paper are the following:

1) We propose to protect the source-location privacy through a two-phase routing process.
2) We develop source-location privacy through routing to a single randomly selected intermediate node.
3) We present two multi-intermediate nodes selection strategies for the source-location privacy scheme.
4) We provide extensive simulation results under ns-2 for

978-1-4244-5837-0/10/$26.00 ©2010 IEEE

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

every scheme we proposed.

The rest of this paper is organized as follows: Section II defines the system model. Section III discusses related works. Section IV describes a source privacy scheme through routing to a single randomly selected intermediate node. Section V and Section VI presents source location privacy schemes based on angle-based randomly selected multi-intermediate nodes, and quadrant-based randomly selected multi-intermediate nodes, respectively. In each of these three Sections, we also provided with security analysis and extensive simulation results. We conclude in Section VII.

II. Models

A. The System Model

We make the following assumptions about our system:

- The networks are evenly divided into small grids. The sensor nodes in each grid are all fully connected. In each grid, there is one header node responsible for communicating with other header nodes nearby. The whole networks are fully connected through multi-hop communications.
- The information of the SINK node is public. It is the destination that all data messages will be transmitted to through multi-hop routing.
- The content of each message will be encrypted using the secret key shared between the node/grid and the SINK node. However, the encryption operation is beyond the scope of this paper.
- The sensor nodes are assumed to have the knowledge of their relative locations and their adjacent neighboring nodes. The information about the relative location of the sensor domain may also be achieved through networks broadcasting [1]–[3].

B. The Adversarial Model

We assume that there are some adversaries in the target area, who try to locate the source node through traffic analysis and tracing back. The adversaries have the following characteristics in this paper:

- The adversaries will have unbounded energy resource, adequate computation capability and sufficient memory for data storage. The adversaries may also compromise some sensor nodes in the networks.
- The adversaries will not interfere with the proper functioning of the networks, such as modifying packets, altering the routing path, or destroying sensor devices, since such activities can be easily identified. However, the adversaries may carry out passive attacks, such as eavesdropping the communications.
- The adversaries are able to monitor the traffic in an area and get all of the transmitted messages. On detecting an event, they could determine the immediate sender by analyzing the strength and direction of the signal they received. However, we assume that the adversaries are unable to monitor the entire WSNs.

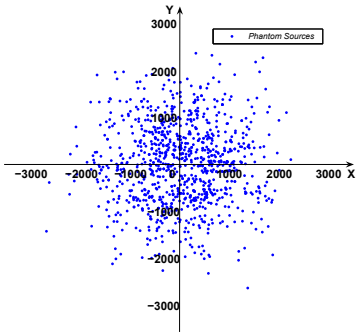


Fig. 1. Random routing: packets=1000, hops=50, routing range=250 meters, average distance=4.2 hops from source, longest distance=12.2 hops from source

III. Related Works

In the past two decades, originated largely from Chaum's mixnet [4] and DC-net [5], a number of protocols have been proposed to provide communication source-location privacy [6]–[18]. The mixnet family protocols use a set of "mix" servers that mix the received packets to make the communication source (including the sender and the recipient) ambiguous. The DC-net family protocols [5], [8], [9] utilize secure multiparty computation techniques. However, both approaches require public-key cryptosystems and are not suitable for WSNs.

Multiple schemes have been proposed to provide destination location privacy. In [12], [13], base station location privacy based on multi-path routing and fake messages injection was proposed. In this scheme, every node in the networks has to transmit messages at a constant rate. Another base station location privacy scheme was introduced in [19], which involves location privacy routing and fake message injection.

In [14], [15], source-location privacy is provided through broadcasting that mixes valid messages with dummy messages. The main idea is that each node needs to transmit messages consistently. Whenever there is no valid message to transmit, the node will transmit dummy messages. The transmission of dummy messages not only consumes significant amount of sensor energy, but also increases the networks collisions and decreases the packet delivery ratio. Therefore, these schemes are not quite suitable for large scale sensor networks.

Routing based protocols can also provide source-location privacy through dynamic routing so that it is infeasible for the adversaries to trace back to the source-location through traffic monitoring and analysis. The main idea is to, first, route the message to a node away from the actual message source randomly, then forward the message to the SINK node using single path routing. However, both theoretical and practical results demonstrate that if the message is routed randomly for h hops, then the message will be largely within $h/5$ hops away from the actual source, see Fig. 1. To solve this problem, several approaches have been proposed. In phantom routing protocol [16], [17] the message from the actual source will be

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

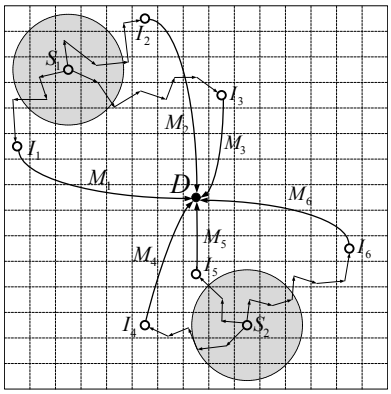


Fig. 2. Illustration of the two-phase routing

routed to a phantom source along a designed directed walk through either sector-based approach or hop-based approach. Take the section-based directed walk as an example, the source node first randomly determines a direction that the message will be sent to. The direction information is stored in the header of the message. Then every forwarder on the random walk path will forward this message to a random neighbor in the same direction determined by the source node. In this way, the phantom source can be away from the actual source. Unfortunately, once the message is captured on the random walk path, the adversaries will be able to get the direction information stored in the header of the message. Therefore, the exposure of direction information decreases the complexity for adversaries to trace back to the actual message source in the magnitude of 2^h. Random walk from both the source node and the SINK node was also proposed in [18]. In this scheme, Bloom Filter was proposed to store the information of all the visited nodes in the networks for each message to prevent the messages from hopping back. However, this design allows the adversaries to recover significant routing information from the received messages. In fact, this design is "not realistic" for large scale sensor networks.

IV. Source-Location Privacy Through Routing to a Random Intermediate Node (RRIN)

In this section, we will describe our proposed scheme on routing through a random intermediate node (RRIN).

In this scheme, each message will be routed through a randomly selected intermediate node. The node is selected based on the relative location of the sensor node, as shown in Fig. 2. The intermediate node is expected to be away from the source node for a minimum distance d_{min} so that it is difficult for the adversaries to get the source-location information of the actual source.

Since we assume that each sensor node only has knowledge of its adjacent nodes. The source node may not have accurate information of the sensor nodes multiple hops away. In particular, the randomly selected intermediate node may not even exist. However, the knowledge of relative location can guarantee that the message packet will be forwarded to an intermediate node in an area with minimum distance d_{min} away from the source node. According to our assumption, the last node in the routing path adjacent to the intermediate node will be able to tell whether such a randomly selected intermediate node exists or not. In the case that such a node does not exist, this node will become the intermediate node. The intermediate node then routes the received message to the SINK node.

Suppose the source node is located at the relative location (x_0, y_0). To transmit a data message, it first determines the minimum distance, d_{min}, that the intermediate node has to be away from the source node. We denote the distance between the source node and the randomly selected intermediate node as d_{rand}. Then we have $d_{rand} \geq d_{min}$.

Whenever the source node wants to generate a d_{rand}, it will first generate a random number x. The value of this random variable is normally distributed with mean 0 and variance σ^2, i.e., $X \sim N(0, \sigma)$. Then the source node can calculate d_{rand} as follows:

$$d_{rand} = d_{min} \times (|x| + 1).$$

Therefore, the probability [20] that d_{rand} is located in the interval $[d_{min}, \rho d_{min})$ is:

$$2\varphi_{0,\sigma^2}(\rho-1)-1 = 2\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(\rho-1)^2}{2\sigma^2}} - 1 = 2\varphi\left(\frac{\rho-1}{\sigma}\right) - 1,$$

where ρ is a parameter larger than 1, φ_{0,σ^2} is the probability density function of Gaussian distribution [21].

If we choose σ to be 1.0, then the probability that d_{rand} falls within the interval $[d_{min}, 2d_{min})$ will be $2\Phi(\frac{1}{1}) - 1 = 0.6827$. The probability that d_{rand} is in the interval $[d_{min}, 3d_{min})$ will be $2\Phi(\frac{2}{1}) - 1 = 0.9545$.

After d_{rand} is determined, the source node randomly generates an intermediate node located at (x_d, y_d) that satisfies:

$$d_{rand} = \sqrt{(x_d - x_0)^2 + (y_d - y_0)^2} \geq d_{min}.$$

Upon receiving a data message, the intermediate node forwards the message to the SINK node.

In the example given in Fig. 2, S_1, S_2 denote two source nodes in the networks, D represents the SINK node and $I_1, \cdots, I_6$ are six randomly selected intermediate nodes. The selection of d_{rand} guarantees that none of the intermediate nodes will be in the shaded areas. The nodes $I_1, \cdots, I_6$ will forward the messages $M_1, \cdots, M_6$ to the SINK node, respectively.

A. Security Analysis

In our RRIN, the intermediate node is randomly selected by the source node based on the relative location of the sensor nodes. From probability point of view, every node away from the source node can be selected as the intermediate node. However, since we assume the source node does not have full knowledge of the sensor node more than one hop away from itself, the intermediate node selected by the source node may not even exist since according to our assumption.

According to our assumption, it is impossible for the adversary to trace back or identify the real message source

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

node based on an individual traffic monitoring. This is because (i) this message is equally likely to be generated by many possible sources, and (ii) the probability for multiple events from the same source to use repeated routing is very low for large scale sensor networks.

If an adversary tries to trace back the source-location from the message packet in the route through which the packet is being transmitted to the mixing ring, then the adversary will be led to the randomly selected intermediate node to the best extend, instead of the real message source. Since the intermediate node is randomly selected for each data message, the probability that the adversaries will receive the messages from one source node continuously is almost zero. As shown in Fig. 2, if the adversaries receive M_2 forwarded by I_2, it would be led to I_2. However, the next intermediate node I_3 is far from I_2, so the adversaries could not receive M_3.

Even if one intermediate node's location is discovered by the adversaries, the source-location is still well protected because the locations of the intermediate nodes are at least d_{min} away from the real source node.

Unlike the directed walk used in random walk, our protocol does not leak side information to the adversaries. Since the intermediate node is determined before each data message is transmitted by the source, the data message carries no observable side information of the message source node's location in its content due to message content encryption. Therefore, our proposed protocol can protect source-location privacy.

However, in this scheme, the possibility of being selected as an intermediate node for a sensor in the WSNs is proportional to the distance between this sensor and the source node. Therefore, for large scale sensor networks, the intermediate nodes tend to be not too far away from the source node. In other words, the intermediate nodes are highly likely to concentrate in a circle area centered at the source node. We carry out a small simulation to illustrate this. As shown in Fig. 3, a reference frame is built on a WSNs terrain with the origin located at the center of the target area. The source node locates at the point $(-1250, 1250)$. We generate 500 intermediate nodes according to the RRIN algorithm above with σ equals to 1. We could see that all the intermediate nodes are located not too far away from the source node and the distribution of the nodes looks like a circle. Therefore, nearly all the messages generated by this source node would be forwarded to the SINK from the intermediate nodes on this circle. The adversaries can be pretty sure that the source node is located in the second quadrant of the reference frame. So for large scale sensor networks, RRIN could only provide local location privacy.

B. Totally Random Intermediate Node Selection

In order to provide global location privacy over the sensor networks, the selection of intermediate nodes has to be totally random, i.e., every sensor node in the networks has the same probability of being selected as the intermediate node for any source nodes.

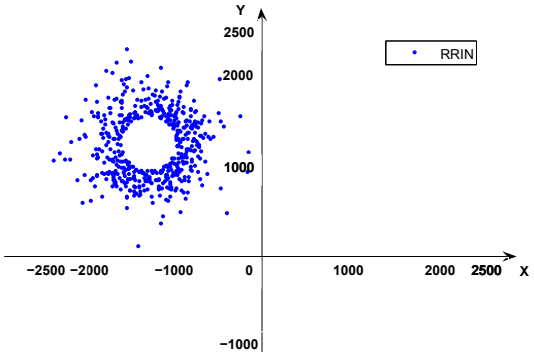


Fig. 3. Distribution of the intermediate nodes

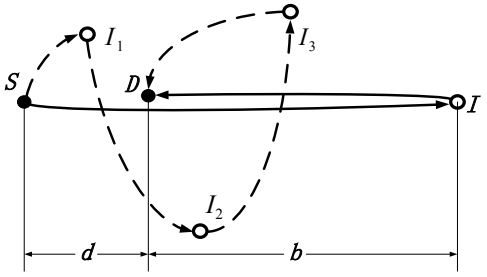


Fig. 4. Message transmission by intermediate nodes

However, if the selection is totally random, then some intermediate nodes' locations could be very close to the real source node. Once such an intermediate node is located by the adversaries, the source's location will also be exposed. To prevent this from happening, the locations of the intermediate nodes should be at least d_{min} away from the real source node.

Unlike RRIN, the intermediate nodes randomly selected are evenly distributed in the networks terrain. Therefore, the messages could be forwarded to the SINK node from all possible directions, which means the adversaries could not get the general location information of the source node. Every node in the networks has the same possibility of being selected as the intermediate node. The intermediate nodes for one source node are different for different messages, so the adversaries will get no information about the source node from the locations of the intermediate nodes. Even if the location of one intermediate node is successfully identified, this location is still d_{min} away from the source-location. Therefore, the global location privacy is achieved.

However, random intermediate node selection without restriction may also have some limitations.

- The length of the routing path tends to be too long. For instance, as shown in Fig. 4, S, D, I are the source node, SINK node and intermediate node, respectively. The distance between S, D and I, D are d and b, respectively. Therefore, if a message is transmitted through I, the total length of the path is nearly $d + 2b$, which is much longer than d. As a result, this routing path consumes much more energy than our proposed scheme.
- The message drop rate may increase and the delivery ratio

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

may decrease, due to the increase of the path length.
- If a single path is too long, it is easier for the adversaries to deduce the information of the source-location. Take the path from S to I in Fig. 4 as an example, once a packet is captured by the adversaries in path, the adversaries may get the direction of the source-location according to the transmission direction of the captured packet.

C. Simulation Results and Performance Analysis

To evaluate the performances of the schemes proposed, we have done some simulations using NS2 on Linux system. In the simulation, 400 nodes are distributed in a square target area of size 3360×3360 meters, while the SINK node is located at the center of the networks. For phantom routing, the average distance between the phantom source and the actual source is 506.12 meters after four routing hops, while for RRIN, the average distance between the intermediate node and the source is 529.14 meters. We also illustrate the performance of the totally randomly selected intermediate nodes. Simulation results are provided in Fig. 5. In the figures, 'total random' means the selection of the intermediate nodes are completely random without considering d_{min}. 'total random with radius' means the intermediate nodes are at least d_{min} from the source node, while d_{min} equals to 480 meters in this simulation.

From the figures, it reasonable to observe that sending the massages to the SINK directly without intermediate node gives the best performance. The performances of RRIN and phantom are of the same level, while RRIN is better in location privacy protection. If the intermediate nodes selection is made totally random, the performance is not as good as the others. The performance of the totally random intermediate nodes selection with the d_{min} constraint is the worst. This is reasonable, because usually there is a tradeoff relationship between the level of security and the performance.

V. Source-Location Privacy Through Angle-Based Multi-Intermediate Nodes

From the discussion in last section we can see that routing through single-intermediate node is more suitable for small scale sensor networks. In this section, we propose routing through multiple randomly selected intermediate nodes for large sensor networks. Compare to the former one, It has the following advantages:

- *More reliable:* If the packets are routed by multi-intermediate nodes, the routing direction would be changed every time this packet is forwarded by an intermediate node. Take the path from S to I in Fig. 4 as an example, if the path is composed of multi-intermediate nodes: I_1, I_2, I_3, the transmission direction is changed completely when the message is forwarded by an intermediate node. So even if the packet is captured by an adversary, he is unable to get the direction of the source node.
- *Energy-efficient:* Using controlled multi-intermediate nodes, we can design routing schemes that can achieve global source-location privacy. Comparing to routing through randomly selected single-intermediate node, the average length of routing path could also be decreased to save energy needed.
- *Higher delivery ratio:* As the length of routing path decreases through multiple intermediate nodes, message transmission reliability and delivery ratio can be improved concurrently.

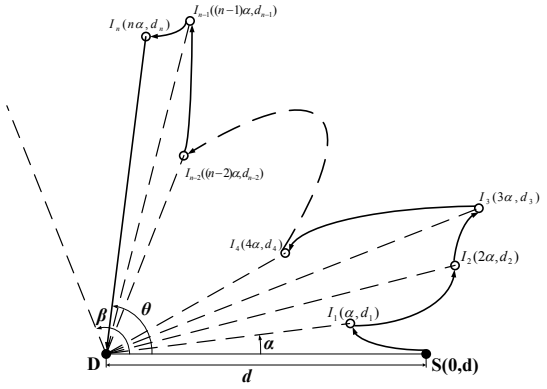


Fig. 6. Angle-based approach

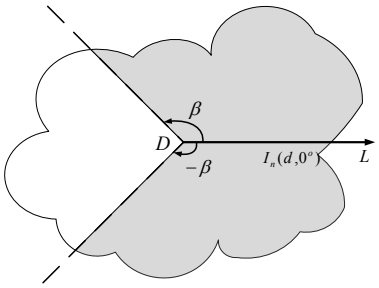


Fig. 7. Possible location of source

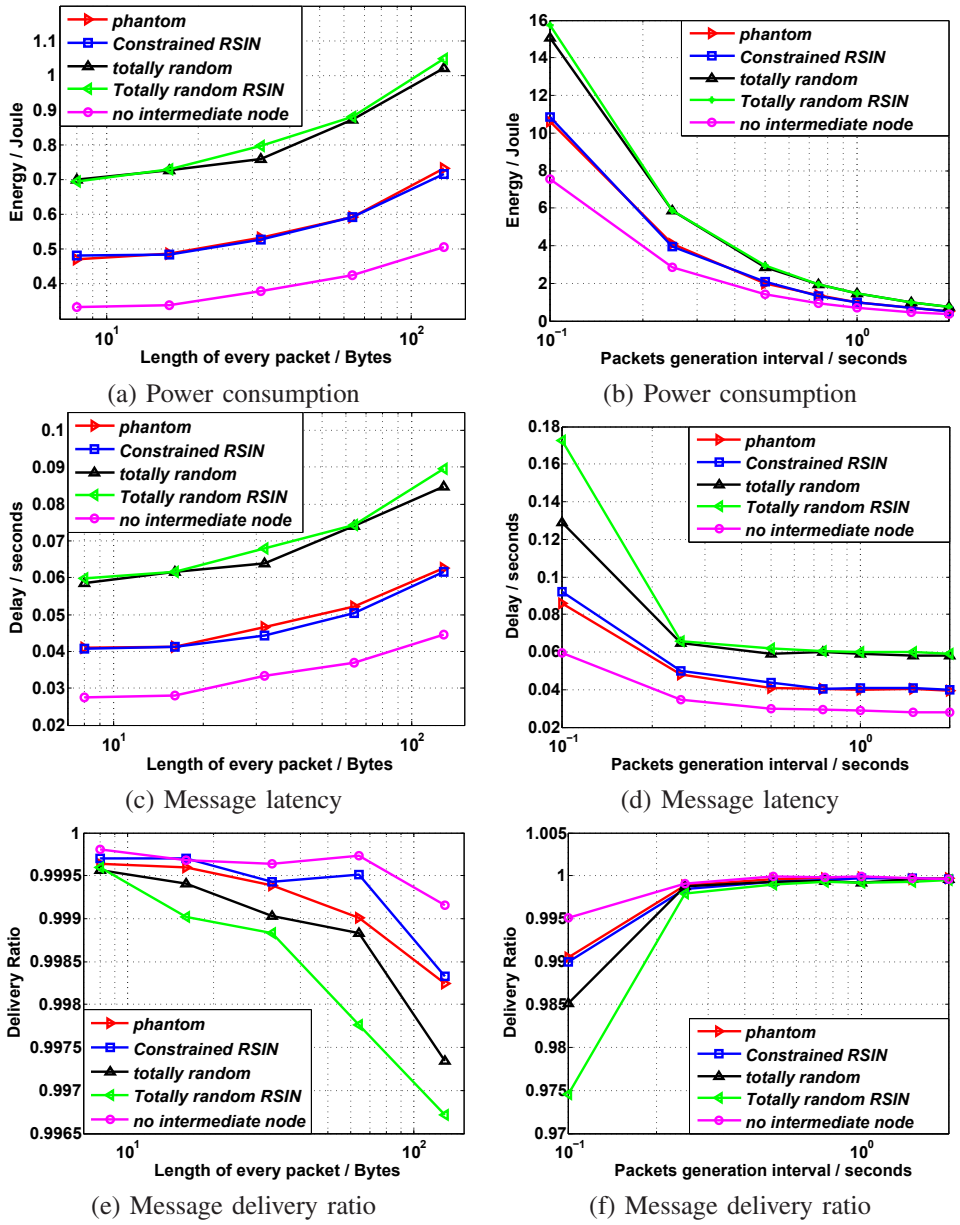
The intermediate nodes are preselected before a message is sent out from the source node. The information of the intermediate nodes is stored in the header of the messages. However, this manner of routing has a security problem. The adversaries could just stay close to the SINK node and wait. Once a message is captured, the adversaries will get the information of all the intermediate nodes. Therefore, the source-location could be deduced from the general routing path formed by the intermediate nodes. To solve this problem, in our scheme, before a message is forwarded by an intermediate node, the information of the former intermediate node(s) will be deleted from the message header, i.e., no information of the former intermediate node(s) will be maintained in the header.

In this section, we will first propose *angle-based* intermediate nodes scheme.

A. Scheme Description

In angle-based intermediate nodes selection, prior to data transmission, the source node needs to determine a maximum angle β between the last intermediate node and the source node according to the SINK node, while $\beta \in [0°, 180°]$. After β is determined, the source node chooses an actual angle θ

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.



(a) Power consumption (b) Power consumption

(c) Message latency (d) Message latency

(e) Message delivery ratio (f) Message delivery ratio

Fig. 5. Performance of routing by single-intermediate node

between the last intermediate node and itself according to the SINK node D, where θ is a random variable evenly distributed in the range $(-\beta, \beta)$. Then the source node needs to determine the number of the intermediate nodes, which is denoted as n here.

Therefore, the angle generated by one intermediate node should be: $\alpha = \theta/n$. The angles between all the intermediate nodes and the source node according to the SINK node are: $\alpha, 2\alpha, 3\alpha, \cdots, n\alpha$, while $n\alpha = \theta$ is the angle between the last intermediate node and the source node according to the SINK node.

After all the angles are determined, the source node generates the distances between the source node and the n intermediate node: $d_1, d_2, d_3, \cdots, d_n$, $d_i (i = 1, 2, \cdots, n)$ is a random variable evenly distributed in the range $(0, R)$, while R is the radius of the networks terrain.

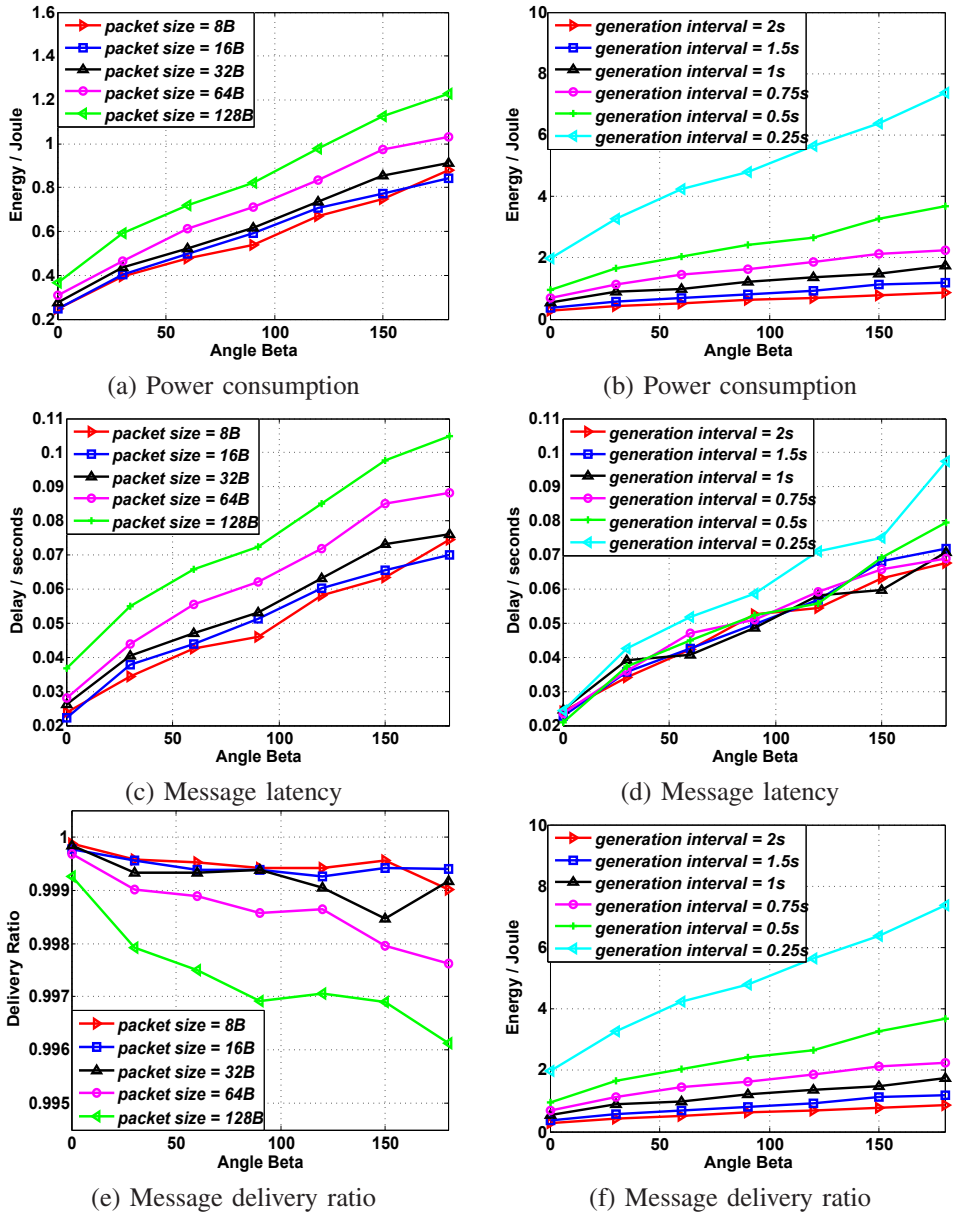
If a polar coordinate system is built on the networks terrain, while the SINK node locates at the origin and the source node is located at $(d, 0)$, where d is the distance between the source and the SINK, then the locations for all the intermediate nodes will be: $(d_1, \alpha), (d_2, 2\alpha), (d_3, 3\alpha), \cdots, (d_n, n\alpha)$.

Fig. 6 illustrates this intermediate nodes selection, in which $S, I_1, \cdots, I_n, D$ are the source node, the intermediate nodes and the SINK node, respectively.

B. Security Analysis

We will analyze that even if the adversaries are able to successfully identify the location of the last intermediate node I_n, the determination of the source-location S is still very difficult according to our assumption. As shown in Fig. 7,

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.



(a) Power consumption (b) Power consumption

(c) Message latency (d) Message latency

(e) Message delivery ratio (f) Message delivery ratio

Fig. 8. Performance of angle-based multi-intermediate nodes

where D, I_n are the SINK node and the last intermediate node, respectively. In the case that the location of I_n is known, a polar coordinate system is built on the networks with D located at the origin and I_n at $(d, 0°)$, where d is the distance from D to I_n. The possible location of S is in the shaded area shown in Fig. 7, i.e, the radian measure range of $(-\beta, \beta)$, where β is a configurable parameter ranging from $0°$ to $180°$. The larger β is, the higher level of location privacy that could be achieved. Moreover, β can also be dynamic, in which case the adversaries are unable to determine the actual β, the possible location of the source node S can be anywhere in the whole domain.

C. Simulation Results

We carried out simulations to evaluate the performance of the angle-based multi-intermediate nodes scheme using NS2 on Linux system. In the simulation, the target area is a square field of size 3360×3360 meters. The SINK node is located at the center of the networks area. The SINK node is also the destination for all packet transmissions. In this simulation, the curve with $\beta = 0$ means the messages are transmitted to the SINK node directly without relying on any intermediate nodes. Simulation results are provided in Fig. 8 to demonstrate the tradeoff relationship between performance and the angle β. With the increase of the value of β, the performance becomes worse, while the security level becomes higher.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

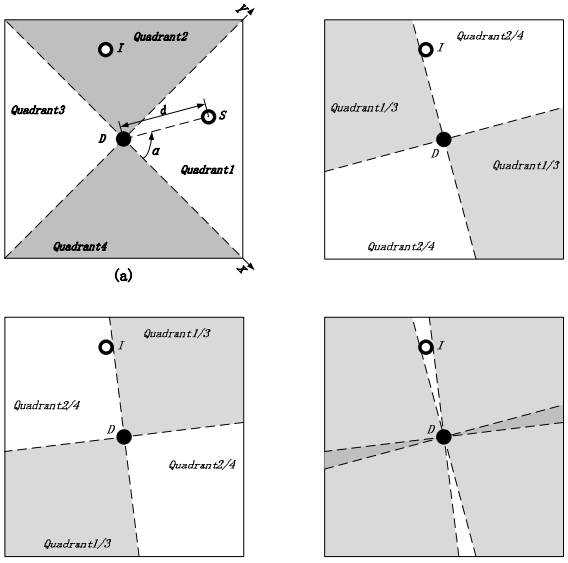


Fig. 9. Quadrant-based intermediate nodes selection

VI. Source-Location Privacy Through Quadrant-Based Multi-Intermediate Nodes

In this section, *quadrant-based* intermediate nodes scheme will be presented.

A. Scheme Description

In quadrant-based approach, for each source node, the whole networks are divided into four quadrants according to its location and the SINK node's location.

First, the source node has to determine the formation of the quadrants. As shown in Fig. 9.(a), S, I, D are the source node, the last intermediate node and the SINK node, respectively. The distance between S and D is d. A reference frame is built on this networks for source node S. The SINK node D is located at the origin with coordinate $(0, 0)$, S's (x_S, y_S) location in $quadrant1$ is: $x_S = d \times cos(\alpha), \quad y_S = d \times sin(\alpha)$, where α is an evenly distributed random variable located in the range of $(0°, 90°)$.

After the reference frame is built up, the source node first needs to determine the angle θ between the last intermediate node and itself according to the SINK node. θ is evenly distributed in $(-90°, 0°)$ and $(90°, 180°)$, which means the last intermediate node can only locate in $quadrant4$ or $quadrant2$ on the reference frame. This terrain is illustrated as the shaded area in Fig. 9.(a). The other intermediate nodes could be determined in the similar way as the angle-based multi-intermediate nodes selection scheme.

B. Security Analysis

In this way, the possible angle between S and I according to D falls in the range $(0°, 180°)$. Even if the adversaries can determine the location of I, they still cannot get the information about the location of the source node. For example, in Fig. 9.(b)-(d), for the same I, the formation of the quadrants could be the one shown in Fig. 9.(b), or the one shown in Fig. 9.(c). In another word, the source node S can be located in the shaded area in Fig. 9.(b), or the shaded area in Fig. 9.(c). Therefore, the possible location area of the source node is the shaded area in Fig. 9.(d), which is almost the whole networks area. In this way, global source-location privacy is achieved.

C. Simulation Results

We also conducted simulations to compare the performances of quadrant-based intermediate node selection scheme and angle-based intermediate node selection scheme. The setup for this simulation is exactly the same as the angle-based approach. The simulation results are shown in Fig. 10. Our simulation demonstrates that the quadrant-based approach can provide better performance than angle-based approach with $\beta = 180°$, while both of these two schemes achieve global location privacy.

VII. Conclusions

Source-location privacy is critical to the successful deployment of wireless sensor networks. In this paper, we first propose and analyze a routing-based scheme through single-intermediate node. Then two multi-intermediate nodes schemes are introduced. For each of these schemes, we carried out simulations to evaluate the performances. Simulation results demonstrate that the proposed schemes can achieve very good performance in energy consumption, message delivery latency and message delivery ratio.

Acknowledgement

This work was supported in part by the NSF under grants CNS-0845812, CNS-0848569, and CNS-0716039.

References

[1] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, pp. 829–835, April 2006.

[2] "Localization for mobile sensor networks," in *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*, (New York, NY, USA), pp. 45–57, ACM, 2004.

[3] X. Cheng, A. Thaeler, G. Xue, and D. Chen, "Tps: a time-based positioning scheme for outdoor wireless sensor networks," *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 4, pp. 2685–2696 vol.4, March 2004.

[4] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, February 1981.

[5] D. Chaum, "The dinning cryptographer problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, 1988.

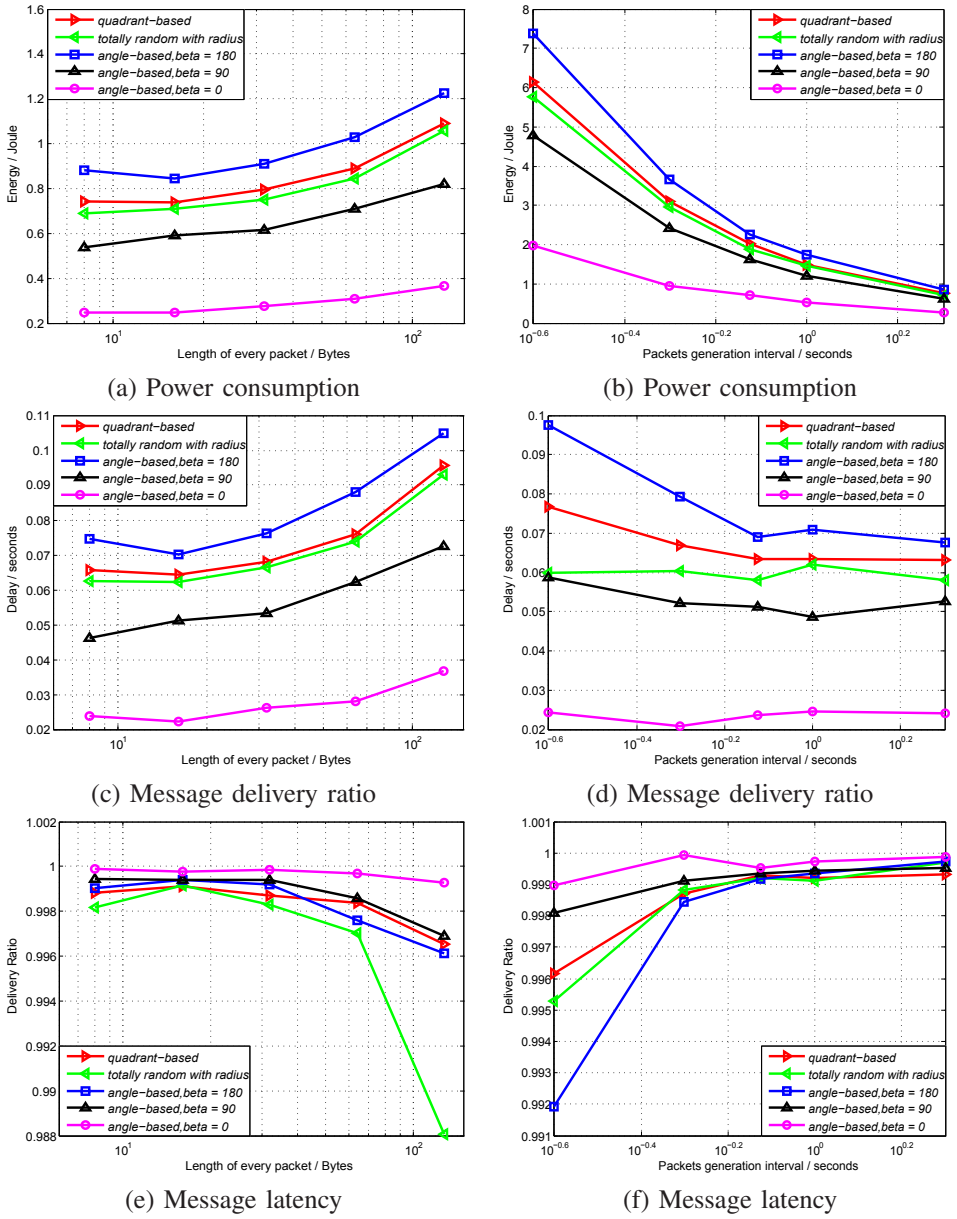
[6] L. Ahn, A. Bortz, and N. Hopper, "k-anonymous message transmission," in *Proceedings of the 10th ACM conference on Computer and Communications Security*, (Washington D.C., USA.), pp. 122–130, 2003.

[7] A. Beimel and S. Dolev, "Buses for anonymous message delivery," *J. Cryptology*, vol. 16, pp. 25–39, 2003.

[8] P. Golle and A. Juels, "Dining cryptographers revisited," in *Advances in Cryptology - Eurocrypt 2004*, LNCS 3027, pp. 456–473, 2004.

[9] S. Goel, M. Robson, M. Polte, and E. G. Sirer, "Herbivore: A Scalable and Efficient Protocol for Anonymous Communication," Tech. Rep. 2003-1890, Cornell University, Ithaca, NY, February 2003.

[10] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," *IEEE J. on Selected Areas in Coomunications, Special Issue on Copyrigh and Privacy Protection*, vol. 16, no. 4, pp. 482–494, 1998.



(a) Power consumption (b) Power consumption

(c) Message delivery ratio (d) Message delivery ratio

(e) Message latency (f) Message latency

Fig. 10. Performance of quadrant-based multi-intermediate nodes

[11] M. K. Reiter and A. D. Rubin, "Crowds: anonymity for web transaction," *ACM Transactions on Information and System Security*, vol. 1, no. 1, pp. 66–92, 1998.

[12] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," in *DSN '04: Proceedings of the 2004 International Conference on Dependable Systems and Networks*, (Washington, DC, USA), p. 637, IEEE Computer Society, 2004.

[13] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, pp. 113–126, Sept. 2005.

[14] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks," in *WiSec '08: Proceedings of the first ACM conference on Wireless network security*, (New York, NY, USA), pp. 77–88, ACM, 2008.

[15] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pp. 51–55, April 2008.

[16] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," *Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on*, pp. 599–608, June 2005.

[17] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *SASN '04*, (New York, NY, USA), pp. 88–93, ACM, 2004.

[18] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks.," in *IPDPS*, IEEE, 2006.

[19] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "A novel scheme for protecting receiver's location privacy in wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 7, pp. 3769–3779, October 2008.

[20] Wikipedia, "Normal distribution." http://en.wikipedia.org/wiki/Normal_distribution.

[21] S. M. Stigler, *Statistics on the Table*. Harvard University Press. chapter 22 (History of the term "normal distribution".