Opportunistic Routing for Enhanced Source-Location Privacy in Wireless Sensor Networks

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

***Abstract*—Wireless sensor networks are designed for a plethora of applications, such as unattended event monitoring and tracking. Source-privacy is one of the looming challenges that threaten successful deployment of these sensor networks, especially when they are used to monitor sensitive objects. In order to enhance source-location privacy in wireless sensor networks, we propose the use opportunistic routing schemes. In opportunistic routing, each sensor transmits the packet over a dynamic path to the destination. Every packet from the source can follow a different path toward the destination, making it difficult for an adversary to backtrack hop-by-hop to the origin of the sensor data. In the context of providing source location privacy for wireless sensor networks, the obtained simulation results demonstrate the efficiency and suitability of opportunistic routing in practical applications.**

I. INTRODUCTION

Wireless sensor networks have been envisioned to have 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 its inherent broadcasting nature, wireless communications typically pose significant challenges on data security and protection, including susceptibility to unauthorized wireless data interception. Although many privacy-related issues can be addressed by security mechanisms, the protection of the source location confidentiality using conventional network security methods appears untenable. Existing privacy techniques for general network scenarios [1], [2], are not suitable to efficient source location protection in sensor networks, where contextual privacy issues associated with sensor communications have not been as thoroughly addressed.

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 instance, cardiologic data packet coming out of a hospital in a mesh network enable an eavesdropper to analyze and find out at-risk heart patients, if the source location of those packets can be determined. Toward that goal, a number of source-location communication protocols have been proposed [3], [4], where the main idea is a mixture of valid and fake messages. Each node transmits either a valid or a fake message, consistently. The main disadvantage of this approach is that the broadcasting of fake messages consumes significant amount of the limited energy in each sensor node. Moreover, because each node has to transmit a packet in every time slot, the effect is increase in number of collisions, and decrease in 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. In [5] the authors introduced the Panda-Hunter model to formalize the problem in sensor networks and proposed a phantom routing technique based on both flooding and single path routing. Phantom routing involves two phases: a random walk phase, and a subsequent flooding/single path routing. Random walk is inefficient in making a fake "phantom" source far enough from the actual source. To address this problem, a direct random walk is proposed in [6]. This can be achieved by storing direction information in the header of the message. The exposure of the direction information decreases the complexity for adversaries to trace back to the true message source.

In this paper, we propose to examine source-location privacy through opportunistic routing [7]. Opportunistic routing takes advantage of wireless medium characteristics. Instead of choosing a single route ahead of time, the proposed approach determines 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 radio availability.

The rest of this paper is organized as follows. In Section II, the sensor network and the threat models are presented. Routing principles are described in Section III. Subsequently in Section IV, simulation results are presented, followed by conclusions in Section V.

II. SENSOR NETWORK AND MODELS

The considered sensor network is similar to the Panda-Hunter game introduced in [5]. 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. Every sensor can be the source, and can send packets to neighboring sensors that are in the limited radio range. The source will continuously send packets until the adversary discovers the source, or the target disappears from the monitoring area.

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.

978-1-4244-5711-3/10/$26.00 ©2010 IEEE

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.
- 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.

Next we will describe two different routing principles and the corresponding privacy protection.

III. ROUTING PROTOCOL PRINCIPLES AND PRIVACY PROTECTION

In this section, we describe the basic principles of the "phantom" routing scheme [5] and the proposed opportunistic scheme and then we compare them in terms of source-location privacy.

A. Phantom routing principles

"Phantom" routing protocol involves two phases: a random walk for a number of hops and a subsequent flooding/single path routing toward the destination.

In the random walk phase, when the source has a packet to transmit, it forwards the packet to a random direction for h_{walk} hops. The node that receives the packet after that phase, becomes the new "phantom" source. This node will transmit the message to the destination through a flooding/single path routing.

The asymptotic probability of the phantom source's location with distance d_{ph} from the real source, after h_{walk} random walk steps, is given by:

$$p = 1 - e^{-d_{ph}^2/h_{walk}}. \quad (1)$$

According to formula (1), the probability for the "phantom" source's location with distance $d_{ph} < h_{walk}$, after h_{walk}, is given by

$$p = e^{-d_{ph}^2/h_{walk}} - e^{-(d_{ph}+1)^2/h_{walk}}. \quad (2)$$

The probability for the distance between the "phantom" and the real source, after $h_{walk} = 10$, is shown in Figure 1. It is highly possible that the distance between the "phantom" source and the real source is within $h_{walk}/2$. Although the packet was transmitted a number of times, equal to the number of h_{walk}, the distance between the "phantom" source and the real source, in hops, is usually smaller than the number of the h_{walk} hops.

During the second phase, one may think that flooding can provide strong privacy protection since almost every node in the network will participate in the data forwarding, leading the adversary far away from the real source. Instead, flooding routing provides only a modicum of privacy protection, since it allows the adversary to track and reach the source location within the minimum safety period. For instance, if the shortest path between the source and the destination is 30 hops, then the hunter will find the source location after 30 messages.

B. Opportunistic Routing Principles

During the last decade, a number of protocols have been developed in order to improve the performance in ad hoc networks. One promising approach is referred to as opportunistic routing [7]–[9], where, a cluster of nodes serve as relay candidates and one node between them will finally transmit the packet. The relay node is opportunistically decided by dynamic network conditions such as interference, channel status and congestions. Based on the principle of opportunistic routing, [7] has also developed opportunistic mesh network and cognitive network concept which further exploits radio spectrum agility beyond the basic opportunistic routing.

Compared to traditional end-to-end multi-hop routing, the core idea in opportunistic routing is that, at each hop, a set of next hop relay candidates receiving the packet successfully compete for acting as relay. Instead of choosing a single route ahead of time, it determines the path as the packet moves through the network, based on which sensor receives each transmission.

Opportunistic wireless mesh networks can provide an attractive solution to the source-location problem. The routing path between the source and the destination dynamically changes based on bandwidth and node availability, which makes it difficult for any adversary to locate the source.

As we increase the number of the nodes in the network, the set of the relay candidates increase, and as a result, the number of the possible paths toward the destination increase. With opportunistic routing we can obtain multiple advantages in source location privacy:

- The adversary does not make progress toward the location of the source with every message. If the adversary moves to a node, in a large-scale network, the possibility that the next packet will be transmitted to that node is minor. Following an opportunistic routing scheme, the packet will be transmitted to another node which is available for immediate transmission while in flooding-based phantom, the adversary makes progress with each message during the flooding phase.
- Opportunistic routing schemes, try to achieve high throughput with lossy wireless links, where there is always the possibility for a packet to be successfully transmitted over a link with high packet error rate (PER), but it is very difficult to follow that link for second or

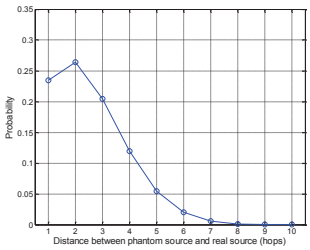

Fig. 1: Probability of the distance between phantom and real source after($h_{walk} = 10$).

third time, especially in sequation. If the adversary has been led to a node with high packet error rate, it will have to stay there for too long or it has to go back to the previous node, while the source keeps sending out packets safely.

- An opportunistic routing scheme is more energy efficient comparing with the phantom routing protocol. In phantom routing, during the random walk phase, the number of the nodes that are used for transmission increases. These nodes should be located away from the source and usually the "phantom" source is further away from the destination than the real source, leading to more hops toward the destination during the single path routing. Moreover,in order to achieve better privacy protection, the number of the random hops should be large. In contrast, in opportunistic schemes the nodes that are used are all located toward the destination. Specifically, the number of the nodes that are used for the transmission of each packet is the minimum, under the current channel condition and node availability.

Therefore, exploiting the spatial diversity in a more efficient way could provide source-location privacy and be energy efficient without increasing the complexity. We compare and prove this by network simulation later in this paper.

C. Simulated Opportunistic Scheme

With regard to the routing policy, we assume that for a given cluster, only the nodes closer to the destination forms the relay candidate set. Such a strategy obviously relies on the assumption that each node has full knowledge of the position of itself and the destination.

In the simulated opportunistic scheme, when a node n_s has to transmit a packet, it finds all its surrounding nodes, in its range, which conform the cluster set E_s.There is a subset $V_s \leq E_s$ conformed by the relay candidates k that are closer to the destination than the sender node:

$$V_s = \{k \in E_s | D(k,d) < D(s,d)\} \tag{3}$$

where $D(x,y)$ is the distance between a node x and a node y, s is the sender node and d the destination node.

The preceding computation on sender node depends on the loss probabilities of each link. Specifically, in every time slot $i \in \{i_0, ..., i_0 + T(i_0)\}$, the transmission strategy is decided by $P_t(i)$ which is 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 $PER(i)$ can be written as [10],

$$PER(i) = 1 - \left(1 - Q\left(\sqrt{\frac{2P_t(i) \cdot G(i)}{\sigma_n^2}}\right)\right)^{F_d}, \tag{4}$$

where 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

$$G(i) = A \cdot D(i,d)^{-n}.$$

If the node fails to transmit a packet, then it repeat the same procedure. Every time a node tries to transmit a packet, the set of the relay candidates changes, based on the opportunistic principles.

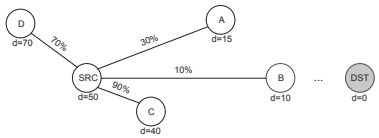

Fig. 2: Example three-node network, with link delivery probabilities shown along the edges of the graph and the distance(d) from the destination node.

D. Network Example

Figure 2 shows an example of the sensor network. The source node has a link with each neighbor node in its range. Each link has been assigned a delivery probability, while for each node there is also the distance (d) between this node and the destination node.

Initially, $E_{src} = \{A, B, C, D\}$ and $V_{src} = \{A, B, C\}$. The sender node will try to transmit to the node closer to the destination, node B. Between each relay candidate in V_{src} and the sender node there is a PER, from formula (4). If the transmission is not successful, due to the PER, the sender will try to transmit to the next available node, closer to the destination, in the example this should be node A. If there is another unsuccessful transmission, it will try to transmit to node C. Node C will probably receive the data, because of the low PER. If the transmission fails in all the nodes in V_{src}, the sender node will count a hop, and repeat the same procedure. The node which will finally receives the packet, it will become the new sender node and repeat the same procedure. This procedure is a way to simulate the opportunistic handshake between the different nodes.

IV. PERFORMANCE EVALUATION AND ANALYSIS

We utilized simulation to study the privacy protection of the proposed scheme. The simulation was performed via the discrete event simulation system OMNET++. The topology was generated through 2000 sensors uniformly randomly distributed over a $200 \times 200(m^2)$ network field. The communication parameters were chosen based on IEEE 802.15.4, as listed in Table I. 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 moves to the node which transmits that packet. In the same time slot, the adversary

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

TABLE I: Communication Parameters Setup

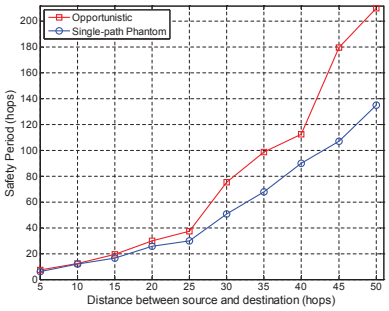

Fig. 3: Safety period for phantom routing ($h_{walk} = 10$) and opportunistic routing for different source-destination separation.

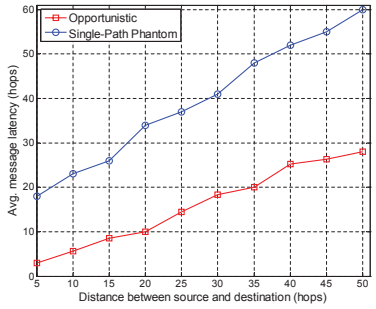

Fig. 4: Average message latency for phantom routing ($h_{walk} = 10$) and opportunistic routing for different source-destination separation.

may detect more than one packet, 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 packet, it moves randomly to one of the transmitters. We simulate the single-path phantom routing, which performs better compare to flooding-based phantom, with $h_{walk} = 10$ random walks. During the opportunistic routing, we choose randomly 10 different pairs of source-destination nodes and we took the average safety period and latency. However, for every pair, the metrics are better comparing to the phantom. Moreover we simulated for different distance, in hops, between the different pairs. For the opportunistic routing, we only consider links with $PER < 80\%$.

Safety period is the number of messages that the source can transmit before the hunter reveals its location or the target disappears from the monitoring area. We show the significant safety period gain achieved by the opportunistic routing, compared to single-path phantom, in Figure 3. In opportunistic routing, the safety period is always greater than that in phantom. In phantom, after the random phase, the "phantom" source follows a single path routing toward the destination. After the arrival of the first packet, and since the "phantom" and the real source are close to each other, the probability the adversary overhears a packet in every time slot and making progress toward the area of the two sources, increase. In opportunistic routing, every node can transmit to one of its neighbors in its relay candidate set, based on the PER, decreasing the probability for the adversary to overhear a packet in every time slot. Furthermore, safety period is greater when we increase the distance between the source and the destination. This is the result of the increased number of dynamic paths that each node has when there are more nodes in the path between source and destination.

Delivery latency is the average number of hops needed for all the messages to arrive at the destination node. If we assume that every sensor consumes energy while transmitting, and the energy consumed in any other state of the sensor is negligible, the average message latency in hops needed to reach the destination can be used as a metric for the energy consumption of each scheme.

Figure 4 shows the results. The delivery latency for the single-path phantom increases with the distance between the source and the destination. In opportunistic routing, delivery latency is smaller than that in phantom. Each node makes use of all the possible nodes in its range, which can decrease the number of hops needed to reach the destination.

V. 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 an opportunistic routing scheme which can deliver better source-location privacy compared to phantom routing without adding latency overhead. Furthermore, it has been argued that enhanced privacy is an inherent property of the opportunistic routing concept.

References

[1] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar, "Spins: Security protocols for sensor networks," in *Wireless Networks*, 2001, pp. 189–199.

[2] Laurent Eschenauer and Virgil D. Gligor, "A key-management scheme for distributed sensor networks," in *In Proceedings of the 9th ACM Conference on Computer and Communications Security*. 2002, pp. 41–47, ACM Press.

[3] Jing Deng, Richard Han, and Shivakant 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, 2004, p. 637, IEEE Computer Society.

[4] Min Shao, Yi Yang, Sencun Zhu, and Guohong Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, Phoenix, AZ, Apr. 2008, pp. 51–55.

[5] P. Kamat, Yanyong Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-location Privacy in Sensor Network Routing," in *Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on*, Columbus, OH, June 2005, pp. 599–608.

[6] Jianbo Yao and Guangjun Wen, "Preserving Source-location Privacy in Energy-constrained Wireless Sensor Networks," in *Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference on*, Beijing, June 2008, pp. 412–416.

[7] Liang Song and Dimitrios Hatzinakos, "Real-time communications in large-scale wireless networks," *International Journal of Digital Multimedia Broadcasting*, vol. 2008, no. 586067, 2008.

[8] Michele Zorzi and Ramesh R. Rao, "Geographic random forwarding (geraf) for ad hoc and sensor networks: Multihop performance," *IEEE Transactions on Mobile Computing*, vol. 2, no. 4, pp. 337–348, 2003.

[9] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple Cooperative diversity method based on network path selection," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 659–672, Mar. 2006.

[10] J.G. Proakis, *Digital Communication*, McGraw-Hill Inc., 1995.