On Providing Sink Anonymity for Sensor Networks

Edith C.-H. Ngai
Department of Information Technology
Uppsala University, Sweden
edith.ngai@it.uu.se

ABSTRACT

The sinks usually in sensor networks usually broadcast their addresses for data collection. However, this common operation opens up vulnerability for adversary to attack the sinks and obstruct their normal functions. In this paper, we suggest sink anonymity as a novel approach for data collection, which protects the privacy of the sinks and avoids them to become the target of attacks. We provide sink anonymity by omitting the address of the sinks in routing, so that the identity and location of the sinks are kept private. Our proposed scheme, Randomized Routing with Hidden Address (RRHA), prevents the attackers from obtaining the receiver address by capturing the destination field of the packets or by predicting the location of the sinks by observing the flow of network traffic. We examined the successful delivery rate, packet delay, and protection strength of our proposed scheme by both analysis and simulations.

Categories and Subject Descriptors

C.2 [**Computer-Communication Networks**]: Network Architecture and Design; D.4.6 [**Security and Protection**]: Information Flow Controls

General Terms

Algorithm Design Security Performance

Keywords

Sensor Networks, Privacy, Data Collection, Wireless Communications

1. INTRODUCTION

Wireless sensor network (WSN) is composed of numerous small sensing devices with limited communication range. Sensors collect data from the environment and report them to the sinks through hop-by-hop communications [14, 19]. Most of the existing routing protocols in sensor networks are based on geographic routing [1, 10, 13, 4], in which the sensors know their neighbors and the location of the sinks. In geographic routing, a sensor usually forwards the packet to the next hop that is closest to the sink, though sometimes it may also consider some additional factors, like delay [10, 7, 15] and energy consumption [4, 8], etc. In order to route a packet to the sink, a sensor must know the destination of the packet and the location of the sink. The sink usually broadcasts its location to all the sensors in the network. However, this mechanism allows the adversary to locate and attack the sink easily. To address this problem, we propose sink anonymity in data collection and routing for sensor networks. Sink anonymous hides the identity and location of the sink and protect its privacy.

Location privacy in sensor networks has attracted much attentions recently. The destination nodes or the sinks, whose locations are discovered by the adversary, may become the targets of the attacks. For example, a soldier, who carries an receiver, will be in great danger if being captured. It is therefore very important to protect sink location privacy in sensor networks. Traffic-analysis attacks, which are performed by adversary who discovers the receiver location by observing the flow of network traffic, have been widely studied. The problem was addressed by dummy packets injection, but this approach increases the network traffic heavily [11, 12, 18]. In addition, it does not consider active attackers who can compromise a node and read the header field of a packet to identify the receiver.

In this paper, we provide sink anonymity in sensor networks to protect the identity and location privacy of the sink. We propose a novel Randomized Routing with Hidden Address (RRHA) scheme which keeps the identity and location of the sink secret in the network. Sensors do not know who and where the sink is when routing the packets. Our scheme does not include the destination field in the header of the packets. The packets are routed from the source to the sink along a random path without a specific destination. When the packet travels along the path and arrives the sink, the sink will decrypt and read the message silently. The packet continues travelling until a predefined hop count is reached. Our system can prevent attackers from capturing or predicting the receiver location by reading the destination field of the packet or observing the network traffic.Keeping the identity and location of the sink private can prevent the sink to become the target of attacks. We also examine the successful delivery probability and the overheads of our scheme, which are affected by the number of sinks, the number of random paths and the path length for delivering the packets.

The remainder of the paper is organized as follow. In Section 2, we describe some related work in the area. In Section 3, we discuss the network model and threat model. In Section 4, we present our Randomized Routing with Hidden Address (RRHA) scheme for providing sink anonymity in WSNs. Sections 5 and 6 summarize the analytical and simulation results, and we conclude the paper in Section 7.

2. RELATED WORK

Privacy issues in sensor networks, especially location privacy [11, 12, 9, 2], have been studied in recent years. The random walk based phantom flooding scheme [12] is proposed to defend against an external adversary who attempts to trace back to the data source in sensor networks and provide source location privacy of the sink.

Other schemes, like ConstRate and ProbRate, which introduce dummy traffic to hide the real event sources, are proposed to provide source event unobservability in the network [18, 17]. Even though some dummy packets can be dropped on their way, the injected dummy traffic still increases the packet delay and consumes more energy in sensor nodes. Also, these schemes focus on source privacy, which are different from our goal of providing sink anonymity and protecting the location and identity of the sinks.

Multpath routing and fake message injection are introduced in [3] to provide receiver privacy. However, it concentrates on the traffic-analysis attack, which determines the location of the sink through the measurement of traffic rates at various locations. Another recent work is proposed to protect receiver-location privacy in WSNs by providing path diversity in combination with fake packet injection [11]. It is solving a similar problem as we do, but it considers only passive attackers who capture the receiver by eavesdropping and performing network traffic analysis. In this work, we also protect the network from active attackers who can compromise an intermediate node and capture the packet. We provide sink anonymity by keeping the location of the sink secret to the nodes in the network.

3. NETWORK AND THREAT MODELS

3.1 Network Model

A wireless sensor network consists of a number of sensors deployed in an area, together with one or multiple sink(s). Each sensor has a transmission range r for wireless communication which allows it to exchange messages directly with its neighboring nodes. Packets rely on multi-hop transmissions to reach the destinations that are located farther away from the source.

Since sensors have limited storage, communication range and computation power, they cannot afford the relatively heavy-load asymmetric cryptography. Instead, they use symmetric cryptographic primitives to provide data confidentially, authentication, integrity, and freshness of the message [16, 5]. We assume that each sensor i shares an unique symmetric key K_i with the sink. Note that multiple sinks can share the same symmetric key K_i with i.

We provide sink anonymity in sensor network, where sensors do not know the ID and location of the sinks. The packets are forwarded randomly in the network. When a packet arrives a sink, the sink will check if the packet is of its interest. If so, it will decrypt the packet with the corresponding symmetric key and read the message.

3.2 Threat Model

We consider attackers who aim at identifying and attacking the sinks. They may discover the location of a sink by capturing an intermediate node along the path and reading the destination field of the packets. The widely adopted geographic routing protocols in sensor networks [1, 10, 13, 4] are vulnerable to this special kind of attack as the location of the receiver must be included in the destination field of a packet for routing.

Apart from that, some attackers may monitor the network traffic passively and predict the location of the receiver. Since the receiver is likely to be the sink in many sensor network applications, the attackers may notice a large amount of traffic flows toward the sink. These passive attackers are usually equipped with some supporting devices, such as antenna, which allow them to eavesdrop the delivery of packets and perform some simple traffic analysis. They can also predict the direction of the receiver based on the signals that they overheard.

3.3 Notations

We use the following notations to describe the cryptographic operations in this paper which are mainly adopted from [16].

- $Y1|Y2$ denotes the concatenation of messages $Y1$ and $Y2$.
- K_i denotes the secret (symmetric) key that is shared between node i and the sink(s).
- $E = \{Y\}_{K_i}$ is the encryption of message Y with the symmetric key shared by node i and sink(s).

4. PROVIDING SINK ANONYMITY

4.1 Randomized Routing with Hidden Address (RRHA)

When a sensor i reports its measurement to the sink, it encrypts the message with its symmetric key K_i and forwards the packet along a random path. Unlike many existing routing algorithms [1, 10, 13, 4], the location or ID of the sink is not included in the packet. The advantage of this approach is to avoid the attackers from obtaining the destination of the packet even they can capture the intermediate nodes and read the packet.

Since i does not know the location of the sink, it forwards the packet randomly to any of its neighbors. When the next hop j receives the packet, it again forwards the packet to one of its neighbors k randomly and increases the hop count field H in the packet by one. The hop count field H in the header of the packet is initialized as zero by the source node. It indicates the number of hops that the packet has travelled. The above forwarding process repeats hop-by-hop until $H = L$, where L is the pre-defined length of the random path. Note that the packet will continue travelling in the network even it has already reached any of the sinks. Similarly, it is possible that the packet has never visited any sink at the end of its travel.

More specifically, node i sends the packet in this format $< i|Y_{type}|H|Y_{K_i} >$, where Y_{type} is the type of message in the packet, Y_{K_i} is the message encrypted by symmetric key

K_i of node i, and H is the number of hops travelled by the packet. The message type Y_{type} allows the sink to recognize the content of the packet. The sink will only decrypt the packet that contains the message of its interest.

A packet may store the ID of the nodes that it has visited, such that the following intermediate nodes can avoid re-visiting them. This mechanism increases the chance for the packet to reach the sink as one can visit more different nodes. It can be achieved by concatenating the ID of the intermediate nodes to the packet, i.e. $< i|Y_{type}|\ H|Y_{K_i}|ID_1|ID_2|\ ...|\ ID_H >$, where $ID_1, ..., ID_H$ are the IDs of the nodes being visited.

Moreover, instead of sending the packet along a single path, the packet can be delivered by multiple paths to increase its chance to reach the sink. For instance, the source node may send the packet to M neighbors, then these neighbors will forward the packet along different random paths independently.

4.2 An Example

Figure 1 shows an example of multiple random paths for delivering a packet with $M = 3$. The source node s forwards the packet with three different random paths. The packet is delivered successfully as long as any of the paths passes through the sink.

Since the packet does not include any destination field, so an active adversary $A1$ cannot achieve the location of the receiver even it can capture an intermediate node and read the packet. In our scheme, all sensors including s do not know the location of the sink. The packet keeps travelling until $L = 8$, no matter it has visited the sink or not. Consider another passive adversary $A2$, which is equipped with an antenna to overhear the network traffic, cannot predict the sink location by traffic monitoring as the packet travels along a random path with no specific destination. The flow of the packet is totally independent of the location of the sink.

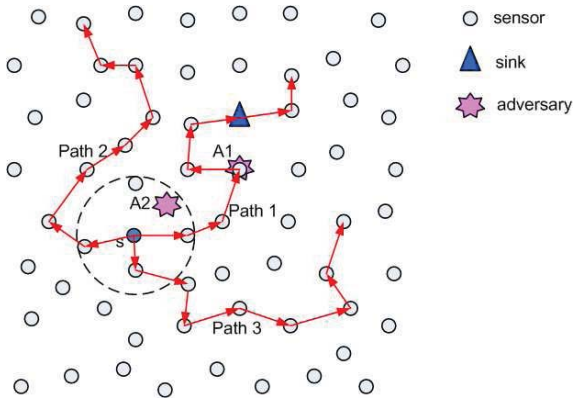

Figure 1: Randomized routing with multiple paths. Source node s forwards the packet with three different random paths. It increases the probability that a packet can reach the sink. The packet is delivered successfully to the sink on Path 2 in this example.

5. ANALYTICAL RESULTS

5.1 Successful Packet Delivery Probability

A packet is delivered successfully if it visits any of the sinks along its random path. We denote $P(S)$ as the probability that the packet is delivered to the sink successfully which can be calculated by

$$P(S) = 1 - (1 - p_{BS})^L, \tag{1}$$

where $p_{BS} = N_{BS}/N_s$ is the probability that a node being visited is a sink, N_{BS} is the total number of sinks and N_s is the total number of sensors in the network.

In multiple path routing, a packet is forwarded along multiple random paths to increase its probability to reach the sink. The probability of successful delivery $P_m(S)$ then becomes

$$\begin{aligned} P_m(S) &= 1 - (1 - P(S))^M \\ &= 1 - (1 - p_{BS})^{L_m M}, \end{aligned} \tag{2}$$

where M is the number of random paths for delivering the packet and L_m is the length of the random paths.

Figure 2 shows the successful delivery probability of the packets varying the path length L. The successful delivery probability increases with L as a packet will visit more nodes on a longer path, so that it has a higher probability to reach the sink. The results also indicate that the successful delivery probability increases when the number of random paths M and the probability p_{BS} increase.

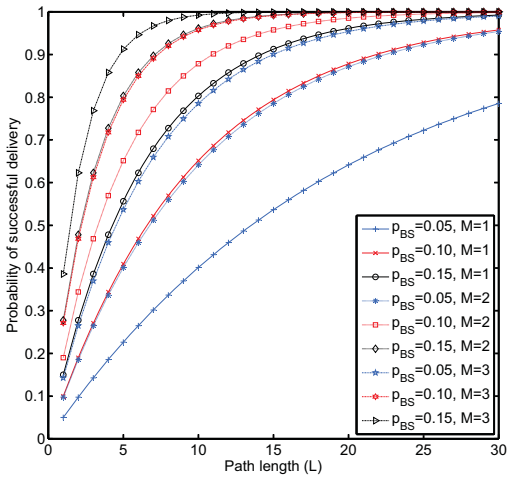

Figure 2: Successful delivery probability varying the path length. The packets have higher probability to be delivered to the sink on longer paths as they can visit more nodes. The successful delivery probability also increases when p_{BS} and M increase.

6. SIMULATION RESULTS

We evaluate the performance of our randomized routing scheme for providing sink anonymity with *ns-2* [6] simulations. The network considered has a total of 100 sensors which are deployed in a 100m x 100m square with uniform random distribution with a communication range 20m. The simulation settings are mainly drawn from [10, 7, 15] We focus on a WSN which collects and reports sensing data to the sink constantly. Any of the sensors has a probability p to be

the source of routine data and generates data independently of the other nodes at a rate of 1pkt/s.

6.1 Successful Packet Delivery Rate

We fixed the number of sinks to four and placed them at locations (25, 25), (25, 75), (75, 25), and (75, 75) in this experiment. We measure the successful delivery rate of packets from the sources to the sinks varying the path length with $p = 0.1$ and $p = 0.5$. Both Figures 3(a) and 3(b) show that the successful delivery rate increases when the length of path increases. It is because a packet will visit more nodes on a longer path, so it has higher probability to reach the sink. The successful delivery rate also increases with the number of random paths M. Since a packet will be sent along multiple random paths if $M > 1$, the chance that one or more packets on these M random paths can reach the sink becomes higher. From the two figures, there is not much difference on the successful packet delivery rate in networks with low and high traffic rates.

6.2 Packet Delay

We examine the average packet delay from the sources to the sinks with $N_{BS} = 4$. The packet delay measures the time that a packet takes from the source to the sink at the first time. If multiple paths are adopted in randomized routing, i.e. $M > 1$, the delay measures the time that the earliest packet taken to reach the sink.

Figures 4(a) and Figure 4(b) show the packet delay varying the length of random path with $p = 0.1$ and $p = 0.5$ respectively. The packet delay is quite low when $p = 0.1$ as there are only ten sources in the network. The packet delay increases with the path length. It is because the total traffic in the network increases when each packet travels more hops. When the number of random paths M increases, a packet will be forwarded by multiple paths, so it can visit more nodes. Since the packet delay measures the time that a packet arrive the sink the earliest among the multiple paths, the packet delay may become lower. However, the packet delay increases dramatically when $M = 3$ and $L = 30$ due to network congestion.

Figure 4(b) shows that the packet delay with $p = 0.5$ is much higher than that with $p = 0.1$ in Figure 4(a). There are 50 sources in the network when $p = 0.5$, so the network congestion causes the increased packet delay. In this situation, multi-path forwarding may degrade the performance.

6.3 Protection Strength

We evaluate the protection strength of RRHA by showing the probability that the sink privacy will be revealed by various kinds of attacks in Table 1. Both LPR [11] and SPR [13] are not resilient to the strong attacker who can capture and read the destination field of a packet. The reason is that they put the receiver address in the packet header to forward the messages. On the contrary, RRHA protects the sink privacy effectively as the address of the sink is not included in the packet. Even an attacker captures an intermediate node, the node only has a 0.033 probability to be the sink in RRHA with $M = 3$ and $L = 10$.

Passive attackers can observe the network traffic and reach the sink by tracing the packets. Again, SPR does not provide any protection to the sink privacy. An passive attacker can trace the packet from the source hop-by-hop to the sink easily in SPR. On the other hand, both LPR and RRHA protect the sink privacy very well against passive attackers. Even multiple passive attackers can trace the packets along all the paths for the real data and dummy packets in LPR, they still cannot tell which path is leading to the sink. Similarly, the passive attackers will not know which intermediate node along the paths in RRHA is the sink.

Table 1: Probability of revealing the sink privacy

Types of attacks	LPR	RRHA	SPR
Active attacker	1	0.033	1
Single passive attacker	0.062	0.033	1
Multiple passive attackers	0.25	0.033	1

7. CONCLUSIONS

In this paper, we have proposed RRHA, a randomized routing scheme with hidden address, which provides sink anonymity for WSNs. The identity and location of the sinks are kept private in the network. Our scheme avoids the identity and the location of the sink to be revealed and to become the target of attacks. The sensors do not specify the destination of the packets when reporting their measurements, so that the attackers cannot obtain the location of the sink even they can read the header fields of the packets. The packets are forwarded along different random paths which are decided by the intermediate nodes randomly and independently, such that the attackers have no hint of the sink from observing the flow of network traffic. We have evaluated our proposed scheme by both analysis and simulations in terms of the successful delivery rate, packet delay and protection strength. The results show that RRHA provides strong protection for the sink privacy against both active and passive attackers. In the future, we will enhance the performance of our proposed scheme and extend our work for the networks with mobile sinks.

8. ACKNOWLEDGMENTS

This work was carried out within the Uppsala VINN Excellence Center for Wireless Sensor Networks WISENET, partly supported by VINNOVA.

9. REFERENCES

[1] J. N. Al-Karaki and A. E. Kamal. Routing techniques in wireless sensor networks: a survey. *Elsevier Ad Hoc Networks Journal*, pages 325–349, 2005.

[2] J. Al-Muhtadi, R. Campbell, A. Kapadia, M. D. Mickunas, and S. Yi. Routing through the mist: privacy preserving communication in ubiquitous computing environment. In *Proc. of IEEE ICDCS*, 2002.

[3] J. Deng, R. Han, and S. Mishra. Countermeasures against trafic analysis attacks in wireless sensor networks. In *Proc. of IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, 2005.

[4] S. C. Ergen and P. Varaiya. Energy efficient routing with delay guarantee for sensor networks. *ACM Wireless Networks*, 13(5):679–690, Oct 2007.

[5] L. Eschenaur and V. Gligor. A key-management scheme for distributed sensor networks. In *Proc. of the 9th ACM Conference on Computer and Communication Security*, 2002.

[6] K. Fall and K. Varadhan. *The ns manual*, Dec 2003. http://www.isi.edu/nsnam/ns.

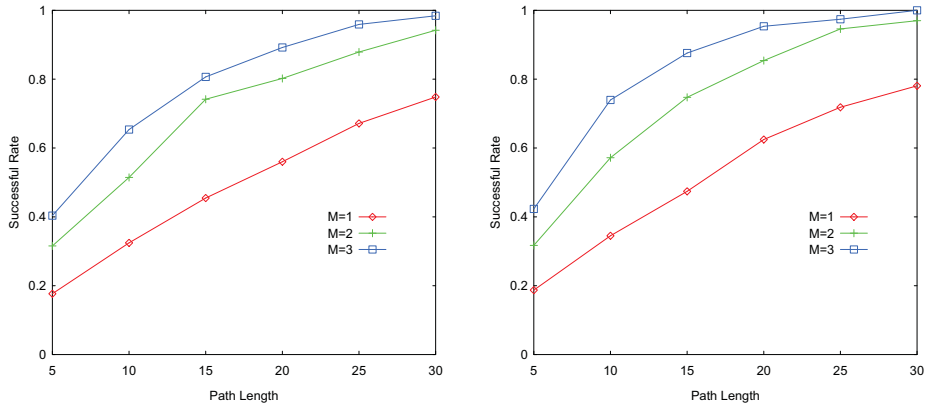

Figure 3: Successful packet delivery rate with four sinks and (a) $p = 0.1$ (b) $p = 0.5$.

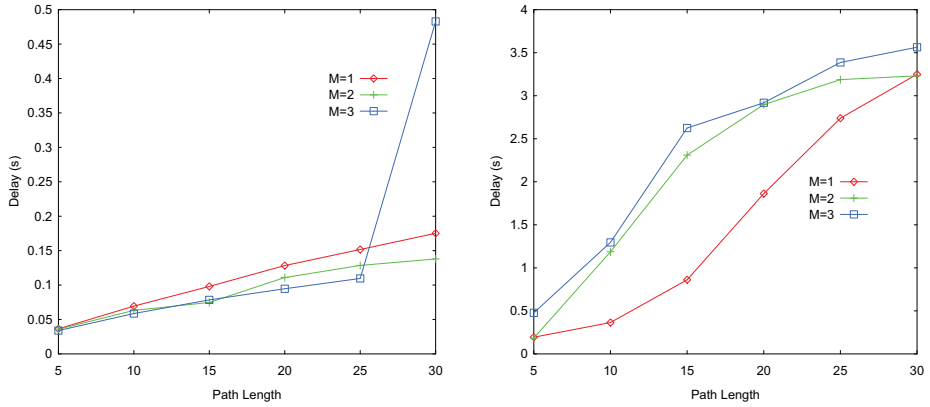

Figure 4: Packet delay with four sinks and (a) $p = 0.1$ (b) $p = 0.5$.

[7] E. Felemban, C.-G. Lee, and E. Ekici. MMSPEED: multipath multi-speed protocol for QoS guarantee of reliability and timeliness in wireless sensor networks. *IEEE Trans. on Mobile Computing*, 5(6):738–754, Jun 2006.

[8] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. *Mobile computing and communication review*, 1(2), 2001.

[9] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald. Privacy-aware location sensor netwroks. In *Proc. of USENIX Workshop on Hot Topics in Operation Systems (HotOS IX)*, 2003.

[10] T. He, J. Stankovic, C. Lu, and T. Abdelzaher. SPEED: a real-time routing protocol for sensor networks. In *Proc. of IEEE ICDCS*, pages 46–55, Providence, RI, U.S., May 2003.

[11] Y. Jian, S. Chen, Z. Zhang, and L. Zhang. Protecting receiver-location privacy in wireless sensor networks. In *Proc. of IEEE Infocom*, pages 1955–1963, 2007.

[12] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk. Enhancing source-location privacy in sensor network routing. In *Proc. of IEEE ICDCS*, Columbus, Ohio, USA, Jun 2005.

[13] B. Karp and H. Kung. GPSR: Greedy perimeter stateless routing for wireless networks. In *Proc. of ACM Mobicom*, Boston, Massachusetts, U.S., 2000.

[14] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson. Wireless sensor networks for habitat monitoring. In *WSNA '02: Proc. of the 1st ACM international workshop on Wireless sensor networks and applications*, pages 88–97, New York, NY, USA, 2002. ACM.

[15] E. C.-H. Ngai, Y. Zhou, M. R. Lyu, and J. Liu. Reliable reporting of delay-sensitive events in wireless sensor-actuator networks. In *Proc. of IEEE MASS*, Vancouver, Canada, Oct 2006.

[16] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Cullar. Spins: security protocols for sensor networks. *Wireless Communications*, 8(5):521–534, 2002.

[17] M. Shao, Y. Yang, S. Zhu, and G. Cao. Towards statistically strong source anonymity for sensor networks. In *Proc. of IEEE Infocom*, 2008.

[18] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao. Towards event source unobservability with minimum network traffic in sensor networks. In *Proc. of ACM WiSec*, Alexandria, Virginia, USA, Apr 2008.

[19] W. Zhang, G. Cao, and T. L. Porta. Data dissemination with ring-based index for wireless sensor networks. *IEEE Transactions on Mobile Computing*, 6(7):832–847, 2007.