Phantom Walkabouts in Wireless Sensor Networks

WARWICK

Chen Gu, Matthew Bradbury and Arshad Jhumka

SAC 2017

Outline

- Introduction
- Related Work
- Phantom Walkabouts
- Experiments and Results

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**

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

Important Considerations

- Wireless Sensor Nodes are energy constrained
- Sending messages is the most expensive task
- Receiving messages is the next most expensive task (Shnayder et al. [7])

The Problem of Source Location Privacy

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: Periodic Collection (Mehta et al. [5])

Phantom Walkabouts

- A modification of Phantom Routing

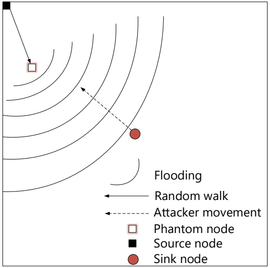
Phantom Routing:

1. Source message is routed towards or away from a landmark node
2. After some number of hops, or when the landmark node is reached the message is routed towards the sink

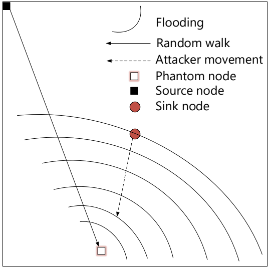
- The landmark node is typically the sink
- This means messages tend not be routed further than the sink

- Phantom Walkabouts experiments with paths past the landmark node (long random walks)
- We test with paths that do not go beyond the landmark node (short random walks)
- Finally, we test with alternating patterns of both (phantom walkabouts)

Considering Walk Lengths



(a) Short Random Walk



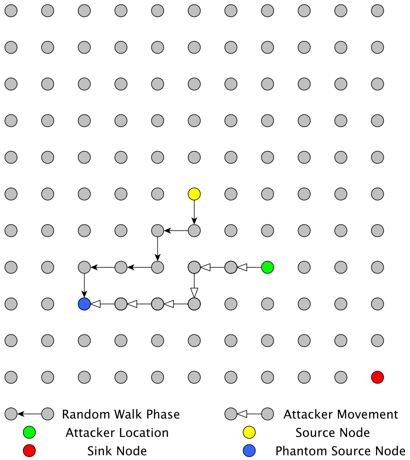
(b) Long Random Walk

- Phantom node can pull the attacker towards the source node with a short random walk
- Phantom node can pull the attacker away from the source node with a long random walk
- Long random walk requires additional messages

Short Random Walk Routing

Short Random Walk Procedure

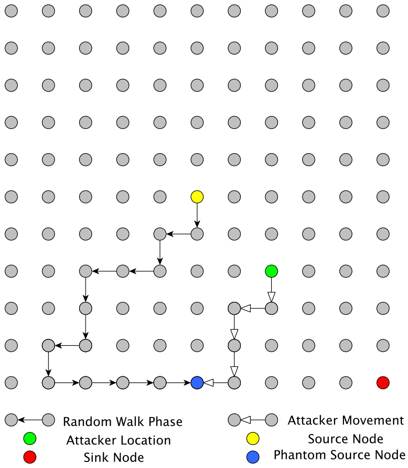
- Each node divides its neighbours into four directions
- Nodes transmit messages to one of four directions
- Phantom source floods messages through the network after a message finishes the random walk
- Short walks are less than the sink-source distance (in hops)



Long Random Walk Routing

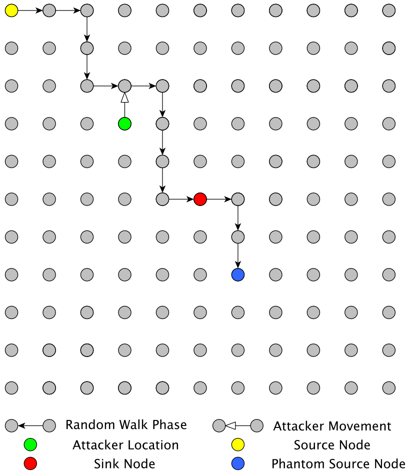
Long Random Walk Procedure

- Each node divides its neighbours into four directions
- Nodes transmit messages to one of four directions
- If message is blocked in the chosen direction, nodes will send the received messages to other direction
- Phantom source floods messages through the network after a message finishes the random walk
- Long walks are greater than the sink-source distance (in hops)



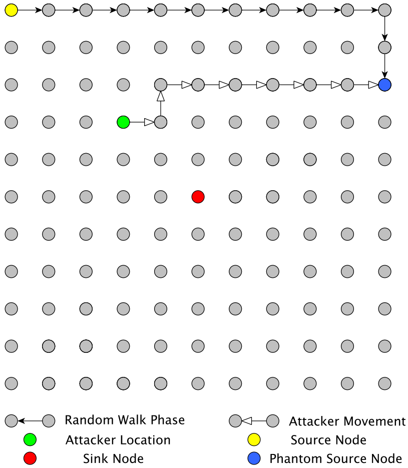
A Problem with Long Walks

- The attacker has high probability capturing messages before long random walk routing ends
- Nodes are always forwarding messages in the closer-to-sink direction



Biased Random Walk

- The message firstly chooses the bias random walk direction (i.e., horizontal or vertical direction)
- Messages have high possibility walking along the chosen direction
- When the message reaches the end of that direction, nodes will send it to other direction to continue the rest random walk
- The message is then flooded to the network after the phantom node is reached



Phantom Walkabouts

- The phantom walkabouts technique extends the phantom routing protocol by adopting variable lengths of phantom routing
- When a source node routes messages using phantom walkabouts, a message m_i is selected to either go on a short random walk of length s or long random walk of length l. The sequencing of messages looks like as follow

$$\underbrace{M_s, \cdots, M_s,}_{m} \underbrace{M_l, \cdots, M_l,}_{n} \underbrace{M_s, \cdots, M_s,}_{m} \underbrace{M_l, \cdots, M_l,}_{n} \cdots$$

- PA(m,n) ($m, n \geq 0$) denotes m short random walk and n long random walk messages

Experimental Setup

- TOSSIM (simulator for TinyOS)
- Square grid network of 11^2, 15^2, 21^2 and 25^2 nodes
- Message rates: 1, 2, 4, 8 messages/second
- Short random walk lengths S: $2, 3, \dots 0.5 \times \Delta_{ss}$ (Δ_{ss} is sink source distance)
- Long random walk lengths L: $2 + \Delta_{ss}, \dots 1.5 \times \Delta_{ss}$
- The phantom walkabouts random walks: $\{(S_i, L_i) \mid 1 \leq i \leq |S|\}$
- Network topology: sink in the centre and source in the corner
- Attacker starts at the location of the sink
- 500 repeats were performed for each combination of source location and parameters

Experiments for multiple sources are in the paper – show similar patterns to single sources

Performance Metrics: Safety Period and Capture Ratio

- Safety Period (simulation time)

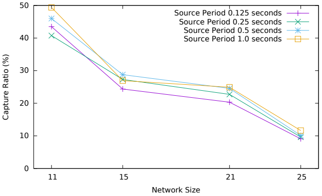
$$1.3 \times tt \tag{1}$$

- tt is the average time it takes an attacker to capture the source when protectionless flooding is used
- Capture Ratio

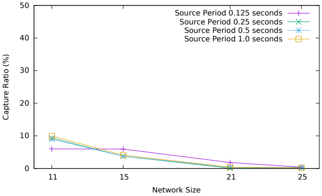
$$CR = \frac{\text{Number of experiments ending in a capture}}{\text{total number of experiments}} \tag{2}$$

- When there are multiple sources in the network, a capture occurs when at least one of the sources are detected

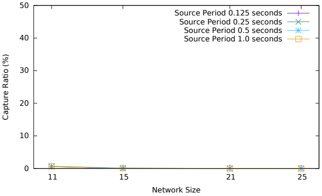
Results: Capture Ratio



(a) *PW*(1, 0): Using **short** random walks



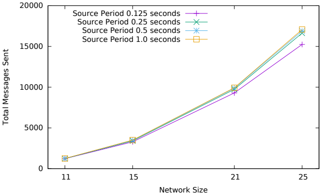
(b) *PW*(1, 1): Using **alternating short and long** random walks



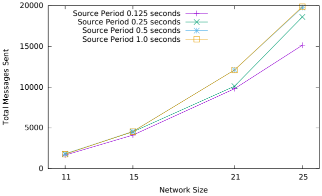
(c) *PW*(0, 1): Using **long** random walks

- The level of SLP increases (capture ratio decreases) with increasing message rate
- PW(1,0) has low SLP while PW(1,1) and PW(0,1) perform much better

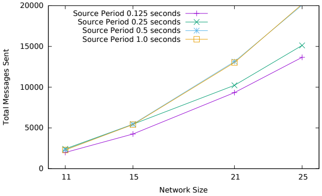
Results: Energy Usage (Messages Sent)



(a) $PW(1,0)$: Using **short** random walks



(b) $PW(1,1)$: Using **alternating short and long** random walks



(c) $PW(0,1)$: Using **long** random walks

- Number of messages increases with increasing network size
- Number of messages transmitted is similar at various message rates
- Multiple nodes does not consume more energy

Summary

- Phantom walkabouts proposes to interleave sequences of short random walks and long random walks to attempt to make the attacker move in the wrong direction
- Phantom walkabouts provides a better level of SLP but at lower additional message overhead
- Phantom walkabouts provides better levels of SLP with certain parameterisations

Future Work

- Develop a dynamic phantom walkabouts that responds to changes in the network
- Consider different network topologies

References I

[1] Zinaida Benenson, Peter M. Cholewinski, and Felix C. Freiling. *Wireless Sensors Networks Security*, chapter Vulnerabilities and Attacks in Wireless Sensor Networks, pages 22–43. IOS Press, 2008.

[2] M. Bradbury, M. Leeke, and A. Jhumka. A dynamic fake source algorithm for source location privacy in wireless sensor networks. In *14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 531–538, August 2015. doi: 10.1109/Trustcom.2015.416.

[3] Pandurang Kamat, Yanyong. Zhang, W. Trappe, and C. Ozturk. Enhancing source-location privacy in sensor network routing. In *25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, pages 599–608, June 2005. doi: 10.1109/ICDCS.2005.31.

[4] Jun Long, Mianxiong Dong, K. Ota, and Anfeng Liu. Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks. *IEEE Access*, 2:633–651, 2014. ISSN 2169-3536. doi: 10.1109/ACCESS.2014.2332817.

[5] K. Mehta, D. Liu, and M. Wright. Protecting location privacy in sensor networks against a global eavesdropper. *IEEE Trans. on Mobile Computing*, 11(2):320–336, February 2012. ISSN 1536-1233. doi: 10.1109/TMC.2011.32.

[6] Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. *Commun. ACM*, 47(6):53–57, June 2004. ISSN 0001-0782. doi: 10.1145/990680.990707.

[7] Victor Shnayder, Mark Hempstead, Bor-rong Chen, Geoff Werner Allen, and Matt Welsh. Simulating the power consumption of large-scale sensor network applications. In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, SenSys '04, pages 188–200, New York, NY, USA, 2004. ACM. ISBN 1-58113-879-2. doi: 10.1145/1031495.1031518.

Questions

Any questions?