Deconstructing Source Location Privacy-aware Routing Protocols

Arshad Jhumka and Matthew Bradbury

SAC 2017
Outline

- Introduction
- Related Work
- Models Used
- Example Techniques
- Source Location Privacy Components
- Case Studies
A wireless sensor network (WSN) is a collection of computing devices called nodes, they have:

- a short range wireless radio
- an array of sensors such as light, heat and humidity
- a simple low powered CPU
- a battery with limited power supply

Applications include:

- Tracking
- Monitoring
What is Context Privacy?

- Privacy threats can be classified as either content-based or **context-based**
- Content-based threats have been widely addressed (using cryptography) (Perrig et al. [6])
- Context-based threats are varied
- We focus on protecting the location context of broadcasting nodes
The Problem of Source Location Privacy (SLP)

Given:
- A WSN that detects valuable assets
- A node broadcasting information about an asset

Found:
- An attacker can find the source node by backtracking the messages sent through the network.
- So by deploying a network to monitor a valuable asset, a way has been provided for it to be captured.

The Problem:
- Panda-Hunter Game
- Difficult
Related Work

- Attacker Models (Benenson et al. [1])
- Phantom Routing (Kamat et al. [3])
- Fake Sources: TFS/PFS (Bradbury et al. [2])
- Combination: Tree-based (Long et al. [4])
- Global Attacker: (Mehta et al. [5])
Privacy Model

- Aim of an SLP protocol: prevent the attacker from capturing an asset through information the WSN leaks.
- A stationary asset cannot be protected as an attacker can perform an exhaustive search.
- Mobile assets will only stay in detection range of a WSN node for a certain amount of time.
- The SLP problem can only be considered when it is time-bounded.
- This captures the maximum amount of time an asset will stay near a certain node.
- The safety period is how long the asset will be protected for.
- Other work has defined the safety period as unbounded and attempted to increase it.
- We assume a bounded safety period.
Attacker Model

- Attacker’s aim is to reach the source within the safety period
- Assume a distributed eavesdropper present in the network
- Attacker range is limited to not cover the entire network
- Attacker is mobile
- Attacker follows first new packet it receives
Example: Protectionless Flooding
Example: Dynamic Fake Sources
Example: Phantom Routing
We argue that routing-based SLP techniques can be separated into two categories:

- **Spatial**
  - Lure the attacker to some other part of the network instead of the source-detecting node.
  - Requires spatial redundancy in the network.

- **Temporal**
  - Delay the attacker on its path to the source, so the safety period expires.
  - Requires delay-tolerant application.

Some algorithms will use a combination of these strategies to delay the attacker.
Component 1: Selection of Decoys

- Decoys need to be selected so there is little or no correlation between them and the source.
- Decoy selection should not indirectly leak the source’s location.

- Spatial Selection
  - Attacker is made to travel a longer route (other than shortest path)
  - Decoys typically change slowly and subsequent decoys are close to one another

- Temporal Selection
  - Attacker is made to miss messages, causing it to be delayed
  - Decoys typically change frequently
Component 2: Use and Routing of Control Messages

- **Spatial Selection**
  - Aim to select decoys close to one another to lure the attacker along a path
  - Decoys need to be chosen in a space away from the source
  - Control messages need to select these decoys
  - Allows different protocols for convergecast routing and control message routing

- **Temporal Selection**
  - Aim to select decoys so that an attacker misses messages and is delayed
  - Decoys can be spread out over an area
  - The control messages typically form part of the convergecast route
Component 3: Use and Routing of Decoy Messages

- Spatial
  - Decoy nodes are luring the attacker, so want the attacker to receive these messages
  - Flooding is a good protocol, as it should lure the attacker from anywhere in the network
- Temporal
  - Decoy messages typically not required
  - As SLP is provided by the attacker missing hearing messages
Case Studies

(a) Dynamic Fake Sources: An example of spatial selection of decoys [2].

(b) Phantom routing: An example of temporal selection of decoys [3].

(c) Tree routing: An example of temporal delay by alternating which branch the source node attaches to.
What does this mean?

Routing-based SLP techniques need to:

▶ Provide spacial redundancy in which to allocate decoy nodes
▶ Delay messages in a suitable way
▶ Not all applications will be able to provide spacial redundancy
▶ Not all applications will be able to tolerate delays
▶ This categorisation helps identify requirements of algorithms that the network deployer needs to provide
Some Exclusions

- Not all SLP techniques can be categorised using these components
- We are focusing on protocols at the routing layer protecting against a local attacker

The following types of protocols are examples that will not decompose this way:
- MAC based protocols
- Data mule approaches
- Global privacy techniques
Routing-based SLP techniques are either spatial, temporal or a combination.

Identified three key components:
- Decoy Selection
- Routing of control messages
- Routing of decoy messages

Given three examples to demonstrate these points.

Future Work:
- We will formalise the components
- Develop correctness proofs for the composition to yield SLP-aware protocols
Any questions?


