Greedy Random Walk Scheme Based MSL Privacy for WSN

Jian-bo YAO¹ and Chao-qiong YANG²

¹School of Mathematics and Computer, Hezhou University, Hezhou Guangxi 542899, China
²Audit Division, Zunyi Normal College, Zunyi Guizhou 563006, China

Keywords: Location, Location privacy, GRWS, WSN.

Abstract. The privacy for station-locations of WSN is a key problem in battlefield. Being exposed for location, the consequences are unthinkable. RDCS (Random Data Collection Scheme) has a problem that message latencies become higher. In this paper, GRWS (Greedy Random Walk Scheme) is proposed to preserve MSL (Mobile-Station-Location) privacy. In GRWS, data are forwarded and stored at pass nodes, the station move to get data sporadically, which prevents the attackers from predicting their locations and movements. Compared to RDCS, GRWS has smaller message latencies, while providing satisfactory MSL privacy.

Introduction

WSN are used in variety of applications for getting information from monitored areas and objects, privacy concerns have become the main obstacle to success when people are participants in WSN [1-8]. Station location privacy in WSN is a key when a WSN is used in military filed. To preserve MSL privacy in WSN, GRWS is proposed to use for mobile-station. The station moves to get data in sensor scatter domain [9-13].

The paper is organized as follows: In Section 2, work for direction relate. In Section 3, threat models for WSN is built. In Section 4, RDCS’s flaw. In Section 5, GRWS is described. In Section 6, performance analysis. In Section 7, conclusions.

Work for Direction Relate

Edith C. -H. Ngai et al. built RDCS [14] which can protect MSL in WSN. The sensing data are stored at nodes with the stations moving randomly and getting data sporadically from neighbors. But RDCS is that the delivery latency is bigger. Some messages will not reach stations.

The [14] Incentive, we have established GRWS. In our scheme, sensor do not know any station-location information, data are forwarded by some path and stored at pass nodes, the station moves to get data from the local nodes sporadically. Compared to RDCS, our scheme reduces the data delivery latency, while providing satisfactory MSL privacy.

Threat Models for WSN

WSN consist of lots sensor nodes. A sensor can send packets to neighboring with its limited radio range. There is a mobile station in WSN. The energy and resource in a sensor are minimum. Each node can build communication link with its neighboring through shared keys.
Sensors get data and store them temporarily. The station will move in GRWS and broadcast sporadically to some local sensors to get data.

Assume that an adversary’s characteristics are as follow:
- He does not interfere with the functions for WSN.
- He has an unlimited power and patience and can physically move from one sensor to another.
- For tracing and attacking, he may discover the station location by reading the information of the packets, following data flow or foreseeing the station movement.

**RDCS’s Flaw**

RDCS supposes WSN with $N$ sensors, on a two-dimensional integer grid, is arrayed with an initial location $(0,0)$ station. Moving randomly with equal probability from north, south, east, or west, i.e. from $\{(1,0), (-1,0), (0,1), (0,-1)\}$, and the same node may visit more than once.

After the $h_{\text{walk}}$ random walk steps with an independent random variable $X_j$, the location is given by $D_{h_{\text{walk}}} = X_1 + X_2 + \cdots + X_{h_{\text{walk}}}$. Examining the central limit theorem, $\frac{D_{h_{\text{walk}}}}{\sqrt{h_{\text{walk}}}}$ converges in distribution to a bivariate Gaussian with mean $O = (0,0)$, covariance matrix $(1/2)I$. Then, $D_{h_{\text{walk}}} \sim N \left( O, \frac{h_{\text{walk}}}{2} I \right)$. Let $B = B(O, d)$ be a ball of radius $d$ centered at $(0,0)$. The asymptotic probability of the station $D_{h_{\text{walk}}}$ being within a distance $d$ for first location, after $h$ random walk steps.

$$P(D \in B) = \frac{1}{h\pi} \int_B e^{-\frac{(x^2+y^2)}{h_{\text{walk}}}} \, dxdy$$

$$= \frac{1}{h\pi} \int_0^d \int_0^{2\pi} e^{-\frac{r^2}{h_{\text{walk}}}} r d\theta dr$$

$$= 1 - e^{-\frac{d^2}{h_{\text{walk}}}} \quad (1)$$

Based on formula (1), purely random walk cans not make the station far from its initial location. Fig1 is the effective hops probability distributing leaving initial location.

Figure 1. The effective hops probability distributing leaving initial location.
The probability for leaving station initial location \( d \) \( (d < h_{walk}) \) hops, after \( h_{walk} \) random walk steps

\[
P = e^{-\frac{d^2}{h_{walk}}} - e^{-\frac{(d+1)^2}{h_{walk}}} \quad (2)
\]

\[
P = e^{-h_{walk}} \quad (3)
\]

Fig. 2 is the probability of \( h_{walk} = 10 \) hops.

![Figure 2. The Probability of \( h_{walk} = 10 \) hops.](image)

**GRWS**

GRWS is presented to avoid random walks not leaving initial location. The sensor of GRWS does not know station-location, forwarding data through path and storing at pass nodes. For getting data from the local nodes sporadically, the station moves in WSN.

Finding object, the sensor will report to the station. The messages are encrypted and forwards through path. Receiving data, any node will store a copy locally.

Station moves randomly to get data in WSN and never reached the location before.

**Performance Analysis**

The section will compare the performance of RDCS and GRWS on liking consumption and delivery latency.

To avoid a sensor has only few neighboring, the simulation WSN is consist of \( n = 10000 \) nodes. The sensors are uniformly distributed in a \( 100 \times 100 \) grids. The packet collisions are ignored.

**Performance Analysis**

(1) **Safety**

In GRWS, the station moves to get data in WSN with \( n \) nodes, the probability is \( 1/n \) by adversary captured. But in RDCS, based on formula (1), the probability is less than \( 1/n \) by adversary captured.

(2) **Consumption**

Consumption are the same for GRWS and random data collection scheme.
(3) Delivery latency

![Graph showing delivery latency comparison between GRWS and RDCS](image)

Figure 3. Getting Data Average Probability for Station.

The delivery latency for GRWS and RDCS lies on mobile-station. In GRWS, if stored data nodes are n and WSNs have N nodes, then the probability of station get data is \( \frac{n}{N} \). If least hops between stored data node and mobile-station is n, then in RDCS, the probability of station get data is \( \left(\frac{1}{4}\right)^n \). GRWS has less delivery latency.

Conclusions

GRWS has established to protect MSL privacy. Compared to RDCS, providing satisfactory MSL privacy, GRWS has smaller the data delivery latency. The comparison of GRWS with RDCS shows that it can get a less delivery latency probability while increasing safety and same energy usage.

Acknowledgements

This research was supported by the Doctor Fund project of Hezhou University under grant HZUBS201809.

References

[1] Gao, Yuan, Ao, Hong, Feng, Zenghui, Zhou, Weigui, Hu, Su,Tang, Wanbin.Mobile Network Security and Privacy in WSN[J].Procedia Computer Science, 2018, 129:324-330.

[2] Han, Meng, Li, Lei, Xie, Ying, Wang, Jinbao, Duan, Zhuojun,Li, Ji, Yan, Mingyuan.Cognitive Approach for Location Privacy Protection[J].IEEE Access, 2018:1-1.

[3] Gao, Kun, Zhu, Yiwei, Gong, Songjie, Tan, Hengsong. Location privacy protection algorithm for mobile networks[J]. EURASIP Journal on Wireless Communications and Networking, 2016, 2016(1):205.

[4] Huang Changqin, Ma Ming, Liu Yuxin, Liu Anfeng .Preserving Source Location Privacy for Energy Harvesting WSNs[J].Sensors, 2017,17(4):724-.
[5] Huang Changqin, Ma Ming, Liu Yuxin, Liu Anfeng. Preserving Source Location Privacy for Energy Harvesting WSNs[J]. Sensors, 2017, 17(4):724-.

[7] Wu, Hao, Hu, Yih-Chun. Location Privacy with Randomness Consistency[J]. Proceedings on Privacy Enhancing Technologies, 2016, 2016(4)

[8] Shokri, Reza, Theodorakopoulos, George, Troncoso, Carmela. Privacy Games Along Location Traces[J]. ACM Transactions on Privacy and Security, 2016, 19(4):1-31.

[9] Li, Yanhui, Cao, Xin, Yuan, Ye, Wang, Guoren. PrivSem: Protecting location privacy using semantic and differential privacy[J]. World Wide Web, 2019.

[10] Galdames, Patricio, Gutierrez-Soto, Claudio, Curiel, Arturo. Batching Location Cloaking Techniques for Location Privacy and Safety Protection[J]. Mobile Information Systems, 2019, 2019:1-11.

[11] Liang Yi, Cai Zhipeng, Han Qilong, Li Yingshu. Location Privacy Leakage through Sensory Data[J]. Security and Communication Networks, 2017, 2017:1-12.

[12] Ye, Hang, Han, Kai, Xu, Chaoting, Xu, Jingxin, Gui, Fei. Toward location privacy protection in Spatial crowdsourcing[J]. International Journal of Distributed Sensor Networks, 2019, 15(3).

[13] Zhang Tingting, Li Xiaojing, Zhang Qinyu. Location Privacy Protection: A Power Allocation Approach[J]. IEEE Transactions on Communications, 2018:1-1.

[14] E. C.-H. Ngai and I. Rodhe, On Providing Location Privacy for Mobile Sinks in WSN, 12th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM’09), 26-30 October 2009, Tenerife, Canary Islands, Spain.