A Near-Optimal Source Location Privacy Scheme for Wireless Sensor Networks

Matthew Bradbury and Arshad Jhumka

TrustCom 2017

Outline

1. Introduction
2. Privacy and Attacker Models
3. Integer Linear Programming Model and Results
4. Near-optimal Heuristic
5. Conclusions

What is a Wireless Sensor Network?

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** (Environment, **Assets**, . . .)

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)
- Context-based threats are varied
  - Location of event source
  - Location of base station
  - Time at which the event occurred
- We focus on protecting the **location** context of the **event source**

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

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.
- A *mobile asset* 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.
- The *safety period* is how long the asset will be protected for.

Attacker Model

Aim of an Attacker: to reach the source within the safety period.

The attacker:

- is present in the network
- is mobile
- has a limited range
- starts at the sink
- follows the first new packet it receives

How to Develop a Technique?

Previous approaches: Have idea $\rightarrow$ implement it $\rightarrow$ test performance

- Developed solutions have had good properties proven about them
- Optimal solutions have been found for global attackers

Better approach:
Find optimal solution $\rightarrow$ create heuristic with similar output $\rightarrow$ test performance

- Performance needs to be tested as the optimal solution may not be implementable
- Optimal solution doesn't give optimal algorithm, so some creativity is still needed to develop a heuristic
- Can use different optimality measures to look for different solutions

Integer Linear Programming Model I

- Integer Linear Programming (ILP) allows an optimal solution to be found to certain problems
- Express SLP-aware routing as an ILP optimisation problem
- A solution is obtained using IBM's ILOG CPLEX

Aim to obtain the best utility for this objective function:

$$
\begin{aligned}
\text{maximise} \quad & \text{The distance from the attacker's final position to the source} \\
\text{subject to} \quad & \text{Routing Constraints ctR1 to ctR6,} \\
& \text{Attacker Constraints ctA1 to ctA7.}
\end{aligned}
\tag{1}
$$

Integer Linear Programming Model II

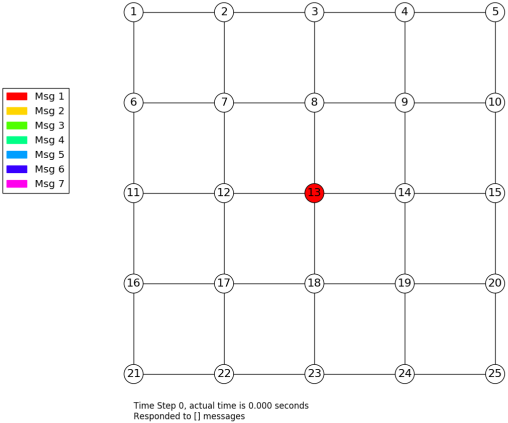
- ctR1 At $t = 0$, no messages are broadcasted.
- ctR2 From $t > 0$, each source node generates a message every P_{src} until the safety period is reached.
- ctR3 A node sends one message or no messages in a time slot.
- ctR4 Once a message is broadcasted by a node it is not broadcasted by that node again.
- ctR5 A node can broadcast a message only after a neighbour broadcasted that message in a previous time slot.
- ctR6 All messages sent by the source(s) must reach the sink.

Integer Linear Programming Model III

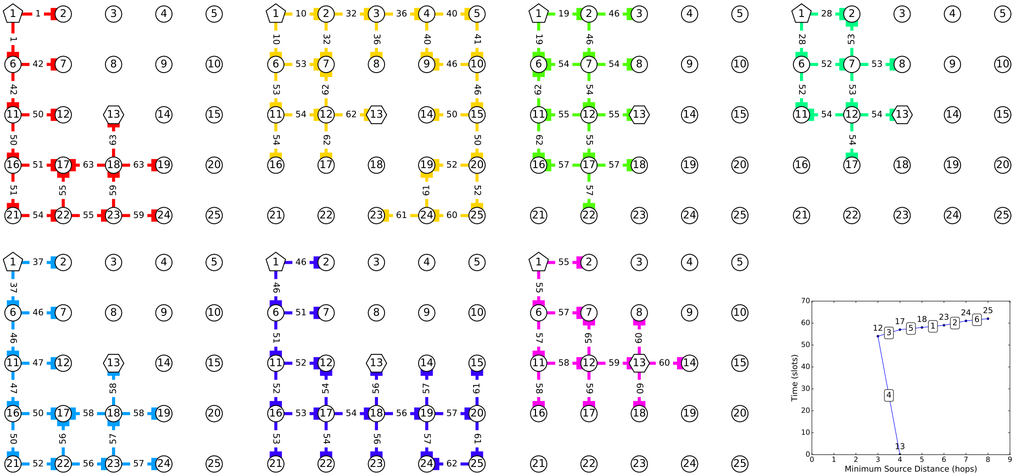
- ctA1 At $t = 0$ the attacker moves from the attacker's starting position to that same position.
- ctA2 The attacker makes exactly one move each time slot.
- ctA3 A move must be from the attacker's current location.
- ctA4 If the attacker moves to n from m at time τ, then it must be because at time τ the node n broadcasted a message.
- ctA5 If the attacker receives a message that it has not previously moved in response to, then the attacker moves in response to that message.
- ctA6 If the attacker moved in response to a message at time τ, then at no time $\tau' > \tau$ will the attacker move in response to that message again.
- ctA7 If no neighbour broadcasts a message the attacker stays where it is.

Model Result I

- Source at node 1 (top left)
- Sink at node 13 (centre)
- Attacker starts at the sink (centre)
- 9 slots per second
- 7 Messages sent
- Source Period 1 second/msg
- Safety Period of 7 seconds



Model Result II



Inspired Heuristic

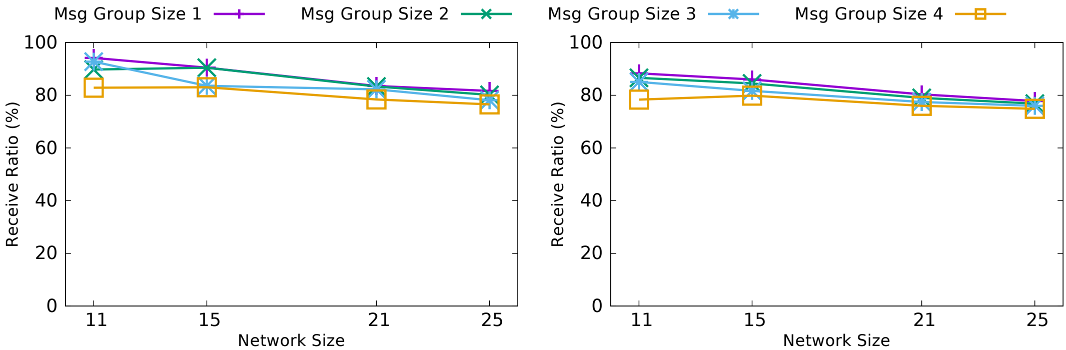
- Implementing the optimal solution requires global knowledge, so is unsuitable for a WSN.
- A heuristic was implemented instead based on these observations:

1. The routing path should go around the sink and approach from the opposite direction to the source.
2. Some routes should take the shortest path from the source to the sink.
3. Messages should be delayed so multiple messages are grouped together.
4. Messages should be delayed as late as possible with respect to the safety period.

Routing Algorithm

1. **AvoidSink**: In this first stage messages are routed around the sink.
2. **Backtrack**: Messages may end up attempting to go towards the sink and not having any valid routes, so they need to backtrack.
3. **ToSink**: Once a message has finished routing to avoid the sink it needs to be delivered to the sink.
4. **FromSink**: Finally, the message is sent in a starburst from the sink.

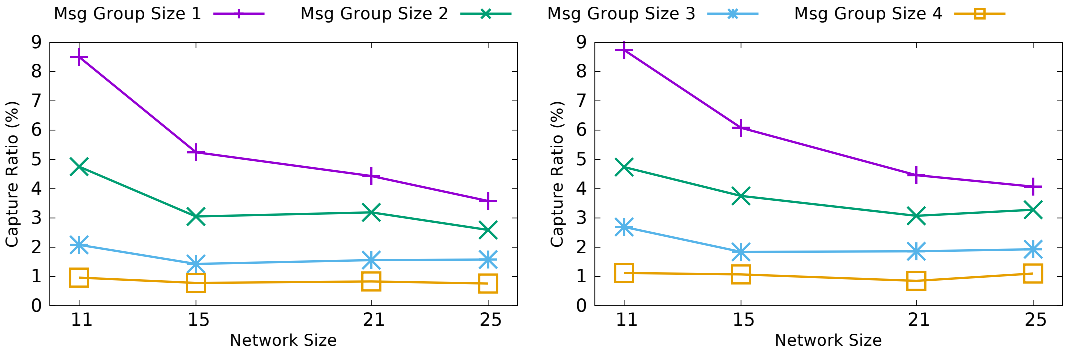
Results – Receive Ratio



(a) Source Period 2.0 seconds

(b) Source Period 0.25 seconds

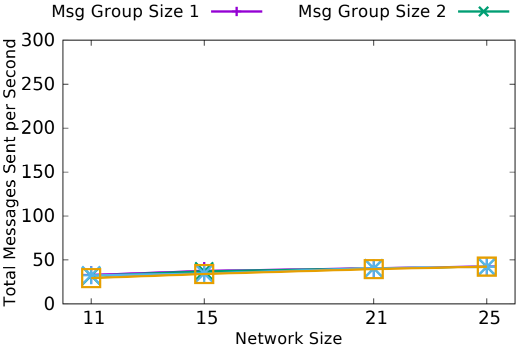
Results – Capture Ratio



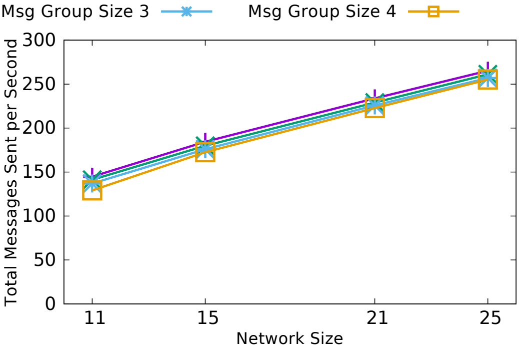
(a) Source Period 2.0 seconds

(b) Source Period 0.25 seconds

Results – Messages Sent per Second

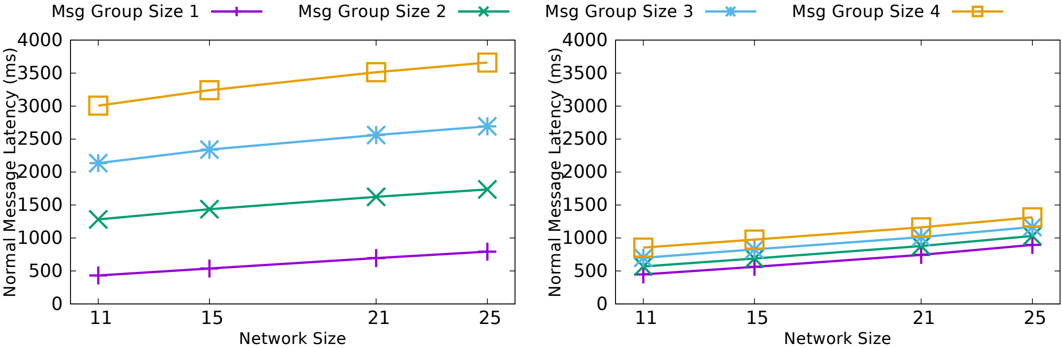


(a) Source Period 2.0 seconds



(b) Source Period 0.25 seconds

Results – Message Latency



(a) Source Period 2.0 seconds

(b) Source Period 0.25 seconds

Discussion

- A different objective function could be optimised for, such as:
  - Latency
  - Messages Sent
- High latency may make this technique unsuitable for some applications
  - for military it may be too high
  - for animal monitoring it should be acceptable
- Different contraints could be used
  - We require delivery of all messages, some applications may not require this
- The ILP model could be extended to support other SLP techniques (e.g., fake sources)

Summary

- Presented a way to model SLP-aware routing as an ILP optimisation problem
- Obtained an optimal solution from that model
- Implemented a near-optimal heuristic based on the optimal model result
- 1% capture ratio can be achieved by trading off for a higher latency

Thank You for Listening

Any Questions?