IJDCST @November Issue- V-1, I-7, SW-12
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Preventing the Leakage of the Local Information from Global Eavesdropper in Sensor Networks

[1] Sk.Afroz Basha, [2] MA.Baseer
[1] Student, SANA ENGINEERING COLLEGE, KODAD, NALGONDA (DIST), ANDHRAPRADESH.
[3] Associate Prof, SANA ENGINEERING COLLEGE, KODAD, NALGONDA (DIST), ANDHRAPRADESH.

Abstract: Providing the confidentiality for the content of messages is the big concern. Hence, many of the protocols providing the confidentiality for the information in the sensor network, which refers as sensor, network security. 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 are several recent studies on providing the local privacy. There are existing approaches which assume a weak adversary model then the adversary sees only local network traffic. Initially we can discuss about the strong adversary model (global eavesdropper), which is often realistic in practice and can defeat the existing approach. We 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. To prevent the leakage of the local information we proposed two different techniques: 1) Periodic Collection 2) Source Simulation. Source simulation provides trade-offs between communication cost, latency and privacy, while Periodic collection provides a high level of location privacy. We demonstrate that the proposed techniques, by our analysis and simulation, are efficient and effective in protecting location information from the attacker.

Keywords: Wireless Sensor Networks (WSN), Preventing, Protecting,

I. INTRODUCTION

A wireless sensor network (WSN) typically comprises a large number of resources, cheap and small constrained sensors that are self-organized as an ad-hoc network to interact with and study the physical world. In the difficult or infeasible to set up wired networks Sensor networks can be used in applications. These applications are subject to a variety of security issues in hostile environments. The efforts to date in sensor network security have focused on providing classic security services such as authentication, availability, integrity, and confidentiality. While these are critical requirements in many applications they are not sufficient. The communication patterns of sensors can expose a great deal of contextual information. Delivering sensor data to the base station may disclose the locations of some critical events in the field. It is particularly important to guarantee location privacy; failure to protect location-based information can completely undermine network applications. Providing location privacy in a sensor network is extremely challenging. An adversary can easily intercept the network traffic due to the use of a broadcast medium for routing packets. We can then perform traffic analysis and identify the source node that initiates the communication with the base station. The locations of critical and high value objects can be revealed being monitored by the sensor network. The resource constraints on sensor nodes make it very expensive to apply traditional anonymous communication techniques for hiding the communication from a sensor node to the base station. The existing solutions can only be used to deal with adversaries who have only a local view of network traffic. On the entire network a highly motivated adversary can easily eavesdrop and defeat all these solutions. The adversary may decide to deploy his own set of sensor nodes to monitor the communication in the target network. We focus on privacy-preserving

communication methods in the presence of a global eavesdropper who has a complete view of the network traffic. The main contribution of this paper is done in two folds:

a. We point out that the assumption of a global eavesdropper who can monitor the entire network traffic is realistic for some applications. Where we also formalize the location privacy issues under this assumption and provide bounds on how much communication overhead is needed to achieve a given level privacy.
b. We propose two techniques that prevent the leakage of location information:
    1) Periodic collection
    2) Source simulation

These two schemes are both very effective at hiding the source sensors that initiate communication with the base station. Our two schemes for protecting location privacy have distinct properties that make them suitable for different applications. The source simulation method provides trade-offs between communication overhead, latency and privacy by simulating the behavior of real objects at multiple places in the field to confuse adversaries. We even show how these two schemes can be integrated together to meet the requirements of multi-application networks.

II. EXISTING SYSTEM

We describe previously-proposed algorithms for source location privacy in wireless sensor networks. Those algorithms were designed to protect real objects in the field from a local eavesdropper by increasing the safety period that can be defined as the number of messages initiated by the current source sensor before the monitored object is traced [4]. The [5] flooding technique has the source node send out each packet through numerous paths to the base station to make it difficult for an adversary to trace the source. The problem is that the base station will still receive packets from the shortest path first. This method consumes a significant amount of energy without providing much privacy in return. The propose fake packet generation [4] that has the base station create fake sources whenever a sender notifies the base station that it has real data to send. The fake senders are away from the real source and approximately at the same distance from the base station as the real sender. Their other technique is phantom single-path routing that achieves location privacy by making every packet generated by a source walk a random path before being delivered to the base station. Packets will reach the base station following different paths as per the results. Energy consumption and privacy provided by this method will increase as the length of the loops increase. All these existing methods assume that the adversary is a local eavesdropper. It can easily defeat to schemes that an adversary has the global knowledge of the network traffic. The adversary only needs to identify the sensor node that makes the first move during the communication with the base station.

III. ADVERSARY MODEL AND NETWORK

Although prior research has attempted to solve location privacy problems for sensor networks motivated adversary. Prior attacker models are not strong enough when we consider a well-funded.

Network Model

There are a number of different types of sensor nodes that have been and continue to be developed. These range from inexpensive, resource and very small poor sensors such as Smart Dust up to PDA-equivalent sensors with ample power and processing capabilities such as Stargate. We consider a homogeneous network model where all of the sensors have roughly the same power sources, expected lifetimes, and capabilities. This is common network architecture for many applications today and will likely continue to be popular moving forward.

Adversary Model

We expect highly-motivated and well-funded attackers whose objective is to learn sensitive location-based information for the kinds of wireless sensor networks that we envision. This information can include the location of the events detected by the target sensor network such as the presence of a panda. In this application a sensor network is deployed to track endangered giant pandas in a

bamboo forest. 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. Consider global eavesdroppers, for a motivated attacker, faster and more effective location identification can be done through eavesdropping on the entire network. 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. Attacker would be able to query his own sensor network to determine the locations of observed communications. It should be feasible to monitor the communication patterns and locations of events in a sensor network via global eavesdropping.

IV. PRIVACY EVALUTION MODEL

We formalize the location privacy issues under the global eavesdropper model. The adversary deploys an attacking network to monitor the sensor activities in the target network. Consider a powerful adversary who can eavesdrop the communication of every sensor node in the target network. We assume that the attacker only monitors the wireless channel and the contents of any data packet will appear random to him, which means that the meaningful information in each observation is only the node ID and the observation time. 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. Dealing with compromised sensor nodes is beyond the scope of this paper.

The Attacker

The goal of the adversary is to identify a set of nodes that represent the set of possible locations for the objects sensed by the target network. It indicates that the adversary believes that the objects being observed are close to some of the nodes at the particular instance of time. The object should generate a trace and that is a set of observations over the lifetime of the network up to time. According to the adversary's perspective a set of observations a candidate trace if the set could have been generated by the detection of a real object. We assume that the pattern analysis does not return fractional values. We say that a pattern analysis function is perfect if it can identify all candidate traces without error, we consider a strong adversary who uses a perfect pattern analysis function.

Measuring Privacy

We assume that the nodes that are equally likely to be the real objects. We always assume that the real object can be anywhere in the deployment field at time. The level of location privacy is measured in terms of the number of bits. The level of location privacy is measured in terms of the number of bits depending on the users and applications. The privacy would go lower if the attacker determines that a particular trace is no longer a candidate trace. The attacker must spend time to investigate candidate locations then the average privacy over time is adequate. We provide a snapshot of the privacy at a given time that can be used for either purpose.

Privacy and Communication Costs

We explore the relationship between the level of privacy and the amount of communication overhead. Here we can shows the relation between privacy and cost. We call a privacy-preserving solution as an optimal solution if it can always achieve a given level of location privacy with the minimum communication cost given. It tells us the minimum average communication overhead needed to achieve certain privacy. The defender only needs to make a few candidate traces in a large sensor network. The defender can make to achieve a certain level of location privacy without increasing the number of traces. The defender can have the candidate traces share as many observations as possible. Similar to a technique from anonymous communications some sensor nodes could wait for several (fake) packets to arrive and forward one instead of many of them. We simplify our model to understand the effect of different policies on the costs and location privacy in the network to characterize this effect. When a sensor node receives multiple dummy packets during a given interval, it only needs to forward one of them to save the cost.

V. RESULT SIMULATION

We evaluate the performance of our techniques using simulation. The performance of the proposed privacy-preserving techniques in terms of energy Consumption and latency and compare our methods with the Phantom single-path method. 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. The presence of any panda will be detected by 10 Sensor nodes on average. We adopt a simple widely used Routing method, where paths are constructed by a beacon packet from the base station.

Periodic collection

The communication overhead in the network remains constant and is independent of both the number of Pandas and their patterns of movement. The focus of Our simulation evaluation is on the latency and the packet drop Rate when there are multiple pandas in the field. Due to nodes Close to the base station receiving multiple reports at the same Time they require them to buffer packets. While the Latency of the packets that do arrive at the base station becomes Stable after a certain point.

Source simulation

The location privacy achieved by source simulation is determined by the number of Virtual sources simulated in the network. The focus of our simulation evaluation is on how much communication cost. We have to pay to achieve a given level of location privacy. We assume that the sensor Network is deployed to handle real-time applications. Whenever a sensor node receives a packet it will forward it to the next hop as soon as possible. The communication cost involved in our Source simulation method to achieve a given level of privacy. We also note that the communication overhead is very close to the performance of the optimal Solution that can be derived. The source simulation method is effective and efficient for achieving privacy in real time Applications.

VI. CONCLUSIONS

Prior work on location privacy in sensor networks had assumed that the attacker has only a local eavesdropping capability. We formalize the location privacy issues under the model of a global eavesdropper and show the minimum average communication overhead needed for achieving a given level of privacy. Here we present two techniques to provide privacy against a global eavesdropper. They are analysis and simulation studies show that they can effectively and efficiently protect location privacy in sensor networks. We assume that the global eavesdropper will not compromise sensor nodes; he can only perform traffic analysis without looking at the content of the packet. We are also interested in the implementation of our methods on real sensor platforms and the experimental results from real sensor applications.

VII. REFERENCE

[1]. H.chan, A.perrig and D.song. Randomky predistribution schemes for sensor network. In IEEE symposium on security and privacy, apges 197-213, may 2003.

[2] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon. Entrapping adversaries for source protection in sensor networks. In Proceedings of the International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM), pages 23–34, June 2006.

[3] C. Ozturk, Y. Zhang, and W. Trappe. Source-location privacy in energy constrained sensor network routing. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN), pages 88–93, October 2004.

[4] J.Hill Horton, R.Kling, and L.Krishnmurthy. The platform enabling wireless sensor networks.commun. ACM, 47(6):41-46,2004.

[5] starNews, Panda paoching gang arrested, shanghai star Telegram, April 2003.

[6] P.Karmat, Y.Zhang, W.trappe, and C.Ozrurk , ”enchanching source location privacy in sensor network riuitng”, In the proceeding of the 25th IEEE international Conference on distributing computing systems, pages 599-608, june 2005.

[7] A. Savvides, C. Han, and M. Srivastava. Dynamic fine-grained localization in ad-hoc networks of sensors. In Proceedings of ACM MobiCom, pages 166–179, July 2001.
[8] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar. SPINS: Security protocols for sensor networks. In Proceedings of Seventh Annual International Conference on Mobile Computing and Networks (MobiCom), July 2001.