Source Location Privacy Considerations in WSNs

Ruben Rios, Javier Lopez

ruben@lcc.uma.es

UCAmI 2010, Valencia
Wireless Sensor Networks

- WSNs can be used in applications where sensors are unobtrusively embedded into systems, involving operations like:
  - Monitoring
  - Tracking
  - Detecting
  - Collecting
  - Reporting

- WSNs enable the AmI paradigm
The Privacy Problem

• The integration of WSNs will not only bring benefits but also serious privacy risks

• Simple observation of network traffic can reveal information about the network itself and the events being monitored, even if messages are cryptographically protected

• Home Sensor Network
  - Empty house
  - Appliances in use
  - Unethical in-house behaviour
  - ...

source: http://pleaserobme.com/
The Location Privacy Problem

- The **path followed** by messages expose both the source and destination
  - **Source Location Privacy**
  - **Receiver Location Privacy**

- Important since it gives the attacker the ability to determine where some **events of interest** to him are taking place
Talk Outline

• Introduction

• Source Location Privacy
  - Node Identity Protection
  - Traffic Pattern Protection

• Conclusions
Nodes Identity Protection

- The first step is to hide nodes identities from being eavesdropped
- The adversary can create a map of the network
- Packet headers contain information in order to route the packets through the network

TinyOS 2.x MAC Header
A pseudonym is a name or identifier that can be used instead of a real name.

Using fixed pseudonyms eventually provides no protection because the attacker relates a pseudonym to a node.

Several schemes have been proposed to create dynamic pseudonyms:
- Pool of pseudonyms (memory)
  - Simple Anonymity Scheme
- Cryptographic schemes (computation)
  - Cryptographic Anonymity Scheme
  - Hashing-based ID Randomization (HIR) and Reverse HIR
Talk Outline

• Introduction

• Source Location Privacy
  - Node Identity Protection
  - Traffic Pattern Protection

• Conclusions
Traffic Pattern Protection

- A more skilled attacker can perform traffic analysis attacks to determine the location of source nodes.

- Problem motivated by the *Panda Hunter Game*:
  - Local adversary
  - Starting by the base station
  - Moves towards received packets

- The hunter finds the source because packets follow fixed paths.
Traffic Analysis Countermeasures

- We present and analyse a taxonomy of solutions based on the power of the adversary.
Multiple Random Paths

• Mislead the adversary by using different routes for every message
  - Phantom Routing
  - Greedy Random Walk

• Every packet follows a different path
• Receptors are away from source because it’s greedy
Multiple Random Paths

- Random Parallel Routing
  - Data packets are evenly distributed on each well-separated path

- Random Intermediate Node
  - Intermediate nodes are far away from the source
Directed Random Paths

- Phantom Routing included directed random walks by separating neighbors in two groups.

- The angle of arrival and the forwarding angle are typically used to direct random walks.
Network Loop Methods

- The aim is either to **trap the adversary** into the loop or to **mix packets** making them indistinguishable.

Cyclic Entrapment Method

Network Mixing Ring
• Introduction

• Source Location Privacy
  - Node Identity Protection
  - *Traffic Pattern Protection*
    - Local adversary
    - Global Adversary

• Conclusions
Fake Message Transmission

• Previous approaches are ineffective against global eavesdroppers since sensor nodes only transmit in the presence of real events.

• Every node transmit fake messages (Fy) to hide the presence of real events (Ex).

• However, this changes the message distribution!
Fake Message Transmission

- Periodic Collection delays (\(\delta\)) real messages in order to follow the same distribution as fake messages
  - Incurs an excessive delay

- The delay can be reduced but this increments energy consumption
Energy-Aware Approaches

- The goal is to provide an adequate privacy level while saving energy and not introducing an excessive delay

- Different solutions
  - *Source simulation*: nodes simulate the *behaviour* of moving objects in the field
  - *Traffic filtering*: in PFS and TFS proxy nodes strategically placed filter out fake traffic
  - Using already *existing traffic*: messages are hidden within beacons
  - *Statistical approaches*: move forward real messages without modifying the message distribution
Statistical Approaches

- Fake messages are transmitted according to a probability distribution \( F_X \) within a sliding window.

- Real events are transmitted a.s.a.p \( (F'_4) \) so that the probability distribution is unaltered.

- The attacker gains no information by performing a statistical test.
Statistical Approaches

- However, a more skilled attacker could spot differences between two sliding windows

- In the presence of real events, next transmissions are delayed
  - By counting the number of short-long inter-delays an attacker can distinguish intervals containing real events

- Solution is to design fake intervals to resemble real intervals as much as possible
Talk Outline

• Introduction

• Source Location Privacy
  - Node Identity Protection
  - Traffic Pattern Protection

• Conclusions
Conclusions

• We have proposed and discussed a taxonomy of solutions to a single privacy problem
  – Local Adversaries → Routing-based approaches
  – Global adversaries → Fake message transmissions

• Privacy preservation is challenging in WSNs because of the extreme limitation of nodes. Solutions must trade-off between the protection level and the cost associated

• New scenarios, adversarial models and solutions are expected to appear with the full integration of WSNs and the Internet
Thanks for your attention!

Ruben Rios, Javier Lopez

ruben@lcc.uma.es

UCAml 2010, Valencia