Detecting Denial-of-Service Attacks against Sensor Networks

Steven Cheung, Bruno Dutertre, Ulf Lindqvist

RAID’05

September 8, 2005

This research is sponsored by DARPA under contract number F30602-02-C-0212 and NSF under grant number CNS-0434997. The views herein do not necessarily reflect the views of the sponsoring agencies.

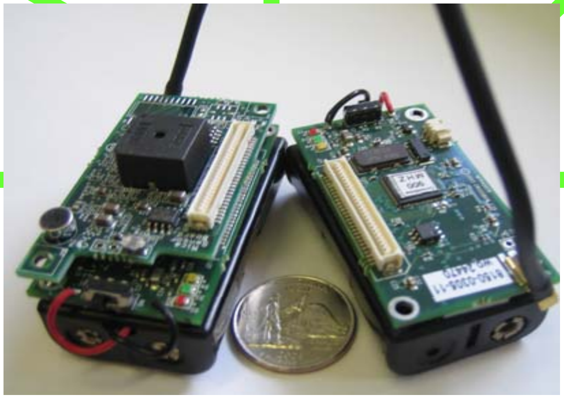
Wireless sensor networks

Structural integrity monitoring

Wildlife monitoring

Protection for critical infrastructure

Precision agriculture



Intruder detection and tracking

Characteristics of wireless sensor networks

- Resource constraints
  - Limited energy reserve, computation power, memory
- Physical exposure
  - Possibly deployed in remote locations, and spread across a large geographic region
- Collaborative processing
  - Use sensor nodes for routing
- Unpredictable communication links

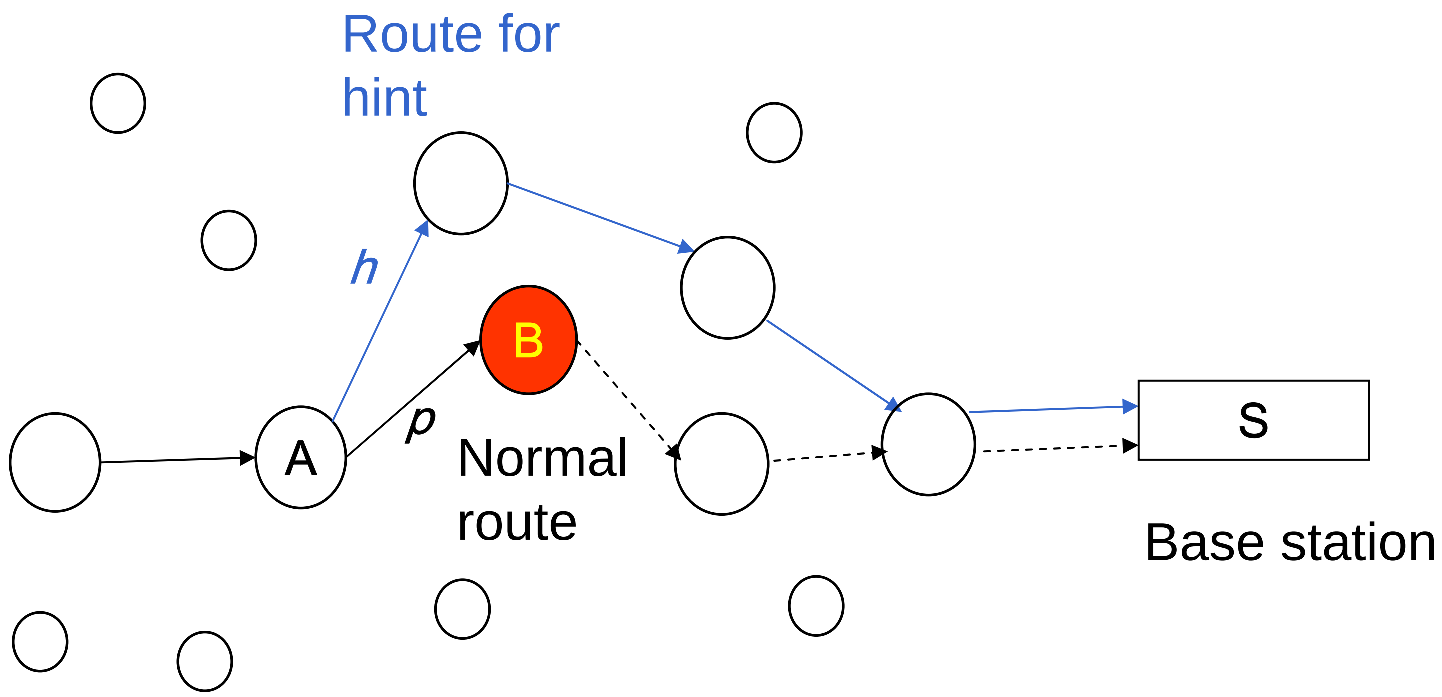
Physical attacks

- Examples:
  - Destroying sensor nodes using physical or electrical means
  - Relocating sensor nodes
  - Turning off sensor nodes
- Detection approaches:
  - Nodes periodically send “I’m alive” packets to the base station
  - Cooperative monitoring: Neighbor nodes exchange heartbeat messages with each other

Disruptive routers

- Compromised sensor nodes may drop or corrupt packets
- Related work:
  - Secure implicit sampling [McCune et al ‘05]
  - Secure trace-route [Padmanabhan-Simon ‘02]
  - Hop-by-hop checking [Marti et al ‘00]
  - Conservation of flow [Cheung-Levitt ‘97, Bradley et al ‘98]
- Need a scheme that is lightweight and can handle “malicious” routers

Hint-based approach



- When a node *A* forwards a packet *p* to its next-hop neighbor *B*, with probability δ it will also send a hint *h* to the base station
- The hint is routed via the path that avoids *B*