Effective Protecting Tract Privacy Using Sink Simulation and Backbone Flooding Techniques

P.Kalaiselvi
Research Scholar, Vivekanandha College for women, Tiruchengode, Tamilnadu.

A.Sankareswari
Assistant Professor, Vivekanandha College for women, Tiruchengode, Tamilnadu.

Abstract: - A wireless sensor network (WSN) is composed of numerous small sensing devices with limited communication range. The sensors collect data from the environment and report them to the sinks. With the promising sensing and wireless technologies, sensor networks are expected to be widely deployed in a broad spectrum of civil and military applications. Location information of the sinks, the sensors, and the objects being tracked are very important in sensor networks. Protecting location privacy in sensor networks is crucial considering different kinds of attacks that may disrupt the normal function of the networks. To identify location privacy issues in sensor networks and computes lower bound on the communication overhead to resolve those issues in order to achieve higher level of privacy. By eaves dropping the sensor nodes transmissions and tracing the packets trajectories in the Wireless Sensor Networks, an adversary can capture the location of a source or sink eventually. Thus, the location privacy of both source and sink becomes a significant issue in Wireless Sensor Networks. Previous research only focuses on the location privacy of the source or sinks independently. In this paper, address the importance of location privacy of both source and sink simultaneously. The proposed techniques are efficient and effective for source and sink location privacy in sensor networks.

Index Terms— Sensor networks, Network security, location privacy, source simulation, sinks simulation.

1. INTRODUCTION

Mobile computing is a generic term used to refer to a variety of devices that allow people to access data and information from wherever they are. Mobile computing is a very broad term which can be used to define any means of using a computer while outside of the corporate office. This could include working from home or on the road at an airport or hotel. The means to perform mobile computing could include kiosks used to remotely connect to the corporate office, home computers, laptops, tablets or smart phones. Specialized or integrated devices could also be considered as mobile computing devices.

Mobile computing is the discipline for creating an information management platform, which is free from spatial and temporal constraints. The freedom from these constraints allows its users to access and process desired information from anywhere in the space. The state of the user, static or mobile, does not affect the information management capability of the mobile platform. A user can continue to access and manipulate desired data while traveling on plane, in car, on ship, etc. Thus, the discipline creates an illusion that the desired data and sufficient processing power are available on the spot, where as in reality they may be located far away.

1.1 Mobile computing

Mobile computing is human computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications. Mobile computing is taking a computer and all necessary files and software out into the field. Mobile computing is being able to use a computing device even when being mobile and therefore changing location. Portability is one aspect of mobile computing.

Mobile computing is the ability to use computing capability without a pre-defined location and/or connection to a network to publish and/or subscribe to information. Mobile computing is distributed computing that involves elements whose

location changes in the course of computation. Elements may be software components - such as mobile agents, data, and hardware - such as palmtops and wireless phones, or users. This being a very broad definition, the common underlying issue is location and its management.

1.1.1 Characteristics

There are several characteristics to mobile devices and mobile computing. Many of these are shared with other technologies but have unique significance when it comes to mobile computing.

Portability

As the name mobile implies, the devices have to be able to easily move to different locations, while remaining functional.

Connectivity

The ease of being able to connect to the Internet and receive or transmit data is an essential component to mobile computing. Connectivity through mobile carriers over a 3G- or 4G-type network, as well as Wi-Fi capabilities, are basic requirements for mobile devices.

Interactivity

This could almost go without saying, but like most other computing technologies, the ability for a mobile device is critical. The interactivity becomes more significant with mobile devices, as they typically have less computing power than other types of technology.

Individuality

Individuality may sometimes be overlooked, but it is a basic component of the concept of mobile computing. Mobile devices, including smart phones and tablets, are designed for individuals and have become a sort of extension to people in many aspects of their lives. From this perspective, how individuals interact with mobile devices remains unique.

These characteristics allow mobile computing technologies to produce unique learning experiences, such as, authentic environment; recognition and reflection on accidental learning; enhanced capabilities to correspond with subject matter experts from the classroom to the field; the ability to share data over diverse geographic locations; and the ability to be individually intrigued by the learning at hand that traditional computing environments don't typically allow for. In addition, the personal nature of these devices provides opportunities for seamless integration of the unit into everyday lifestyles encouraging continuous learning opportunities regardless of time sensitivity and location.

1.2 Wireless Sensor Network

A Wireless Sensor Network is a collection of nodes organized in a network. Each node consists of one or more microcontrollers, CPUs or Digital Signal Processor (DSP) chips, a memory and a RF transceiver, a power source such as batteries and accommodates various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion.

Wireless Sensor Networks are collection of compact-size and inexpensive computational nodes that measure local environmental conditions or other parameters and forward such information to a central point for appropriate processing. WSNs nodes can sense the environment, can communicate with neighboring nodes, and can, in many cases, perform basic computations on the data being collected. WSNs support a wide range of useful applications. Each node in the sensor network consists of three functions: the sensor node senses the environment, the processing unit performs local computation on the sensed data, and the communication field is responsible for message exchange with neighboring sensor nodes. In many WSN applications, the deployment of sensor node is performed in ad hoc fashion. Once deployed, the sensor nodes must be able to automatically organize themselves into a wireless communication network.

Architecture

A Wireless Sensor Network (WSN) provides a low-cost and multifunctional means to link communications and computer networks to the physical world. It consists of base stations and a number of wireless sensors. Each sensor is a unit with wireless networking capability that can collect and process data independently. Sensors are used to monitor activities of objects in a specific field and transmit the information to the base station.

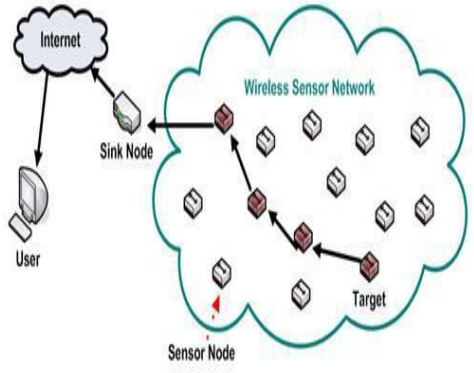

Figure1.1 Overview of Sensor Networks

1.2.1 Components

The main components of a sensor node are a microcontroller, transceiver, ternal memory, power source and one or more sensors.

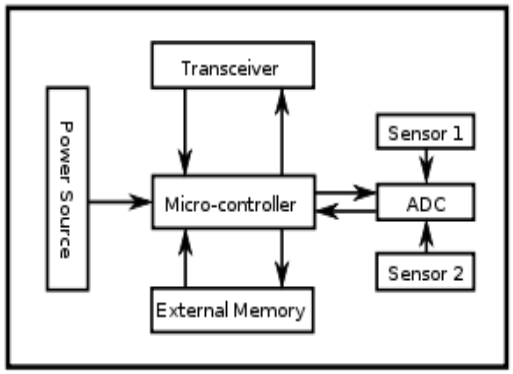

Fig.1.2 Components of WSN

1.2.2 Working of Wireless Network

A Wireless Local Area Network (WLAN) links two or more devices using some wireless distribution method and usually providing a connection through an access point to the wider Internet. This gives users the mobility to move around within a local coverage area and still be connected to the network. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.

Wireless LANs have become popular in the home due to ease of installation, and in commercial complexes offering wireless access to their customers; often for free.

1) Architecture
2) Stations
3) Basic Service Set
4) Extended Service Set
5) Distribution System

1.3 Location privacy issues

Location privacy is very important in hostile environments. Failure to protect such information can completely destroy the intended purposes of sensor network applications. Location privacy measures 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. Preserving the privacy for sensor nodes is essential in current Wireless Sensor Network applications. Privacy issues in WSNs fall into two categories: content-privacy and contextual-privacy.

An adversary can easily intercept network traffic due to the use of a broadcast medium for routing packets and exploit the information like packet transmission time and frequency to perform traffic analysis and infer the locations of monitored objects and data sinks. On the other hand, 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. So find alternative means to provide location privacy that accounts for the resource limitations of sensor nodes as well as provide privacy preserving protocols for source and sink location in such sensor networks.

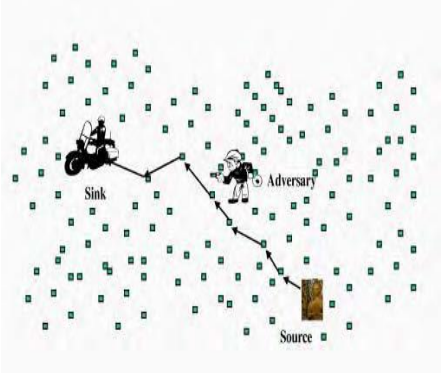

Fig.1.3 Adversary Eavesdropping

When the adversary tends to eavesdrop or manipulate the content of packets transmitted over a Wireless Sensor Network, threats against content-privacy emerge. To address the content-privacy issue, a number of specific encryption and authentication mechanisms are proposed. On the other hand, the contextual information may expose the user secret to adversaries due to the open nature of Wireless Sensor Network. In particular, the location information about the sink (or the base station) and the source nodes is not well protected in most Wireless Sensor Network. An adversary can easily eavesdrop and trace packet flows, so as to locate the sink or the source nodes. For example, in a panda monitoring applications, each panda is a source node, which is sensitive and considerable, should be well protected from the poacher. Meanwhile, as the centre of data collection and processing, the sink is the most critical node in the whole network. Once the sink is destroyed or controlled by an adversary, for example in a hostile environment, the entire Wireless Sensor Network becomes useless.

2. RELATED WORK

2.1 Analysis of Related Works

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 and private information retrieval have been developed for this purpose. In pervasive computing, user's location privacy can be compromised by observing the wireless signals from user devices. 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, which is the number of messages initiated by the current source sensor before the object is located by the attacker. The flooding technique 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 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 achieves location privacy by making every packet walk along a random path before being delivered to the sink. Cyclic entrapment 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 in the network.

A global eavesdropper can easily defeat these schemes by locating the first node initiating the communication with the base station. Recently, 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. Shao et al. propose to reduce the latency of real events without reducing the location privacy under a global eavesdropper. This technique ensures that the adversary cannot determine the real traffic from statistical analysis.

To mitigate these two kinds of attacks, Deng et al. introduced a multiple-parent routing scheme, a controlled random walk scheme, a random fake path scheme, and a hot spots scheme. A protocol called LPR was proposed for sink location privacy. The LPR algorithm provides privacy to the sink by adding redundant hops and fake packets when data are sent to the sink. However, these techniques all assume that the adversary is a local eavesdropper. A global eavesdropper can easily defeat these schemes. For example, the global eavesdropper only needs to identify a region of high activity, i.e., the region exhibiting a high number of transmissions, to locate the sink. In this paper, we focus on privacy-preserving techniques designed to defend against a global eavesdropper.

3. METHODOLOGY

The proposed privacy preserving techniques for protecting the location information of monitored objects and data sinks. Assume that all communications between sensor nodes in the network are encrypted so that the contents of packets appear random to the global eavesdropper.

3.1 Source-Location Privacy Technique

Two techniques to provide location privacy to monitored objects in sensor networks are Periodic Collection and Source Simulation. The Periodic Collection method achieves the optimal level of 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 tradeoffs between privacy, communication overhead, and latency.

The queue size q is the number of real packets that a sensor node can buffer. This will affect how well the periodic collection method can handle situations in which real events are frequently observed and reported by the sensors. Increasing the value of q will allow the queuing of more real packets and thus will help the network in forwarding more information about real objects to the sink. In other words, the number of packets dropped in transit can be reduced. However, a large value of q may increase the average latency of a real packet reaching the sink. This occurs because a newly received packet that carries real data may need to wait for a long time before getting forwarded in case of a large queue.

Protocol Description

In the source simulation approach, a set of fake objects will be simulated in the field. Each of them generates a traffic pattern similar to that of a real object to confuse the adversary.

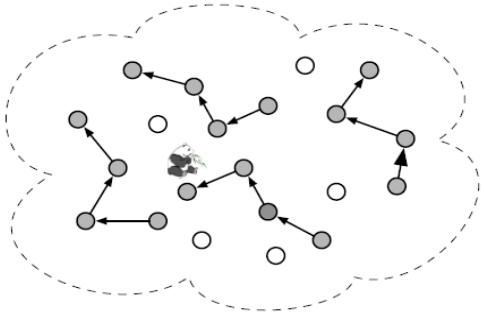

Fig3.1 Simulating Fake Source in the Field

Source simulation works as follows,

Before deployment, it randomly selects a set L of sensor nodes and pre-loads 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, it calls the node holding a token the token node. It also assumes that the profile for the behavior of real objects is available to create candidate traces.

After deployment, every token node will emit a signal mimicking the signal used by real objects for event detection. This will trigger event detection in the local area and generate traffic as if a real event was detected. The token node will then determine who in its neighborhood (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 pair wise key established between them.

3.2 Sink Location Privacy Techniques

Two privacy-preserving routing techniques for sink location privacy in sensor networks: sink simulation and backbone flooding. 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. Both techniques provide trade-offs between privacy, communication cost, and latency. In this work, focus on protection of passive sinks that only receive data from sensors.

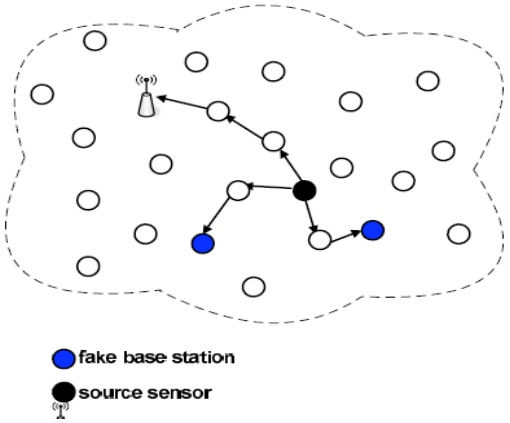

Fig.3.2 Simulating Fake Sink in the Field

During deployment, it place real sinks and select locations where fake sinks are to be simulated. A subset of the sensors will be used as fake sinks. It is also required that each real sink have a fake sink simulated in its communication range. It will only send messages to the fake sinks and have all fake sinks perform a one-hop broadcast of the message, ensuring full concealment of the real sink locations.

However, in practice, selecting fake sinks that are too close to each other may reduce the location privacy drastically. An attack on one of them can destroy others as well. For example, if an adversary needs to destroy sinks using missile, nearby sinks may be destroyed in one attack. Similarly, the adversary can physically check and locate nearby sinks with little additional effort.
Thus, the locations of fake sinks should be made as far away from each other as possible.

Once fake sinks are selected after deployment, the sensors should have routing paths to send data to places where fake sinks are simulated. During the network operations, whenever a source node senses an event, a report will be sent to all fake sinks. Whenever a fake sink receives a packet, it broadcasts it locally so that the adversary would believe that a real sink could be in range of any of the fake sinks.

3.3 Backbone Flooding

In Backbone Flooding, send packets to a connected portion of the network, the backbone, instead of sending them directly to a few sinks. The packets are only flooded among the backbone members, the sensors that belong to this backbone. As long as the real sinks are located in the communication range of at least one backbone member, they can receive packets from any source in the field. Clearly, for a global eavesdropper, the sink

could be anywhere near the backbone. It assumes that the backbone is created soon after the sensor network is deployed and that the adversary does not eavesdrop on the network until the backbone is created.

The main component of backbone flooding is the construction of the backbone. Existing studies have focused on finding the minimal number of sensors that are needed to flood a packet so that the entire network can receive it. In our case need to flood the packets to cover an area large enough to achieve the desired level of location privacy.

In Backbone Flooding, it creates a backbone consisting of |L| members, such that each sink is within the range of at least one backbone member. Given |L|, the backbone formed should cover as large an area as possible for maximum location privacy. When it says that a sensor v covers some other sensors, we mean that v is responsible for directly delivering the received packets to these sensors via local broadcast. The backbone formation will terminate when the backbone members cover the required number of sensors for the desired level of location privacy.

4. EXPERIMENTS AND RESULTS

In this section, use simulation to evaluate the performance of our techniques in terms of energy consumption and latency. The Panda-Hunter example was introduced, and will use the terminology from this example to describe our simulation. In this application, a sensor network is deployed to track endangered 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. It includes 5,093 sensor nodes distributed randomly in a square field of 1000× 1000 square meters to monitor the pandas. The base station is the sink for all real data traffic. 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. In noticed that, on average, each sensor node has 40 neighbors and that the presence of any panda will be detected by 10 sensor nodes. For source location privacy techniques, assume that the base station is located at the center of this field. For sink location privacy techniques, 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. In this method, the routing paths are constructed by a beacon packet from the base station. Each node, on receiving the beacon packet for the first time, sets the sender of the beacon packet as its parent. In this way, each node will likely select a parent that is closest to the base station.

Source Location Privacy Periodic Collection

The periodic collection method achieves optimal location privacy. In addition, the communication overhead in the network remains constant and is independent of both the number of pandas and their patterns of movement. Hence, the focus of our simulation evaluation is on the latency and the packet drop rate when there are multiple pandas in the field. We set the time interval for periodic collection as $\Delta = \tau$.

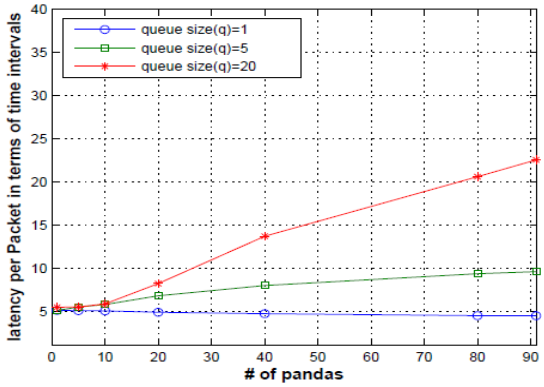

Fig.4.1 Latency Vs number of pandas (periodic collection scheme)

The above figure shows the latency of packet delivery when there are multiple pandas in the field. As the number of pandas increases, the latency increases. This is because the nodes close to the base station receive multiple reports at the same time, which requires them to buffer the packets.

During the simulation, assume that there is only one panda in the network. Multiple fake pandas are created and simulated in the field. The initial positions of the fake pandas are randomly selected In other words, whenever a sensor node receives a packet, it will forward it to the next hop as soon as possible. Thus, while set the time interval for periodic collection as $\Delta = \tau$, we set it to $\Delta = \tau/10$ for source simulation. In other words, in source simulation, nodes will forward packets ten times faster than in the periodic collection method.

Sink Location Privacy Sink Simulation

The location privacy achieved and the amount of energy consumed by the sink simulation scheme depends on the number of fake base stations simulated in the network. The packets generated by the sources are sent to all fake and real base stations.

Hence, the focus of our simulation evaluation is on the latency and the packet drop rate when there are multiple base stations in the field.

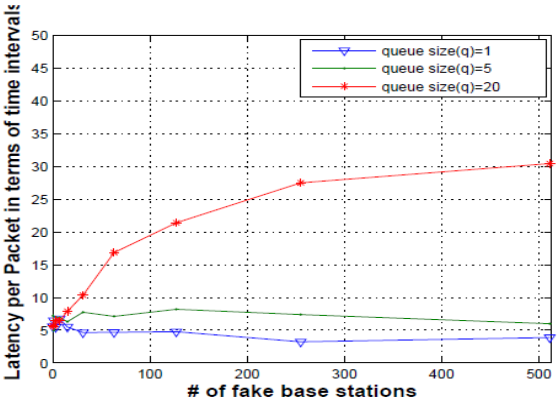

Fig. 4.2 Effect of number of fake base stations on Latency (sink simulation scheme)

The above figure shows the latency of packet delivery when there are multiple fake base stations in the field. As the number of fake base stations increases, thereby providing more location privacy, the latency increases. This is because having more base stations causes more traffic in the network and thus more packets to be buffered. When the number of fake base stations grows too large, the buffered packets start being dropped due to nodes limited queue sizes, while the latency of the packets that do arrive at the base station becomes stable after a certain point. When the queue size q decreases, packets.

5. 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. In this thesis, it has formalized the location privacy issues under a global eavesdropper and estimated the minimum average communication overhead needed to achieve a given level of privacy. It also presented techniques to provide location privacy to objects and sinks against a global eavesdropper. In particular, in this thesis, assume that the global eavesdropper will not compromise sensor nodes; he/she can only perform traffic analysis without looking at the content of the packet. It used analysis and simulation to show how well these techniques perform in dealing with a global eavesdropper. In future, design an optimal combination from these decomposed schemes to achieve a highest location privacy protection for both ends. Thus further increase the location privacy by simulation approach to protect the location of destination node. Extend our study to networks with multiple sources and sinks, and will also formally analyze the performance of our schemes.

REFERENCES

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

[2] W. Du, J. Deng, Y.S. Han, and P.K. Varshney, “A Pair wise Key Predistribution Scheme for Wireless Sensor Networks,” Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Oct. 27-31 2003, pp.42-51.

[3] J. Deng, R. Han, and S. Mishra, “Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks," Elsevier Pervasive and Mobile Computing Journal, Special Issue on Security in Wireless Mobile Computing Systems, vol. 2,pp. 159-186, April 2006.

[4] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, “Protecting receiver-location privacy in wireless sensor networks," May 2007, pp. 1955-1963.

[5] J. Deng, R. Han, and S. Mishra, “Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks,” Proc. of IEEE International Conference on Dependable Systems and Networks (DSN), 2004.

[6] L. Eschenauer and V. D. Gligor. “A key-management scheme for distributed sensor networks,” In Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS), pages 41-47, November 2002.

[7] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, “Protecting receiver-location privacy in wireless sensor networks," May 2007, pp. 1955-1963.

[8] J. Deng., R. Han, and S. Mishra, “Enhancing base station security in wireless sensor networks," 2003.

