On the Performance of Source Location Privacy Protocols with Multiple Source Nodes in WSNs

Lilian C. Mutalemwa and Seokjoo Shin*
Department of Computer Engineering, Chosun University, Gwangju 61452, South Korea
Email: lilian.mutalemwa@gmail.com, *sjshin@chosun.ac.kr (corresponding author)

***Abstract*—Source location privacy (SLP) protection is essential in safety-critical monitoring wireless sensor networks. Therefore, a recent study presented some investigations on the performance of SLP protocols in various network configurations. However, the study failed to investigate the performance of the protocols under varied number of source nodes per event. In this study, we analyze the SLP performance and energy efficiency of the protocols under varied number of source nodes. Analysis results show that an increase in the number of source nodes per event can result in energy-inefficient communications and reduced levels of SLP protection.**

Keywords—source location privacy; wireless sensor network; routing protocol; energy efficiency; privacy protection.

I. INTRODUCTION

Wireless sensor networks (WSNs) are widely used in many applications including national security, asset monitoring, automation, intelligent transportation systems, and military surveillance [1], [2]. Often, WSNs operate in unattended environments and are mostly battery-powered, so their performances are vulnerable to energy and environmental factors [3]. Furthermore, WSNs are usually deployed in random areas with no protection. Consequently, the networks are vulnerable to traffic analysis attacks. In monitoring WSNs, adversaries may focus on analyzing the network traffic to obtain critical information such as the location information of the source nodes [2], [4]. The source location reveals valuable information about the monitored asset. Thereafter, the asset can be easily attacked. Therefore, it is important to guarantee source location privacy (SLP) protection in safety-critical monitoring WSNs.

Fake packet-based SLP protocols are capable of effectively protecting the SLP in monitoring WSNs [5]-[7]. The protocols employ different fake packet routing strategies [8]. In this study, we investigate the routing strategies of the distributed fake source with phantom node (DfpR) protocol [9] and the probabilistic routing protocol (PbrR) [10].

A recent study in [8] presented comprehensive performance evaluations of several fake packet-based protocols. The study investigated the performance of the protocols under varied network parameters and configurations. The performance was observed under varied sensor node residual energy, source-sink distance, network operation duration, network size, source packet rate, and node density. However, the study failed to analyze the privacy performance or energy efficiency of the protocols under varied number of source nodes per event. Therefore, in this study, we analyze the privacy performance and energy efficiency of the DfpR and PbrR protocols under varied number of source nodes per event. We conduct a series of experiments and measure the privacy performance in terms of capture ratio and the energy efficiency in terms of energy ratio.

II. RELATED WORK

Since the problem of SLP was introduced in 2004, numerous protocols have been proposed to provide SLP protection [11]-[13]. Many of the protocols were discussed in [6], [7], [11]-[13]. There exist many fake packet-based SLP protocols including the data dissemination routing protocol [14], tree-based diversionary routing protocol [15], protocol based on phantom nodes, rings, and fake paths [12], protocol based on anonymity cloud [5], distributed fake source with phantom node protocol [9], and the probabilistic routing protocol [10]. The study in [8] presented some performance evaluations of several fake packet-based SLP protocols. Various network parameters and settings were considered.

III. MODELS

A. Network Model

The network model is adopted from [11]. The sensor nodes are equipped with a wireless interface and have limited resources and computational capabilities. The network is event-triggered. A node senses an asset and becomes a source node, then it sends packets periodically to the sink node. The sensor nodes employ multi-hop communication for energy conservation. During the network configuration phase, network initialization process is performed for localization of the sensor nodes. The *k*-nearest neighbor tracking approach [16] is employed to track the assets.

B. Adversary Model

The adversary model is adopted from [11]. The adversary is assumed to be more powerful than the sensor nodes in the network. It is equipped with spectrum analyzers and has sufficient resources such as adequate computation capabilities, memory, and unlimited power. The adversary is mobile, initially residing in the neighborhood of the sink node. It is capable of localizing an immediate sender node when a packet is received from a node within the adversary hearing range. It performs a hop-by-hop back tracing attack towards the source node, until it locates the source node.

IV. PERFORMANCE EVALUATIONS

A. Simulation environment

MATLAB simulation environment was used to evaluate the performance of the DfpR and PbrR protocols. For comparative analysis, the traditional intermediate node routing (IntR) protocol was included in the analysis [8]. A network of size 2000 × 2000 m^2 was simulated with 2500 randomly distributed sensor nodes. The network simulation parameters are summarized in Table I. Simulation was run for 500 iterations and average values were considered. Two performance metrics were used: capture ratio was used to measure the privacy performance while energy ratio measured the energy efficiency. Results of the analysis are discussed below.

TABLE I: NETWORK SIMULATION PARAMETERS

Parameter	Value
Network area (m^2)	2000 × 2000
Number of nodes	2500
Number of sink nodes	1
Sensor node communication range (m)	30
Adversary hearing range (m)	30
Adversary waiting timer (source packets)	4
Adversary initial location	In the vicinity of sink node
Packet size (bit)	1024
Source packet rate (packet/second)	1
Sensor node initial energy (J)	0.5

B. Results and Discussions

1) Capture Ratio

Capture ratio (CR) is the ratio between the number of experiments where the adversary ends in locating the source node and the total number of experiments. To locate the source node, an adversary must back trace the packet routes and reach at the location of the source node. Thus, the adversary must co-locate with the source node. To compute CR, equation (1) was assumed [8].

$$CR = \frac{Number\ of\ experiments\ with\ located\ source}{Total\ number\ of\ experiments} \quad (1)$$

The CR has an inversely proportional relationship with the SLP protection as shown in equation (2). When the CR of a protocol is minimized, the SLP protection is maximized.

$$\min\ (CR) = \max\ (SLP_{Protection}) \quad (2)$$

The CR of the protocols was observed under varied number of source nodes at a trace time of 2000 source packets. The results are shown in Fig. 1. It is shown that the DfpR protocol achieves significantly lower levels of CR than the PbrR and IntR protocols. To achieve low levels of CR, DfpR distributes a considerable amount of fake packet traffic simultaneously with the transmission of the real packets. As a result, the adversary is tackled with multiple packets and finds it difficult to identify the exact immediate sender node of the real packets. Therefore, the back tracing attack is made more complex and the CR is reduced. PbrR distributes a significantly reduced amount of fake packet traffic. As a result, the obfuscation effect on the adversary is reduced and the CR is increased. Furthermore, in PbrR, the fake packet sources are located near the sink node, making the fake packet routes short and easy to predict by the adversary. Moreover, PbrR isolates fake packet sources from the real packet sources. As a result, the routing paths of the real packets become predictable to the adversary, the back tracing attack becomes less complex, and the CR is increased.

Fig. 1 also shows that the CR of all the protocols tend to increase with the increase in number of source nodes per event. The increase in CR is mainly because when the number of source nodes is increased, the amount of packet traffic around the event location is also increased. Therefore, the event location becomes an obvious hotspot region. Furthermore, due to the increase in packet traffic, the adversary captures an increased number of packets from the real source nodes and improves its attack success rate and CR. The CR of DfpR increases at a slower rate because DfpR distributes a large amount of fake packet traffic, does not isolate fake source nodes from the real source node, and generates fake source nodes throughout the WSN domain. The results in Fig. 1 reveal that the DfpR, PbrR, and IntR protocols provide improved levels of SLP protection when the number of source nodes per event is reduced.

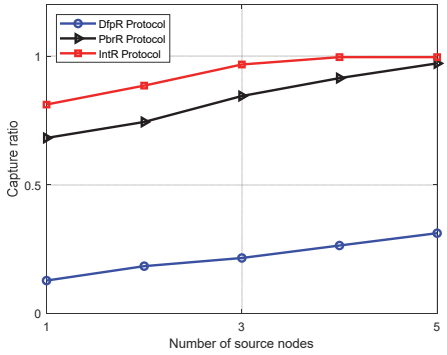


Fig. 1. Capture ratio of the protocols.

2) Energy Efficiency

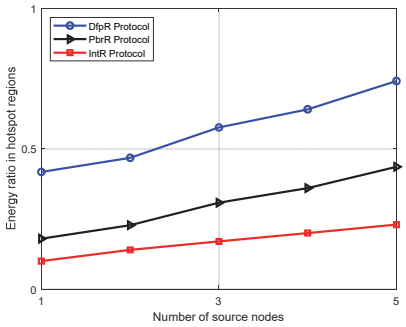
The energy consumption and energy efficiency of the protocols were analyzed using the energy consumption model in [11], [15]. Equations (3) and (4) were used to compute the energy consumption of the sensor nodes. The details of the equations are presented in [11].

$$E_{trans} = \begin{cases} lE_{loss} + lE_{fs}d^2, & if\ d < d_0 \\ lE_{loss} + lE_{amp}d^4, & otherwise. \end{cases} \quad (3)$$

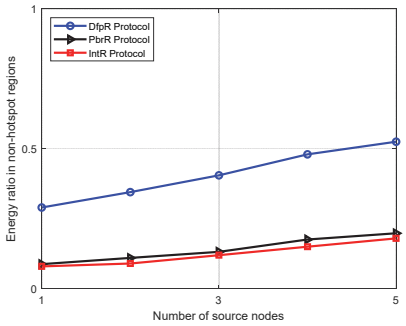
$$E_{rec} = lE_{loss} \quad (4)$$

To measure the energy efficiency of the protocols, we used the energy ratio parameter. We define the energy ratio (ER) as the ratio of the energy that is used in 600 rounds to the total energy. High ER corresponds to low energy efficiency.

The ER was computed for the near-sink regions (hotspot regions) and the away from sink node regions (non-hotspot regions) as shown in Fig. 2. All sensor nodes with source-sink



(a)



(b)

Fig. 2. Energy efficiency of the protocols. (a) Energy ratio in hotspot regions. (b) Energy ratio in non-hotspot regions.

distance < 25 hops were considered to be located in the hotspot regions. Fig. 2 shows the ER of the protocols at varied number of source nodes. It is shown that the DfpR protocol has significantly higher ER than the traditional IntR protocol. Also, in hotspot regions, PbrR has higher ER than IntR. This means that compared to the IntR, the DfpR and PbrR are less energy-efficient. The DfpR and PbrR incur high ER because they transmit real and fake packet traffic.

Fig. 2 also shows that the ER of all the protocols tend to increase with the increase in number of source nodes per event. This is mainly because when the number of source nodes per event is increased, the amount of packet traffic is also increased and a higher amount of energy is consumed to transmit the packets. As a result, the ER is increased. Thus, the energy efficiency of the protocols is significantly reduced when the number of source nodes per event is increased. The ER of DfpR increases at a fast rate because a large amount of fake packets is distributed for each real source node packet. In PbrR, few fake packets are distributed in the hotspot regions.

V. Conclusion and Future Work

This paper presents some investigations on the privacy performance and energy efficiency of fake packet-based SLP protocols. Performance of the protocols is evaluated under varied number of source nodes per event. It is observed that the level of SLP protection and energy efficiency are significantly reduced when the number of source nodes per event is increased. Thus, it is important to regulate the number of source nodes per event in order to achieve energy-efficient communications and high levels of SLP protection. As part of our future work, we will analyze the network lifetime of the protocols under varied number of source nodes.

Acknowledgment

This research is supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1B07048338).

References

[1] J. Zhang, J. Tang, and F. Wang, “Cooperative relay selection for load balancing with mobility in hierarchical wsns: A multi-armed bandit approach,” *IEEE Access*, vol. 8, pp. 18110–18122, January 2020.

[2] G. Han, X. Miao, H. Wang, M. Guizani, and W. Zhang, “CPSLP: A cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2739–2750, March 2019.

[3] X. Fu, Y. Yang, and O. Postolache, “Sustainable multipath routing protocol for multi-sink wireless sensor networks in harsh environments,” *IEEE Transactions on Sustainable Computing*, vol. 6, no. 1, pp. 168–181, March 2021.

[4] M. Kamarei, A. Patooghy, A. Alsharif, and V. Hakami, “SiMple: A unified single and multi-path routing algorithm for wireless sensor networks with source location privacy,” *IEEE Access*, vol. 8, pp. 33818–33829, February 2020.

[5] N. Wang, J. Fu, J. Li, and B. K. Bhargava, “Source-location privacy protection based on anonymity cloud in wireless sensor networks,” *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 100–114, 2020.

[6] J. Jiang, G. Han, H. Wang, and M. Guizani, “A survey on location privacy protection in wireless sensor networks,” *J. Netw. Comput. Appl.*, vol. 125, pp. 93–114, Jan. 2019.

[7] Z. Hong, R. Wang, S. Ji, and R. Beyah, “Attacker location evaluation-based fake source scheduling for source location privacy in cyber-physical systems,” *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1337–1350, May 2019.

[8] L. C. Mutalemwa, and S. Shin, “Comprehensive performance analysis of privacy protection protocols utilizing fake packet injection techniques” *IEEE Access*, vol. 8, pp. 76935–76950, April 2020.

[9] P. K. Roy, J. P. Singh, P. Kumar, and M. Singh, “Source location privacy using fake source and phantom routing (FSAPR) technique in wireless sensor networks,” *Procedia Comput. Sci.*, vol. 57, pp. 936–941, 2014.

[10] H. Wang, G. Han, W. Zhang, M. Guizani, and S. Chan, “A probabilistic source location privacy protection scheme in wireless sensor networks,” *IEEE Trans. Veh. Technol.*, vol. 68, 5917–5927, 2019.

[11] L. C. Mutalemwa, and S. Shin, “Secure routing protocols for source node privacy protection in multi-hop communication wireless networks,” *Energies*, vol. 13, p. 292, 2020.

[12] Z. Xiong, H. Wang, L. Zhang, T. Fan, and J. Shen, “A ring-based routing scheme for distributed energy resources management in iiot,” *IEEE Access*, vol. 8, pp. 167490–167503, September 2020.

[13] Q. Wang, J. Zhan, X. Ouyang, and Y. Ren, “SPS and DPS: Two new grid-based source location privacy protection schemes in wireless sensor networks,” *Sensors*, vol. 19, p. 2074, May 2019.

[14] N. Jan, A. Al-Bayatti, N. Alalwan, and A. Alzahrani, “An enhanced source location privacy based on data dissemination in wireless sensor networks (DeLP),” *Sensors*, vol. 19, no. 9, p. 2050, 2019.

[15] J. Long, M. Dong, K. Ota, and A. Liu, “Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks,” *IEEE Access*, vol. 2, pp. 633–651, 2014.

[16] Y. Liu, J.-S. Fu, and Z. Zhang, “K-nearest neighbors tracking in wireless sensor networks with coverage holes,” *Pers. Ubiquitous Comput.*, vol. 20, no. 3, pp. 431–446, June 2016.