IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

Protecting Location Privacy in Sensor Networks against a Global Eaves Dropper

C. Ragavi[1*], R. Meera[2]

[1]M.Sc Computer Science, Idhaya College for Women, Kumbakonam, Tamilnadu, India
[2]Department of Computer Science, Idhaya College for Women, Kumbakonam, Tamilnadu, India

Corresponding Author: meera2992@gmail.com

Available online at: www.ijcseonline.org

***Abstract*—**The sensor network security provide confidentiality for the content of messages, contextual information usually remains exposed. Such contextual information can be exploited by an adversary to derive sensitive information such as the locations of monitored objects and data sinks in the field. Attacks on these components can significantly undermine any network application. Existing techniques defend the leakage of location information from a limited adversary who can only observe network traffic in a small region. However, a stronger adversary, the global eavesdropper, is realistic and can defeat these existing techniques. This paper first formalizes the location privacy issues in sensor networks under this strong adversary model and computes a lower bound on the communication overhead needed for achieving a given level of location privacy. This system then proposes two techniques to provide location privacy to monitored objects (source-location privacy) periodic collection and source simulation and two techniques to provide location privacy to data sinks (sink-location privacy) sink simulation and backbone flooding. These techniques provide trade-offs between privacy, communication cost, and latency. Through analysis and simulation, this project demonstrates that the proposed techniques are efficient and effective for source and sink-location privacy in sensor networks.

***Keywords*—**Wireless Sensor Network, Sink Simulation, Location Privacy, Eaves Dropper.

I. INTRODUCTION

A wireless sensor network (WSN) typically consists of a large number of small, multifunctional, and resource constrained sensors that are self-organized as an ad hoc network to monitor the physical world. Sensor networks are often used in applications where it is difficult or infeasible to set up wired networks. Examples include wildlife habitat monitoring, security and military surveillance, and target tracking. For applications like military surveillance, adversaries have strong incentives to eavesdrop on network traffic to obtain valuable intelligence. Abuse of such information can cause monetary losses or endanger human lives. To protect such information, researchers in sensor network security have focused considerable effort on finding ways to provide classic security services such as confidentiality, authentication, integrity, and availability. Though these are critical security requirements, they are insufficient in many applications. The communication patterns of sensors can, by themselves, reveal a great deal of contextual information, which can disclose the location information of critical components in a sensor network. For example, in the Panda-Hunter scenario, a sensor network is deployed to track endangered giant pandas in a bamboo forest. Each panda has an electronic tag that emits a signal that can be detected by the sensors in the network. A sensor that detects this signal, the source sensor, then sends the location of pandas to a data sink (destination) with help intermediate sensors. An adversary (the hunter) may use the communication between sensors and the data sinks to locate and then capture the monitored pandas. In general, any target-tracking sensor network is vulnerable to such attacks. As another example, in military applications, the enemy can observe the communications and locate all data sinks (e.g., base stations) in the field. Disclosing the locations of the sinks during their communication with sensors may allow the enemy to precisely launch attacks against them and thereby disable the network. Location privacy is, thus, very important, especially in hostile environments. Failure to protect such information can completely subvert the intended purposes of sensor network applications. Location privacy measures, thus, need to be developed to prevent the adversary from determining the physical locations of source sensors and sinks. Due to the limited energy lifetime of battery-powered sensor nodes, these methods have to be energy efficient. Since communication in sensor networks is much more expensive than computation, we use communication cost to measure the energy consumption of our protocols. Providing location privacy in a sensor network is challenging. First, an adversary can easily intercept

network traffic due to the use of a broadcast medium for routing packets. He can use information like packet transmission time and frequency to perform traffic analysis and infer the locations of monitored objects and data sinks. Second, sensors usually have limited processing speed and energy supplies. It is very expensive to apply traditional anonymous communication techniques for hiding the communication between sensor nodes and sinks. It needs to find alternative means to provide location privacy that accounts for the resource limitations of sensor nodes.

II. METHODOLOGY

Data Collection

Most of the existing works on location privacy has been an active area of research in recent years. In location-based services, a user may want to retrieve location-based data without revealing her location. Techniques such as k-anonymity [2] and private information retrieval [10] have been developed for this purpose. In pervasive computing, users' location privacy can be compromised by observing the wireless signals from user devices [24], [27]. Random delay and dummy traffic have been suggested to mitigate these problems. Location privacy in sensor networks also falls under the general framework of location privacy. The adversary monitors the wireless transmissions to infer locations of critical infrastructure.

However, there are some challenges unique to sensor networks. First, sensor nodes are usually battery powered, which limits their functional lifetime. Second, a sensor network is often significantly larger than the network in smart home or assisted living applications. Prior work in protecting the location of monitored objects sought to increase the safety period, i.e., the number of messages sent by the source before the object is located by the attacker [15]. The flooding technique [20] has the source node send each packet through numerous paths to a sink, making it difficult for an adversary to trace the source. Fake packet generation [15] creates fake sources whenever a sender notifies the sink that it has real data to send. The fake senders are away from the real source and approximately at the same distance from the sink as the real sender. Phantom single-path routing [15] achieves location privacy by making every packet walk along a random path before being delivered to the sink. Cyclic entrapment [19] creates looping paths at various places in the network to fool the adversary into following these loops repeatedly and thereby increase the safety period. However, all these techniques assume a local eavesdropper who is only capable of eavesdropping on a small region. A global eavesdropper can easily defeat these schemes by locating the first node initiating the communication with the base station. several techniques have been proposed to deal with global eavesdroppers. Yang et al. propose to use proxies to shape the network traffic such that global eavesdroppers cannot infer the locations of monitored objects [29]. Shao et al. propose to reduce the latency of real events without reducing the location privacy under a global eavesdropper [26]. This technique ensures that the adversary cannot determine the real traffic from statistical analysis. In [6], Deng et al. described a technique to protect the locations of sinks from a local eavesdropper by hashing the ID field in the packet header. In [8], it was shown that an adversary can track sinks by carrying out time correlation and rate monitoring attacks.

Data Evaluation

There are two types of routing in opportunistic approach mesh based pull and tree-based push methods. The pull methods use swarming content delivery. Each node advertises to its neighbors which messages it has received and the neighbors explicitly request messages if needed. Two representative pull schemes are Chainsaw and PRIME. PRIME incorporates swarming into streaming applications and points out the design tradeoffs of such systems. To achieve a low delay, a node in such systems should advertise as soon as it receives a new message, increasing the control overhead greatly. The tree-based push methods achieve a fast dissemination with low overhead. The main concern is the vulnerability to node failures. Our CRP method falls into this type. The CRP extracts dissemination tree from a churn-resilient overlay, which provides sufficient alternative overlay links for tree to achieve good fault resilience. The preliminary idea was reported in an IEEE IPDPS-2008 paper. In an existing network, the link latency is measurable. The node capacity of a node represents the maximum number of adjacent nodes to which it can forward the data items, concurrently. Anode's out degree is bounded by its capacity, the notations used in these existing papers. The proximity-aware overlay is built around a unidirectional ring with extra bidirectional chord links. The overlay is heterogeneous since links are associated with different weights. A node's neighbors are those that are directly connected by either ring or chord links with it, while its chord neighbors are those that are connected by chord links. Initially, the base ring is assumed empty before any node joining the system. The first node is located at any position on the base ring. Most of the existing protocols apply both network proximity and capacity proximity in CRP protocol. The network proximity is measured by the latency or closeness of two nodes in physical IP networks. This proximity enables faster transferring data items. The capacity proximity is measured by the closeness of nodes with respect to node capacities. The capacity proximity allows us to put high-capacity nodes at higher positions on delivery trees, which reduces the delivery hop count. Most of the extensive work on resource allocation in wireless ad-hoc networks focuses on one-way communication. There are, however, several recent publications on wireless adhoc networks that focus on two-way communication including. In particular existing systems provides bidirectional routing abstractions (called BRA) for

mobile ad hoc networks by maintaining multi-hop reverse routes for unidirectional links, addresses power control for sensor networks to ensure the connectivity graph has bidirectional links, discusses coding approaches for bidirectional broadcast channels, combines physical layer coding with network coding for bidirectional relaying, and uses a type of network coding called "reverse carpooling" tailored to bidirectional communication. In contrast to the existing systems is distinct from the above works in that *i*) our focus is on statistical characterization of spatial reuse under a bidirectionality constraint as opposed to bidirectional coding and/or routing, ii) our transmission capacity metric is distinct from the above which focus on throughput, delay, and coding rates, and *iii*) our primary tool is leveraging the statistical properties of the assumed transmitter locations.

III. METHODOLOGY

The proposed system is on privacy-preserving communication methods in the presence of a global eavesdropper who has a complete view of the network traffic. In this system, consider a homogeneous network model. In the homogeneous network model, all sensors have roughly the same computing capabilities, power sources, and expected lifetimes. This is common network architecture for many applications today and will likely continue to be popular moving forward. It is well studied and provides relatively straightforward analysis in research as well as simple deployment and maintenance in the field. Although our research can be applied to a variety of sensor platforms, most sensors run off battery power, especially in the kinds of potentially hostile environments that are under study. Given this, each sensor has a limited lifespan and the network must be designed to preserve the sensors' power reserves. It has been demonstrated that sensors use far more battery power transmitting and receiving wireless communications than any other type of operation. Thus, we focus our evaluation on the amount of communication overhead incurred by our protocols. For the kinds of sensor networks that we envision, we expect highly motivated and well-funded attackers whose objective is to learn sensitive information such as the locations of monitored objects and sinks. The objects monitored by the network can be critical. Such objects could be soldiers, vehicles, or robots in a combat zone, security guards in a protected facility, or endangered animals in the wild. If the locations of these objects were known to an adversary, the endangered animals could be captured for profit, security guards could be evaded to enable theft of valuable property, and military targets could be captured or killed. Sinks are also critical components of sensor network. In most applications, sinks act as gateways between the multihop network of sensor nodes and the wired network or a repository where the sensed information is analyzed. Unlike the failure of a subset of the sensors, the failure of a sink can create permanent damage to sensor network applications. Compromise of a sink will allow an adversary to access and manipulate all the information gathered by the sensor network, because in most applications, data are not encrypted after they reach a sink. In some military applications, an adversary could locate sinks and make the sensor network nonfunctional by destroying them. Thus, it is often critical to the mission of the sensor network to protect the location information of monitored objects as well as data sinks.

- It points out that the assumption of a global eavesdropper who can monitor the entire network traffic is often realistic for highly motivated adversaries. We then formalize the location privacy issues under such an assumption and apply an analysis based on Steiner trees to estimate the minimum communication cost required to achieve a given level of privacy.

- So this system provides the first formal study of how to quantitatively measure location privacy in sensor networks. We then apply the results of this study to evaluate our proposed techniques for location privacy in sensor networks. These include two techniques that hide the locations of monitored objects periodic collection and source simulation and two techniques that provide location privacy to data sinks simulation and backbone flooding. Our analysis and simulation studies show that these approaches are effective and efficient.

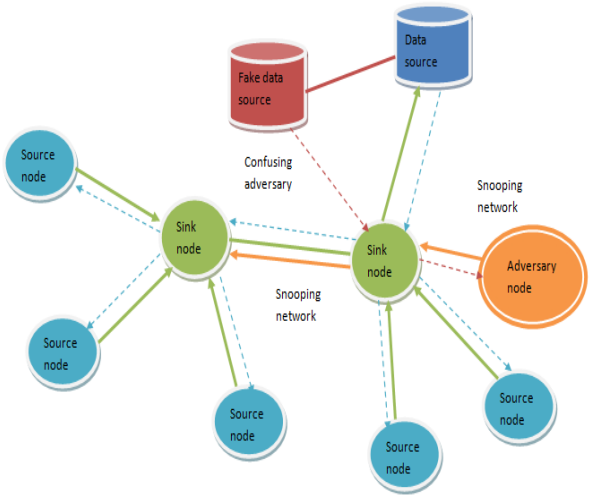

FIGURE 1: SYSTEM ARCHITECTURE

IV. CONCLUSION

The location privacy issues under a global eavesdropper and estimated the minimum average communication overhead needed to achieve a given level of privacy. This project presented techniques to provide location privacy to objects and sinks against a global eavesdropper. This system

analyzed and simulation to show how well these techniques perform in dealing with a global eavesdropper. The global eavesdropper does not compromise sensor nodes. The global eavesdropper may be able to compromise a subset of the sensor nodes in the field and perform traffic analysis with additional knowledge from insiders. It takes time for the observations made by the adversarial network to reach the adversary for analysis and reaction.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[2] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacygrid," Proc. Int'l Conf. World Wide Web (WWW '08), 2008.

[3] BlueRadios Inc., "Order and Price Info," http://www.blueradios.com/orderinfo.htm, Feb. 2006.

[4] B. Bollobas, D. Gamarnik, O. Riordan, and B. Sudakov, "On the Value of a Random Minimum Weight Steiner Tree," Combinatorica, vol. 24, no. 2, pp. 187-207, 2004.

[5] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp. Security and Privacy (S&P '03), pp. 197-213, May 2003.

[6] J. Deng, R. Han, and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Technical Report CU-CS-951-03, Univ. of Colorado, Dept. of Computer Science, 2003.

[7] J. Deng, R. Han, and S. Mishra, "Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks," Proc. Int'l Conf. Dependable Systems and Networks (DSN '04), June 2004.

[8] J. Deng, R. Han, and S. Mishra, "Decorrelating Wireless Sensor Network Traffic to Inhibit Traffic Analysis Attacks," Pervasive and Mobile Computing J., Special Issue on Security in Wireless Mobile Computing Systems, vol. 2, pp. 159-186, Apr. 2006.

[9] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security (CCS '02), Nov. 2002.

[10] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.L. Tan, "Private Queries in Location Based Services: Anonymizers are not Necessary," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '08), 2008.

[11] H. Gupta, Z. Zhou, S. Das, and Q. Gu, "Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution," IEEE/ACM Trans. Networking, vol. 14, no. 1, pp. 55-67, Feb. 2006.

[12] J. Hill, M. Horton, R. Kling, and L. Krishnamurthy, "The Platforms Enabling Wireless Sensor Networks," Comm. ACM, vol. 47, no. 6, pp. 41-46, 2004.

[13] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting Receiver-Location Privacy in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 1955-1963, May 2007.

[14] D.B. Johnson, D.A. Maltz, Y. Hu, and J.G. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," IETF Internet draft, Feb. 2002.

[15] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," Proc. Int'l Conf. Distributed Computing Systems (ICDCS '05), June 2005.

[16] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security (CCS '03), Oct. 2003.

[17] K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks against a Global Eavesdropper," Proc. IEEE Int'l Conf. Network Protocols (ICNP '07), 2007.

[18] D. Niculescu and B. Nath, "Ad Hoc Positioning System (APS) Using AoA," Proc. IEEE INFOCOM, pp. 1734-1743, Apr. 2003.

[19] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "Entrapping Adversaries for Source Protection in Sensor Networks," Proc. Int'l Conf. World of Wireless, Mobile, and Multimedia Networking (WoWMoM '06), June 2006.

[20] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy-Constrained Sensor Network Routing," Proc. Workshop Security of Ad Hoc and Sensor Networks (SASN '04), Oct. 2004.

[21] V. Paruchuri, A. Duressi, M. Duressi, and L. Barolli, "Routing through Backbone Structures in Sensor Networks," Proc. 11th Int'l Conf. Parallel and Distributed Systems (ICPADS '05), 2005.

[22] C.E. Perkins, E.M. Belding-Royer, and S.R. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," IETF Internet draft, Feb. 2003.

[23] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proc. ACM MobiCom, July 2001.

[24] T.S. Saponas, J. Lester, C. Hartung, S. Agarwal, and T. Kohno, "Devices that Tell on You: Privacy Trends in Consumer Ubiquitous Computing," Proc. USENIX Security Symp., 2007.

[25] A. Savvides, C. Han, and M. Srivastava, "Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors," Proc. ACM MobiCom, July 2001.

[26] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE INFOCOM, 2008.

[27] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting Your Daily In-Home Activity Information from a Wireless Snooping Attack," Proc. Int'l Conf. Ubiquitous Computing (UbiComp '08), 2008.

[28] H. Takahashi and A. Matsuyama, "An Approximate Solution for the Steiner Problem in Graphs," Math.Japonica, vol. 24, pp. 573-577, 1980.

[29] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks," Proc. ACM Conf. Wireless Network Security (WiSec '08), 2008

