International Journal of Computer Science Engineering & Technology
IJCSET
Approved by
National Science Library (NSL)
National Institute of Science Communication and Information Resources (NISCAIR)
Council of Scientific and Industrial Research (CSIR)– New Delhi. India .
ISSN :2455-9091

LOCATION PRIVACY-PRESERVING ROUTING FOR PROTECTING VULNERABLE WSN FROM UNIVERSAL EAVESDROPPER

[1] A.Dhivya, [2] Dr.A.Suphalakshmi, M.E.,Ph.D.,
[1, 2] PG ScholarHead of the department in computer science,
[1, 2] Paavai Engineering CollegePaavai Engineering College.

ABSTRACT: While many protocols for sensor network security provide confidentiality for the content of messages, contextual information usually remains exposed. Such information can be critical to the mission of the sensor network, such as the location of a target object in a monitoring application, and it is often important to protect this information as well as message content. There have been several recent studies on providing location privacy in sensor networks. First argue that a strong adversary model, the global eavesdropper, is often realistic in practice and can defeat existing techniques. And then formalize the location privacy issues under this strong adversary model and show how much communication overhead is needed for achieving a given level of privacy. Also, it propose two techniques that prevent the leakage of location information: periodic collection and source simulation. Periodic collection provides a high level of location privacy, while source simulation provides trade-offs between privacy, communication cost, and latency. Through analysis and simulation, then demonstrate that the proposed techniques are efficient and effective in protecting location information from the attacker.

KEY WORDS: [Wireless sensor Network (WSN), Location privacy routing (LPR), Proxy-based Filtering Scheme (PFS) and Tree-based Filtering Scheme (TFS).]

1. INTRODUCTION

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. Recently, several techniques have been proposed to deal with global eavesdroppers.

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, use communication cost to measure the energy consumption of the protocols.

Providing location privacy in a sensor network is very challenging. First, an adversary can easily intercept network traffic due to the use of a broadcast medium for routing packets. Who 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. Need to find alternative means to provide location privacy that accounts for the resource limitations of sensor nodes.

These existing solutions can only be used to deal with adversaries who have only a local view of network traffic. A highly motivated adversary can easily eavesdrop on the entire network and defeat all these solutions. For example, the adversary may decide to deploy his own set of sensor nodes to monitor the communication in the target network. However, all these existing methods assume that the adversary is a local eavesdropper. If an adversary has the global knowledge of the network traffic, it can easily defeat these schemes. For example, the adversary only needs to identify the sensor node that makes the first move during the communication with the base station. Intuitively, this sensor node should be close to the location of adversaries' interest. Exiting Privacy Techniques used Source Location Privacy Techniques and Sink Location Privacy Techniques.

Related work

B. Bamba, L. Liu, P. Pesti, and T. Wang said that Supporting Anonymous Location Queries in Mobile Environments with Privacy gridthis paper presents PrivacyGrid - a framework for supporting anonymous location-based queries in mobile information delivery systems. The PrivacyGrid framework offers three unique capabilities. First, it provided a location privacy protection preference profile model, called location P3P, which allows mobile users to explicitly define their preferred location privacy requirements in terms of both location hiding measures (e.g., location k-anonymity and location l-diversity) and location service quality measures (e.g., maximum spatial resolution and maximum temporal resolution). Second, it provides fast and effective location cloaking algorithms for location k-anonymity and location l-diversity in a mobile environment. To develop dynamic bottom-up and top-down grid cloaking algorithms with the goal of achieving high anonymization success rate and efficiency in terms of both time complexity and maintenance cost. A hybrid approach that carefully combines the strengths of both bottom-up and top-down cloaking approaches to further reduce the average anonymization time is also developed. Last but not the least, PrivacyGrid incorporates temporal cloaking into the location cloaking process to further increase the success rate of location anonymization. It also discussPrivacyGrid mechanisms for supporting anonymous location queries. Experimental evaluation shows that the PrivacyGrid approach can provide close to optimal location k-anonymity as defined by per user location P3P without introducing significant performance penalties.

Ying JianShigang Chen Zhan Zhang Liang Zhang described that Protecting Receiver-Location Privacy in Wireless Sensor Networks Due to the open nature of a sensor network, it is relatively easy for an adversary to eavesdrop and trace packet movement in the network in order to capture the receiver physically. After studied the adversary's behavior patterns, it present countermeasures to this problem. And it proposed a location privacy routing protocol (LPR) that is easy to implement and provides path diversity. Combining with fake packet injection, LPR is able to minimize the traffic direction information that an adversary can retrieve from eavesdropping. By making the directions of both incoming and outgoing traffic at a sensor node uniformly distributed, the new defense system makes it very hard for an adversary to perform analysis on locally gathered information and infer the direction to which the receiver locates. Here evaluate our defense system based on three criteria: delivery time, privacy protection strength, and energy cost. The simulation results show that LPR with fake packet injection is capable of providing strong protection for the receiver's location privacy.

H. Chan, A. Perrig, and D. Song described that Random Key Predistribution Schemes for Sensor Networks key establishment in sensor networks is a challenging problem because asymmetric key cryptosystems are unsuitable for use in resource constrained sensor nodes, and also because the nodes could be physically compromised by an adversary. They presented three new mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node. First, in the q-composite keys scheme, trade off the unlikeliness of a large-scale network attack in order to significantly strengthen random key predistribution's strength against smaller-scale attacks. Second, in the multipath-reinforcement scheme, then show how to strengthen the security between any two nodes by leveraging the security of other links. Random-pairwise keys are used. The random-pairwise keys scheme, which perfectly preserves the secrecy of the rest of the network when any node is captured, and also enables node-to-node authentication and quorum-based revocation.

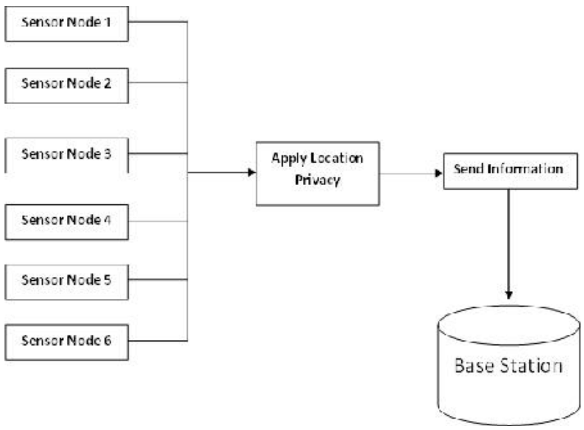
Yi Yang, Min Shao, Sencun Zhu, BhuvanUrgaonkar, Guohong Cao Described that Towards Event Source Unobservability with Minimum Network Traffic in Sensor Network Sensors deployed to monitor the surrounding environment report such information as event type, location, and time when a real event of interest is detected. An adversary may identify the real event source through eavesdropping and traffic analysis. Previous work has studied the source location privacy problem under a local adversary model. In this work, it aims to provide a stronger notion: event source unobservability, which promises that a global adversary cannot know whether a real event has ever occurred even if this is capable of collecting and analyzing all the messages in the network at all the time. Clearly, event source unobservability is a desirable and critical security property for event monitoring applications, but unfortunately it is also very difficult and expensive to achieve for resource-constrained sensor networks. A main idea is to introduce carefully chosen dummy traffic to hide the real event sources in combination with mechanisms to drop dummy messages to prevent explosion of network traffic. To achieve the latter, we select some sensors as proxies that proactively filter dummy messages on their way to the base satiation. Used Techniques: Proxy-based Filtering, Tree-based Filtering Here proposed Proxy-based Filtering Scheme (PFS) and Tree-based Filtering Scheme (TFS) to accurately locate proxies. Simulation results show that the schemes not only quickly find nearly optimal proxy placement.

J. Deng, R. Han, and S. Mishra said that Intrusion Tolerance and Anti- Traffic Analysis Strategies for Wireless Sensor Networks Wireless sensor networks face acute security concerns in applications such as battlefield monitoring. A central point of failure in a sensor network is the base station, which acts as a collection point of sensor data. In this paper, to investigate two attacks that can lead to isolation or failure of the base station. In one set of attacks, the base station is isolated by blocking communication between sensor nodes and the base station, e.g. by DOS attacks. In the second attack, the location of the base station is deduced by analyzing data traffic towards the base station, which can lead to jamming and/or discovery and destruction of the base station. To defend against these attacks, two secure strategies are proposed.

2. METHODOLOGY

The proposed techniques assume a routing protocol for sensor networks, though the choice of routing protocol does not affect the results. Here compare the techniques with the optimal technique. The proposed location privacy techniques in this project have many advantages when compared with each other. Here briefly summarize and understanding of which solutions should be used for different applications. Then also implement the source location privacy and sink location privacy with security access. Here implement the both location privacy in a single phase.

Architecture Diagram



The periodic collection and source simulation methods can be used for providing source location privacy. The periodic collection method provides the highest location privacy and is hence useful when we are monitoring highly valuable objects. Additionally, the communication cost though high does not increase with the number of monitored objects. Thus, it is suitable for applications that collect data at a low rate from the network about many objects. The source simulation method provides a trade-off between privacy and communication costs. It is suitable for scenarios where the object movement pattern can be properly modeled and it need to collect real-time data from the network about the objects. The sink simulation and backbone flooding methods can provide location privacy for the sinks. The backbone flooding method is clearly more suitable for the cases where a high level of location privacy is needed, However, when the required level of location privacy is below a certain threshold, the sink simulation method becomes more attractive, since it is more robust to node failure in the network. In the backbone flooding idea, need to always keep the backbone connected and rebuild the backbone from time to time to balance the communication costs between nodes. Here Proposed Privacy Technique Both Location Privacy and Restrict Techniques.

3. SYSTEM MODULES

1. Attackers Modules.
2. Privacy-Preserving Routing Techniques.
3. Adversary Model
4. Privacy Evaluation Model
5. Security Analysis

PROBLEM DESCRIPTION

1.Attackers Modules

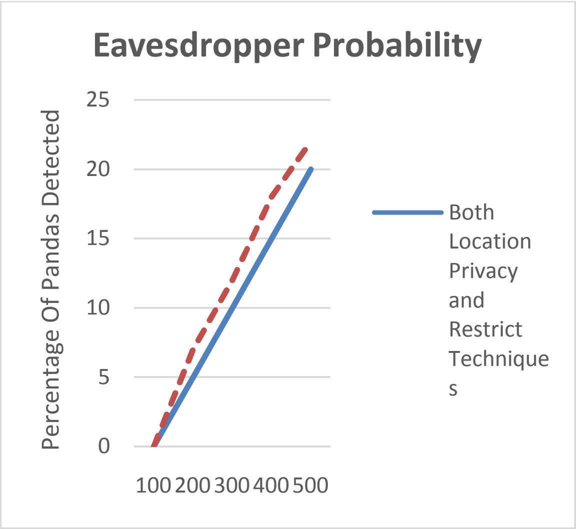
In this module it form the WSN network area and the appearance of an endangered animal (Attackers) in a monitored area that is survived by wireless sensor, at the each time the inside and outside sensors are sensing to find out the attackers location and the timing. This information is passed to the server for analyzing. After analyzing the commander and Hunter they are also can participate this wireless network. In the commander and hunter itself some intruders are there, aim to capture the attackers before attempting the network.

2. Privacy-Preserving Routing Techniques

In this module presents two techniques for privacy preserving routing in sensor networks, a periodic collection method and a source simulation method. The periodic collection method achieves the optimal location privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. The source simulation method provides practical trade-offs between privacy, communication cost, and latency; it can be effectively applied to real-time applications. In this paper, it assume that all communication between sensor nodes in the network is protected by pair wise keys so that the contents of all data packets appear random to the Global eavesdropper. This prevents the adversary from correlating different Data packets to trace the real object.

3. Adversary Model:

For the kinds of wireless sensor networks that envision, it expect highly-motivated and well-funded attackers whose objective is to learn sensitive location-based information. This information can include the location of the events detected by the target sensor network such as the presence of a panda. The Panda-Hunter example application was introduced in, and it will also use it to help describe and motivate our techniques. In this application, 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 clever and motivated poacher could use the communication in the network to help him discover the locations of pandas in the forest more quickly and easily than by traditional tracking techniques. In any case, it should be feasible to monitor the communication patterns and locations of events in a sensor network via global eavesdropping. An attacker with this capability poses a significant threat to location privacy in these networks, and therefore focusto attention for this type of attacker.



Fake Pandas

4. Privacy Evaluation Model:

In this module, it formalize the location privacy issues under the global eavesdropper model. In this model, the adversary deploys an attacking network to monitor the sensor activities in the target network. Then it consider a powerful adversary who can eavesdrop the communication of every Sensor node in the target network. Every sensor node i in the target network is an observation point, which produces an observation (i, t, d) whenever it transmits a packet d in the target network at time t. In this paper, it assume that the attacker only monitors the wireless channel and the contents of any data packet will appear random.

5. SECURITY ANALYSIS:

The generation number of a packet can be hidden in the secure routing scheme through link-to-link encryption. In this way, attackers cannot find the generation number of a packet for their further analysis.

Notice that secure routing paths are only required to be established at the beginning of each session; during the packet transmission, secure routing paths are not required to change or re-established for each new generation.

CONCLUSION

Prior work on location privacy in sensor networks assumed a local eavesdropper. This assumption is unrealistic given a well-funded, highly motivated attacker. In this paper, formalized the location privacy issues under a global eavesdropper and estimated the minimum average communication overhead needed to achieve a given level of privacy. And also presented techniques to provide location privacy to objects and sinks against a global eavesdropper.Then used analysis and simulation to show how well these techniques perform in dealing with a global eavesdropper. There are a number of directions that worth studying in the future. First, in this paper, assume that the global eavesdropper does not compromise sensor nodes. However, in practice, 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. This presents interesting challenges to this methods. Second, it takes time for the observations made by the adversarial network to reach the adversary for analysis and reaction. Studying the impact of such “delayed” analysis and reaction will be another interesting research direction.

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.