Securing the Location Privacy in wireless Sensor Networks

V. Rini
II M.E, Computer Science and Engineering, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India.

K. Janani
Assistant Professor, Department of Computer Science and Engineering, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India.

Abstract

Wireless sensor network is composed of small low cost resource constrained sensor nodes (motes).There are many issues in wireless sensor networks. The two main issues are energy conservation and location privacy, the privacy preservation problem has drawn the attention of the research community because of its challenging nature. In existing techniques like source simulation and backbone flooding techniques are impossible when the node is compromised by the global eavesdropper. These techniques are implemented to solve privacy issues only in homogeneous WSNs where all sensor nodes have same capabilities. So we present a packet altering scheme, which has lesser overhead compared to a source simulation or backbone flooding. This paper aims to maintain source and sink privacy under eavesdropping and node compromise attacks. The majority of the above mentioned efforts attempt to solve privacy issues in heterogeneous WSNs where all sensor nodes have different Capabilities.

Keywords— Location privacy, sensor networks.

1. Introduction

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**.**WSN provide potential benefit to society such as Military applications such as battlefield surveillance, Industrial process monitoring and machine control, Health monitoring of patients and so on. In many WSN applications, the deployment of sensor node is performed in adhoc fashion. Once deployed, the sensor nodes must be able to automatically organize themselves into a wireless communication network.

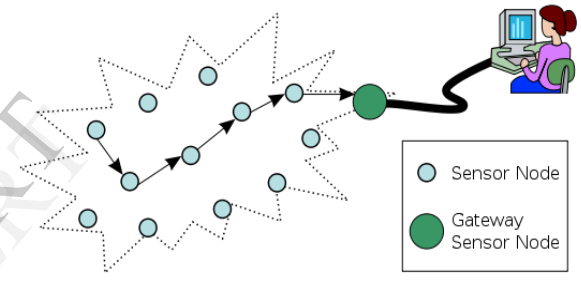

Fig 1.1: Wireless Sensor Network

Fig 1.1 shows a wireless sensor network (WSN) generally consists of a base station (or "gateway") that can communicate with a number of wireless sensors. Data is sensed at the wireless sensor node, and passed to the gateway directly or it may use other wireless sensor nodes to forward data to the gateway. The data is then passed to the system by the gateway connection. The sensed data passed through the network to main location. The purpose of this chapter is to provide a brief introduction about wireless sensor networks and present a few applications in which wireless sensor networks are enabling.

2. Related Work

Privacy in WSNs can be classified into content privacy and contextual privacy [3]. Threats against content privacy arise due to the ability of adversaries to observe and manipulate the content of packets sent over a WSN. This type of threats is countered by encryption and authentication. However, even after strong encryption and authentication mechanisms [6], [1] are applied, wireless communication media still exposes

contextual information about the traffic carried in the network. For example, an attacker can deduce sensitive information from a WSN by eavesdropping on the network traffic and analyzing traffic patterns.

It identifies two classes of traffic analysis attacks in WSNs [2]. The first attack is rate monitoring attack in which an attacker monitors the packet transmission rate of nodes near to the attacker and move near to the nodes that have a higher packet sending rate. The second attack is time correlation attack, an attacker observes the correlation in sending time between a node and its neighbour node that is assumed to be forwarding the same packet, and deduce the path by following the sound of each forwarding operation as the packet propagates towards a sink node [1]. Although the defender is able to buffer incoming packets in the nodes for some random period before forwarding them and thereby to defend against a time correlation attack, a senior adversary can pro-actively trigger the packet forwarding by generating abnormal sensory events such as abnormal temperature that needs to forward as soon as possible. A few schemes [1,2] based on source location privacy were proposed, which deal with traffic analysis attack. Their main ideas include using numerous paths to send packets to sinks and then forms a looping paths to forward packets and associates real sources with faked sources and requiring real sources to send packets periodically. Some schemes [2, 3-4] were proposed based on receiver location privacy. For example, Jian proposed a new location-privacy routing protocol to preserve the receiver's location privacy [2]. This scheme employs fake packet injection to minimize the information that an adversary can deduce from the overhead packets about the direction towards the receiver.

However, all of the above schemes do not take into consider the sink location privacy. Nezhad A.A et. al. proposed anonymous topology discovery protocol where all nodes are allowed to broadcast route discovery messages and coming/outgoing labels assigned to nodes are used to forward packets [5]. This method will hide the location of sink node. However, there is a chance that some nodes may not be discovered. Another method that is using *k*-anonymity model was proposed for the data privacy [5]. Using its model, the record of an individual is hidden in a group of at least *k* records of other individuals.

3. Network Model and Attacker Model

Our system assumes that a number of sensors, deployed into particular region. Each sensor has a transmission range, and they can communicate with each other directly or indirectly. We assume that a sink node works as the network controller to collect event data from the source nodes via various neighboring nodes. In this paper, we assume that the attacker is external, passive and global. By external, we mean that the attacker does not control any sensors. By passive, we mean that the attacker cannot conduct active attacks such as traffic injection, channel jamming and denial of service. By global, we mean that the attacker can monitor, eavesdrop and analyse all communication tasks occurring within the network. Besides, a global eavesdropper can keep track of the number of messages that pass through local nodes. Thus, he can easily deduce sink location by detecting nodes' traffic volumes. Note that this global eavesdropper does not have the capability of distinguishing between original and fake messages. Because we assume all messages are encrypted by a pair-wise secret key.

4. Privacy-Preserving Routing

In this section, we present the proposed privacy-preserving techniques for protecting the location information of monitored objects and data sinks. We assume that all communications between sensor nodes in the network are encrypted so that the contents of packets appear random to the global eavesdropper. Many key predistribution protocols can be used [6], [1], [3].

In sink simulation protocol, the simulated sinks are static. As a result, if the real sinks are mobile, then the attacker will be able to directly distinguish the simulated sinks from the real ones in the field. There are two options available to deal with mobile sinks. The first option is to create a movement model for simulate the sinks, similar to what we proposed for simulating the sources in the source location privacy. Another option is to use the backbone flooding method, where the mobile sink will be able to receive the packets as long as it is within the communication range of at least one backbone node. In backbone flooding protocol, the backbone is static since the backbone nodes will need to forward more packets than other nodes in the network, in which power get reduced quickly. So we need to distribute the backbone function evenly across the network. We can adopt one or more of the following options. The first option is to periodically rebuild the flooding backbone for balancing the load in the network. During backbone reconstruction we would need to consider the remaining energy at each sensor node. The second option is to construct multiple backbones at the beginning such that each node belongs to approximately the same number of backbones. Each event packet will be delivered to sinks using a randomly selected backbone. In this way, the sensor

nodes in the network will roughly forward the same number of event packets. We will investigate these issues in future work.

We present an approximation algorithm for this problem.When we say that a sensor v covers some other sensors, we mean that v is responsible for directly delivering 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.

5. Simulations

We evaluated the performance of our approach through simulation using GLOMOSIM [4]. The simulated scenario which has one sink and 32 nodes is shown in Fig. 5.1. Each node generates a data packet (The size of data packet is 1024 bytes) per interval time 1 sec from the starting time 5sec.

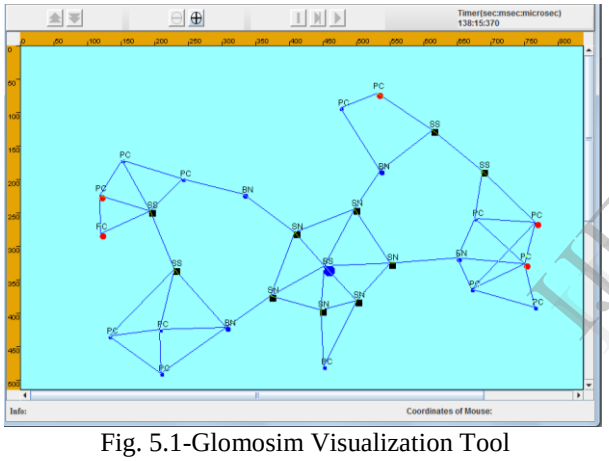

Fig. 5.1-Glomosim Visualization Tool

We now evaluate the proposed sink-location privacy approaches described in this paper. We focus on the location privacy achieved and the communication overhead introduced by each technique. In terms of privacy, we have already shown that none of the previous methods can provide location privacy under the assumption of a global eavesdropper. Both methods provide sink-location privacy against a global eavesdropper. 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. In the backbone flooding, we need to always keep the backbone connected and rebuilds the backbone from time to time to balance the communication costs between nodes.

5.1. Energy Consumption

For a privacy-preserving routing technique, its energy consumption is measured by the additional communication used for hiding the traffic carrying real data. Based on the transmission, the energy consumption varies for each node. The axis profile for energy consumption graph which contains node number on X-axis and energy consumption on Y-axis. The output shown in fig 5.2.

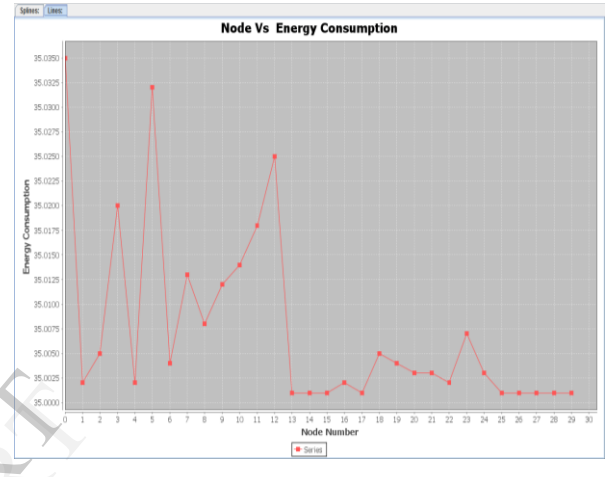

Fig. 5.2- Node vs. Energy Consumption

5.2. Delay

The delay for transmission varies at every node. The axis profile for Delay graph which contains node number on X-axis and Delay on Y-axis. The output shown in fig 5.3.

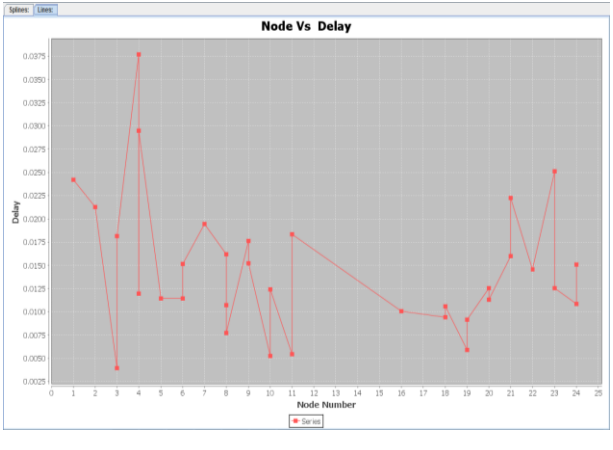

Fig. 5.3-Node vs. Delay

5.3. Collision

When the large amount of sensing information is received at a node collision occurs. The graph describes the collision rate. The axis profile for Collision graph which contains node number on X-axis and Collision on Y-axis. The output shown in fig 5.4.

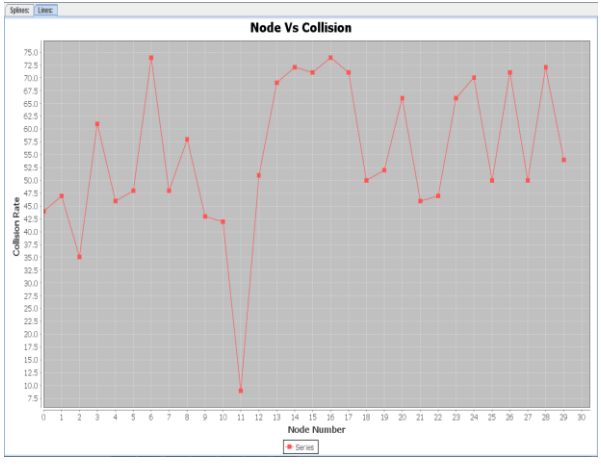

Fig.5.4- Node vs. collision

5.4. Throughput

Based on the received sensing information, the throughput for each node is determined. The axis profile for Throughput graph which contains node number on X-axis and Throughput on Y-axis. The output shown in fig 5.5.

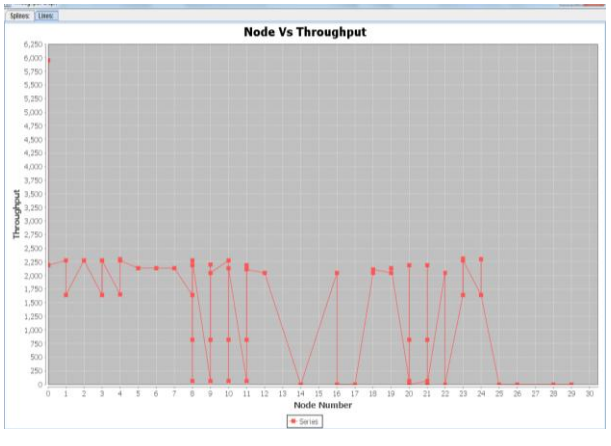

Fig.5.5- Node vs. Throughput

6. Conclusions

There are a number of directions that worth studying in the future. First, in this paper, we 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 our 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.

Future research on the topic includes how to reduce the energy cost while guaranteeing the sink's location privacy. This paper aims to maintain source and sink privacy under eavesdropping and node compromise attacks. The majority of the above mentioned efforts attempt to solve privacy issues in heterogeneous WSNs where all sensor nodes have different Capabilities.

References

[1] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp. Security.

[2]Privacy (S&P '03), pp. 197-213, May 2003.J. Breckling, Ed., *the Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

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

[4] Lokesh Bajaj, Mineo Takai, Rajat Ahuja, Ken Tang, Rajive Bagrodia, Mario Gerla,"GloMoSim: A Scalable Network Simulation "

[5] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source location privacy in sensor network routing," in Proc. Of IEEE ICDCS, Columbus, Ohio, USA, Jun 2005.

[6]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.