Indian Journal of Research in Communication Engineering(IJRCE)
Vol1.No.1 2013 pp 18-23.
available at: www.goniv.com
Paper Received :12-02-2013
Paper Published:10-03-2013
Paper Reviewed by: 1. Prof K. Rajakanna 2. Hendry Goyal
Editor : Prof. P.Muthukumar

ENHANCING SOURCE AND SINK LOCATION PRIVACY IN SENSOR NETWORKS

D. Lakshmi Prabha[1], Mr.M.RajaKani[2]
[1,2]Department of Computer Science Engineering,
Mepco Scehlenk Engineering College,
Sivakasi
lp8394@gmail.com rajakani@gmail.com

ABSTRACT

One of the most notable challenges threatening the successful deployment of sensor systems is privacy. Due to the open nature of a sensor network, it is relatively easy for an adversary to eavesdrop. This paper first formalizes the location privacy issues in sensor networks under this strong adversary model and then proposes two techniques to provide location privacy to source-location privacy(periodic collection and source simulation) and to provide location privacy to data sinks that is sink-location privacy (sink simulation and backbone flooding). The periodic collection method provides the highest location privacy and it is suitable for applications that collect data at a low rate from the network about many objects. In the source simulation approach, a set of fake objects will be simulated in the field. The sink simulation method achieves location privacy by simulating sinks at specified locations and the backbone flooding method provides location privacy by flooding the event reports in a backbone network that covers the data sinks.

Keywords – Sensor networks, location privacy

1.INTRODUCTION

A wireless sensor network (WSN) typically comprises a large number of cheap, small, and resource-constrained sensors that are self-organized as an ad-hoc network to interact with and study the physical world. Sensor networks can be used in applications where it is difficult or infeasible to set up wired networks. Examples include target tracking, habitat monitoring, and military surveillance. These applications are subject to a variety of security issues in hostile environments. Most of the efforts to date in sensor network security have focused on providing classic security services such as confidentiality, authentication, integrity, and availability. While these are critical requirements in many applications, they are not sufficient. The communication patterns of sensors can, by themselves, expose a great deal of contextual information. For example, delivering sensor data to the base station may disclose the locations of some critical events in the field, revealing valuable intelligence.

In hostile environments, it is particularly important to guarantee location privacy; failure to protect location based information can completely undermine network applications. For example, in military applications, disclosure of the locations of soldiers due to nearby sensors communicating with the base station may allow an opposing force to launch accurate attacks against them. Providing location privacy in a sensor network is extremely challenging. On the one hand, an adversary can easily intercept the network traffic due to the use of a broadcast medium for routing packets. He can then perform traffic analysis and identify the source node that initiates the communication with the base station. This can reveal the locations of critical and high- value objects (e.g., soldiers) being monitored by the sensor network. On the other hand, the resource constraints on sensor nodes make it very expensive to apply traditional anonymous

Paper Received :12-02-2013
Paper Published:10-03-2013
Paper Reviewed by: 1. Prof K. Rajakanna 2. Hendry Goyal
Editor : Prof. P.Muthukumar

communication techniques for hiding the communication from a sensor node to the base station. A number of privacy-preserving routing techniques have been developed recently for sensor networks. However, 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. This is particularly true in a military or industrial spying context where there are strong incentives to gain as much information as possible from observing the traffic in the target network. Given a global view of the network traffic, the adversary can easily infer the locations of monitored objects. For example, the sensor node that initiates the communication with the base station should be close to the location of the object. In this paper, we focus on privacy-preserving communication methods in the presence of a global eavesdropper who has a complete view of the network traffic. The contributions in this paper are two-fold.

- We point out that the assumption of a global eavesdropper who can monitor the entire network traffic is realistic for some applications.

- We propose two techniques that prevent the leakage of location information: Source and sink location privacy. These two schemes are both very effective at hiding the source and sink sensors that initiate communication with the base station. We analyze their effectiveness and evaluate their communication overhead in both analysis and simulation.

Our two schemes for protecting location privacy have distinct properties that make them suitable for different applications. The periodic collection method ensures a high level of location privacy by making every sensor node periodically generate cover traffic. The source simulation method provides trade-offs between privacy, communication overhead, and latency by simulating the behavior of real objects at multiple places in the field to confuse adversaries. We also show how these two schemes can be integrated together to meet the requirements of multi-application networks.

The rest of the paper is organized as follows. Section II presents the network and adversary models. Section III formalizes the privacy issues and gives the privacy evaluation model. Section IV discusses the proposed techniques for location privacy. Section VI concludes this paper.

2. NETWORK AND ADVERSARY MODEL

Although prior research has attempted to solve location privacy problems for sensor networks, prior attacker models are not strong enough when we consider a well-funded, motivated adversary. In this section, we describe the network and adversary models that we study in this paper.

A. Network Model

Sensor networks are a relatively recent innovation. There are a number of different types of sensor nodes that have been and continue to be developed [5]. These range from very small, inexpensive, and resource-poor sensors such as SmartDust up to PDA-equivalent sensors with ample power and processing capabilities such as Stargate. Applications for networks of these devices include many forms of monitoring, such as environmental and structural monitoring or military and security surveillance.

In this paper, we consider a homogeneous network model. In the homogeneous network model, all of the sensors have roughly the same capabilities, power sources, and expected lifetimes.

B. Adversary Model

For the kinds of wireless sensor networks that we envision, we expect highly-motivated and well-funded attackers whose objective is to learn sensitive location-based information. The objects monitored by the network may be critical. Any damage to such objects can cause monetary losses or issues in critical military applications. Destinations are also critical components of sensor networks. In most applications, destinations act as gateways between the multi-hop network of sensor nodes and the wired network or a repository where this information is analyzed. Unlike failure of some sensors, failure of destinations can create permanent damage to sensor network applications. Compromise of a destination will allow an adversary to gather all the information because in most applications data won't be encrypted after it is received by a destination. In some military applications, an adversary could locate destinations and make the critical sensor network non-functional by destroying them.

In this paper, we consider global eavesdroppers. For a motivated attacker, faster and more effective location identification can be done through eavesdropping on the entire network. While an array of targeted antennae may be possible, a simple way for the attacker to do this would be to deploy his own sensor network to monitor the target network. Note that, at the current price for a BlueRadios SMT Module at $25, the attacker needs only $25,000 to build a network of 1000 nodes [1]. Thus, for even moderately valuable location information, this can be worth the cost and trouble. Although such an eavesdropping sensor network would face some system issues in being able to report the precise timing and location of each target network event, we do not believe that these would keep the attacker from learning more approximate data values. This kind of attacker would be able to query his own sensor network to determine the locations of observed communications. 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 we therefore focus our attention to this type of attacker

.

3. PRIVACY EVALUATION MODEL

In this section, we 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. 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, we assume that the attacker only monitors the wireless channel and the contents of any data packet will appear random to him.

A. The Attackers

The appearance of an endangered Attackers in a monitored area 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, our aim to capture the attackers before attempting the network. In this paper, we assume that an adversary cannot compromise any sensor node. While this is true for some applications, there are also scenarios where the adversary is able to compromise a few sensor nodes in the field. Compromising sensor nodes certainly allows the adversary to identify the locations of the objects more effectively.

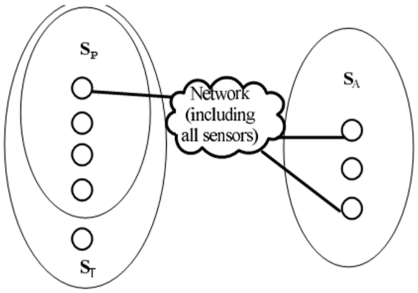

Figure .1 Network Viewed As a Graph

S_P	The set of component to be protected
S_T	The set of sensors in whose range the adversary expects to find the protected component
S_A	The set of component whose location are known to the adversary

As shown in the Figure 3.1, a sensor network deployed for an application can be viewed as a graph G = {V;E} where the set of vertices V is the union of the set I of sensor nodes, the set of sources, and the set of destinations. The set E of edges includes all direct communication links between sensor nodes physically close to each other. At any point in time, from the global eavesdropper's point of view, the network can be considered to be including a set S_P comprising of a set of sources, a set S_A which represents the destinations where the data is sent, and a set of

Indian Journal of Research in Communication Engineering(IJRCE)
Vol1.No.1 2013 pp 18-23.
available at: www.goniv.com
Paper Received :12-02-2013
Paper Published:10-03-2013
Paper Reviewed by: 1. Prof K. Rajakanna 2. Hendry Goyal
Editor : Prof. P.Muthukumar

sensors that transfer data between sources and destinations as shown in the Figure 3.1.

B. Privacy and Communication Cost

To minimize the communication overhead, we need to minimize the total communication overhead required for all the candidate traces in the network. We model the communication in sensor networks as a discrete time system with a granularity of Δ. Specifically, the time line is divided into a number of time intervals with equal length of Δ. The communication between sensor nodes happens at the end of each time interval, i.e., at time {Δ, 2Δ… i*Δ}. A sensor node can receive all the packets targeted to it and will send or forward no more than one packet at any time interval. Clearly, when a sensor node receives multiple dummy packets during a given time interval, it only needs to forward one of them to save the communication cost. Intuitively, the larger the value of Δ, the more communication cost we can save. Let α be the number of time intervals required for an event regarding an object to occur in the network. Thus there will be a communication round between a source and destinations every interval.

4. PRIVACY PRESERVING ROUTING TECHNIQUES

A. Periodic Collection

In the periodic collection method, every sensor node is a potential source node. To reduce energy consumption, we choose to reduce the number of potential sources in the network. To achieve this, we have every sensor node independently and periodically send packets at a reasonable frequency regardless of whether there are real data to send or not. Specifically, each sensor node has a timer that triggers an event every Δ second, as well as a first-in-first-out (FIFO) queue of size q for buffering received packets that carry real data reports. If so, it dequeues the first packet, encrypts it with the pairwise key it shares with the next hop, and forwards it to that node. Otherwise, it sends a dummy packet with a random payload that will not correctly authenticate at the next hop. Since every sensor node only accepts the packets that correctly authenticate, dummy packets do not enter the receiver's queue. When the queue at a sensor node is full, it will stop accepting new packets.

Privacy

The periodic collection method provides the optimal location privacy one can ever achieve in the network since the traffic pattern is entirely independent of the activity of real objects.

Energy consumption

For a privacy-preserving routing technique, its energy consumption can, thus, be measured by the additional communication used for hiding the traffic carrying real data. Since the network starts operation at time 0, the total number of data packets transmitted in the network can be estimated by (T*N)/Δ. Certainly, a small Δ indicates a large amount of additional traffic for our periodic collection method. This means that this method cannot handle real- time applications very well. The problem is to find the Steiner tree that connects all N nodes with the sinks they communicate with. In this case, the Steiner tree problem is reduced to finding the weight of a minimum spanning tree of the graph [4]. The weight of a minimum spanning tree for a graph of N nodes and one or more sinks is at least N. Thus, the minimum communication cost by the end of time T would be $\omega_T = (T*N)/(\alpha*\Delta)$.

B. Source Simulation

In the source simulation approach, a set of virtual objects will be simulated in the field. Each of them will generate a trace pattern similar to that of a real object.

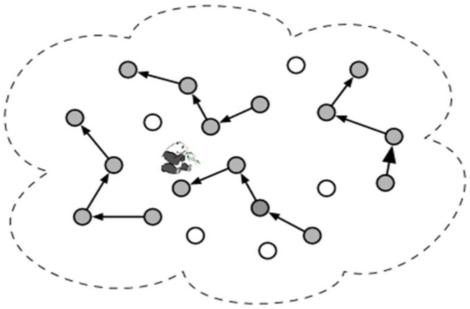

Figure.2 Movement pattern leaks the location of object

Figure. 2 illustrates the idea of this approach. In this example, objects move randomly in the field. Both the adversary and the defender have a model of this random movement pattern. After network deployment, each virtual object is treated like a real object, as sensors detect it and send the object's information to the destination. The protocol works in rounds. In every round, the node simulating the fake object will randomly pick a sensor node in its neighborhood (including itself) and ask this node to simulate the real object in the next round. In this way, there will be multiple movement patterns similar to that of real objects. Figure 4.1 shows three such virtual objects that simulate real objects.

Source simulation works as follows: before deployment, we randomly select a set L of sensor nodes and preload each of them with a different token. Every token has a unique ID. These tokens will be passed around between sensor nodes to simulate the behavior of real objects. For convenience, we call the node holding a token the token node. We also assume that the profile for the behavior of real objects is available for us to create candidate traces. After deployment, every token node will emit a signal mimicking the signal used by real objects for event detection. The token node will then determine who in its neighborhood and also including itself should run the next round of source simulation based on the behavior profile of real objects. The token will then be passed to the selected node. The delivery of the token between sensor nodes will always be protected by the pairwise key established between them.

Sink Simulation

Similar to the source simulation technique, an intuitive solution for destination location privacy would be to confuse the adversary by creating virtual destinations in the network. For this purpose, we propose to create multiple candidate traces towards fake destinations in the network to hide the trace generated for communication between real objects and real destinations.

5. SIMULATION MODEL

In this section, we use simulation to evaluate the performance of our techniques in terms of energy consumption and latency. The Panda-Hunter example was introduced in [2], and we will use terminology from this example to describe our simulation. 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. We include 5,093 sensor nodes distributed randomly in a square field of 1000 * 1000 meters to monitor the location of pandas in the network.

A base station is the destination for all the real trace. Each sensor node can communicate with other sensor nodes in a radius of 50 meters, while an electronic tag attached to a panda can emit radio signals that can reach sensor nodes within 25 meters. We noticed that, on average, each sensor node has 40 neighbors and that the presence of any panda will be detected by 10 sensor nodes on average. For source location privacy techniques, we assume that the base station is located at the center of this field. For destination location privacy techniques, we randomly choose the locations of fake base stations in the field. The proposed techniques assume a routing protocol for sensor networks, though the choice of routing protocol does not affect our results. For simplicity, we adopt a simple and widely-used routing method in many studies such as [13].

In this method, the routing paths are constructed by a spatial histogram from the base station. Each node, on receiving the data aggregated packet for the first time, sets the sender of the packet as its parent. In this way, each node will likely select a parent that is closest to the base station. For the purpose of simulation, we assume that the network application only needs to detect the locations of pandas and always wants to know the most recent locations. We thus have every sensor node drop a new packet if it has already queued an identical packet that was generated from the same event. In our simulation, we assume that the adversary has deployed a network to monitor the trace in the target network. Specifically, he is able to locate every sensor node in the target network and eavesdrop every packet this node delivers. For simplicity, we assume the adversary can always reliably collect all the observations in the network

Analysis:

Finally minimum communication overhead achieved. Figure 3 show the performance analysis graph between simulation time and loss rate of packet delivery. The x-axis represents the simulation time and the y-axis represents the loss rate of packet delivery. Increase delay when increase simulation time. When increase simulation time loss rate also reduced.

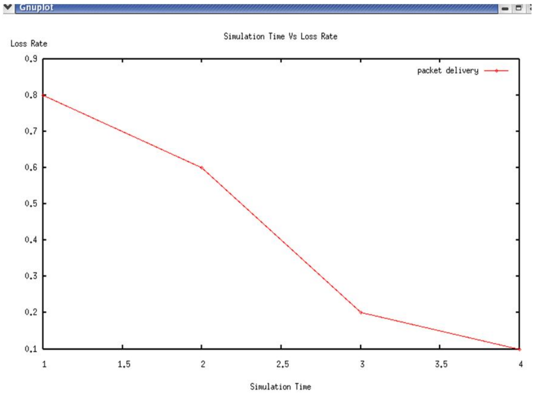

Figure.3 Simulation Time vs Loss Rate

6. CONCLUSION

Prior work that studied location privacy in sensor networks had assumed that the attacker has only a local eavesdropping capability. This assumption is unrealistic given a well-funded, highly-motivated attacker. We formalized the location privacy issues under the model of a global eavesdropper, and show the minimum average communication overhead needed for achieving certain privacy. We also presented two techniques to provide location privacy to objects and destinations against a global eavesdropper.

REFERENCE

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

[2] Bamba, L. Liu, P. Pesti, "Enhancing Source Location Privacy in Sensor Network," Proc. Int'l Conf. ICDCS '05.

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

[4] 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.

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

[8] 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.

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

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

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

[12] 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.

[13] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," in 2004 International Conference on Dependable Systems and Networks (DSN), June 2004.