Angle-based Dynamic Routing Scheme for Source Location Privacy in Wireless Sensor Networks

Petros Spachos*, Dimitris Toumpakaris§ and Dimitrios Hatzinakos*
*Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada
§Wireless Telecommunications Laboratory, Department of Electrical and Computer Engineering
University of Patras, Rio Achaias, Greece 265 00
E-mail: {petros,dimitris}@comm.utoronto.ca, dtouba@upatras.gr

***Abstract*—Subject monitoring and tracking is one of the most appealing classes of applications for Wireless Sensor Networks (WSNs). Numerous inch scale nodes can sense, collect and distribute crucial information with low deployment cost. For instance, the movement of endangered species in a national park can be monitored with a WSN. However, in such applications privacy issues can jeopardize the successful deployment of the network. An adversary might trace the network traffic over the same paths and eventually locate the source in the network. In this paper, we propose a source-location privacy scheme that employs randomly selected intermediate nodes based on inclination angles. The introduced Angle-based Dynamic Routing Scheme (ADRS) is analysed and is compared with the Phantom Single-path Routing Scheme (PSRS). Simulation results demonstrate that ADRS improves the safety period and the packet latency.**

I. Introduction

Wireless sensor nodes can be inch scale, low-cost autonomous devices that consist of sensing, data processing and communication components. However, their storage and computing capabilities are limited by strict energy supplies. Usually the nodes are designed to work unattended and recharging or replacing their batteries is sometimes infeasible or impossible. Hence, sensor nodes can be active or inactive at any time. An efficient routing scheme should be able to quickly adapt to those changes.

The nodes are organized into a Wireless Sensor Network (WSN), which can be appealing to a plethora of applications, with event monitoring and tracking being one of the most common. In such networks, packet latency is of high importance. For instance, in a national park a WSN can be deployed to monitor the movement of endangered species. Sensor networks rely on wireless communication to deliver crucial data to the destination. However, the wireless channel is an open medium and the lack of physical boundaries makes WSNs vulnerable to security threats. An adversary equipped with radio transceivers may interact with the network and collect important traffic information. It is possible for the adversary to use this information to find the location of the source using tracking techniques, even if the network packets are well encrypted. A description of the problem, also known as the Panda-Hunter game, was introduced in [1]. Similar security issues can arise in other applications, such as monitoring the patients and doctors in a hospital [2], [3], and tracking friendly soldiers on the battlefield [4].

In this paper, we propose an Angle-based Dynamic Routing Scheme (ADRS) designed to enhance the source location privacy in WSNs. The introduced scheme uses the location information of the nodes and calculates the inclination angle formed between the transmitter and the receiver and the transmitter and the destination to form a candidate set of neighbor nodes to forward the packet. One of the nodes in the candidate set is selected randomly and becomes the next relay node. The candidate set changes at every packet transmission, leading to multiple paths towards the destination. The candidate set is formed based on an inclination angle that can be used to control the latency and the safety period of the protocol. As the paths change dynamically, the scheme can provide privacy to the location of the source without increasing significantly the packet latency. Our analysis shows that ADRS can provide sufficient source-location privacy. In comparison with the Phantom Single-path Routing Scheme (PSRS), the introduced scheme shows an increase up to 70% in safety period and improved packet latency.

The rest of this paper is organized as follows: The related work is reviewed in Section II. Section III defines the models, whereas Section IV describes the Angle-based Dynamic Routing Scheme. Section V presents simulation results and the performance analysis. We conclude in Section VI.

II. Related Work

In [1] the Phantom Routing Scheme (PRS), which consists of two phases is introduced. During the first phase, the packet follows a random walk towards any direction and creates a fake "phantom" source. In the second phase this "phantom" source floods the packet to the network. In [5], the Phantom Single-path Routing Scheme (PSRS) substitutes the second phase of PRS with single-path routing. In [6] it is shown that terminating the random walk permanently has a negative impact on the safety period. An improvement of PSRS was introduced in [7]. Phantom Routing with Locational Angle (PRLA) improves the safety period with a minor increase in the energy overhead.

The work of D. Toumpakaris was supported by the European Union (European Social Fund - ESF) and Greek national funds through the Operational Program Education and Lifelong Learning of the National Strategic Reference Framework through the Research Funding Program Thales - Investing in knowledge society through the European Social Fund.

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC), and by the MRI-Ontario under an ORF-RE grant.

978-1-4799-4482-8/14/$31.00 ©2014 IEEE

An improvement of the random walk is introduced in [8]. In Direct Random Walk (DROW) each node selects its parent nodes based on their distance from the destination and the hop count. When a node has a packet to transmit, it forwards the packet to one of its parent nodes randomly. DROW works well when each node has multiple parents. In [9] a randomly selected intermediary node scheme (RRIN) was proposed. There are two versions of RRIN. In the first version the source forwards the packet to an intermediate node that is at least in a minimum distance from the source. Compared to PRS this approach improves the safety period, without affecting the latency. In the second approach the source forwards the packet to any intermediate node randomly. The second approach has better safety period but also higher latency.

Apart from the random walk, there are also solutions based on geographic routing. These approaches use location information of the nodes in the network. In [4], a combination of geographic routing along with encryption techniques was proposed. Each node divides its neighbour nodes in four sets based on the location of the destination. The sets are prioritized based on their trustworthiness to deliver the packet. Then a node of the most reliable set is randomly selected and receives the packet. The main drawback of this approach is that it might introduce cycles and, as a consequence, increase the latency. In [10] the toroidal region routing (STaR) algorithm is introduced. It improves the energy consumption of RRIN and provides a balance in power consumption and source location privacy. This approach also assumes a WSN that spans a large area and consists of multiple grids. In the literature there are also solutions that provide timing and temporal privacy through delay [11]. In [12], [13] opportunistic routing was used to enhance source-location privacy. In [14], a brief description of the state-of-the art protocols in source location privacy is presented.

The proposed scheme is a combination of random node selection and geographical routing. An inclination angle is employed to avoid cycles around the source, whereas the random node selection helps improve the privacy.

III. Models

In this section the necessary models of the Panda-hunter game along with their requirements will briefly be described.

A. System Model

The considered system model has similar requirements to the Panda-Hunter game [1]. A number of sensor nodes are randomly deployed in a large predefined area, which needs to be monitored, according to the Poisson distribution. The nodes are static and more nodes can join the network at any time. Nodes can also leave the network because of malfunctions or because they run out of energy.

Each sensor node in the network field knows its relative location. Information about sensor location can also be obtained through network broadcasting [15], [16]. The network can have only one source and one destination at any given time. The location of the source can change over time. Every node in the network knows the relative location of the destination node in order to transmit the packet. Every node can be the source node of the network.

B. Adversary Model

The adversary model of the Panda-Hunter game will be used. The adversary tries to determine the location of the source node by being well-equipped and having some technical advantages over the nodes. By employing RF localization techniques the adversary can use hop-by-hop backtracking to determine the location of the source node. It has unlimited energy so it can move between nodes for a long time period and also possesses adequate memory and computation capabilities. Moreover, it knows the location of the destination node and can monitor the traffic area around the node that it observes. When a packet arrives to the observed node, the adversary can determine the location of the sender node and physically move to the sender node.

The adversary starts beside the destination node. When the first packet arrives, it moves to the sender node of the packet. By repeating this strategy the adversary will eventually find the source. At any time, the adversary does not interfere with the proper functioning of the network by deactivating nodes or modifying packets in order to avoid triggering other security mechanisms. Hence, it is assumed that any node in the network is not aware of the location of the hunter.

IV. The Angle-based Dynamic Routing Scheme

In this section, the Angle-based Dynamic Routing Scheme (ADRS) will be introduced along with a theoretical analysis of the resulting latency.

A. Scheme description

In ADRS, when a node has a packet to transmit it floods a Request To Send (RTS) message to all the neighbor nodes in the transmission range, r_2. On reception of the Clear To Send (CTS) messages from the neighbor nodes, the node calculates the distance to the neighbor node and the inclination angle ϕ between the source node and the neighbor node with respect to the destination node, as shown in Fig.1. If the distance to the neighbor node is larger than a predefined distance r_1 and the inclination angle does not exceed a predefined angle $\frac{\theta}{2}$ the neighbor node is added to the candidate node set.

The nodes can reply with a CTS message after time $T_{Backoff}$ [13], which is inversely proportional to the distance between the sender node and the responding node. Following this approach, the sender node will receive the first CTS message from the neighbor node that is closest to the destination. At the same time and after receiving all the CTS messages, the sender node can prioritize the nodes in the candidate set with respect to their distance from the destination. In a network with high density, when the sender node waits for all the CTS messages, the energy consumption and the packet latency increase. Instead of waiting for all the CTS messages, the sender node can wait only for N CTS messages and form the candidate set.

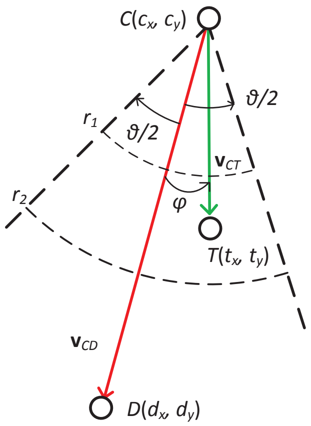

Fig. 1: Selection of a candidate node T.

From the N nodes in the candidate set, one will be selected randomly to be the next relay node. The next relay node will follow the same routing principles until the packet reaches the destination. Figure 1 depicts one step of the routing process.

The use of the RTS/CTS handshake also helps the network to quickly adapt to any changes in the number of the nodes in the network area. If a node leaves the network, this node will not participate in the handshake, whereas if a node joins the network it can acquire relative location information from its neighboring nodes. This way, there is no need for an initialization phase every time the source node or the network density changes.

The selection of r_1 and θ is important in ADRS. A small value of r_1 will increase the size of the candidate nodes set, but many candidate nodes will be close to the source node. Hence, the number of hops needed to reach the destination will increase, increasing the packet latency as well. On the other hand, a large r_1 will limit the number of candidate nodes. Therefore, the network density should be sufficient to guarantee connectivity. Similarly, a small inclination angle will require a higher network density while a large inclination angle might lead to paths that are of large distance from the shortest path, hence increasing the number of hops.

B. Selection of the next node

To determine the next node where a packet will be sent, a given node applies two criteria. First, the node should be at distance R satisfying $r_1 \leq R \leq r_2$, where r_2 is typically the transmission range. Moreover, as can be seen in Fig. 1, the inclination angle ϕ that is formed between the segment CD connecting the current node C to the destination node D and the segment CT connecting the current node C to the candidate node T should not exceed a given value $\theta/2$.

Definition: The *inclination angle* ϕ between any node and a neighbor node T in the network is the angle formed by the line that connects the node and the neighbor node T and the line that connects the node and the destination node D.

The value of R is determined based on the topology of the network. R is random, since the topology is random, but once the topology has been fixed it is assumed that a node knows or can determine its distance to its neighboring nodes.

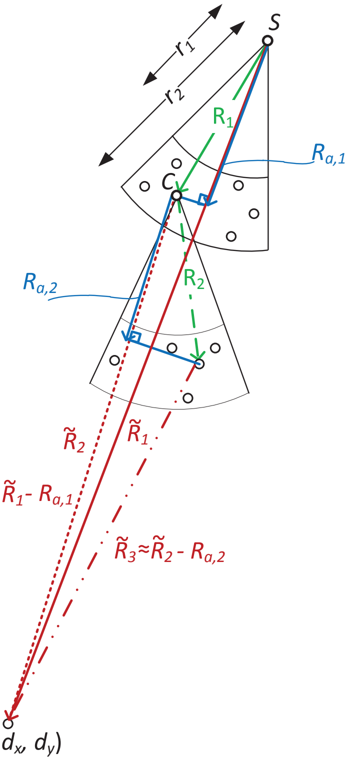

Fig. 2: Calculation of the average latency.

The angle can be found using the inner (dot) product between two vectors. Let $\mathbf{v}_{CD}$ and $\mathbf{v}_{CT}$ be the vectors connecting a node C to the destination D and to a candidate node T, respectively, as shown in Fig. 1. $\mathbf{v}_{CD}$ and $\mathbf{v}_{CT}$ can be calculated easily using the coordinates of points C, D and T. Then

$$\langle \mathbf{v}_{CD}, \mathbf{v}_{CT} \rangle = \|\mathbf{v}_{CD}\| \cdot \|\mathbf{v}_{CT}\| \cdot \cos(\phi) \Rightarrow$$
$$\phi = \arccos\left[\frac{\langle \mathbf{v}_{CD}, \mathbf{v}_{CT} \rangle}{\|\mathbf{v}_{CD}\| \cdot \|\mathbf{v}_{CT}\|}\right]. \tag{1}$$

If $\phi \in \left[-\frac{\theta}{2}, +\frac{\theta}{2}\right]$ node T is added to the candidate set.

C. Mean number of hops

Since it is assumed that the nodes follow the 2-dimensional Poisson distribution, they are uniformly distributed in the $x-y$ plane. Each node C selects its neighbors based on their distance and the inclination angle. We want to calculate the distribution of the distance by which a packet advances towards the destination at each hop. We first calculate the distribution of the distance R_i between the current node and the next node. For simplicity from now on we omit the hop index, i, from R and all other related quantities. Because the nodes follow the Poisson distribution and because the algorithm only selects nodes that form a maximum inclination angle $\pm\frac{\theta}{2}$, the angle ϕ of Fig. 2 is uniformly distributed in the interval $\left[-\frac{\theta}{2}, +\frac{\theta}{2}\right]$. On the other hand, the distribution of R can be found as follows.

$$F_R(r) = \Pr\{R \leq r\} = \frac{\frac{r^2\theta}{2} - \frac{r_1^2\theta}{2}}{\frac{r_2^2\theta}{2} - \frac{r_1^2\theta}{2}} = \frac{r^2 - r_1^2}{r_2^2 - r_1^2}, \; r \in [r_1, r_2]. \tag{2}$$

In (2) we have used the fact that the probability of finding a node in a given region is proportional to the area of the region, and the restriction imposed from the algorithm that the selected node be at a distance satisfying $r_1 \leq R \leq r_2$. Therefore, the probability density function equals

$$f_R(r) = \frac{d}{dr} F_R(r) = \frac{2r}{r_2^2 - r_1^2}, \ r \in [r_1, r_2]. \tag{3}$$

Now, let R_a be the projection of R on the segment CD connecting the node to the destination, as shown in Fig. 2. This is the distance by which the packet advances towards the destination along CD during a given hop. Clearly,

$$\begin{aligned} F_{R_a|\Phi}(r_a|\phi) &= \Pr\{R_a \leq r_a|\phi\} \\ &= \Pr\left\{R \leq \frac{r_a}{\cos(\phi)}\right\} = F_R\left(\frac{r_a}{\cos(\phi)}\right) \\ &= \frac{\frac{r_a^2}{\cos^2(\phi)} - r_1^2}{r_2^2 - r_1^2}, \ r_a \in [r_1\cos(\phi), r_2\cos(\phi)]. \end{aligned} \tag{4}$$

Hence,

$$f_{R_a|\Phi}(r_a|\phi) = \frac{2r_a}{\cos^2(\phi)(r_2^2 - r_1^2)}, \ r_a \in [r_1\cos(\phi), r_2\cos(\phi)]. \tag{5}$$

Given (5) we can calculate the expectation of R_a.

$$\begin{aligned} \mathbb{E}[R_a] &= \mathbb{E}_\phi\left[\mathbb{E}[R_a|\phi]\right] \\ &= \mathbb{E}_\phi\left[\int_{r_1\cos(\phi)}^{r_2\cos(\phi)} r_a \frac{2r_a}{\cos^2(\phi)(r_2^2 - r_1^2)} dr_a\right] \\ &= \mathbb{E}_\phi\left[\frac{2r_a^3}{3\cos^2(\phi)(r_2^2 - r_1^2)}\Bigg|_{r_1\cos(\phi)}^{r_2\cos(\phi)}\right] \\ &= \mathbb{E}_\phi\left[\frac{2\cos(\phi)(r_2^3 - r_1^3)}{3(r_2^2 - r_1^2)}\right] \\ &= \frac{2(r_2^3 - r_1^3)}{3(r_2^2 - r_1^2)} \int_{-\theta/2}^{+\theta/2} \frac{1}{\theta}\cos(\phi)d\phi \\ &= \frac{2(r_2^3 - r_1^3)}{3(r_2^2 - r_1^2)} \frac{\sin(\theta/2)}{\theta/2}. \end{aligned} \tag{6}$$

Therefore, the average projection of the distance that a packet covers towards the destination on the segment CD of Fig. 2 is given by (6). If the packet is not very close to the destination, we can approximate $\tilde{R}$ in Fig. 2 as $\|CD\| - R_a$. Hence, R_a is approximately equal to the distance by which the packet advances towards the destination. Clearly, the accuracy of this approximation worsens as the packet nears the destination, and $\tilde{R} > \|CD\| - R_a$. However, it will be good for the majority of the hops towards the destination.

If the distance between the source and the destination is equal to $\|SD\|$, the average number of hops can be approximated by

$$\bar{H} = \frac{\|SD\|}{\mathbb{E}[R_a]}. \tag{7}$$

Even if the value of $\mathbb{E}[R_a]$ were exact, the average latency (7) would not be perfectly accurate either, since in the last hop when the last intermediate node locates the destination it will send the packet deterministically to the destination. However, as will be shown in Section IV, (7) leads to an estimate of the average number of hops that, although slightly optimistic, is fairly accurate.

D. *Minimum and maximum number of hops*

The minimum number of hops can be found easily by assuming that during each hop the packet progresses along the segment SD of Fig. 2 and by the maximum distance, r_2. Hence,

$$H_{\min} = \frac{\|SD\|}{r_2}.$$

Similarly to the calculation of the average latency, the maximum latency can be approximated by assuming that $\tilde{R} \approx \|CD\| - R_a$, that the packet moves by the minimum allowed distance r_1 and that at every hop the packet moves away from the segment SD with the largest possible angle. For the worst-case angle $\theta/2$, $R_a = r_1\cos(\theta/2)$. Thus,

$$H_{\max} \approx \frac{\|SD\|}{r_1\cos(\theta/2)}.$$

It is also possible to obtain analytic lower and upper bounds for the safety period. However, this analysis is omitted due to space constraints.

V. Simulation Results and Performance Analysis

A discrete event-based simulator – OMNeT++ – was used to evaluate the Phantom Single-path Routing Scheme (PSRS) [5], and the introduced ADRS. The two protocols were compared in terms of safety period and packet latency.

A. *Simulation Parameters*

The sensor nodes are randomly deployed in a $100 \times 100\ m^2$ area. The nodes follow the Poisson distribution with $\lambda = 0.101$. In the distribution, λ is chosen so that the probability that there are at least $N = 3$ neighbor nodes in the selected area, as defined by $r_1 = 8$ and $r_2 = 12$ and $\theta = 90°$, and described in Section III-A, be 0.99.

Ten topologies with number of nodes ranging between 948 to 1091 were evaluated. The distance between the source and the destination varies between 40 to 140 meters. For each topology the source generates 1000 packets towards the destination.

In both schemes, the transmission range of each node is 12m. PSRS starts with a number of random hops, h. The node that will have received the packet after these h hops will become a "phantom" source and will forward the packet to the destination following single-path routing. In our simulations $h = 10$. ADRS uses $\theta = 90°$ and selects $N = 3$ candidate nodes according to the scheme of Section IV-A. Among the 3 candidate nodes one is selected randomly to receive the packet.

B. *Performance Analysis*

The two routing schemes are compared in terms of the average safety period and the average packet latency for different source-destination distances.

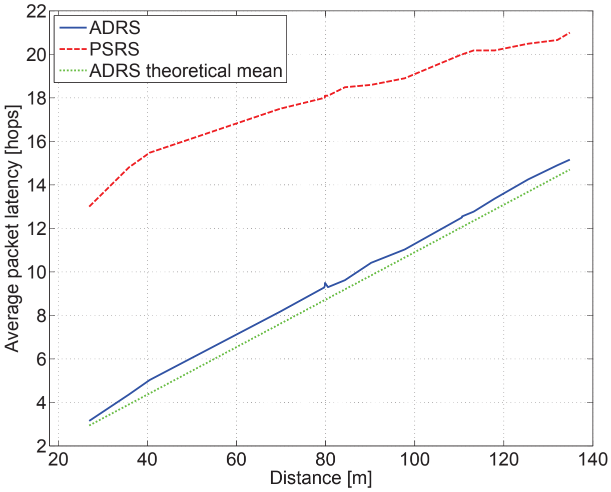

Fig. 3: Average packet latency over different distances.

1) Packet latency: The latency of a packet depends on the length of the path that the packet follows toward the destination. The path can also be described in terms of the number of hops. The packet latency ia equal to the number of hops that a packet needs to reach the destination. Figure 3 shows the average packet latency of the two algorithms as well as the theoretical mean for ADRS as calculated in Section IV-C. It can be seen that the theoretical mean is slightly optimistic but very close to the simulation results. ADRS has lower packet latency than PSRS. This is because ADRS always uses nodes located towards the destination. Following the inclination angle approach, these nodes do not deviate significantly from the shortest path. Hence, the number of the hops is close to optimal. On the other hand, PSRS forwards the packets towards a random location for the initial 10 hops. If this location is not towards the destination, the packet latency increases considerably.

2) Safety period: The safety period is the number of the packets that the source can send toward the destination before the adversary determines the location of the source. Figure 4 shows the average safety period. ADRS outperforms PSRS in terms of safety period. The main reason is the random selection criterion of the next relay node. For every packet transmission the transmitter node has a set of $N = 3$ candidate nodes and selects one of them randomly. As the distance between the source and the destination increases, the number of the required hops to reach the destination also increases. As a consequence, more nodes participate in every packet transmission. As more nodes participate in the transmissions, more paths need to be discovered by the adversary. Hence the safety period increases.

VI. Conclusions

In this paper, an Angle-based Dynamic Routing Scheme (ADRS) is proposed. Analysis and simulations of the introduced scheme show that it can enhance source location privacy. In comparison with PSRS, ADRS can achieve better safety period up to 70% and improve packet latency without increasing the complexity.

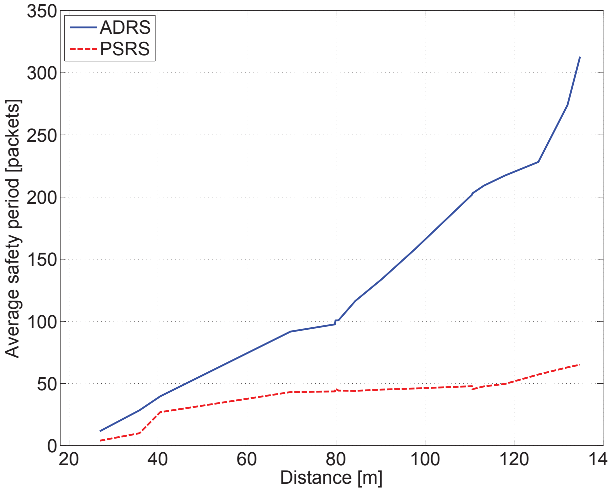

Fig. 4: Average safety period over different distances.

References

[1] C. Ozturk and Y. Zhang, "Source-location privacy in energy-constrained sensor network routing," *In ACM SASN*, pp. 88–93, 2004.

[2] S. Pai, S. Bermudez, S.B. Wicker, M. Meingast, T. Roosta, S. Sastry, and D.K. Mulligan, "Transactional confidentiality in sensor networks," *IEEE Security Privacy*, vol. 6, no. 4, pp. 28–35, 2008.

[3] M. Mohammadian, D. Hatzinakos, and P. Spachos, "Computational intelligence for user and data classification in hospital software development," *International Conference on AIAI*, pp. 145–154, 2012.

[4] R. A. Shaikh, H. Jameel, B. J. DAuriol, H. Lee, S. Lee, and Y.J. Song, "Achieving network level privacy in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 1447–1472, 2010.

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

[6] L. Zhang, "A self-adjusting directed random walk approach for enhancing source-location privacy in sensor network routing," *Proceedings of the 2006 international conference on Wireless communications and mobile computing*, pp. 33–38, 2006.

[7] W. Wei-Ping, C. Liang, and W. Jian-xin, "A source-location privacy protocol in wsn based on locational angle," *IEEE International Conference on Communications (ICC)*, pp. 1630–1634, 2008.

[8] J. Yao and G. Wen, "Preserving source-location privacy in energy-constrained wireless sensor networks," *International Conference on Distributed Computing Systems Workshops (ICDCS)*, pp. 412–416, 2008.

[9] Y. Li, L. Lightfoot, and J Ren, "Routing-based source-location privacy protection in wireless sensor networks," *IEEE International Conference on Electro/Information Technology*, pp. 29–34, 2009.

[10] L. Lightfoot, Y. Li, and J. Ren, "Preserving source-location privacy in wireless sensor network using star routing," *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pp. 1–5, 2010.

[11] X. Hong, P. Wang, J. Kong, Q. Zheng, and J. Liu, "Effective probabilistic approach protecting sensor traffic," *Military Communications Conference, 2005. MILCOM 2005. IEEE*, pp. 169–175 Vol. 1, 2005.

[12] P. Spachos, L. Song, and D. Hatzinakos, "Opportunistic routing for enhanced source-location privacy in wireless sensor networks," *Biennial Symposium on Communications (QBSC)*, pp. 315–318, May 2010.

[13] P. Spachos, L. Song, F.M. Bui, and D. Hatzinakos, "Improving source-location privacy through opportunistic routing in wireless sensor networks," *Computers and Communications (ISCC), 2011 IEEE Symposium on*, pp. 815–820, 2011.

[14] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 1238–1280, 2013.

[15] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 4, pp. 829–835, 2006.

[16] L. Hu and D. Evans, "Localization for mobile sensor networks," *Proceedings of the 10th annual international conference on Mobile computing and networking*, pp. 45–57, 2004.