CMPE 259
Sensor Networks

Katia Obraczka

Winter 2005

Security
Announcements

- Hw3 due today.
- Project presentations tomorrow from 4-7pm.
- Project reports due tomorrow by midnight.
Security in sensor networks
Security in sensor networks

- For many sensor network applications, security is critical.
  - Public safety, special operations, healthcare, etc.

- Sensor network protocols should incorporate security mechanisms in the original design.
DoS in Sensor Networks [Wood et al.]

- What is DoS?
  - Attack that reduces or eliminates the network’s ability to perform its function.
  - E.g., hardware failures, software bugs, resource exhaustion, etc.

- Paper looks at protocol layers and possible DoS attacks.
Physical layer

 Attacks:
  ☐ Jamming.
  ☐ Tampering.

 Defenses:
  ☐ Jamming:
    • Spread-spectrum techniques.
    • Lower duty cycle with priority messages.
    • Alternate modes of communication.
  ☐ Tampering:
    • “Self-destruction”
    • Hiding nodes.
Link layer

 Attacks:
 - Collision induction.
 - Battery exhaustion.
 - Unfairness.

 Defenses:
 - Collision induction.
   • Error correcting codes (?)
   • Collision detection.
   • Collision-free MAC.
 - Battery exhaustion.
   • Rate limitation.
   • Streamlined protocols.
Network layer: attacks

- “Neglect and greed”.
- “Homing”.
- Misdirection.
- Gray/black holes.
Network layer: defenses

- Authorization.
  - Only authorized nodes participate in routing.
    - Need authentication mechanisms.
  - Monitoring.
    - Monitor node behavior.
- Probing.
- Redundancy.
Transport layer

attacks:
  - Flooding.
  - Desynchronization.
    - Message fabrication to get end points out of sync.

defenses:
  - Flooding:
    - Limit number of connections.
    - Challenges/puzzles to clients.
  - Desynchronization:
    - Authenticate all messages (including header fields)
Sample protocol vulnerabilities

- Adaptive rate control [Woo et al.]
  - MAC layer modifications to 802.11.
  - Preference to route-through traffic.
  - Vulnerabilities?

- RAP [Lu et al.]
  - Similar vulnerability.
  - Differentiated services can be exploited by attacker.
Focus

- Communication security in sensor networks.
- Data classification and related security threats.
- Location-based security mechanism.
Types of data

- Mobile code.
- Sensor node location.
- Application data.

**Goals:**
- Minimize security-related energy consumption.
- Different protection levels.
Target sensor net architecture

- Localized algorithms.
- Local broadcast.
- Mobile code.
Security threats

- Insertion of malicious code.
- Interception of messages with node location information.
- Interception of application data.
- Injection of false data.

Lower risk.
Security architecture

- Symmetric key encryption.
  - All messages encrypted.

- Three security levels:
  - Level I: mobile code.
  - Level II: node location information.
  - Level III: application data.

- Encryption strength:
  - Level I > level II > level III.

- Encryption algorithm with adjustable strength (number of rounds).
Security architecture (cont’d)

- Group keys.
- Every user: set of keys, pseudorandom generator, and seed.
- Periodically and synchronously, nodes change keys.
Security levels

- Level I uses strongest encryption for mobile code injection.
  - 32 rounds.

- Level II:
  - Location-based keys.
    - Different for different “cells”.
    - Protect network from compromised keys.

- Level I:
  - Weakest security.
  - 22 rounds.
Performance

- Cost of encryption/decryption.
- Energy considerations.
  - Rockwell WINS node.
“Secure Routing...” [Karlof et al.]
Focus

- Routing security in sensor networks.

Problem:
- Current routing protocols for sensor networks do not consider security.
- Vulnerable to attacks.
- Not easy to make these protocols secure.
Contributions

- Threat models and security goals for sensor network routing.
- Two new attacks: sinkhole and HELLO floods.
- Security analysis of routing and topology control algorithms.
- Attacks against these protocols.
- Countermeasures and design issues for secure routing in sensor networks.
Deployment and platform

- Heterogeneous deployment.
- *Mica* motes with TinyOS.
- Base stations.
- Aggregation points.
Sensor- and ad-hoc networks

- Traffic considerations:
  - Ad hoc networks exhibit more general patterns.
  - Sensor networks:
    - Many-to-one.
    - One-to-many.
    - Local.

- Capabilities.
  - Sensor nodes are typically more limited.

- Trust relationships.
  - E.g., to perform aggregation, duplicate pruning, etc.
Attacks

- Spoofed, altered, replayed routing information.
- Selective forwarding.
  - Black/gray hole.
- Sinkhole.
- Sybil.
  - Single nodes presents multiple id’s to others.
- Wormhole.
- HELLO flood.
- (Link-layer) ACK spoofing.
Countermeasures

- **Outsider attacks:**
  - Link layer encryption and authentication.
  - Shared keys.

- **Insider attacks:**
  - Identity verification.
  - Multipath routing.
  - Bi-directional link verification.
  - Limiting number of neighbors.

- **Sinkhole and wormhole attacks are harder to circumvent.**
  - Design routing protocols where these attacks are ineffective.
  - E.g., geographic routing.