LOCATION PRIVACY IN SENSOR NETWORKS AGAINST A GLOBAL EAVESDROPPER

Bhillare P B[1], Bhusari D G[2]

[1] *H.O.D., Computer Engineering, Aditya Polytechnic, Maharashtra, India*
[2] *Lecturer, Computer Engineering, Aditya Polytechnic, Maharashtra, India*

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. We first argue that a strong adversary model, the global eavesdropper, is often realistic in practice and can defeat existing techniques. 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. We also 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, we demonstrate that the prop used techniques are efficient and effective in protecting location information from the attacker.

Keyword: - *Eavesdropper, Privacy, Sensor networks.*

1. INTRODUCTION

A wireless sensor network (WSN) typically consists of a large number of small, multifunctional, and resource constrained sensors that are self-organized as an ad hoc network to monitor the physical world . 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. Abuse of such information can cause monetary losses or endanger human lives. To protect such information, researchers in sensor network security have focused considerable effort on finding ways to provide classic security services such as confidentiality, authentication, integrity, and availability. Though these are critical security requirements, they are insufficient in many applications. The communication patterns of sensors can, by themselves, reveal a great deal of contextual information, which can disclose the location information of critical components in a sensor network. For example, in the Panda-Hunter scenario, 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 sensor that detects this signal, the source sensor, then sends the location of pandas to a data sink (destination) with help of intermediate sensors. An adversary (the hunter) may use the communication between sensors and the data sinks to locate and then capture the monitored pandas. In general, any target-tracking sensor network is vulnerable to such attacks. As another example, in military applications, the enemy can observe the communications and locate all data sinks (e.g., base stations) in the field.

2. EXISTING SYSTEM

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 solutio ns. 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.

2.1 Privacy in Wireless Sensor Network

Since wireless sensor network are deployed in an open environment so the privacy is one of the major concerns in randomly deployed sensor networks. Privacy in WSNs are basically categorized in two parts.(i) Data privacy and (ii) Context-based privacy. Different types of privacy issues in wireless sensor networks are shown in Fig.1. Data or Content privacy focuses on, amongst others, providing integrity, non -repudiation, and confidentiality of the messages exchanged in a WSN. Data privacy requires strong cryptographic techniques to be placed in sensor networks and it is out of purview of the current work. On the other hand, context privacy can be grouped in two categories called as temporal and location contexts. In this article, we mainly concentrate on the source location privacy which is a type of location privacy.
SLP requires more than just confidentiality of the messages exchanged between nodes. SLP requires that the flow of the messages does not give away the location of a source node.

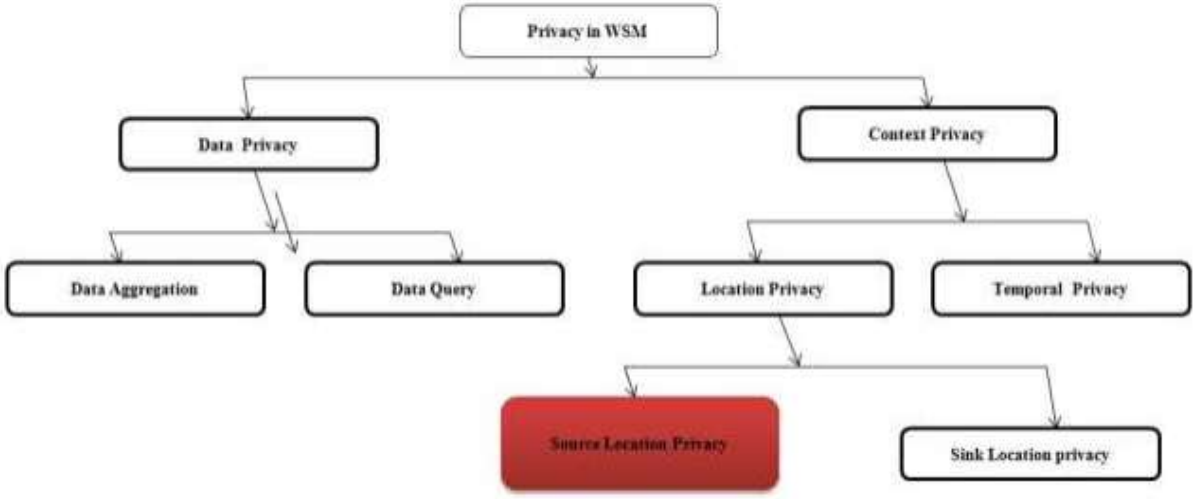

Fig. 2.1. Hierarchy of privacy in WSN's

2.2 Related Work

We show 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, a method that is effective only against local eavesdroppers. 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 a packet that was generated on the same event. In our simulation, we assume that the adversary has deployed a network to monitor the traffic in the target network.

3. NETWORK AND ADVERSARY MODEL

In this section, we outline the network model we have considered for our proposal. Here we explain our network model whereas in subsection, we discuss the nature and capabilities of the adversary.

3.1 Network Model

The considered network consists of a Source node, a Phantom node, a Base station, some fake source nodes and large number of homogeneous sensor node which was deployed randomly to monitor an asset like a Panda as in Panda Hunter game2. The source node, phantom node and fake nodes have the same capabilities as the other homogeneous nodes have. They are only performing some special tasks when required to do that. The node which senses the event like presence of panda is called the Source node. The nodes which forward packets to the base

station on behalf of source node is called a phantom node. The fake nodes generates fake packets which are identical to the real packet generated by the source node. The base station on the other hand has more capabilities in terms of storage, transmission power, computing capabilities and energy compared to the other nodes.

3.2 Adversary Model

The adversary tries to find the location of the source node as a passive attacker and is having some technical advantages over the sensor nodes. The adversary is assumed to have the following characteristics:
• An adversary knows the location of the base station and try to determine the location of the source node from the instance of the messages it overhears. Initially, the adversary starts from the base station. The hearing radius of an adversary is equal to the transmission radius of the nodes. As a result, the adversary can monitor only the traffic area around the node which it observes and not the whole network. An adversary has a radio transceiver, a workstation and any equipment it might need to have illegal access to the network.
• An adversary is resource-rich. It can physically move from one sensor to another and has an unlimited amount of power. The adversary will not interfere with the proper functioning of the network, such as destroying sensor nodes or modifying packets in order to not trigger other security mechanisms. They has enough storage capabilities also. It can remember all the messages it has overhear and decide if a message is new or it is the same with another it has already overheard. This is because, same messages can follow different paths toward the destination and use the same nodes in different time slots. They should be able to verify the new messages.

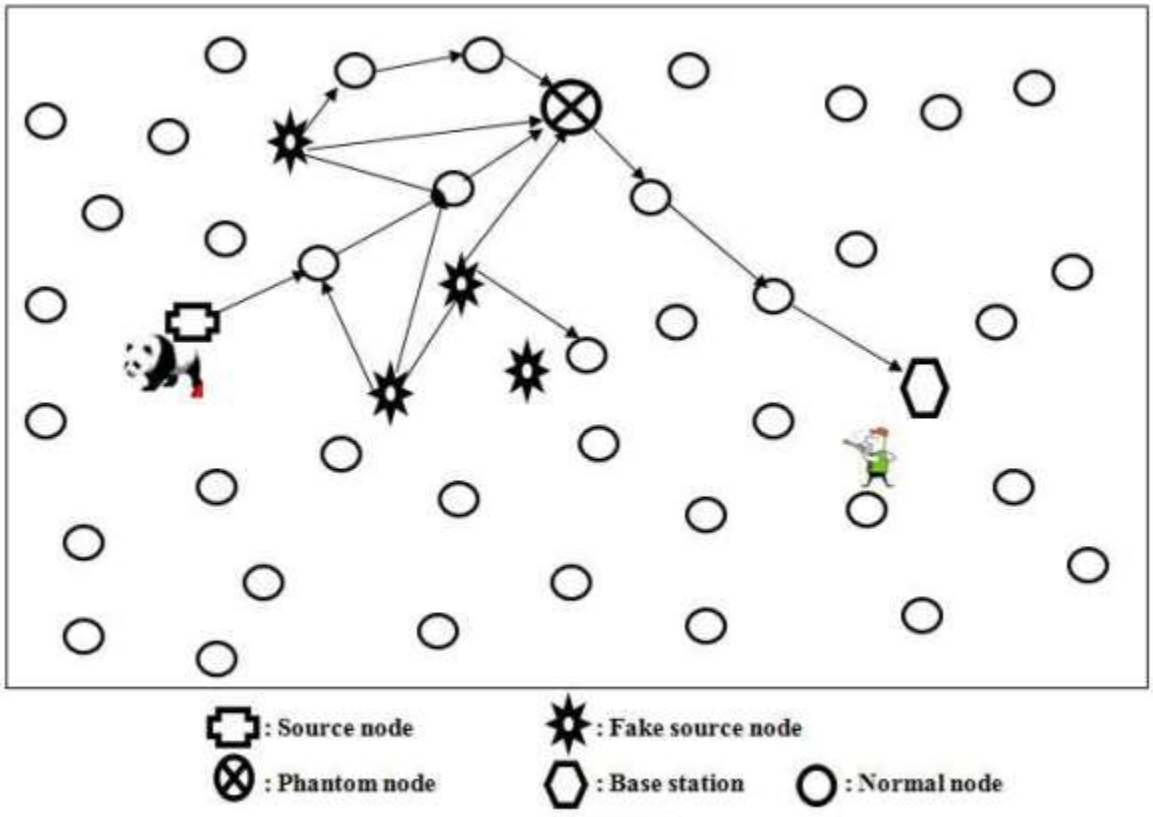

Fig. 3.2 Network Model Architecture of WSN

3.3 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 n odes in the network are encrypted so that the contents of packets appear random to the global eavesdropper. Many key predistribution protocols can be used for this purpose.

3.3.1 Source-Location Privacy Techniques

In this section, we present two techniques to provide location privacy to monitored objects in sensor networks, periodic collection and source simulation. The periodic collection method achieves the optimal 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 overhead, and latency.

3.3.2 Sink-Location Privacy Techniques

This section presents 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, we focus on protection of passive sinks that only receive data from sensors. We will consider location privacy for sinks that broadcast packets in future work.

4. CONCLUSIONS

Source location privacy is one of the important issues in random deployment of sensor networks which is used for asset monitoring. Even with strong cryptographic techniques in place the context of location and time may be traced by an adversary by just tracing and analyzing the traffic. In this article, we have proposed an algorithm to protect the location information of a sensor node sensing an event and sending it to the base station. In this section, We present the result of our experimentation under the different circumstances. A metric called Hit ratio is used to denote the privacy level of source location. The Hit ratio *ht* is defined as

$$ht = \frac{\text{total packet sent by the source}}{\text{total packet traced by the adversary}}$$

If the *Hit ratio* is near to 0 then we can say that the privacy level is high and if the *Hit ratio* is near to 1 then we can say the privacy level is minimum. We shows that the Hit ratio is be inversely proportional to the number of fake sources. i.e, if the number of fake source increases the Hit ratio will be decrease and vice-versa.

5. ACKNOWLEDGEMENT

Our thanks to the experts who have contributed towards the development of this paper.

6. REFERENCES

[1]. R. Agrawal, A. Evfimievski, R. Srikant,, "Information sharing across private databases in:" : Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data, 2003, pp. 86–97.
[2]. Jian, Y., Chen, S., Zhang, Z., Zhang, L... A novel scheme for protecting receiver's location privacy in wireless sensor networks. *IEEE Transactions on Wireless Communications* 2008;**7**(10):3769–3779. doi:10.1109/T-WC.2008.070182.
[3] Kamat, U., Zhang, Y., Ozturk, C.. Enhancing source-location privacy in sensor network routing. In: *25th IEEE International Conference on Distributed Computing Systems ICDCS*. 2005, p. 599–608.
[4]. K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks against a Global Eavesdropper," Proc. IEEE Int'l Conf. Network Protocols (ICNP '07), 2007