Concealing of the Sink Location in WSNs by Artificially Homogenizing Traffic Intensity

Bidi Ying[1,2], Jose R. Gallardo[1], Dimitrios Makrakis[1], Hussein T. Mouftah[1]
Broadband Wireless & Internetworking Research Laboratory,
School of Information Technology and Engineering, University of Ottawa, Ottawa, Canada[1]
Zhejiang Gongshang University, Hangzhou, China[2]
{byiung, dimitris, mouftah} @site.uottawa.ca

Abstract—**For sensor networks deployed to collect and transmit events into a sink node, sink anonymity is a critical security property. Traditional encryption and authentication are not effective in terms of preserving the sink's location because attackers can determine its location through traffic analysis. In this paper, we propose an easy to implement Concealing of the Sink Location (CSL) technique, which is based on the use of fake message injection. CSL is able to prevent attackers from acquiring valuable information on the sink's location through the traffic analysis attack. Simulation results demonstrate clearly that CSL protocol can hide effectively the sink's location. Although using fake messages consumes additional energy, the network's lifetime is not impacted, as will be shown.**

Keywords-Sensor network; sink location; privacy.

I. INTRODUCTION

Typical Wireless Sensor Networks (WSNs) are deployed to support the communication needs of sensing devices, most important of which is the transferring of data collected by sensors to specified sinks. With the availability of low cost wireless technologies and micro-sensing devices, sensor networks are expected to be widely deployed in the near future. However, sensor networks are also vulnerable to many threats such as node compromise, routing disruption and false data injection.

Among all these threats, privacy (especially sink anonymity) is very important, since knowledge of the sink's location makes it vulnerable to cyber / physical attacks, which cannot be fully defended by traditional security mechanisms such as encryption and authentication. Currently, a larger number of secure mechanisms [1-4] are developed to protect the anonymity of a source node or receiver node, while a few mechanisms are able to conceal the geographic location of a sink node. However, sink nodes are the most critical elements in WSNs, since their compromise or destruction makes the entire WSN network unable to convey useful sensing information to its user, thus it becomes useless. Therefore, protecting the location privacy of the sink node is extremely crucial for WSNs' normal operations.

In most cases, sensing data are transmitted along relatively fixed paths connecting source nodes to sink nodes. This produces quite easily identifiable traffic patterns that reveal a sink's location and functionality. By following the traffic traces, the sink's location can be identified, since the point flows converge to it. In addition, the sensing nodes having one-hop distance from the sink have to forward a significantly greater volume of packets, since they have to route all the traffic generated by all those nodes that are farther than one-hop away the sink. An adversary having global view of WSN's activity can deduce the location of the sink by analyzing the traffic patterns over adequately long time intervals.

Preservation of sink's anonymity in sensor networks is challenging. Due to scarce energy, computation and communication resources available most sensors, can only afford to only lightweight, energy efficient and privacy-conserving mechanisms. For example, almost exclusive use by sensors of low-cost radio devices and standardized wireless communication technologies makes easy for an adversary to eavesdrop on the communication between sensors and gather intelligent valuable information.

Despite of its importance, sink location privacy has not received enough attention yet. The contributions in the open literature are very limited and briefly described. Nezhad et. al. proposed an anonymous topology discovery protocol where all nodes are allowed to broadcast route discovery messages and coming/outgoing labels assigned to nodes are used for the forwarding of packets [5]. This method hides the location of a sink node. However, when this method is used, some nodes might not be discovered. Some other techniques were proposed to protect the privacy and confidentiality of a sink node (e.g. [6-8]). They apply data packet encryption. For example, in [8], pair-wise key schemes were proposed to protect the privacy and confidentiality of a sink node. However, an adversary still can derive significant information by processing passively monitored traffic volume and identifying traffic paths in the sensor network.

Because traffic analysis is a very effective method for determining the geographic location of a sink and is also relatively inexpensive and easy to perform in the wireless environment, research concerning sink-location privacy in sensor networks attracted considerable attention, producing several new techniques. For example, in [14], dummy sinks are introduced to confuse an adversary from tracking a packet as it moves towards a sink node. Although the dummy sinks approach can protect a sensor network from local adversaries, that are using passive overhearing and analysis of traffic, it also generates larger volumes of traffic. The immediate consequence is faster draining of nodes' energy resource,

which leads to potential deterioration of the network's reliability.

In the present work, in order to simplify the presentation of the designed technology, we consider a sensor network with a single sink. As mentioned earlier, the proposed concealing of the sink' location method generates fake messages. It consists of the topology discovery phase, which selects several nodes to generate fake messages, and the data transmission phase, during which each selected node sends fake messages with constant size. The remainder of the paper is organized as follows. In Section II, the related work is surveyed. In section III, the concealing of the sink' location method is described in detail. Section IV provides performance analysis results. Finally, section V concludes the paper.

II. Related Work

Privacy in WSNs can be classified into content privacy and contextual privacy [3]. Threats against content privacy arise due to the ability of adversaries to observe and manipulate the content of packets sent over a WSN. This type of threats is countered by encryption and authentication. However, even after strong encryption and authentication mechanisms [9], [10] are applied, wireless communication media still exposes contextual information about the traffic carried in the network. For example, an attacker can deduce sensitive information from a WSN by eavesdropping on the network traffic and analyzing traffic patterns.

Deng et al. in [20], identified two classes of traffic analysis attacks in WSNs, namely: a rate monitoring attack and a time correlation attack. In a rate monitoring attack, an attacker monitors the packet transmission rate of nodes close to the attacker and move close to the nodes that have a higher packet sending rate. In a time correlation attack, an attacker observes the correlation in sending time between a node and its neighbor node that is assumed to be forwarding the same packet, and deduces the path by following the sound of each forwarding operation as the packet propagates towards a sink node [11]. Although the defender is able to buffer incoming packets in the nodes for some random period before forwarding them and thereby to defend against a time correlation attack, a senior adversary can pro-actively trigger the packet forwarding by generating abnormal sensory events such as abnormal temperature that needs to forward as soon as possible. A few schemes [1, 3-4, 12] based on source location privacy were proposed, which deal with traffic analysis attack. Their main ideas include using numerous paths to send packets to sinks, forming looping paths to forward packets, associating real sources with faked sources and requiring real sources to send packets periodically. Some schemes [2, 13-14] were proposed based on receiver location privacy. For example, Jian proposed a new location-privacy routing protocol to preserve the receiver's location privacy [2]. This scheme employs fake packet injection to minimize the information that an adversary can deduce from the overhead packets about the direction towards the receiver.

However, all of the above schemes do not take into consider the sink location privacy. Nezhad A.A et. al. proposed anonymous topology discovery protocol where all nodes are allowed to broadcast route discovery messages and coming/outgoing labels assigned to nodes are used to forward packets [5]. This method will hide the location of sink node. However, there is a chance that some nodes may not be discovered. Another method that is using *k*-anonymity model was proposed for the data privacy [15]. Using its model, the record of an individual is hidden in a group of at least *k* records of other individuals.

III. Concealing of the Sink's Location Protocol

A. Network Model and Attacker Model

Our system assumes that a number of sensors, deployed into a certain region. Each sensor has a transmission range, and they can communicate with each other directly or indirectly. We assume that a sink node works as the network controller to collect event data. In this paper, we assume that the attacker is external, passive and global. By external, we mean that the attacker does not control any sensors. By passive, we mean that the attacker cannot conduct active attacks such as traffic injection, channel jamming and denial of service. By global, we mean that the attacker can monitor, eavesdrop and analyze all communication tasks occurring within the network. Besides, a global eavesdropper can keep track of the number of messages that pass through local nodes. Thus, he can easily deduce sink location by detecting nodes' traffic volumes. Note that this global eavesdropper does not have the capability of distinguishing between original and fake messages. Because we assume all messages are encrypted by a pair-wise secret key.

B. CSL Approach

Our scheme includes topology discovery phase and data transmission phase.

1) Topology discovery protocols

Recently, several topology discovery protocols were proposed, such as directed diffusion protocol [11], probabilistic flooding protocol [16], and controlled flooding protocol [17], which cannot support sink location privacy. An attacker could deduce the sink's location by analyzing traffic volumes and patterns.

Nezhad et. al. proposed an anonymous topology discovery protocol [5] where a node generates a Route DIScovery (RDIS) packet with probability *p*. RDIS packets are distributed within the network using controlled flooding which means an intermediate node forwards only one copy of such message and discards the other copies. The sink follows the same rules as the other nodes, which hides its identity and location. However, An RDIS packet may fail to discover all sensors since to only one copy of the RDIS packet is forwarded by each node, in other words, this protocol may lead to some sensors become isolated or separated from the network.

The goal of our proposed network topology discovery protocol is to let the sink learn the relative positions (not necessaries the geographical coordinates) of all sensors in the network in the case of preserving sink location privacy. We assume that all sensors are pre-installed a pair-wise secret keys from a big key pool (For example, we can use key pre-distributed scheme to pre-install keys into sensors [10]).

After sensors are deployed into the area, the sink generates RDIS message which contains a globally unique sequence number, source ID, and a variable-length field called the route field, and then broadcasts the encrypted RDIS message. An intermediate node forwards only one copy of such an encrypted message and discards the other copies. That means, the intermediate node receives and forwards the first copy of the message, and records its own ID into the route field. For very large networks, a hierarchical architecture may be employed.

To preserve the sink location privacy, several nodes are randomly selected to generate Fake RDIS (FRDIS) message to confuse the attacker. FRDIS message includes a globally unique sequence number, source ID, and the same size of RDIS message (Note that, the purpose of the same size between FRDIS and RDIS message is that the attacker cannot distinguish which node is sink node by monitoring the traffic volume around these nodes. Thus, in order to carry out the purpose, we should pre-distribute fixed length of route field in the format of messages.). An intermediate node receives and forwards the first copy of such FRDIS message. Fig. 1 shows the process of topology discovery generated by the protocol. In this figure, and in the rest of this paper, we denote the unique network identity (ID) of a node *i* with s_i. After receiving the RDIS message for the first time, s_2 inserts its ID into the route field and forwards this message RDIS(s_2). Node s_0 and node s_1 broadcast FRDIS messages to confuse the attacker.

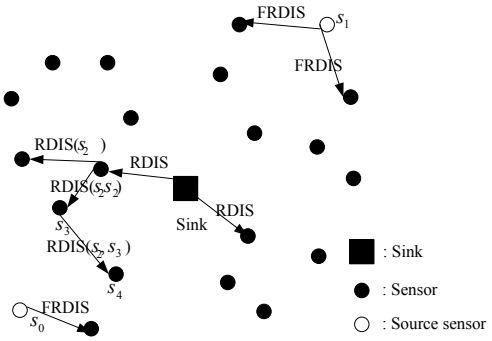

Fig.1 Topology discovery

This method resolves the weakness the scheme proposed in [5] has, i.e, having the possibility some nodes might become isolated from the sensor network, and also hides the location of sink by using FRDIS messages. However, this method causes more overhead. In order to limit the amount of control traffic, an FRDIS message contains a Time to Live (TTL) field where a value *K* is stored initially. When a node receives a FRDIS message, it decrements *TTL* parameter by 1. If the value of *K* is larger than zero, the node forwards the FRDIS. When the value of TTL becomes zero, the FRDIS message is discarded.

2) Data transmission phase

After topology discovery phase, a topology map has been generated which has a tree-like structure with the sink being the root. Fig.2 shows an example of the topology tree.

From the topology tree, those nodes that are one-hop from the sink tend to have larger number of messages to send, while nodes far from the sink have fewer messages to send. Thus, the attacker can easily detect the behavior and deduce the location of sink. In order to solve the problem, we instruct each node to send the same number of messages. Therefore, the attacker cannot identify the sink node.

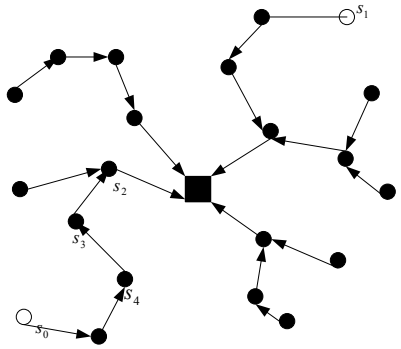

Fig.2 Topology tree

The process of transmitting data messages is as follows.

① Each node is able to encrypt (with a pair-wise key shared with the sink node) and forward Real Data (RD) messages. (These messages consist of the one the sensor generates and those for which the node act as a relay station.)

② At the same time, this node generates *m*(*i*) Fake Data (FD)messages that have the same size as the RD messages and encrypts and sends them. (Note that the purpose of the same size between FRDIS and RDIS message is that the attacker cannot distinguish which node is sink node by monitoring the traffic volume around these nodes.) In the following subsection, the way to determine the value of *m*(*i*) will be presented.

③ Upon reception, the receiving node discards the FD messages, re-encrypts the RD messages and forwards them towards the sink node according to the information on provided in the message's route field. (Note that each node can differentiate FD messages from RD messages because they can properly decrypt the messages using the corresponding pair-wise keys.) It also generates its own FD messages in according to the process described earlier.

Though there is a large account of energy cost in the CSL scheme, sensors that die first are usually those located at one-hop distance from the sink when these sensors die, the sink cannot receive any more data from the remaining operational sensors nodes. Thus, the network is not functioning any more with the new approach.

C. Determine the Value of m(i)

We assume that *N* sensors are uniformly deployed into the deployment area. All sensors generate *m* messages at the same rate, and these messages have the same size *L* bits. We suppose that the communication radius of each sensor is r_1. From Fig.3, r_i ($r_i = ir_1$) is the radius of *i*-hops of one sensor, A_1 is the area size of one sensor's range (1-hop range of one sensor, $A_1 = \pi r_1^2$).

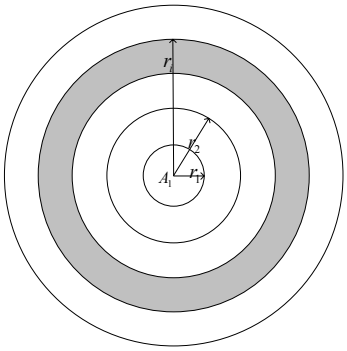

Fig.3 Range of i^{th} hop

Let N_{A_i} be the number of sensors located in the i-hops range of one sensor and S_{whole} be size of this deployment area, thus,

$$N_{A_i} = N\pi r_i^2 / S_{whole} = Ni^2 A_1 / S_{whole} \quad (1)$$

Let R_i be the area size of the i^{th} hop' ring (In Fig. 3, we use a gray color to mark i^{th} hop' ring), hence,

$$R_i = \pi(r_i^2 - r_{i-1}^2) = (2i-1)A_1 \quad (2)$$

Assume that the maximum number of hops between one leaf node and sink node in topology tree is h, thus we could compute the area size of the ring from the i^{th} hop to the h^{th} hop,

$$SR_i = \sum_{j=i}^{h} R_j = \sum_{j=i}^{h}(2i-1)A_1 = A_1[h^2 - (i-1)^2] \quad (3)$$

We define TPN_i as the traffic that has to be transmitted by in each node located in the i^{th} hop' ring, since it is traffic generated by the node itself, or since by nodes in the outer rings and has to be forwarded by the relevant node, hence,

$$TPN_1 = \frac{SR_1 \times N / S_{whole} \times mL}{R_1 \times N / S_{whole}} = \frac{h^2}{2} mL \quad (4)$$

$$TPN_i = \frac{SR_i \times N / S_{whole} \times mL}{R_i \times N / S_{whole}} = \frac{h^2 - (i-1)^2}{2i-1} mL \quad (5)$$

In equation (4) and (5), the numerator represents the number of nodes present in R_i and all of the outer rings times the amount of traffic that each node generates; the denominator in turn represents the number of nodes present in R_i , which will be in charge of forwarding the traffic calculated in the numerator.

Thus, if we define $Y(i)$ as

$$Y(i) = \frac{TPN_1}{TPN_i} = \frac{h^2(2i-1)}{h^2 - (i-1)^2} \quad (6)$$

Then, each node in different i^{th} hop' ring should generate $m(i)$ FD messages. Hence,

$$m(i) = TPN_1 - TPN_i = \frac{2ih^2 - 2h^2 + (i-1)^2}{2i-1} mL \quad (7)$$

From Eq. (7), we can see that $m(i)$ mainly depends on the values of i and h. Fig.4 shows different hops affect on the values of TPN_1 / TPN_i and the values of $2i-1$. To be simple, we assume each node generates one unit message (one unit message equals m messages) in the figure 4. The value of $Y(i)$ is approximately linear for nodes that are i-hops away from the sink, as long as i is considerably smaller than (about half) the maximum number of hops h in the network. In other words, when i^{th} hop is less than half of maximum number of hops, the values of $Y(i)$ is very close to the values of $2i-1$. The maximum number of hops that is about 25 is large enough for the network applications, thus, Eq. (7) is approximately

$$m(i) = TPN_1 - TPN_i \approx \frac{(2i-2)(h^2-1)}{2i-1} mL \quad (8)$$

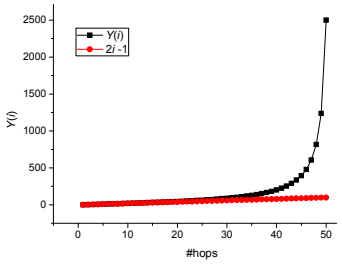

Fig.4 Values of TPN_1 / TPN_i

D. Energy Cost Analysis

Traffic volume is defined as traffic rate × message size × distance. According to the approach, we can see that each node has the same size of messages and we assume that all sensors generate m messages at the same rate. Therefore, we only need consider total messages transmission distance.

In our work, we use a simple model shown in Fig. 5 [18]. In this model, the radio dissipates E_{elec} =50nJ/bit in transmit or receive circuitry and E_{amp} =100pJ/bit/m^2 for the transmit amplifier. Thus, to transmit a L bit message with d distance, the energy cost by transmitting this message is

$$E_{T_x}(L,d) = E_{elec} \times L + \varepsilon_{amp} \times L \times d^2 \quad (9)$$

And the energy cost by receiving this message is

$$E_{R_x}(L,d) = E_{elec} \times L \quad (10)$$

Thus, energy cost in the data transmission phase is

$$\cos t_{Data} = (\sum_{i=1}^{N} TPN_1 \times h(i) \times (E_{T_x}(L,d) + E_{R_x}(L,d))) / L$$

$$= (\sum_{i=1}^{N} (h^2/2) \times h(i) \times (E_{T_x}(L,d) + E_{R_x}(L,d))) \quad (11)$$

Where h is the maximum number of hops between one leaf node and sink node in topology tree, N is the total number of sensors in the network, the value of $h(i)$ is the hop between node i to the sink.

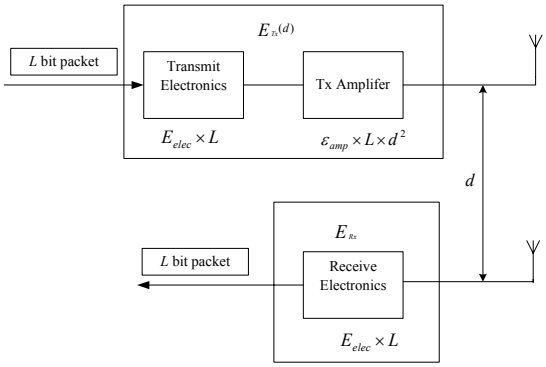

Fig.5 A simple model

In the topology discovery phase, each node who does not receive the RDIS or FRDIS message should broadcast the RDIS or FRDIS message. Define L_{RDIS} (bits) be the size of the RDIS or FRDIS message. We assume the number of the selected source nodes is a, thus,

$$\cos t_{Topo} = (E_{T_x}(L_{RDIS}, d) + E_{R_x}(L_{RDIS}, d)) \times (\frac{N\pi r_1^2}{S_{whole}} - 1) \times (N + aK) \quad (12)$$

Where S_{whole} is the size of the deployment area, r_1 is the radius of each sensor, and K is the TTL's parameter.

Therefore, the total energy cost is

$$\cos t_{Basic} = \cos t_{Topo} + \cos t_{Data} \quad (13)$$

IV. SIMULATIONS

We evaluated the performance of our approach through simulation using OPNET [19]. The simulated scenario which has one sink and 69 nodes is shown in Fig. 6. Each node generates a data packet (The size of data packet is 1024 bytes) per interval time 1.0 sec from the starting time 5.0sec. The sink node broadcasts the RDIS message per interval time 30.0sec. The radius of each node is 40m. Initial energy of each node is 10.0J. From the Fig.6, we can see that node 4, node 5, node 9, node 11, node 13, node 15 and node 16 are the one-hop of the sink.

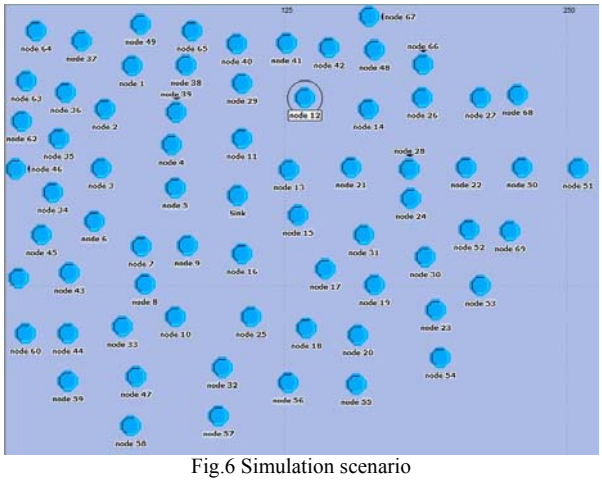

Fig.6 Simulation scenario

Fig.7 illustrates that the average RD message delay delivery time is dependent on the simulation time. Note that conventional scheme means we do not add FD messages during the phase of data transmission. There is no dead node during the simulation time 30.0 sec. The CSL scheme has the higher RD message delay compared to the conventional scheme. At the beginning, in the CSL scheme, the RD message delay is fluctuate, however, it keeps stable with the value 0.0125sec after the simulation time 15.0sec. Due to no FD message in the data transmission phase, the RD message delay in the conventional scheme keeps the value of 0.0062sec.

Fig.8 describes the fraction of packets received by sink node. Note that the fraction is equal to the total number of RD packets received by sink / the total number of generated RD packets by nodes. From the Fig.8, we can see that both of these schemes have very high fraction, which is close to 0.98. Besides, the number of nodes in the network has little effect on the fraction.

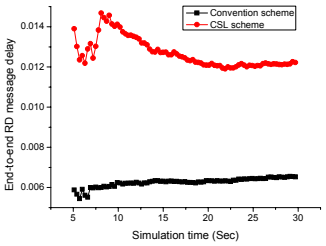

Fig. 7 End-to-end delay

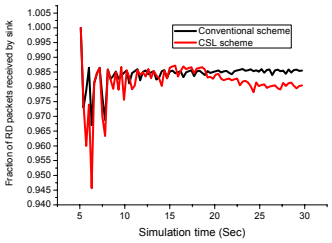

Fig. 8 Fraction of RD packet received by sink

Fig. 9 provides some information on how the total energy cost is impacted by the different number of nodes. According to the simple radio energy model where the radio dissipates E_{elec} =50nJ/bit in transmit or receive circuitry and E_{amp} =100pJ/bit/m^2 for the transmit amplifier [18]. From the Fig. 9, the CSL scheme has much more energy cost than the conventional scheme. The main reason is that there are many FD messages transmitted in the CSL scheme.

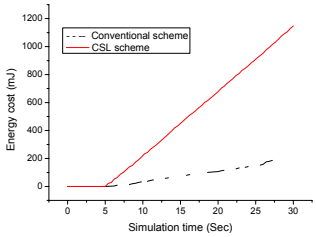

Fig. 9 Energy cost

In order to confuse the attacker who launches traffic analysis attacks, the CSL scheme make each node has the similar traffic volume. We observer the traffic volumes when the attacker locates at the around of node 11, node 42, node 66, node 67, node 4, node 3, node 65. Note that the route path of node 66 is 0, 11, 12, 14, 26, 66; the route path of node 67 is 0, 11, 12, 42, 48, 67; the route path of node 65 is 0, 4, 39, 38, 65; and the route path of node 3 is 0, 4, 3. Fig. 10-*a* depicts the traffic volumes of the node 11, node 42, node 66 and node 67 in the conventional scheme. Node 11 has the largest traffic volume, so that, the attacker can deduce node 11 is close to the

sink compared to node 42, node 66 and node 67. Node 66 and node 67 has the lower traffic volume. From the Fig. 6 (Simulation scenario), we can see that node 11 is the sink' neighbor; node 66 and node 67 are deployed on the edge of the scenario. Therefore, the attacker can easily deduce the sink's location. The curves in Fig.10-*c* are very closely, which means, the traffic volumes in node 11, node 42, node 66 and node 67 are similar, so that the attacker cannot deduce who is close to the sink. Thus, the CSL scheme can hide the sink's location.

Fig.10-*b* and Fig.10-*d* show that traffic volume in each node which is located another route path. In the conventional scheme, according to the traffic volume of node 4, node 3 and node 65, the attacker can drive a conclusion that node 4 is located to the sink, while node 3 and node 65 are4 far away from the sink. In the CSL scheme, the traffic volumes of node 3 and node 4 are very close, while the traffic volume of node 65 is a litter lower. That means, the attacker can deduce the node 3 and node 4 are close to the sink, however, actually, node 3 is far away from the sink.

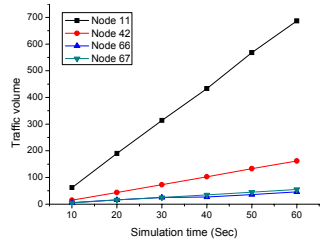

Fig. 10-*a* Convention scheme

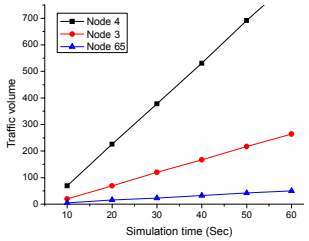

Fig. 10-*b* Convention scheme

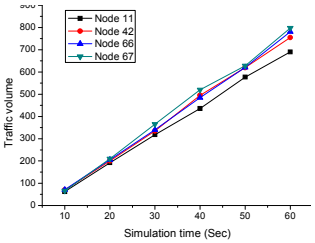

Fig. 10-*c* CSL scheme

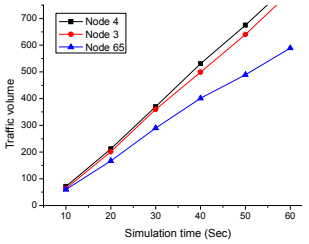

Fig. 10-*d* CSL scheme

Fig. 10 Traffic volume in each node

V. CONCLUSIONS

In this paper, after analyzing the sink anonymity problem under the traffic analysis attacker model, we provide a concealing of the sink's location protocol which can preserve the sink's location by using fake message injection. Performance evaluations demonstrate that the sink's location privacy could be preserved and the fraction of RD packets received by the sink is close to 0.98.

Future research on the topic includes how to reduce the energy cost while guaranteeing the sink's location privacy.

ACKNOWLEDGMENT

This work was supported by the Government of Ontario under the ORF-RE WISENSE project (3074600) and the Natural Sciences and Engineering Research Council (NSERC) of Canada under NSERC Grant 193961-2006.

REFERENCES

[1] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," In 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks, October 2004.

[2] Y. Jian, S. Chen, et. al, "Protecting receiver location privacy in wireless sensor networks," in Proc. of IEEE Infocom, pp. 1955–1963, 2007.

[3] 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.

[4] 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, April 2008.

[5] A.A. Nezhad, D.Makrakis and A. Miri, "Anonymous topology discovery for multihop wireless s ensor networks," 3rd ACM International Workshop on QoS and Security for Wireless and Mobile Networks, Chania, Crete Island, Greece, October, 2007.

[6] J. Deng, R. Han, and S. Mishra, "Inrusion tolerance and antitraffic analysis strategies in wireless sensor networks," In IEEE 2004 International Conference on Dependable Systems and Networks (DSN'04), Florence, Italy, June 2004.

[7] E.M. Shakshuki, T.R. Sheltami and et. al., "Tracking anonymous sinks in wireless sensor networks," International Conference on Advanced Information Networking and Applications, 2009. pp. 510-516. 2009.

[8] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 482–494, 1998.

[9] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, "Spins: security protocols for sensor networks," Wireless Networks, vol. 8, no. 5, pp. 521-534, 2002.

[10] L. Eschenaur and V. Gligor, "A key-management scheme for distributed sensor networks," in Proc. 9th ACM Conference on Computer and Communications Security, 2002.

[11] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," IEEE/ACM Transactions on Networking (TON), vol. 11, no. 1, pp. 2-16, 2003.

[12] Y. Xi, L. Schwiebert, and W. Shi. Preserving source location privacy in monitoring-based wireless sensor networks. In SSN '06.

[13] R. Shokri, A. Nayyeri, and et. al., "Efficient and adjustable recipient anonymity in Mobile ad hoc networks," IEEE International Conference on Mobile Ad hoc and Sensor Systems, 2007, pp. 1-3, 2007.

[14] X.Wu, J.Liu and et. al., "Achieving anonymity in mobile ad hoc networks using fuzzy position information," http://www.springerlink.com/content/r28p427178j188w5/.

[15] L. Sweeney, "K-anonymity: a model for protecting privacy," International Jounal on Uncertainity, Fuzziness and Knowledge-based Systems, vol. 10(5), pp. 557-570, 2002.

[16] K.Oikonomou and I.Stavrakakis, "Performance analysis of probabilistic flooding using random graphs," In Proc. AOC2007, June 2007.

[17] N.B. Chang, M.Y. Liu, "Controlled flooding search in a large network," IEEE Transaction on Networking, Vol. 15(2), pp. 436-449, 2007.

[18] W.T. Heinzelman, A. Chandrakasan and H. Balakrishnam, "Energy-efficient conmunication protocol for wireless microsensor network," Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000, vol. 2, pp. 1-10, Jan. 4-7, 2000.

[19] Opnet, http://www.opnet.com.

[20] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic 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.