# Mixing Ring-Based Source-Location Privacy 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 consist of low-cost and low-power radio devices and are deployed in open and unprotected areas. 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 wireless sensor networks, computationally intensive cryptographic algorithms (such as public-key cryptosystems) and large scale broadcasting-based protocols are not suitable. In this paper, we propose a scheme to provide source-location privacy through a three-phase routing: routing to a randomly selected intermediate node, routing in a network mix ring, and message forwarding to the SINK node. While being able to provide source-location privacy for WSN, our simulation results also demonstrate that the proposed scheme is very efficient and can be used for practical applications.**

## 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 communications, 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 network communications. The adversaries may use expensive radio transceivers, powerful workstations and interact with the network from a distance since they are not restricted to using sensor network hardware. It is possible for the adversaries to identify the message source or even identify the source-location, 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 network 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 WSN is further complicated since the sensor nodes consist of only low-cost and low-power radio devices and 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, are not suitable for WSN. This makes privacy preserving communications in WSN an extremely challenging research task. To optimize the sensor nodes for the limited node capabilities and the application specific nature of the networks, traditionally, security requirements were largely ignored. This leaves the WSN under network security attacks. In the worst case, an adversary may be able to undetectably take control of some sensor nodes, compromise the cryptographic keys and reprogram the sensor nodes.

In this paper, we propose a scheme that provides source-location privacy through a three-phase routing process. In the first routing phase, the message source randomly selects an intermediate node in the sensor domain and then transmits the data packet to the randomly selected intermediate node (RRIN) before it is routed to a ring node. This phase provides the local source-location privacy. In the second routing phase, the data packet will be mixed with other packets through a network mixing ring (NMR). This phase offers network-level (global) source-location privacy. Finally, the data packet will be forwarded to the SINK node from certain specific nodes on the mixing ring. While being able to provide source-location privacy for WSN, our simulation results also demonstrate that the proposed scheme is very efficient and can be used practical applications.

The rest of this paper is organized as follows: In Section II, the related works are reviewed. The system model is described in Section III. Section IV details the proposed source-location privacy scheme. Security analysis and performance analysis are provided in Section V and Section VI, respectively. We conclude in Section VII.

## II. Related Works

In the past two decades, a number of source-location private communication protocols have been proposed [1]–[13], which originated largely from Chaum's mixnet [14] and DC-net [15]. 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 [3], [4], [15] utilize secure multiparty computation techniques. However, both approaches require public-key cryptosystems and are not suitable for WSN.

978-1-4244-4581-3/09/$25.00 ©2009 IEEE

In [7], [8], Deng et al. proposed to address the location privacy of base station through multi-path routing and fake messages injection. In their scheme, every node in the network has to transmit messages at a constant rate. Another base location privacy scheme is introduced in [16], which involves location privacy routing and fake messages injection. This proposed scheme is interested in protecting the destination location privacy, while our scheme cares about source location privacy protection.

In [9], [10], 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 are no valid messages, the node has to transmit dummy messages. The transmission of dummy messages consumes significant amount of sensor energy while increasing the network collisions and decreasing the packet delivery ratio. Therefore, these schemes are not quite suitable for large sensor networks.

Routing based protocols can also provide source-location privacy. The main idea is to prevent the adversaries from tracing back to the source-location through traffic monitoring and analysis. A phantom routing protocol is introduced in [11], [12]. Phantom routing involves two phases: a random walk phase and a subsequent flooding/single path routing phase. In the random walking phase, the message from the real source will be routed to a phantom source along a random path or a designed directed path. The phantom source is expected to be far away from the real source, which will make the real source's location hard to be traced back by the adversaries. However, theoretical analysis shows that if the message is routed $h$ hops randomly, then it is highly possible that the distance between the phantom source and the real source is within $h/5$. To solve this problem, directed walk was proposed in [11]. Directed walk can be achieved either through section-based directed random walk or hop-based directed random walk. Let's take the section-based directed walk as an example. The source node first randomly determines a direction that the message will be sent. This direction information is stored in the header of the message. 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 directed random walk will determine a phantom source that is away from the real 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 true message source in the magnitude of $2^h$. [13] proposed to implement random walk from both the source node and the SINK node. Different from the directed walk, Bloom Filter is proposed to store all the visited nodes in the network for each message to prevent the adversaries from hopping back. However, for large scale sensor networks, this is not realistic.

## III. System Models

### A. The System Model

We made the following assumptions about our system:

- The network is evenly divided into small grids. The sensor nodes in each grid are all fully connected. There is one header node in each grid. The whole network is fully connected through multi-hop communications.
- The SINK node is the destination location that data messages will be transmitted to.
- Each sensor node is assumed to know the relative locations of themselves and their adjacent neighbors. The information about the relative location of the sensor domain may also be broadcasted through this network for routing information update [17]–[19].
- The key management and the message content confidentiality are beyond the scope of this paper. Interested readers are referred to [20]–[22].

### B. The Adversaries Model

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

- The adversaries have sufficient energy resource, adequate computation capability and enough memory for data storage. On detecting an event, they could determine the immediate sender easily and move to this sender's location without too much delay. The adversaries may also compromise some sensor nodes in the network.
- The adversaries will not interfere with the proper functioning of the network, 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 of the communications.
- The adversaries are able to monitor the traffic and get all the transmitted messages in certain area. However, we assume that the adversaries are unable to monitor the entire network. In fact, if the adversaries could monitor the entire wireless sensor networks, then they can monitor the events directly without relying on the sensor network.

## IV. Proposed Source-Location Privacy Scheme

In this paper, we propose a three-phase routing protocol to provide source-location privacy. The first phase (RRIN) provides local source-location privacy. The second phase (NMR) offers the network-level source-location privacy. The last phase forwards the message to the SINK node.

After the formation of all the grids, a large ring, called the *mixing ring*, is generated in the WSN to provide network-level traffic mix. The mixing ring is composed of multiple header nodes, which are named *ring nodes*. The ring nodes are further divided into *relay ring nodes* and *normal ring nodes*. The messages that will be transmitted in the mixing ring are referred to as *vehicle messages*. Vehicle messages will be transmitted in

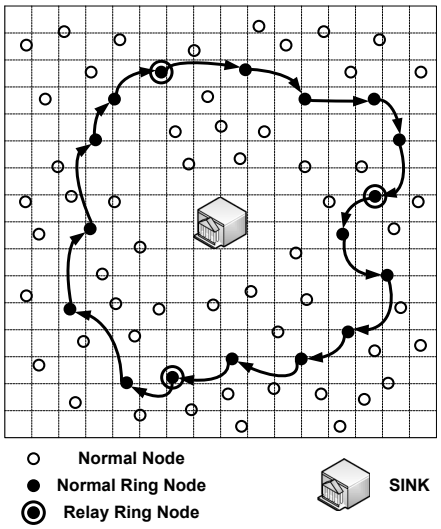



Fig. 1. Grids Formation

the ring in the clockwise direction, called *ring direction*. Only relay ring nodes can generate vehicle message. We also define the grids containing ring node as *ring grids*, the grids without ring nodes as *normal grids*. The sensor nodes in normal grids are defined as *normal nodes*, the messages sent by the normal nodes are referred as *data messages*.

### A. Routing through a Random Intermediate Node (RRIN)

In the first phase, the message source first randomly selects an intermediate node at the sensor domain based on the relative location of the sensor node defined in the grid shown in Fig. 1. The goal of this phase is to provide local source-location privacy. The intermediate node is expected to be far away from the real source node so that it is difficult for the adversaries to get the information of the real source from the intermediate node selected.

Since we assume that each sensor node only has knowledge of its adjacent nodes. The source node has no accurate information of the sensor nodes more than one hop away. In particular, the randomly selected intermediate node may not even exist. However, the relative location can guarantee that the message packet will be forwarded to the area of the intermediate node. The last node in the routing path adjacent to the intermediate node should 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 a ring node and the first phase routing is accomplished.

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

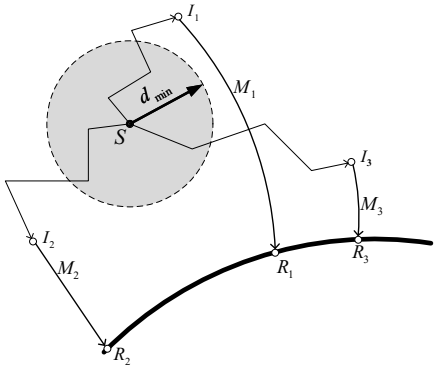



Fig. 2. Illustrate of the first two phases routing

variable is normally distributed with mean 0 and variance $\sigma^2$, 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 that $d_{rand}$ is located in the interval $[d_{min}, \rho d_{min})$ is:

$$2\phi_{0,\sigma^2}(\rho - 1) - 1 = 2\phi(\frac{\rho - 1}{\sigma}) - 1,$$

where $\rho$ is a parameter larger than 1, $\phi_{0,\sigma^2}$ is the cumulative distribution function (CDF) of $N(0, \sigma)$, and $\phi$ is the CDF of normal distribution: $N(0, 1)$.

If we choose $\sigma$ to be 1.0, then the probability that $d_{rand}$ falls within the interval $[d_{min}, 2d_{min})$ will be $2\phi(\frac{1}{1}) - 1 = 0.6826$. The probability that $d_{rand}$ is in the interval $[d_{min}, 3d_{min})$ will be $2\phi(\frac{2}{1}) - 1 = 0.9544$.

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 data message, the intermediate node forwards the message to the closest ring node.

An example is given in Fig. 2, where $S$ indicates a source node in the network and $I_1, I_2, I_3$ are three intermediate nodes. The selection of $d_{rand}$ guarantees that none of the intermediate nodes will be in the shaded area. Then $I_1, I_2, I_3$ will forward these messages $M_1, M_2, M_3$ to the ring nodes $R_1, R_2, R_3$, respectively.

### B. Network Mixing Ring (NMR)

In the second routing phase, the messages will be forwarded hop-by-hop in the ring. The message can hop along the ring direction for a random number of times before it is being transmitted to the SINK node.

This routing process provides source-location privacy that resembles the airport terminal transportation system. The message transmission in the ring acts as a network level mix. As long as it is infeasible for an adversary to distinguish the message initiator from the message forwarder in the mixing ring, then it would be infeasible for the adversaries to identify the real message source-location. Therefore, our goal is to

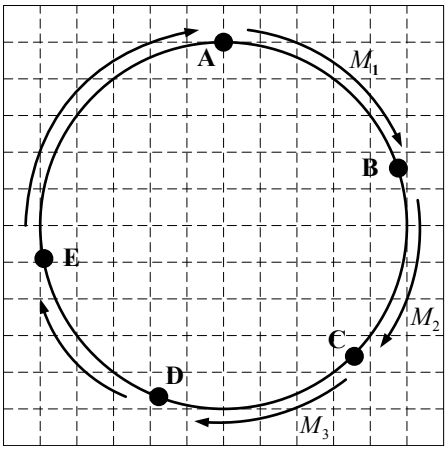



Fig. 3. Message transmission in the ring

design security mechanisms such that it is infeasible for anyone to distinguish the message source node from the message forwarding node.

Relay ring nodes generate vehicle messages to be transmitted in the mixing ring. The normal ring nodes can store data messages received from the normal nodes. The vehicle messages may contain several data units. These units are left unused initially. If a unit in the vehicle message is not used, we name this unit as *dummy unit*, composed of any fixed data structure, such as all 0s. The length of a unit is the same as the data message sent by a normal node. Upon receiving a vehicle message, if a normal ring node has a real data message received and there is still a dummy unit in the vehicle message, it can replace this dummy unit with the data message. The updated vehicle message will then be forwarded to its successor ring node. If this normal ring node has not received any data messages from the normal nodes, or there is no dummy units left in the vehicle message, it simply forwards this vehicle message. The vehicle message should be sent at the rate which could ensure that all the data messages could be embedded in vehicle messages and forwarded to the SINK with minimum delay.

In our scheme, to thwart message source analysis, the message transmission in the ring is encrypted. Each ring node shares a secret key with its predecessor ring node and a secret key with its successor ring node. As an example, in Fig. 3, ring node $B$ shares a key $K_{AB}$ with ring node $A$ and a key $K_{BC}$ with ring node $C$. When node $B$ receives a packet $M_1$ from node $A$, it first decrypts $M_1$ using the share secret key $K_{AB}$. Let $m_1 = D_{K_{AB}}(M_1)$. Upon decryption, node $B$ will be able to find the dummy unit(s) in $m_1$ and replace the dummy unit(s) with the data message(s) that it received from the normal nodes. Denote the updated message as $\{D_{K_{AB}}(M_1)\}$. The updated vehicle message will be encrypted using the shared secret $K_{BC}$ before it is transmitted to the node $C$. Denote the message that generated in node $B$ as $M_2$, then we have

$$M_2 = E_{K_{BC}}(\{D_{K_{AB}}(M_1)\}). \quad (1)$$

When DES or AES encryption algorithm is being used to provide message encryption, then it is computationally infeasible to find the correlation between $M_1$ and $M_2$.

Apparently, the energy drainage for the relay ring nodes will be faster than the normal ring nodes. To balance the energy consumption, the normal ring nodes can take turns to be the relay ring nodes. Similarly, since the energy drainage for the ring nodes will be faster than the regular grid nodes, the nodes in the selected ring grid can take turns to be the ring node.

### C. Forwarding to the SINK

After a vehicle message arrives at a relay ring node, it will be forwarded to the SINK by this relay ring node with certain probability $p$. Here $p$ is a parameter related to the number of relay ring nodes on the mixing ring. If this vehicle message is not forwarded to the SINK by the relay ring node, it will be forwarded to the next ring node until another relay ring node is reached.

## V. Security Analysis

We will first analyze that the proposed routing to a random intermediate node (RRIN) in phase one can provide local source-location privacy. Unlike phantom routing, which has no control over the phantom source without leaking significant side information, in our proposed RRIN scheme, the intermediate node is determined before each data message is transmitted by the source-location, the data message carries no observable side information of the message source-location in its content. Therefore, it does not have the security drawbacks of phantom routing discussed before. It is also impossible for the adversary to trace back and identify the real message source based on an individual traffic monitoring. This is because the probability for multiple events from the same source to use the same routing path and intermediate node is very low for large 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 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 pretty small. As shown in Fig. 2, if an adversary receives $M_2$ 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. Therefore, our proposed protocol can provide the local source-location privacy.

As shown in Fig. 2, the intermediate nodes $I_1, I_2, I_3$ forward messages to ring nodes $R_1, R_2, R_3$, respectively. This means that messages generated from one source node will not be forwarded to a specific ring node. Conversely, the data messages

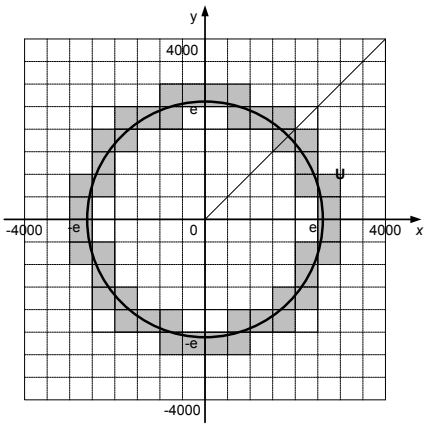



Fig. 4. Ring selection in simulation setup

received from one ring node could also be transmitted from many different source nodes in the network.

The routing in the mixing ring is the second phase routing. This phase aims at providing network-level source-location privacy. This is achieved by hop-by-hop message encryption. Without hop-by-hop message encryption, by comparing the vehicle message that a node received and transmitted, the adversary can determine whether a data message has been loaded into the updated vehicle message. However, once the hop-by-hop message encryption is implemented, it is computationally infeasible for an adversary to distinguish the message initiator and message forwarder in the mixing ring. The messages across the network are totally mixed up. As shown in Fig.2, a data message received by ring node $B$ could be sent to the SINK node from a completely different ring node, maybe node $E$ for instance. Therefore, the network-level source-location privacy is achieved.

## VI. Performance Analysis and Simulation Results

In our design, all data messages will be delivered to the SINK node through the mixing ring. While providing network level source-location privacy, the location of the ring should be selected to ensure that the overall energy consumption and latency for message transmission to be lowest for the normal nodes to complete these operations. We assume that each sensor node in the network has complete knowledge of its relative location in the sensor network and also some ring nodes. We also assume that the energy drainage for each transmission is proportional to the square of the distance, i.e.

$$\mathcal{E} = \alpha \times d^2,$$

where $\mathcal{E}$ denotes the energy consumption, $\alpha$ is a constant parameter and $d$ is the distance of the transmission. Fig. 4 gives an example of a target area of size $8000 \times 8000$ meters. The shaded grids are selected as the ring grids. The line in the middle of the shaded area is indicated by the solid line. If the density of the sensor nodes in the sensor network is $\lambda$, then the total energy consumption for each sensor in this area to transmit one message to a ring node can be calculated as follows:

$$\begin{aligned} \mathcal{E}_{total} &= 8\mathcal{E}_U \\ &= 8\alpha\lambda \int_0^{\pi/4} \int_0^{4000/\cos\theta} (r-e)^2 r dr d\theta, \end{aligned}$$

where $\mathcal{E}_U$ is the energy consumption for area $U$ as demonstrated in Fig. 4. It can be calculated that when $e = 3061$, the overall power consumption $\mathcal{E}_{total}$ achieves the minimum. In this way, we get the optimal ring location.

In practical application, for large sensor network, usually only a small fraction of the sensor nodes in the network has events to report. We name these nodes as *active nodes*. We also define two parameters in our simulation: $\tau$, the number of data messages a normal node generates in each second, and $a$, active nodes ratio.

Assume the network is composed of $g$ normal nodes, and the ring consists of $r$ ring nodes. On average, one ring node should be responsible for delivering the data messages from $g/r$ normal nodes. Assume data messages are $l$-bit long, then on average, in each second, a ring node will receive:

$$\gamma = \frac{g}{r} \times l \times a \times \tau = \frac{gla\tau}{r},$$

messages.

If vehicle messages are $L$-bit long, the number of vehicle messages generated by a ring node in one second is:

$$\frac{gla\tau}{r} \times \frac{1}{L} = \frac{gla\tau}{rL}.$$

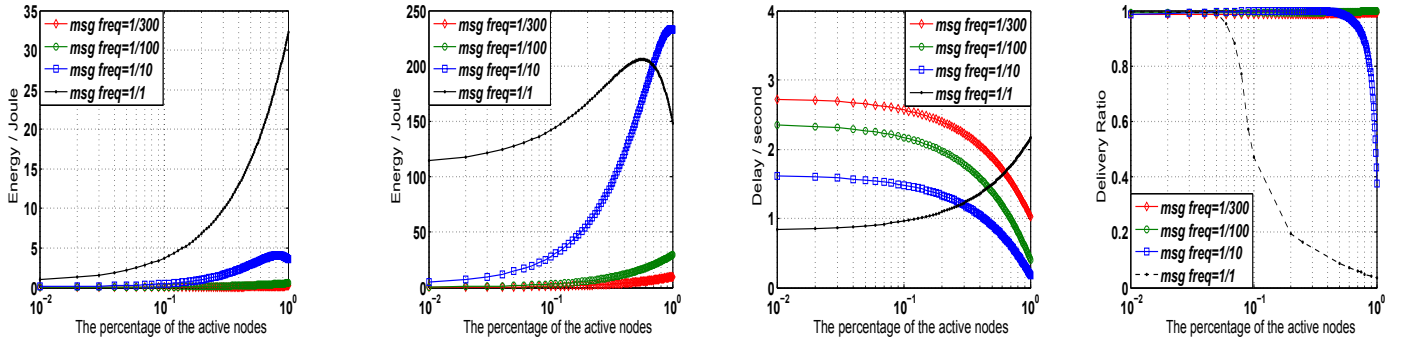
Since only the relay ring nodes on the ring can generate vehicle messages. If there are $n$ relay ring nodes on the ring, then each relay ring node needs to generate at least

$$\frac{gla\tau}{rL} \times \frac{r}{n} = \frac{gla\tau}{nL},$$

vehicle messages each second.

Simulation results are provided in Fig. 5 to demonstrate the power consumption for both normal nodes and ring nodes, message latency and message delivery ratio of the proposed scheme. Our simulation was performed using NS2 on Linux system. In the simulation, the target area is a square field of size $8000 \times 8000$ meters. We partition this field into 2400 normal grids/nodes. The mixing ring is composed of 80 grids, i.e, $r = 80$. There are four relay ring nodes in the mixing ring, i.e, $n = 4$. We assume that the randomly selected intermediate node is at least 600 meters away from the real message source. The data messages are 8-bit long, i.e, $l = 8$. The vehicle messages are 16-bit long, i.e, $L = 16$.

From the Fig. 5.(a) and (b), we can see that ring nodes consume more energy than normal nodes. To solve this problem, the nodes in ring grids can take turns to be the ring nodes. It is also noticed that the delivery ratio drops exponentially when the traffic volume increases. It is primarily because of the traffic collisions and packet losses caused by the increased traffic volume. For a large sensor network, it is usually not necessary for all the sensor nodes to be active at the same time. In practice, the percentage of active nodes might be very low.




(a) Power consumption of normal nodes (b) Power consumption of ring nodes (c) Message latency (d) Message delivery ratio

Fig. 5. Performance of the proposed routing and encryption scheme

The transmission frequency also tends not to be very high. In other words, the traffic volume may be low. In this scenario, we can ensure almost 100% delivery ratio, as shown in Fig. 5.(d). Our simulation results demonstrate that the proposed scheme is very efficient and can be used for practical applications.

## VII. Conclusions

Source-location privacy is critical to the successful deployment of wireless sensor networks. In this paper, we have proposed a scheme that can achieve source-location privacy in the wireless sensor networks through a three-phase routing: routing to a randomly selected intermediate node (RRIN), routing in a network mix ring (NMR), and message forwarding to the SINK node. The optimal location for the mixing ring is also derived. Our proposed scheme provides excellent local source privacy and global source-location privacy. Simulation results demonstrate that the proposed scheme can achieve very good performance in energy consumption, message delivery latency while assuring high message delivery ratio.

## VIII. Acknowledgments

This research was partially supported by the US National Science Foundation under grants CNS-0716039, CNS-0848569, and CNS-0845812.

## References

[1] 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.

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

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, (New York, NY, USA), pp. 88–93, ACM, 2004.

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

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

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

[16] 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.

[17] 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.

[18] L. Hu and D. Evans, "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.

[19] 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.

[20] H. Chan and A. Perrig, "Pike: peer intermediaries for key establishment in sensor networks," *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, vol. 1, pp. 524–535 vol. 1, March 2005.

[21] P. Traynor, R. Kumar, H. Choi, G. Cao, S. Zhu, and T. La Porta, "Efficient hybrid security mechanisms for heterogeneous sensor networks," *Mobile Computing, IEEE Transactions on*, vol. 6, pp. 663–677, June 2007.

[22] S. Zhu, S. Setia, and S. Jajodia, "Leap: efficient security mechanisms for large-scale distributed sensor networks," in *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, (New York, NY, USA), pp. 62–72, ACM, 2003.