Juni Khyat
(UGC Care Group I Listed Journal)
ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

A Probabilistic Source Location Privacy Protection Scheme in Wireless Sensor Networks

[1] **P. Vijaya bhaskar Reddy** [2] **P. Vennelamma**

[1] *Associate Professor, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.*

[2] *PG Scholar, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.*

Abstract—With the recent developments of Wireless Sensor Networks (WSNs), computing and communication have experienced huge advancement. Meanwhile, security has not received the same attention to go along with such developments. We focus on the source location privacy problem in WSNs, a hot research topic in security, and propose a probabilistic source location privacy protection scheme (PSLP) for WSNs. A more powerful adversary, which can use Hidden Markov Model (HMM) to estimate the state of the source, is considered in this study. To cope with this type of adversary, phantom nodes and fake sources, which are responsible to mimic the behavior of the source,are utilizedtodiversify the routing path.Then, theweight of each node is calculated as a criterion to select the next-hop candidate. In addition, two transmission modes are designed to transmit real packets. The simulation results demonstrate that the proposed PSLP scheme improves the safety time without compromising the energy consumption.

Keywords—Wireless sensor networks, source location privacy, phantom node, fake source.

I.INTRODUCTION

Wireless Sensor Networks (WSNs) consist of numerous sensorconsists of service like information authentication event awarenessand node charging These nodes play the role of microcomputer and are distributed in various environments. There are a lot of data transmissions and communication behaviors between nodes. So, such as data privacy and location privacy . Data privacy can be protected by encryption algorithms while location privacy cannot be protected to the extreme. Due to the time correlation in data transmission between two nodes, the adversary can infer location information through analysis. From a time, correlation perspective, location privacy consists of the source location privacy and the sink location privacy.

we focus on the source location privacy, which is an emerging research topic in the field of security. There are many techniques, like secure routing , fake sources , phantom nodes , fake cloud , and cluster.That can be applied to protect the source location privacy. We propose a probabilistic source location privacy protection scheme (PSLP), which adopts phantom nodes and fake sources for the reason that these two techniques can diversify the routing path. The steps of PSLP are as follows:

- Both phantom nodes and fake sources are integrated into the proposed PSLP, which enhance the source location privacy.
- A more powerful local adversary, which can use Hidden Markov Model to estimate the state of the source, is taken into consideration.
- Two data transmission modes are designed based on the distance between the source and the sink, which further enhance the source location privacy.

II. BACKGROUND WORK

Many researchers have paid attention to the location privacy since Ozturk first proposed his concept . Recently, location privacy has been widely researched in industrial wireless sensor networks , vehicular ad-hoc networks , cloud computing , social network and so on.

Location privacy covers the source location privacy and the sink location privacy. we focus on the source location privacy protection. Manjula et al. used virtual sources to protect the source location privacy . In their scheme, a routing technique was proposed to maximize the safety time. By adding random walk into the routing process, nodes in non-hotspot areas participated in the establishment of multiple routing paths. Hence, the safety time increased without influencing the network lifetime.

We proposed two algorithms using fake sources to protect the source location privacy . In the first algorithm, fake sources were dynamically deployed around the sink. Then, the sink used flooding to select fake sources. This algorithm can provide a good source location privacy at the expense of the huge energy consumption. To cope with this, another algorithm called dynamic single path routing algorithm (DynamicSPR) was proposed.

To considered a more powerful adversary and proposed a privacy enhancing routing algorithm to protect location privacy . In their research, a global adversary using Bayesian maximum-a-posteriori (MAP) estimation strategy tried to monitor the communication between nodes. Then, a decision-making framework was put forward to reduce the adversary's detection probability. Finally, the problem was converted into the adjustment of parameters.

We focused on the energy utilization rate in WSNs while maintaining the source location privacy. They proposed a redundancy branch-based source location privacy scheme. In their scheme, many redundancy branches were generated from the source to the sink. The number of branches was determined by the energy collected by nodes.

To proposed a constrained random walk mechanism. In their mechanism, a next-hop candidate selection domain was generated based on the offset angle of current node's neighbors and the danger distance, which made the selection domain look like an ellipse. Then, the weight of each node in the domain was calculated by the ratio between a current node's offset angle and the sum of total offset angle.

An utilized phantom nodes and proposed a limited flooding algorithm to protect the source location privacy . The limited flooding was performed by the source to get the information of nodes in the limited flooding area. Then, nodes on the edge of the limited flooding area were chosen as phantom nodes to simulate the function of the source.

proposed a scheme using random intermediate nodes and ring to protect the source location privacy. First, the authors introduced the criteria to quantitatively measure the source location information leakage. Then, to reduce the leakage probability, random intermediate nodes were added to make the routing path disperse.

In this scheme, the sink was located in the center of the network and regions were generated around the sink. The transmission between regions was implemented by a set of relay nodes which were selected strategically. These strategic relay nodes took up two regions and were responsible for forwarding packets to the sink.

considered the source location privacy against a new type of adversary in . The adversary model had two properties, global and local. Under normal circumstances, the adversary was a local adversary. When a potential area where the source may stay was located, the adversary became a global adversary in this area. To cope with it, a message mapping sharing method was presented and a cloud containing many dummy packets was created around the source to hide the location.

Considering the time correlation during the transmission between sensor nodes, Mayank et al. used the data mule to protect the source location privacy . Data mule worked as the mobile data collection unit and collected data when the source was in its communication radius. In this condition, the source location privacy was changed into the protection of the mule's moving track. Then, the authors proposed three extended versions of angle-based scheme to protect the source location. However, since the mule moved grid by grid, the protection of the mule was not given enough attention. There was still a lot of research space in reducing the time correlation.

III. PROPOSED WORK

- . we focus on the source location privacy protection. In their scheme, a routing technique was proposed to maximize the safety time. By adding random walk into the routing process, nodes in non-hotspot areas participated in the establishment of multiple routing paths. Hence, the safety time increased without influencing the network lifetime.
- proposed two algorithms using fake sources to protect the source location privacy [8]. In the first algorithm, fake sources were dynamically deployed around the sink. Then, the sink used flooding to select fake sources. This algorithm can provide a good source location privacy at the expense of the huge energy consumption. To cope with this, another algorithm called dynamic single path routing algorithm (DynamicSPR) was proposed.

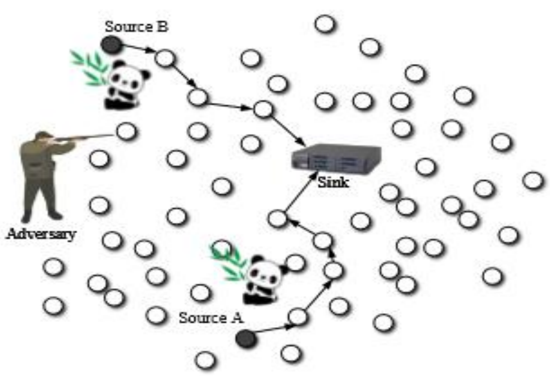

Fig. 1: The Panda-Hunter model.

IV. RESULTS AND DISCUSSION

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

In this section, four metrics are evaluated in the simulation, namely, the safety time, the energy consumption, the network lifetime, and the transmission delay. First of all, we give the definition of each metric. The safety time is the difference between the time when the source sends the first packet and when the adversary finds the source's location. To be more specific, we use the hop count of backtracking taken by the adversary to represent the safety time. The energy consumption represents the average energy costed per simulation run. As control packets only take up very little energy, so we ignore this part and mainly focus on the energy consumption during packets transmission. The network lifetime refers to the time difference between the network establishment and the death of the first node. The transmission delay means the average packet transmission and the data processing time per simulation run.

PSLP is compared with two other schemes, which are the dynamic single path routing algorithm (DynamicSPR) [8] and the enhanced protocol for source location protection (SLPE) . DynamicSPR uses fake sources to protect the source location, while the SLP-E adopts phantom nodes to implement this. These two methods are integrated in PSLP.

The longer the safety time, the safer the network is. As two cases and fake sources are taken into consideration (as mentioned in Section IV), the safety time is different on both sides of the threshold T between the source and the sink, which looks like a split point. As shown in Fig. 1, when the hop count between the source and the sink is five (which is the pre-set threshold), there is an obvious decline. This is because the transmission of packets changes when the hop count is larger than five. When the hop count is larger than five, the next-hop candidate is selected by the weight of nodes, so the safety time is stabilized due to the fact that packets are routed towards the sink.

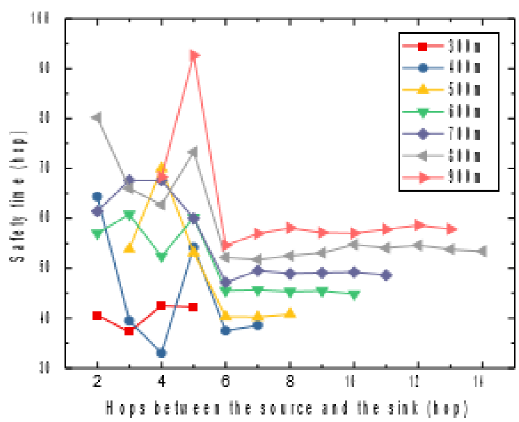

Fig.2: Safety time versus various hopes between the source and the sink

communication radius. When the hop count is larger than five, nodes on the routing path are selected by the weight and, therefore, the energy consumption is stabilized. When the hop count is less than five, the randomness of the selection of phantom nodes makes the energy consumption fluctuate. In addition, the weight is considered in the selection of the nexthop candidates, and as a result each node's next-hop candidate may change. So the energy consumption is balanced in each node.

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

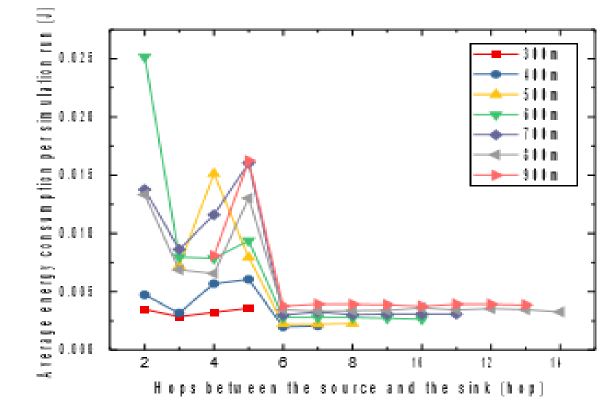

Fig.3: Average energy consumption versus various hopes between the source and the sink

Infigure 3 shows the energy consumption per simulation run. The X and Y axes are the network side length in meter, while the Z axis is the residual energy of each node per transmission in Joule. The white area indicates that the node has consumed energy, which are responsible for the transmission from the source to the The 3-D residual energy distribution of two transmission modes is presented in Fig. 3. Considering there are two transmission modes in PSLP.

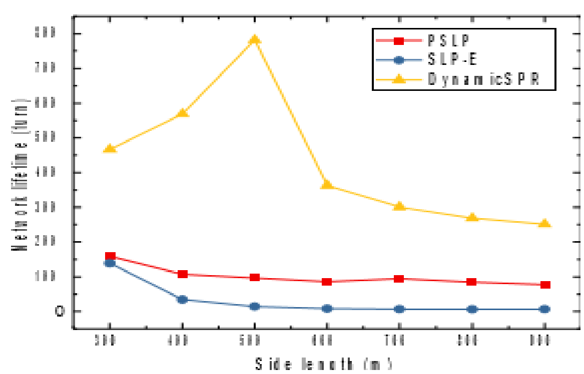

Fig.4: Network life time of three schemes

V. CONCLUSION

We focused on the source location privacy, a research hotspot in security, and proposed a probabilisticsourcelocation privacy protection scheme(PSLP) based on WSNs. A powerful adversary which utilizes Hidden Markov Model (HMM) is considered in this study. To cope with it, phantom nodes, fake sources,

and weight are adopted to changethepackets' transmission directions.Considering the distance between the source and the sink, two types of routing modes are designed. Compared with DynamicSPR and SLPE, the simulation results demonstrate that the proposed PSLP achieves a high safety time and balances the energy consumption of each node. Future studies will concentrate on protecting the source location by reducing the adversary's monitoring probability and secure communication among nodes.

REFERENCES

1. H. Lu and J. Li, "Privacy-preserving authentication schemes for vehicular ad hoc networks: a survey," Wireless Communications and Mobile Computing, vol. 16, no. 6, pp. 643-655, Apr. 2016.
2. G. Han, X. Yang, L. Liu, S. Chan, and W. Zhang, "A Coverage Aware Hierarchical Charging Algorithm in Wireless Rechargeable Sensor Networks," IEEE Network Magazine, pp. 1-7, Nov. 2018, DOI: 10.1109/MNET.2018.1800197.
3. G. Han, H. Guan, J. Wu, S. Chan, L. Shu, and W. Zhang, "An Uneven Cluster-Based Mobile Charging Algorithm for Wireless Rechargeable Sensor Networks," IEEE Systems Journal, pp. 1-12, Nov. 2018, DOI: 10.1109/JSYST.2018.2879084
4. G. Han, H. Wang, J. Jiang, W. Zhang, and S. Chan, "CASLP: A Confused Arc-Based Source Location Privacy Protection Scheme in WSNs for IoT," IEEE Communications Magazine, vol. 56, no. 9, pp. 42-47, Sept. 2018.
5. H. Lu, J. Li, and M. Guizani, "Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 3, pp. 750-761, Mar. 2014.
6. G. Han, L. Zhou, H. Wang, W. Zhang, and S. Chan, "A Source Location Protection Protocol Based on Dynamic Routing in WSNs for Social Internet of Things," Future Generation Computer Systems, vol. 82, no. 5, pp. 689-697, Aug. 2018.
7. H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Clusterbased Wireless Sensor Networks Using ID-based Digital Signature," Proceedings of IEEE Global Communications Conference, Dec. 2010.
8. M. Bradbury, A. Jhumka, and M. Leeke, "Hybrid online protocols for source location privacy in wireless sensor networks," Journal of Parallel and Distributed Computing, vol. 115, pp. 67-81, May 2018. [9] J. Chen, Z. Lin, Y. Hu, and B. Wang, "Hiding the Source Based on Limited Flooding for Sensor Networks," Sensors, vol. 15, no. 11, pp. 29129-29148, Nov. 2015.
9. 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 Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2739-2750, Jan. 2019.
10. G. Han, H. Wang, M. Guizani, S. Chan, and W. Zhang, "KCLP: A kmeans Cluster-Based Location Privacy Protection Scheme in WSNs for IoT," IEEE Wireless Communications Magazine, vol. 25, no. 6, pp. 84-90, Dec. 2018.

11. C. Ozturk, Y. Zhang, and W. Trappe, “Source-Location privacy in energy-constrained sensor network routing,” ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 88-93, Jan. 2004.
12. J. Wang, R. Zhu, S. Liu, and Z. Cai, “Node Location Privacy Protection Based on Differentially Private Grids in Industrial Wireless Sensor Networks,” Sensors, vol. 18, no. 2, pp. 410-425, Jan. 2018.
13. A. Boualouache, S. Senouci, and S. Moussaoui, “A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks,” IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 770-790, First quarter. 2018.
14. Y. Gong, C. Zhang, Y. Fang, and J. Sun, “Protecting Location Privacy for Task Allocation in Ad Hoc Mobile Cloud Computing,” IEEE Transactions on Emerging Topics in Computing, vol. 6, no. 1, pp. 110-121, Mar. 2018.
15. J. Du, C. Jiang, K. Chen, Y. Ren, and H.V. Poor, “Community-Structured Evolutionary Game for Privacy Protection in Social Networks,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 574-589, Mar. 2018.
16. R. Manjula and D. Raja, “A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs,” Pervasive and Mobile Computing, vol. 44, pp. 58-73, Feb. 2018.
17. Rajasekar, P. and Mangalam, D. (2016) Efficient FPGA implementation of AES 128 bit for IEEE 802.16e mobile WiMax standards. *Circuits and Systems*, **7**, 371-380. doi: 10.4236/cs.2016.74032.
18. J. Koh, D. Leong, G. Peters, I. Nevat, and W. Wong, “Optimal PrivacyPreserving Probabilistic Routing for Wireless Network,” IEEE TransactionsonInformationForensicsandSecurity,vol.12,no.9,pp.2105-2114, Sept. 2017.
19. W. Chen, M. Zhang, G. Hu, X. Tang, and A. Sangaiah, “Constrained Random Routing Mechanism for Source Privacy Protection in WSNs,” IEEE Access, vol. 5, pp. 23171-23181, Sept. 2017.
20. Y. Li, J. Ren, and J. Wu, “Quantitative measurement and design of source-location privacy schemes for wireless sensor networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 7, pp. 1302-1311, July 2012.
21. L. Mutalemwa and S. Shin, “Strategic Location-Based Random Routing for Source Location Privacy in Wireless Sensor Networks,” Sensors, vol. 18, no. 7, July 2018, DOI:10.3390/s18072291.
22. N. Wang, J. Fu, J. Zeng, and B. Bhargava, “Source-location privacy full protection in wireless sensor networks,” Information Sciences, vol. 444, pp. 105-121, May 2018.
23. R. Mayank, N. Li, D. Liu, W. Matthew, and K. Sajal Das, “Using data mules to preserve source location privacy in Wireless Sensor Networks,” Pervasive and Mobile Computing, vol. 11, pp. 244-260, Apr. 2014.
24. A. Proa˜ no, L. Lazos, and M. Krunz, “Traffic Decorrelation Techniques for Countering a Global Eavesdropper in WSNs,” IEEE Transactions on Mobile Computing, vol. 16, no. 3, pp. 857-871, Mar. 2017.

Author’s Profile:

P. Vijay Bhaskar Reddy has received his PG Degree in Master Of Computer Applications from Geethanjali Institute PG studies, affiliated to SVU, Tirupati in

2008 and he received M.Tech degree in Computer Science from Gokula Krishna College of Engineering, affiliated to JNTU, Anantapur. At present he is the Head of the Dept. of MCA&Associate Professor in Narayana Engineering College, Gudur, Andhra Pradesh, India.

P. Vennelamma has received her Bsc degree in Computer Science from Sri Srinivasa Degree College,Balayapalli affiliated to Vikrama Simhapuri University,Nellore in 2017.And pursuing PGdegree in Master of Computer Applications from Narayana Engineering college, Gudur affiliated to Jntu Anantapur,Andhra Pradesh, India.