Improving Source-Location Privacy Through Opportunistic Routing in Wireless Sensor Networks

Petros Spachos, Liang Song, Francis M.Bui, and Dimitrios Hatzinakos

Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada
E-mail: {petros,songl,bui,dimitris}@comm.utoronto.ca

***Abstract*—Wireless sensor networks (WSN) can be an attractive solution for a plethora of communication applications, such as unattended event monitoring and tracking. One of the looming challenges that threaten the successful deployment of these sensor networks is source-location privacy, especially when a network is deployed to monitor sensitive objects. In order to enhance source location privacy in sensor networks, we propose the use of an opportunistic mesh networking scheme and examine four different approaches. Each approach has different selection criteria for the next relay node. In opportunistic mesh networks, each sensor transmits the packet over a dynamic path to the destination. Every packet from the source can therefore follow a different path toward the destination, making it difficult for an adversary to backtrack hop-by-hop to the origin of the sensor communication.**

I. INTRODUCTION

Wireless sensor networks have been envisioned to have tremendous potential in a variety of applications for collecting information from monitored environments and objects, e.g., military and civilian applications, environmental monitoring and traffic monitoring. However, due to the inherent broadcast nature of wireless communications, it typically poses significant challenges on data security and protection, including susceptibility to unauthorized wireless data interception. As a result, an adversary with the necessary equipment, like a radio transceiver and a workstation might be able to illegally access the network. It could also eavesdrop the communication between sensor nodes, and either identify the source packet or even reveal the source-location, without interfering with the proper functioning of the network.

Location privacy is an important security issue. Lack of location privacy can lead to subsequent exposure of significant traffic information on the network and the physical world entities. For example, a wireless sensor network can be used to monitor the activities or the presence of endangered species. These information should be kept unavailable to any illegal hunter who may try to reveal the location of the source and finally reveal the location of the animals. In order to provide sufficient network privacy in a military intelligence network, the source of a packet and the corresponding path toward the destination should be protected from any eavesdropper.

In this paper, we propose four different approaches based on opportunistic mesh networking to provide source-location privacy through dynamic routing. Opportunistic routing takes advantage of characteristics of the wireless medium. Instead of choosing a single route ahead of time, our approaches determine the path as the packet moves through the network, based on which sensor receives each transmission. This strategy increases the complexity for the adversary to reveal the source, because each packet can follow different path, based on the sensor availability.

The rest of this paper is organized as follows. In Section II, the related works are reviewed. The system model and the adversary model are presented in Section III while the main opportunistic principles are described in Section IV. In Section V, three different opportunistic routing extensions are presented, followed by security analysis in Section VI and simulation evaluation in Section VII. Conclusions remarks are presented in Section VIII.

II. RELATED WORK

In the past decade, a number of source-location privacy communication protocols have been proposed. In [1] and [2], the main idea is a mixture of valid and fake packets. Each node transmits either a valid or a fake packet, consistently. The main disadvantage of this approach is that the broadcasting of fake packets consumes significant amount of the limited energy in each sensor node. Moreover, because in every time slot each node has to transmit a packet, this increase the number of collisions and decrease the packet delivery ratio. Therefore, these approaches are not suitable especially for large scale wireless sensor networks.

Routing based protocols can also provide source-location privacy [3]–[6]. In [3] the authors introduced the Panda-Hunter model to formalize the problem in sensor networks. They proposed a technique called phantom routing. Phantom routing involves two phases: a random walk phase, and a subsequent single path routing. It can be proved that random walk is inefficient at making the "phantom" source far enough from the real source. In [5] a greedy random walk is proposed which offers more energy effectiveness but increases the packet delivery delay. In [6] a direct random walk is proposed. Initially the source chooses a direction for the random walk of the packet. This can be achieved by storing direction information in the header of the packet. The exposure of the direction information decreases the complexity for the adversaries to trace back to the true packet source.

In [7] a non-geographical, overlay routing method for packet delivery was adopted to provide source-location privacy. In [8], [9], the authors introduced a randomly selected intermediate

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

node scheme for local source location privacy protection. In [10], [11], a two-phase routing process is proposed. In the first phase, the packet selects randomly an intermediate node before it is routed to a ring node. In the second phase, the data packet is mixed with other packets through a network mixing ring before being transmitted to the destination.

III. MODELS

This section introduces the system model and the adversary model, to capture the relevant features of wireless sensor networks and any potential adversaries in source-location applications.

A. System Model

The considered system is similar to the Panda-Hunter game introduced in [3]. We assume a large predefined geographical area that needs to be monitored, and deploy a wireless sensor network consisting of many randomly distributed sensor nodes. The network continuously monitors activities and locations of the target in the area.

When the target is discovered, the corresponding sensor becomes the source of the network. This source node starts sending packets to neighboring sensors that are in its limited radio range. The source node will continuously send packets until the adversary discovers the source, or the target disappears from the monitoring area. We make the following assumptions about our system:

- There is only one destination node at any time, while there can be more than one source nodes.
- Any node in the network can become the source node.
- Every node in the network knows the address of the destination node. The information of the destination node location is made public.
- Every node in the network knows its relative location. The information about the relative location of each node can also be broadcasted through the network for routing information update.

B. Adversary Model

The adversary will try to reveal the location of the source node by being well equipped and having some technical advantages over the sensor nodes. The adversary is assumed to have the following characteristics:

- The adversary knows the location of the destination and can determine the location of the sender sensor from the instance of the packet that it overhears. Initially, the adversary is located beside the destination node.
- The adversary can monitor only the traffic area around the node which it observes.
- The adversary can physically move from one sensor to another and has unlimited amount of power.
- The adversary will not interfere with the proper functioning of the network, such as destroying sensor nodes or modifying packets in order not to trigger other security mechanisms.

IV. OPPORTUNISTIC ROUTING PRINCIPLES

In this section, we introduce the main principles of the proposed opportunistic routing protocol.

Opportunistic wireless mesh networks [12] can provide an attractive solution to the source-location problem, based upon the cognitive networking concept, in which every node in the network observes network conditions and—in accordance with prior knowledge gained from previous interactions in the network—plans, decides and acts on this information. The routing path between the source and the destination dynamically changes according to node availability, which makes it difficult for any adversary to locate the source.

A. Network address

Network address is related to the context and is subjected to a "cost of delivery" criterion. Given a node address n and the destination address d of a data packet, this "cost of delivery" $c_{n,d}$ should be locally obtained. This could indicate the average or the approximate cost of delivering a packet from the node n toward the destination d, independent of any dynamic change in the network. Usually, in large-scale wireless sensor networks $c_{n,d}$ is correlated with the distance between the two nodes.

In data-collecting networks, the source wants to deliver a number of packets to the destination, in the absence of cross-traffic, which corresponds to our case of monitoring networks. Initially, the destination node broadcasts a number of identity advertisement packets and every nodes thereon flood the packet to the network. On the reception of a packet, a node can count the smallest number of hops from the destination and use it as "cost of delivery" criteria, $c_{n,d}$. Whenever a new node joins the network, it can estimate its logic address by acquiring the logic address of its neighbor nodes. If the destination node changes, the procedure should start from the beginning. When the source node changes there is no need to repeat the procedure. If a node leaves the network, it will not take part in the selection process as we will see in following section.

B. Transmission process

In every time slot $i \in \{i_0, ..., i_0 + T(i_0)\}$, the transmission strategy is decided by the transmission power at the sensor node. We assume that only one packet can be transmitted in one time slot. Every lost packet will be retransmitted in the next assigned slot. If we use BPSK without channel coding, the Packet Error Rate, $P\hat{E}R(i)$, can be written as [13],

$$P\hat{E}R(i) = 1 - \Big(1 - Q\Big(\sqrt{\frac{2P_t(i) \cdot \hat{G}(i)}{\sigma_n^2}}\Big)\Big)^{F_d}, \qquad (1)$$

where P_t is the transmission power, F_d is the length of the data, σ_n^2 is the noise power, $Q(x) = \frac{1}{\sqrt{\pi}} \cdot \int_{\frac{x}{\sqrt{2}}}^{\infty} e^{-t^2} dt$ and

$$\hat{G}(i) = A \cdot \hat{D}_s(i)^{-n}, \qquad (2)$$

where A is a constant, $\hat{D}_s(i)$ is the distance between the sender node s and the next node i, and n is wireless channel path loss component.

Every packet transmission process is subjected to PER.

C. Next node selection process

We are using four types of packets during the packet relaying process: Request To Send (RTS), Confirm To Send (CTS), DATA and ACK. RTS/CTS are used during the handshake process between neighbor nodes while ACKs are used for verification of DATA delivery.

When a node s has to transmit a packet, it first broadcasts a RTS packet, which includes its own address and the destination address, d. Then node s keeps listening. All the surrounding nodes which are in the range of s are able to hear this request, conforming a set of nodes E_s. There is a subset $V_s \leq E_s$ conformed by any node $i \in E_s$ satisfying the cost condition $c_{i,d} < c_{s,d}$ so,

$$V_s = \{i \in E_s | c_{i,d} < c_{s,d}\}. \quad (3)$$

If a node is in V_s subset and is available for receiving a packet, it should send a CTS packet back to the sender node s. In order to prioritize the nodes based on their distance from the destination, each node $i \in V_s$ initializes a timer, with timeout period as T_i, which is inversely proportional to the difference $c_{s,d} - c_{i,d}$ and can be determined for example as:

$$T_i = \frac{C_0}{c_{s,d} - c_{i,d}} + SIFS, i \neq d \quad (4)$$

where C_0 is a constant and SIFS is the smallest time interval between the RTS and CTS.

The node which is closer to the destination will respond first with a CTS packet, if no packet error occurred during the RTS/CTS transmission, and it will be the next relay node. All the four types of packets are subjected to PER during the transmission process.

D. Node state diagram

The state diagram of a single node is shown in Figure 1. At the beginning, every module is at the sleep stage, (A). If the target appears in the range of a sensor, this node becomes the source node and creates a packet with all the necessary information about the target location, time of appearance etc, (B1). Then, the source node keeps sensing each channel in the data group channel until it finds a vacant data channel, (B2). When an available channel is found, the source node sends a polling tone to its surrounding nodes and waits for the first CTS, (B3). When a CTS is received, the node sends the DATA packet to the next node and waits for ACK, (B4). Finally it goes to sleep mode, (A).

When a node receives an activation request, it starts listening to the channel for RTS, (C1). If there is RTS, it backoffs for T_i time, (C2). After T_i time it sends a CTS, (C3). If it receives any data, it sends back an ACK, (C4), and tries to transmit the packet, (B2).

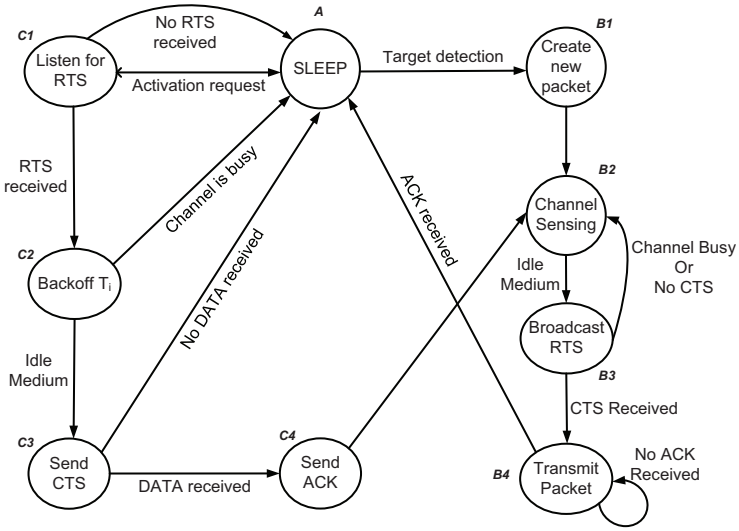

Fig. 1: Node State diagram.

If any of the packets failed to be transmitted, because of packet error, the module goes back to its previous state.

This state diagram tries to reduce the energy consumption of the network. When a node is not participating in any packet transmission, it should be in a state of low power consumption. This will expand the lifetime of each individual node and consequently the lifetime of the network.

V. DIFFERENT OPPORTUNISTIC APPROACHES

In the previous section, the main principles of the first opportunistic routing approach has been described. In this section, three additional extension approaches will be introduced. The differences are on the next relay node selection process.

Sensor networks should be relatively stable for sufficiently long durations of time during their operation. In a stable network, nodes location are fixed and there are not many changes in the network. In this situation, the same node will always win the competition in each hop, the source-destination link will be fixed (which is usually the case in WSN) and the adversary will simply find the location of the source. To alleviate this problem, we introduce three extensions, one with memory in order to avoid using the same nodes in sequence transmissions and two with random selection criteria. A performance comparison of all four approaches is also made.

A. Non-repeating opportunistic routing

In this second approach, every node in the network uses a memory in order to avoid transmitting sequential packets to the same node. That memory contains a flag that initiates if the node will participate in a packet transmission. When the flag is true the node can not participate in a packet transmission because it has participated in another packet transmission recently.

Initially, the flag in all the nodes is *false*. When a node transmits a packet in a time slot, the flag in the node becomes

true. In the next time slot, if this node gets a RTS packet, it will not respond with a CTS packet but will change the status of the flag to *false* again. In this way, a node will not transmit two packets in a sequence, and the adversary could not make progress toward the destination in every time slot.

B. Opportunistic routing with random delay

Opportunistic routing with random delay includes a random factor in the response time of each candidate node. As it was explained in section IV, when a node receives a RTS packet, it will reply with a CTS packet after time T_i, equation 4. In this third approach, a random number in the range of $[0, 1)ms$ is added in that time interval. In this way, the backoff time for each node is not based only on the distance between the sender and the candidate node.

In the calculated T_i time, this approach adds a random delay in the range of $[0, 1)ms$. The new backoff time T_{delay} for that approach is:

$$T_{delay} = T_i + dblrand(0, 1) \tag{5}$$

where dblrand(0,1) is a *random number generator function* to generate a *double* number in the range of $[0, 1)$.

C. Opportunistic routing with random relay

Opportunistic routing with random relay tries to take advantages of the opportunistic routing, with random selection criteria in the next relay node process. In that approach, when a node has a packet to transmit, it will wait for almost all the nodes in its coverage area to reply with a CTS packet. Some of those nodes may not get a RTS packet or their CTS does not reach the sender node because of channel error, based on equation 1. In that case, the sender node will wait for a specific time and then randomly choose between the CTS packets that it received, the next relay node.

The time that the sender node has to wait, $T_{R_{all}}$, should be sufficient for nodes located in the borders of the coverage area of the sender node, to reply with a CTS packet. This time is equal to:

$$T_{R_{all}} = R \cdot C_0 + SIFS, \tag{6}$$

where C_0 is a constant and R is the transmission range of the sensor, in meters.

D. Performance analysis of the different approaches

To evaluate the performance of the proposed schemes, we pursued simulations using OMNET++ [14], in terms of energy consumption and delivery ratio under different traffic volumes. In the simulations, 500 nodes with radio transmission range 12 meters, are uniformly randomly distributed over a square target area 100×100 meters. The communication parameters were chosen based on IEEE 802.15.4, as listed in Table I. The number of transmission power level was set to 15.

Let the node power consumption in transmitting and receiving/idle modes be denoted by P_t and $P_{r/i}$ respectively. The sleeping mode power consumption is practically 1000 times

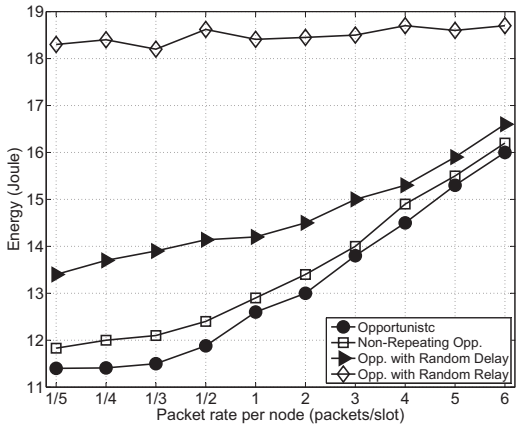

Fig. 2: Energy Consumption.

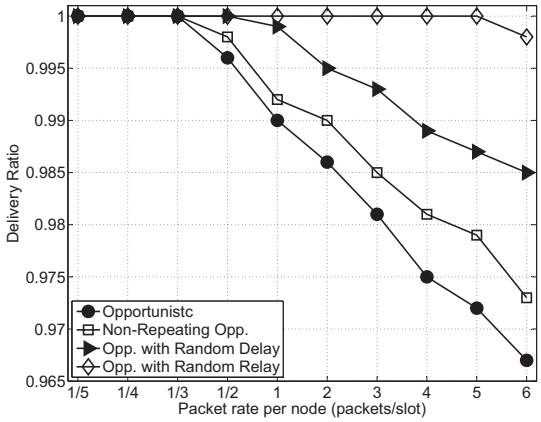

Fig. 3: Delivery ratio.

smaller than P_t and $P_{r/i}$, which is negligible. Let $P_t = 15mW$ and $P_{r/i} = 10mW$.

Figure 2 shows that opportunistic routing consumes the least energy compared to the other approaches. The selection criterion of the next relay node at this approach is the distance from the destination. The packets follow the shortest available path to the destination. However, as the packet rate is increased, the relay node on the shortest path might not be available to transmit a packet at a specific time slot. That node might have a packet to transmit from a previous failed transmission. Then, other nodes will serve as next relay, creating different paths toward the destination with more hops and increasing the energy consumption.

Non-repeating opportunistic routing has similar energy consumption with opportunistic routing. This approach tries to use the shortest path toward the destination, consist of nodes

Parameter	Unit	Value
F_d	*bit*	128×8
n		2.5
A	*dB*	-31
σ_n^2	dBm	-92
P_t	dBm	-4

TABLE I: Communication Parameters Setup

that did not participate in a packet transmission the previous time slot. These two approaches tend to use paths with similar number of hops and have similar power consumption.

Opportunistic routing with random delay consumes a little more energy than the previous two approaches. The nodes have to stay active longer, waiting for a CTS, due to the extra delay added. Moreover, as the packet rate is increased, the energy consumption is increased. This is because of the next node selection criterion which is a combination of the distance to the destination and a random delay.

Opportunistic routing with random relay consumes the most energy over all. In this approach, every node that has a packet to transmit stays the maximum time active, waiting for more than one CTS. Moreover, the next relay node selection process is completely random, leading to different paths to the destination, with different number of hops. This approach tends to use all the available nodes in the network under any packet rate, because the selection criterion is random.

Delivery ratio is shown in Figure 3. For the first three approaches, delivery ratio drops when the packet rate is increased, because the same nodes are selected to serve as relay node. This can potentially lead to traffic collisions and packet losses. Opportunistic routing with random relay drops less packets because random nodes are selected every time and the probability to use the same node in sequent transmissions is small. Usually, for large scale monitoring networks, the transmission frequency tends not to be very high, i.e., the traffic volume may be low. If the transmission frequency is one packet in every two or more time slots we can ensure 100% delivery ratio for all the four approaches.

VI. SECURITY ANALYSIS

Opportunistic routing can provides sufficient privacy to the source. The routing path between the source and the destination changes dynamically based on the network conditions and channel availability. Relay node selection process is according to PER and the distance between the relay node and the destination. However, in a stable network, the same nodes will be chosen as relay, making it easy for the adversary to track the location of the source.

The main advantage of that approach is that it is simple to be implemented, because only simple processing in the nodes is needed. This approach does not add any overhead while it is easy to program the nodes in order to take advantage of the broadcast nature of wireless communication. Although it can provide enough source-location privacy, with low energy consumption and message latency, the network condition may not be stable. This approach is ideal to be used in a network where nodes are added and removed constantly or the channel has a great interference.

Non-repeating opportunistic routing can increase the security level, by avoiding using the same nodes for the sequential packet transmissions. In that case, the adversary is unable to overhear a packet transmission in each time slot. The adversary has to stay at the same node for longer period. However, that approach has the same disadvantage with the opportunistic routing. In a stable network, after a number of transmissions the adversary will finally manage to reveal the source location.

To cope with that problem, we introduced opportunistic routing with random delay and opportunistic routing with random relay. Opportunistic routing with random delay includes some extra processing in the nodes because of the use of the extra timer needed. In a stable network, that approach performs much better than the other two approaches and can deliver enough safety period to the source. The routing path changes dynamically and in a random way.

Opportunistic routing with random relay can also enhance the security in a stable network. The selection criterion is completely random, following different paths toward the destination in each packet transmission. However, the main disadvantage of that approach is the energy consumption. The nodes have to remain active longer to receive CTS packets from all the possible relay nodes.

VII. SIMULATION EVALUATION

In this section, we will compare the performance of our approaches to that of the phantom routing [3], with respect to the safety period and the average packet latency.

We utilized simulation to study the privacy protection of the proposed schemes. The simulation was performed via the discrete event simulation system OMNET++ with 2000 nodes, with radio transmission range 12 meters, uniformly randomly distributed over a square target area $40,000(m^2)$. The communication parameters were chosen based on IEEE 802.15.4, as listed in Table I while the number of transmission power levels was set to 15.

Initially, the adversary is located next to the destination node. Once it detects a packet, it physically moves to the node which transmits the packet and continues overhearing packets from that node. In the same time slot, the adversary may detect more than one packets, because in the opportunistic routing each packet can choose different paths to the destination node, with different number of hops. When the adversary detects multiple packets, it moves randomly to one of the transmitters. Algorithm 1 illustrates the adversary model.

We simulate the single-path phantom routing, which performs better compared to flooding-based phantom, with $h_{walk} = 10$ random walks. During the four opportunistic routing approaches, we chose randomly 10 different pairs of source-destination nodes and took the average safety period

Algorithm 1: Adversary Strategy.

```
1 adversaryLocation=destination;
2 while (adversaryLocation != sourceLocation) do
3     overhear(node[adversaryLocation]);
4     packet= node[adversaryLocation].ReceivedMessage();
5     if (packet == isNewPacket()) then
6         adversaryLocation= packet.GetSenderNode();
7         MoveTo(packet.GetSenderNode());
8     end
9 end
```

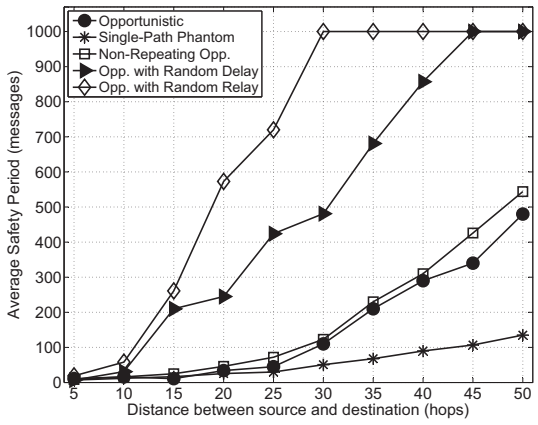

Fig. 4: Average safety period for different source-destination separation.

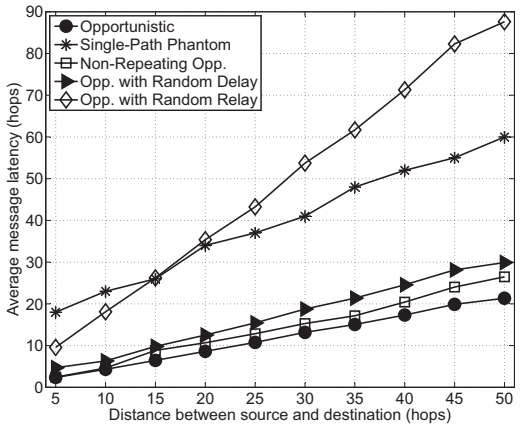

Fig. 5: Average packet latency for different source-destination separation.

and average packet latency. However, for every pair, the metrics are better comparing to the phantom. Moreover we simulated different distances, in hops, between the different pairs. For all the opportunistic routing approaches, we only consider links with $PER < 80\%$. If there is no CTS or there are no more neighbor nodes, a hop count is added to the packet which is transmitted back to the previous node.

Safety period is the number of packets that the source can transmit before the hunter reveals its location or the target disappears from the monitoring area. We assume that the target disappears when the destination node successfully receives 1000 packets. Figure 4 shows the significant safety period gain achieved by the opportunistic routing approaches, compared to single-path phantom. In every opportunistic routing approach, the safety period is always greater than that in phantom.

Non-repeating opportunistic routing performs similarly to simple opportunistic routing when the distance between the source and the destination is small. Only when the distance is greater, and there are more nodes between the source and the destination that the non-repeating scheme leads to better performance. For the opportunistic routing with random delay, the performance is much better. Moreover, for greater distance between the source and the destination, the target is provided with enough safety period to disappear from the area. This is because there are more nodes, and as a result more choices for the opportunistic routing with random delay. Opportunistic routing with random relay performs better than all the others because it can use any relay node in every time slot, increasing the different paths toward the destination and making difficult for the adversary to overhear any packet.

The main drawback of the preceding approach is the delivery latency. As can be seen in Figure 5, because a node waits for all the neighbor nodes to respond to a RTS, this leads to the worst delivery latency compared to all the other approaches and the phantom. The other three opportunistic routing approaches perform much better than the phantom with respect to the delivery latency.

VIII. CONCLUSIONS

Source-location privacy is critical to the successful deployment of many wireless sensor networks, especially in monitoring applications. In this paper, we have investigated four different approaches of an opportunistic routing scheme. Opportunistic routing with random delay proved to enhance source-location privacy without adding latency overhead and be energy efficient compared to the other approaches. Furthermore, we have shown that enhanced privacy is an inherent property of the opportunistic concept.

REFERENCES

[1] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," in *DSN '04*, 2004.
[2] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," in *INFOCOM 2008*, 2008.
[3] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-location Privacy in Sensor Network Routing," in *ICDCS 2005*.
[4] 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*, 2004.
[5] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," in *Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International*, Rhodes Island, Apr. 2006.
[6] J. Yao and G. Wen, "Preserving Source-location Privacy in Energy-constrained Wireless Sensor Networks," in *Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference on*, Beijing, Jun. 2008, pp. 412–416.
[7] L. Kazatzopoulos, C. Delakouridis, G. F. Marias, and P. Georgiadis, "ihide: Hiding sources of information in wsns," in *SECPERU '06*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 41–48.
[8] J. Ren, Y. Li, and T. Li, "Routing-based source-location privacy in wireless sensor networks," in *ICC '09.*, 2009.
[9] Y. Li, L. Lightfoot, and J. Ren, "Routing-based source-location privacy protection in wireless sensor networks," in *Electro/Information Technology, 2009. eit '09*, june 2009, pp. 29 –34.
[10] Y. Li and J. Ren, "Preserving Source-location Privacy in Wireless Sensor Networks," in *SECON '09. 6th Annual IEEE*, Jun. 2009, pp. 1–9.
[11] Y. Li and J. Re, "Mixing ring-based source-location privacy in wireless sensor networks," in *ICCCN '09*, 2009.
[12] L. Song and D. Hatzinakos, "Real-time communications in large-scale wireless networks," *International Journal of Digital Multimedia Broadcasting*, vol. 2008, no. 586067, 2008.
[13] J. Proakis, *Digital Communication*. McGraw-Hill Inc., 1995.
[14] OMNeT++ discrete event simulator, "http://www.omnetpp.org."