Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

Chris Karlof       David Wagner
University of California at Berkeley


2010-11-24
최훈규 (2008-20999)
Contents

- Introduction
- Background
- Attacks on sensor network routing
- Attacks on specific sensor network protocols
- Countermeasures
- Conclusion
Introduction

- Wireless Sensor Network (WSN)
  - Application: monitoring disaster areas
Example

In-Network Processing

$\theta_1 = 67^\circ, \ldots, \theta_2 = 68^\circ$

Aggregation Point

$f(\theta_1, \ldots, \theta_2)$

Resource constraints
Sensor Nodes

network
Background

**Sensor Network**

- **Sensor Node**: Limited in power, computational capacities, memory, and battery.
- **Base Station (BS)**: Point of centralized control.
- **Gateway**: Gateway to another network, powerful data processing unit, or point of human interface.
- **Aggregation Point**: Node at which the messages are processed before sending to the base station.

**Diagram Elements**:
- **Base station**: Square
- **Sensor node**: Circle
- **Low power radio link**: Solid line
- **Low latency, high bandwidth link**: Dashed line

DIP2010F 5
WSN vs. Ad-hoc Wireless Networks

- **Similarity**
  - Support Multi-hop networking

- **Differences**
  - Sensor: Supports Specialized communication patterns
    - Many-to-One
    - One-to-Many
    - Local Communication
  - Sensor nodes more resource constrained than Ad-hoc nodes
    - Public key cryptography not feasible
  - Higher level of trust relationship among sensor nodes
  - In-network processing, aggregation, duplication elimination
Overview

- Current sensor routing protocols are not designed for security and be insecure, mostly optimized for the limited capabilities of the nodes.
- Wireless sensor network (WSN) cannot depend on many of the resources available to traditional networks for security.
- Analyze current protocols to find attacks and suggest countermeasures and design consideration.
- The effective solution for secure routing is to design such sensor routing protocols with security in mind.
Problem Statement

Network Assumptions
- Insecure Radio links
  - Eavesdropping, injection and replay
- Malicious nodes collude to attack the system
  - By purchasing or capturing them
- None tamper resistant
  - Adversary can access all key material, data, and code stored on the captured node

Trust Requirements
- Base stations are trustworthy
- Nodes (and aggregation points) may not necessarily be trustworthy
Problem Statement

- Threat Models
  - Based on device capability
    - Mote-class attacker
      - Access to few sensor nodes
    - Laptop-class attacker
      - Access to more powerful devices
      - More battery power, better CPU, sensitive antenna, powerful radio TX, etc
  - Based on attacker type/location
    - Outside attacks
      - Attacker external to the network
    - Inside attacks
      - Authorized node in the network is malicious
Security Goal

- Integrity, authenticity, and confidentiality
  - Guaranteed by link layer security mechanisms
- Availability
  - Still must rely on the routing protocol

- In the presence of outsider adversaries
  - Conceivable to achieve these goals
- In the presence of insider adversaries
  - These goals are not fully attainable -> Graceful degradation
- Protection against the replay attack is not a security goal of a secure routing protocol
  - Delegate it to the application layer
Attack Model

- Spoofed, altered, or replayed routing information
- Selective forwarding
- Sinkhole attacks
- Sybil attacks
- Wormholes attacks
- HELLO flood attacks
- Acknowledgement spoofing
Attack Model

- Spoofed, altered or replayed routing information
  - May be used for loop construction, attracting or repelling traffic, extend or shorten source route

- Selective forwarding
  - A malicious node behaves like a black hole
  - Refuse to forward certain messengers, selective forwarding packets or simply drop them
Attack Model

- Sinkhole attacks
  - Attacker creates metaphorical sinkhole by advertising for example high quality route to a base station
    - Almost all traffic is directed to the fake sinkhole

- The Sybil Attack
  - Forging of *multiple identities* - having a set of faulty entities represented through a larger set of identities.
  - Sybil Attack undermines assumed mapping between identity to entity

- Wormholes
  - Tunneling of messages over alternative low-latency links,
  - e.g. confuse the routing protocol, create sinkholes. etc.
  - Exploit routing race condition
Attack Model

- HELLO flood attack
  - An attacker sends or replays a routing protocol’s HELLO packets with more energy

- Acknowledgement spoofing
  - Spoof link layer acknowledgement to trick other nodes to believe that a link or node is either dead or alive
Attacks on specific protocols

- TinyOS beaconsing
- Directed diffusion
- Geographic routing
TinyOS beaming

- Base station broadcast Route update (beacon) periodically, Nodes received the update and mark the base station as parent and broadcast it

- Relevant Attack mode
  - Bogus routing information
  - Selective forwarding
  - Sinkholes
  - Sybil
  - Wormholes
  - Hello floods
TinyOS beaconing

- Spoof information

Bogus and replayed routing information (such like “I am base station”) send by an adversary can easily pollute the entire network
TinyOS beaconing

- Wormhole & sinkhole Combination
  - Tunnel packets received in one place of the network and replay them in another place
  - The attacker can have no key material. All it requires is two transceivers and one high quality out-of-band channel
TinyOS Beaconing

- Wormhole & sinkhole Combination
  - Most packets will be routed to the wormhole
  - The wormhole can drop packets directly (sinkhole) or more subtly selectively forward packets to avoid detection
Directed Diffusion

- Data and Application Specific
- Content based naming
- Interest distribution
  - Interests are injected into the network from base station
  - Interval specifies an event data rate
  - Interest entry also maintains gradients
  - Data flows from the source to the sink along the gradient
- Data propagation and reinforcement
  - Reinforcement to single path delivery
  - Multipath delivery with selective quality along different paths
Directed Diffusion

“In what direction is that lion in region Y moving?”

Source

Sink

interest
gradient
reinforcement
data
Directed Diffusion

- Relevant Attack
  - Due to the robust nature of floodings, it may be difficult for an adversary to prevent interesting
  - Replay of interest by the adversary
  - Selective forwarding and data tampering
  - Spoofing positive/negative reinforcements
Geographic Routing

- Two protocols
  - GPSR (Greedy Perimeter Stateless Routing)
  - GEAR (Geographic and Energy Aware Routing)

- Description
  - Greedy forwarding routing each packet to the neighbor closest to the destination
  - GEAR weighs the choice of the next hop by both remaining energy and distance from the target

![Diagram of geographic routing](image)
Geographic Routing

- Relevant attack
  - Sybil attack
  - Bogus routing information
Countermeasures

- Secret shared key & Link layer encryption
  - Prevents the majority of outsider attacks
    - False routing information, Selective forwarding, Sinkhole attacks, Sybil attacks, ACK spoofing
  - This does not prevent to tunnel or amplify legitimate message
    - Wormhole attacks
    - HELLO flood attacks
      - By amplifying an overheard broadcast packet with sufficient power
  - Every node shares a unique symmetric key with the base station
Countermeasures

- Wormhole and Sinkhole attacks
  - These are very difficult to defend especially when used in combination
  - Geographic routing protocol can be one solution
    - Topology in geographic protocol is constructed using localized interaction

- Selective Forwarding
  - Multipath routing can be used to counter these types of selective forwarding attacks
  - Messages routed over $n$ paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most $n$ compromised nodes
Conclusion

- Link layer encryption and authentication, multipath routing, identity verification, bidirectional link verification and authenticated broadcast is important.

- Cryptography is not enough for insiders and laptop-class adversaries, careful protocol design is needed as well.