THE UNIVERSITY OF WESTERN AUSTRALIA

Achieving International Excellence

Mobile and Wireless Computing CITS4419 Week 9 & 10: Holes in WSNs

Rachel Cardell-Oliver
School of Computer Science & Software Engineering

semester-2 2018

Motivation

- Holes cause WSN to fail its role
- Holes can be unintended (sensing, routing)
- Holes can be caused by a malicious attacker

- WSN apps requiring secure communication
  - Health monitoring
  - Battlefield tracking
  - Smart vehicles on roads
  - Smart house controls etc

Topics (week 10)

- Jamming holes
- Black hole holes

- Reading: The Holes Problem in WSNs A Survey, Ahmed et al, Mobile Computing and Communications Review, 1(2), 2005

WSN vulnerabilities

- Shared communication medium
- Ad hoc networks: anyone can join
- Limited resources on the nodes
  - Limited bandwidth
  - Limited message exchanges
  - Limited storage
  - Limited processing power
- Changeable environment

Jamming Holes

Jamming

- Suppose some object in the network has jammers capable of jamming the radio frequency being used for communication among the sensor nodes
- Nodes are unable to communicate back to the sink because of the communication jamming
- This zone of influence centered at the jammer is referred to as a jamming hole

Deliberate Jamming

- In deliberate jamming an adversary is trying to impair the functionality of the sensor network
- *laptop-class attacker:* has more resources and capable of affecting a larger area of the sensor net- work
- *mote-class attacker:* one of the deployed nodes that has been compromised and is now acting maliciously to create a denial of service condition

- Source: Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermea- sures. In *1st IEEE International Workshop SNPA’03*, May 2003

Combatting Jamming

- Various spread spectrum techniques for radio communications
- Different transmission media eg infra-red or optical combined with radio
- CON: cost and complexity

JAM protocol

- Detect jamming holes with heuristics to distinguish jamming from normal interference
- Once detected, use carrier sense overriding to send a JAMMED message
- On receiving JAMMED, nodes send BUILD to neighbours to find the boundary of the hole
- Now route around the hole

Anthony D. Wood, John A. Stankovic, and Sang H. Son. JAM: A jammed-area mapping service for sensor networks.
24th IEEE Real Time System Symposium (RTSS'03), pages 286–298, Dec 2003.

Jamming and LoRa

- Continuous:
- Triggered: once a LoRa tx detected on a selected channel, attacker starts tx to jam
- Continuous and Triggered affect all devices on some frequency, so can be detected and addressed

Source: Selective Jamming of LoRaWAN using Commodity Hardware, Mobiquitous 2017, https://arxiv.org/pdf/1712.02141.pdf

Selective Jamming

- Selective jamming: Jams only selected msgs, since other devices are not jammed,
- Hard to detect
- Approach
  1. Detect LoRaWAN packet (preamble symbols)
  2. Start rx that packet
  3. Abort rx if content triggers the jam policy
  4. Else, immediately jam the channel

Black Holes

Denial of Service attacks

- Sink hole / Black hole:
  - B advertises attractive routes to the sink,
  - Neighbours select B as next hop,
  - B can drop, select or change msgs before relaying
  - B also causes congestion and so exhausts other nodes

Denial of Service (2)

- Worm holes
  - Nodes B1 and B2 create a tunnel between them
  - Forward packets from B1 to B2 using a separate channel
  - B2 replays msgs in another part of the network causing incorrect routing decisions and energy depletion by other nodes

Mitigating DoS

- Against Sink Holes:
  - authentication and link layer encryption
  - Prevents B changing msgs or injecting msgs
  - Listen to B to check msg is forwarded
  - Multi-path routing: maintain disjoint paths
  - Probing to detect sink holes and check routes

- Challenges
  - Public key cryptography not possible on low resource nodes
  - High communication overhead for authorisation
  - Listening only detects suppressed msg, not replayed

Summary

- Routing holes can be caused by a malicious attacker in a WSN
- Jamming blocks the shared comms channel
- Denial of Service attacks remove or replay msgs or fake routes
- Mitigation of the Risks
  - Avoidance: New authentication methods for low power nodes
  - Tolerance: Multiple routes and multiple channels
  - Mitigation: Protocols to detect attacks