Investigating the Packet Delivery Reliability of Source Location Privacy Protocols 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*—When Wireless Sensor Networks (WSNs) are used in mission-critical and delay sensitive applications, it is important to ensure low latency and reliable packet delivery. This study presents some performance evaluations of end-to-end delay and packet delivery ratio for source location privacy (SLP) protocols in WSNs. Four categories of SLP routing protocols are considered. Analysis results reveal that angle-based SLP protocol presents the best performance by achieving a good balance between SLP protection and packet delivery reliability.**

Keywords—source location privacy; wireless sensor network; routing protocol; packet delivery ratio; end-to-end delay.

I. INTRODUCTION

Source location privacy (SLP) protection is defined as the process of minimizing the traceability and observability of a source node by an attacker in monitoring wireless sensor networks (WSNs). It can also be defined as the process of keeping the location of a source node hidden from an attacker [1]-[4]. SLP protection is an essential procedure in asset monitoring WSNs because it ensures the security of the monitored assets. When the WSNs are used in mission-critical and delay sensitive applications, it is important to ensure that the SLP protocols achieve low latency and reliable packet delivery.

Various SLP protocols exist in the literature [2], [5], [6]. Tree-based, intermediate node-based, phantom node-based, and angle-based protocols are among the most popular categories of SLP routing protocols. The main objective of this study is to perform an experimental analysis of some representative protocols for each category. The analysis aims to evaluate the privacy performance and packet delivery reliability of the protocols using three important performance metrics: safety period, packet delivery ratio (PDR), and end-to-end delay (EED). The representative protocols for the tree-based, intermediate node-based, phantom node-based, and angle-based routing protocols are the tree-based diversionary routing [7], strategic location-based routing [1], phantom single-path routing [8], and the constrained random routing [9], respectively.

Thus, the main contribution of this study is to investigate the privacy, PDR, and EED performance of four representative protocols, namely tree-based diversionary routing, strategic location-based routing, phantom single-path routing, and constrained random routing protocols.

The remainder of this paper is organized as follows: Section II presents a review of the literature on routing protocols for SLP protection. Section III highlights some assumptions and details of the network and adversary models. Experimental analysis and simulation results are discussed in section IV. In section V, the paper is concluded.

II. RELATED WORK

Since the problem of SLP was introduced in 2004, numerous protocols for SLP protection have been proposed. Many of the protocols are described in [2], [5], [6], [10]-[13]. Examples of tree-based routing protocols include the tree-based diversionary routing, bidirectional tree, dynamic bidirectional tree, and zigzag bidirectional tree routing [7]. Intermediate node-based protocols include the randomly selected intermediary node routing, strategic location-based routing, three-phase intermediate node routing with network mixing ring, sink toroidal region routing, and all-direction random routing [7]. In the case of phantom node-based routing protocols, examples include the phantom single-path routing, phantom routing with locational angle, and greedy random walk routing [2]. Examples of angle-based routing protocols include the angle-based dynamic routing, constrained random routing, and 2-phantom angle-based routing [2], [12]. This study focuses on the performance of four protocols: the tree-based diversionary routing, strategic location based routing, phantom single-path routing, and the constrained random routing.

III. MODELS

A. Network Model

The network model, similar to [12] is assumed. The network is composed of a set of sensor nodes and links. A sensor node is equipped with a wireless interface, limited resources, and computational capabilities. The sink node is located at the center of the network domain. The network is event-triggered.

B. Adversary Model

The adversary model, similar to [12] is assumed. The adversary 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.

IV. PERFORMANCE EVALUATION

A. Simulation environment

MATLAB simulation tool was used to evaluate the performance of four SLP routing protocols: tree-based diversionary routing (TDR), strategic location-based routing

(STRA), phantom single-path routing (PHA), and the constrained random routing (CONS). The network simulation

TABLE 1: NETWORK SIMULATION PARAMETERS

Parameter	Value
Network area (m^2)	2000 × 2000
Number of nodes	2500
Number of sink nodes	1
Sensor node sensing range (m)	30
Adversary detection range (m)	30
Adversary waiting timer (source packets)	4
Adversary initial location	In the vicinity of the sink node
Target monitoring scheme	k-nearest neighbor tracking
Packet size (bit)	1024
Source packet rate (packet/second)	Varied from 1 to 6

Parameters are summarized in Table 1.

B. Results and Discussion

We use three performance metrics to evaluate the performance of the protocols. Safety period is used to measure the level of SLP protection, while PDR and EED are used to measure the packet delivery reliability. High PDR and short EED corresponds to high packet delivery reliability, while low PDR and long EED corresponds to low packet delivery reliability.

1) Safety Period (SP): the time required for an adversary to backtrace the packet routes and successfully capture the asset. SP is used to measure the privacy performance of the protocols. Longer SP provides stronger SLP protection. To evaluate the SLP performance, equation (1) was assumed from [13].

$$\max\ (SP) = \max\ (SLP_{Protection}) \qquad (1)$$

The analysis results in Fig. 1 show that TDR achieves the strongest SLP protection, followed by STRA, and CONS protocols. PHA achieves the lowest privacy level. The TDR protocol achieves the strongest SLP protection by integrating many routing techniques. It uses long backbone routes with many diversionary routes. At the end of each diversionary route, fake packets are emitted periodically. It also employs phantom nodes located far away from the source node. As a result, the eavesdropping adversary is effectively obfuscated.

The routing paths for the STRA and CONS are highly random and unpredictable to the eavesdropping adversary. STRA uses mediate and diversion nodes which are strategically positioned to ensure the routing paths are highly randomized and packets arrive at the sink node from various directions, to obfuscate the adversary. A new mediate or diversion node is randomly selected for each successive packet. As a result, strong SLP protection is guaranteed. In CONS, relay node selection is based on the transmission of offset angles and constrained probability. It also considers the prohibited distance to ensure no location information of the relay node or the source node is exposed to the adversary. As a result, packets are transmitted with a longer safety period and strong SLP protection is achieved by CONS. PHA is a traditional protocol which uses a simple algorithm with less random routing paths. Therefore, the adversary can easily backtrace the routing paths. As a result, PHA achieves weak SLP protection.

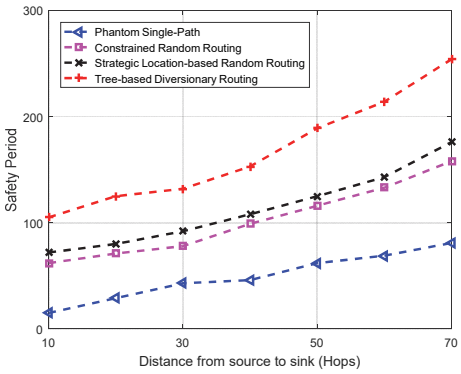

Fig. 1. Privacy performance of the routing protocols.

2) Packet delivery ratio (PDR): the ratio between the total number of packets successfully delivered to the destination sink node and the number of packets transmitted by the source node. To evaluate the PDR performance, equation (2) was assumed from [13].

$$PDR = \frac{P_{Rec}}{\sum_{i=1}^{n} P_{Trans_i}} \qquad (2)$$

Fig. 2 shows the PDR performance at the source-sink distance of 25 hops. It shows that PDR decreases with the increase in the source node packet generation rate. This is mainly due to the fact that when more packets are generated per second, the probability of packet collision and packet loss events is increased and PDR is affected.

PHA protocol shows good PDR performance because it employs short and less random routing paths with reduced number packet collision and packet loss events. However, it offers poor SLP protection as shown in Fig. 1. The CONS protocol employs relatively short routing paths. The short routing paths incur fewer packet forwarding events (hops) and low probability of packet collision or packet loss events. Hence, the PDR of CONS is relatively high.

The STRA protocol deploys rings of diversion and mediates nodes at some distance away from the sink node to elongate and randomize the packet routes. This results in high SLP protection. However, the PDR is affected. The TDR incurs the lowest PDR performance due to the integration of many routing strategies. The use of backbone routes, diversionary routes, phantom nodes, and fake packets results in a high probability of packet collision and packet loss events. Consequently, the PDR of TDR is reduced.

Overall, the analysis results in Fig. 2 show that PHA achieves the highest packet delivery reliability, followed by CONS and STRA protocols while TDR achieves the lowest.

3) End-to-end delay (EED): the time taken for a packet to be transmitted across the network from a source node to the destination sink node. To evaluate the EED, the average sum of the different delay of each data packet received by the sink node and the time a data packet is sent by the source node is considered. Equation (3) is assumed from [13].

$$EED = \frac{\sum_{i=1}^{P_{Rec_i}} (T_{Rec_i} - T_{Trans_i})}{P_{Rec}} \qquad (3)$$

Fig. 3 shows the EED performance at a source-sink distance of 25 hops. It shows that EED increases with the increase in

source node packet generation rate. This is mainly due to the fact that as more packets are generated per second, the probability of packet collision, packet loss, and packet retransmission is increased. When packet retransmission events occur, the EED is increased.

The TDR protocol incurs the longest EED due to the integration of many routing strategies. The use of backbone routes, diversionary routes, phantom nodes, and fake packet routing creates routing paths with high probability of packet collision, packet loss, and packet retransmission events, which greatly affects the EED performance. The STRA protocol incurs long EED due to the designated location of the diversion and mediates nodes. The nodes are located at a distance away from the sink node, hence packets experience long delay in traversing through the selected diversion or mediating nodes. The CONS protocol ensures relatively short routing paths. The short routing paths offer a fewer number of packet forwarding events (hops), low probability of packet collision, and fewer packet retransmission events. As a result, CONS incurs reduced EED compared to STRA. PHA protocol shows good EED performance due to the utilization of short and less random routing paths that experience fewer packet loss and packet retransmission events.

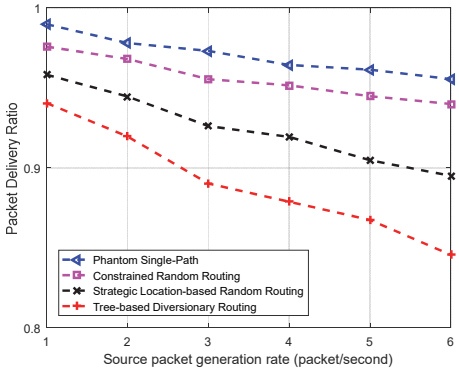

Fig. 2. Packet delivery ratio under varied source node packet generation rate.

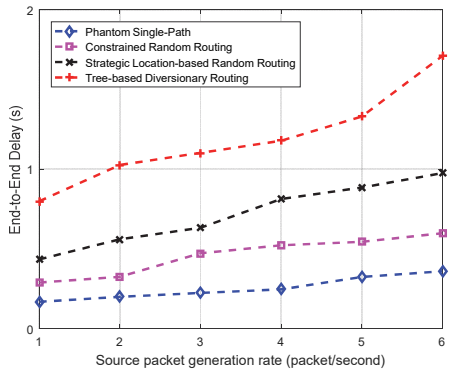

Fig. 3. End-to-end delay under varied source node packet generation rate.

V. Conclusion and Future Work

This paper presents performance evaluations and investigations on the privacy performance and packet delivery reliability of SLP protocols. The safety period, packet delivery ratio, and end-to-end delay performance of representative protocols for tree-based, intermediate node-based, phantom node-based and angle-based SLP protocols are considered. Analysis results show that the angle-based routing protocol has superior performance features. It achieves high levels of SLP protection with improved packet delivery reliability. On the contrary, the tree-based protocol is capable of achieving significantly high levels of SLP protection but its packet delivery reliability is very much compromised. In our future work, we will consider performance evaluation of more recent SLP protocols.

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] L.C. Mutalemwa, and S. Shin, “Strategic location-based random routing for source location privacy in wireless sensor networks,” *Sensor*, vol.18, no.7, 2291, 2018.

[2] J. Jiang, G. Han, H. Wang, and M. Guizani, “A survey on location privacy protection in wireless sensor networks,” *Journal of Network and Computer Applications*, vol.125, pp. 93–114, January 2019.

[3] M. Bradbury, A. Jhumka, and M. Leeke, “Hybrid online protocols for source location privacy in wireless sensor networks,” *J. Parallel Distrib. Comput*., vol. 115, pp. 67–81, 2018.

[4] J. Kirton, M.S. Bradbury, and A. Jhumka, “Source location privacy-aware data aggregation scheduling for wireless sensor networks,” in *Proc. 37th IEEE International Conference on Distributed Computing Systems*, Atlanta, GA, USA, 5–8 June 2017, pp. 2200–2205.

[5] L.C. Mutalemwa, and S. Shin, “Routing protocols for source location privacy in wireless sensor networks: a survey,” *J. Korean Inst. Commun. Inf. Sci*., vol. 43, no. 9, pp. 1429–1445, September 2018.

[6] M. Conti, J. Willemsen, and B. Crispo, “Providing source location privacy in wireless sensor networks: a survey,” *IEEE Communications Surveys Tutorials*, vol. 15 no. 3 pp. 1238-1280, 2013.

[7] 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.

[8] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, “Enhancing source-Location privacy in sensor network routing,” in *Proc. 25th International Conference on Distributed Computing Systems (ICDCS'05)*, Ohio, USA, June 2005, pp. 599-608.

[9] W. Chen, M. Zhang, G. Hu, X. Tang, and A.K. Sangaiah, “Constrained random routing mechanism for source privacy protection in WSNs,” *IEEE Access*, vol. 5, pp. 23171–23181, September 2017.

[10] A. Bushnag, A. Abuzneid, and A.Mahmood, “Source anonymity against global adversary in wsns using dummy packet injections: A survey,” *Electronics*, vol. 7, no. 10, p. 250, 2018.

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

[12] L.C. Mutalemwa, and S. Shin, “Regulating the packet transmission cost of source location privacy routing schemes in event monitoring wireless networks,” *IEEE Access*, vol.7, pp. 140169–140181, 2019.

[13] 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.