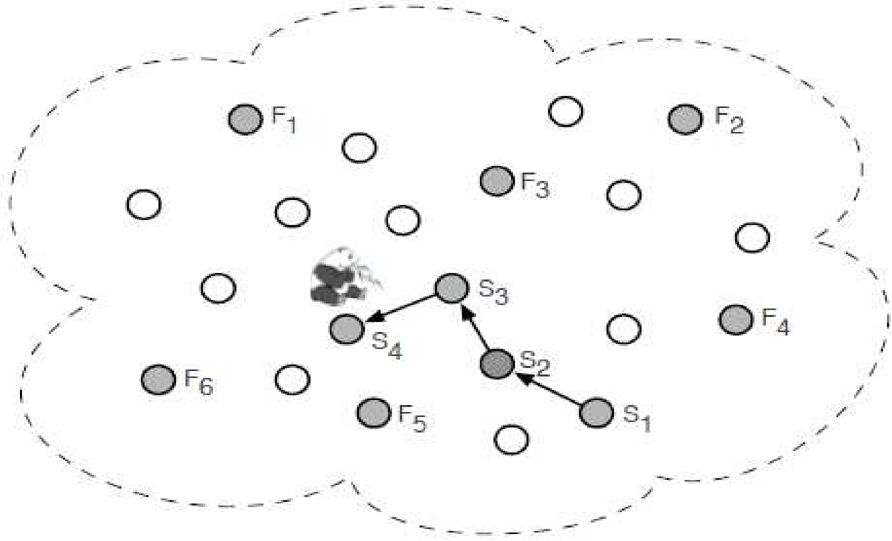
Protecting Location Privacy in Sensor Networks Against a Global Eavesdropper

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 proposed techniques are efficient and effective in protecting location information from the attacker.

Architecture:



Movement pattern leaks the location of the panda

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 solutions. 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.

Disadvantages:

However, these existing approaches assume a weak adversary model where the adversary sees only local network traffic.

Proposed System:

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.

Advantages:

Specifically, he is able to locate every sensor node in the target network and eavesdrop every packet this node delivers.

Modules:

1. Attackers Modules.
2. Privacy-Preserving Routing Techniques.
3. Adversary Model.
4. Privacy Evaluation Model.
5. Security Analysis.

1. Attackers Modules:

The appearance of an endangered animal (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.

2. Privacy-Preserving Routing Techniques:

This section presents two techniques for privacy-preserving routing in sensor networks, a *periodic collection* method and a *source simulation* method. The periodic collection method achieves the optimal 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 trade-offs between privacy, communication cost, and latency; it can be effectively applied to real-time applications. In this paper, we assume that all communication between sensor nodes in the network is protected by pair wise keys so that the contents of all data packets appear random to the Global eavesdropper. This prevents the adversary from correlating different Data packets to trace the real object.

3. 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. This information can include the location of the events detected by the target sensor network such as the presence of a panda. The Panda-Hunter example application was introduced in, and we will also use it to help describe and motivate our techniques. 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. 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.

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.

4. 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. We consider a powerful adversary who can eavesdrop the communication of every

Sensor node 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.

5. Security Analysis:

The generation number of a packet can be hidden in the secure routing scheme through link-to-link encryption. In this way, attackers cannot find the generation number of a packet for their further analysis. Notice that secure routing paths are only required to be established at the beginning of each session; during the packet transmission, secure routing paths are not required to change or re-established for each new generation.

Algorithm:

Localization algorithm:

where ¨OT is the set of all possible observations, i.e., ¨OT ={(i, t)}i□I,0≤t≤T . This function returns the identity of the location of the object at time T , if the set of observations is a candidate trace, and returns □ otherwise. For simplicity, we assume that the pattern analysis does not return fractional values, e.g. a probabilistic measure of the chance that a trace is a candidate trace or not.We say that a pattern analysis function is *perfect* if it can identify all candidate traces without error, i.e. without false positives or false negatives. In this paper, we consider a strong adversary who uses a perfect pattern analysis function.

System Requirements:

Hardware Requirements:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

Software Requirements:

- Operating system : - Windows XP.
- Coding Language : C#.net
- Data Base : SQL Server 2005