Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

Chris Karlof & David Wagner
University of California at Berkeley
Published in SNPA 2003

Han Bing
binghan@mmlab.snu.ac.kr
2014.11.25
Outline

• Introduction and contributions
• Background
• Sensor vs. ad-hoc wireless networks
• Problem statement
• Attacks on sensor network routing
• Attacks on specific sensor network protocols
• Countermeasures
• Conclusions
Introduction

• Current sensor routing protocols do not consider security
  • Insecure wireless communication
  • Limited node capabilities
  • Possible insider threats
  • Adversaries with powerful and high energy

• The sensor network routing protocols must be designed with security in mind
Contributions

• Threat models and security goals

• Two new attacks
  • Sinkhole & HELLO floods

• How to adapt attacks against ad-hoc wireless networks into powerful attacks

• Security analysis of all the major routing protocols

• Countermeasure and design considerations
Background

• Wireless Sensor Networks (WSNs)
  • Huge of low-power, low-cost nodes having a CPU, power source, radio...
  • Base Station (sinks), Aggregation points
  • Power is the scarcest resource

• A representative sensor network architecture
Background cont’d

• Example of WSNs
Environment settings

- Berkeley Tiny OS sensor platform

<table>
<thead>
<tr>
<th>Component</th>
<th>Spec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>4MHz 8-bit CPU with 128KB inst. memory</td>
</tr>
<tr>
<td>RAM</td>
<td>4KB for data</td>
</tr>
<tr>
<td>Storage</td>
<td>512KB of flash memory</td>
</tr>
<tr>
<td>OS</td>
<td>Tiny OS</td>
</tr>
<tr>
<td>Radio</td>
<td>916 MHz from RFM / 40Kbps to dozen meters</td>
</tr>
<tr>
<td>Power</td>
<td>Two AA batteries with 2850mA at 3v</td>
</tr>
<tr>
<td>Sensor</td>
<td>Temperature, magnetometer, accelerometer, microphone, sounder, ...</td>
</tr>
</tbody>
</table>

### CPU Consumption

<table>
<thead>
<tr>
<th>CPU</th>
<th>Consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>5.5mA at 3 volts</td>
</tr>
<tr>
<td>Sleep</td>
<td>2 orders of magnitude less</td>
</tr>
</tbody>
</table>

### RFM Radio Consumption

<table>
<thead>
<tr>
<th>RFM Radio</th>
<th>Consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive</td>
<td>4.8mA at 3 volts</td>
</tr>
<tr>
<td>Transmit</td>
<td>12mA</td>
</tr>
<tr>
<td>Sleep</td>
<td>5uA</td>
</tr>
</tbody>
</table>
Sensor vs. ad-hoc wireless networks

- Both are multi-hop networking

- Differences
  - SWNs supports specialized communication patterns
    - Many-to-One
    - One-to-Many
    - Local Communication
  - Starved nature resource
  - Points of centralized control such as BS
  - Trust relationships between nodes assumed
  - Public key cryptography not feasible
Problem statement

• Network Assumptions
  • Radio links are insecure
    • Eavesdrop, inject and **replay**
  • Adversary can deploy a few malicious nodes
    • Malicious nodes with similar hardware capabilities as the legitimate nodes
  • No tamper resistant
    • Adversary can extract all key material, data and code stored on node

• Trust requirements
  • Base stations are trustworthy
  • Aggregation points may not necessarily be trustworthy
Problem statement cont’d

• Threat Models
  • Based on types of attacker capabilities
    • Mote-class attackers
      • Access to few sensor nodes
    • Laptop-class attackers
      • Access to more powerful devices
      • Greater battery power, more capable CPU, high-power radio transmitter, or a sensitive antenna
  • Based on attacker location
    • Outsider attacks
      • Attacker external to the network
    • Insider attacks
      • Authorized node in the network is malicious
Problem statement cont’d

• Security Goals
  • Guarantee the integrity, authenticity, and availability of messages

• For outsider adversaries
  • Conceivable to achieve these idealized goals

• For insider adversaries
  • Goals are not fully attainable
  • Graceful degradation
Attacks on sensor network routing

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

• Create routing loops, attract or repel network traffic, extend or shorten source routes

• Goals
  • Generate false error messages, partition the network, increase end-to-end latency and etl...
Spoofed, altered, or replayed routing information

Fig. 4. A representative topology constructed using TinyOS beaconing with a single base station.

Fig. 5. An adversary spoofing a routing update from a base station in TinyOS beaconing.
Selective forwarding

• Malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further

• Goals
  • Attempt to include itself on the actual path of the data flow
Selective forwarding

- Event
- Aggregation node
- Sensor node
- Malicious node
- Drop
- Base station
- Outside Network
Acknowledgement spoofing

• Spoof link layer acknowledgments for “overheard” packet addressed to neighboring nodes

• Goals
  • Convincing the sender that a weak link is strong or that a dead or disabled node is alive
  • Enable selecting forward attack
Acknowledgement spoofing

Outside Network

Event

Aggregation node

Sensor node

Malicious node

bad node

Lost

Base station
Sinkhole attacks

• Making a compromised node look especially attractive to surrounding nodes

• Goals
  • Lure nearly all the traffic from a particular area through a compromised node, create a metaphorical sinkhole with the adversary at the center
  • Enable selecting forward attack
Sinkhole attacks

Fig. 4. A representative topology constructed using TinyOS beaconing with a single base station.
Wormholes

• Tunnel messages received in one part of network over a low-latency link and replays them in a different part

• Goals
  • May be able to completely disrupt routing if an adversary situated close to a base station
  • Enable sinkhole attack
  • Exploit routing race condition
Wormholes

Fig. 4. A representative topology constructed using TinyOS beaconing with a single base station.

Fig. 6. A laptop-class adversary using a wormhole to create a sinkhole in TinyOS beaconing.
Sybil attack

• A single node presents multiple identities to other nodes in the network

• Goals
  • Significantly reduce the effectiveness of fault-tolerant schemes
Sybil attack

Fig. 8. The Sybil attack against geographic routing. Adversary A at actual location (3,2) forges location advertisements for non-existent nodes A1, A2, and A3 as well as advertising her own location. After hearing these advertisements, if B wants to send a message to destination (0,2), it will attempt to do so through A3. This transmission can be overheard and handled by the adversary A.
HELLO flood attack

• A laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor

• Goals
  • Enable wormhole attack by broadcasting wormholes
HELLO flood attack

Fig. 7. HELLO flood attack against TinyOS beaconing. A laptop-class adversary that can retransmit a routing update with enough power to be received by the entire network leaves many nodes stranded. They are out of normal radio range from the adversary but have chosen her as their parent.
Attacks on specific sensor network protocols

• Tiny OS beaconing
• Directed diffusion
• Geographic routing
Tiny OS beaconing

• 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 & wormholes
  • Sybil
  • HELLO floods
Directed diffusion

• Designed for robustness, scaling and energy efficiency

• Data centric
  • Sinks place requests as interests for named data
  • Sources satisfying the interest can be found
  • Intermediate nodes can cache or transform data directly toward sinks

• Name based

• Data aggregation

• Interest, data aggregation and data propagation are determined by localized interactions
Directed diffusion

Interest propagation
Initial gradients setting
Data delivery along reinforced path

• Relevant attack mode
  • Suppression, Cloning, Path influence, Selective forwarding and data tampering, Wormholes attack, Sybil attack
Geographic routing

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

• 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
Geographic routing

Greedy forwarding example:
Y is x’s closest neighbor to D

Greedy forwarding failure:
X is a local maximum in its geographic proximity to D; w and y are farther from D
Geographic routing

Routing void problem:
Node x’s void with respect to destination D
Geographic routing

• Relevant attack

Sybil attack:
An adversary may present multiple identities to other nodes. The Sybil attack can disrupt geographic and multi-path routing protocols by “being in more than one place at once” and reducing diversity.

From B->C, now will go through B->A3->C

Creating routing loop in GPSR:
From B->D, A forge a wrong information to claim B is in (2,1), so C will send packets back to B which cause loop at last.
Summary of attacks

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Relevant Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>TinyOS beaconsing</td>
<td>Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods</td>
</tr>
<tr>
<td>Directed diffusion and its multipath variant</td>
<td>Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods</td>
</tr>
<tr>
<td>Geographic routing (GPSR, GEAR)</td>
<td>Bogus routing information, selective forwarding, Sybil</td>
</tr>
<tr>
<td>Minimum cost forwarding</td>
<td>Bogus routing information, selective forwarding, sinkholes, wormholes, HELLO floods</td>
</tr>
<tr>
<td>Clustering based protocols (LEACH, TEEN, PEGASIS)</td>
<td>Selective forwarding, HELLO floods</td>
</tr>
<tr>
<td>Rumor routing</td>
<td>Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes</td>
</tr>
<tr>
<td>Energy conserving topology maintenance (SPAN, GAF, CEC, AFECA)</td>
<td>Bogus routing information, Sybil, HELLO floods</td>
</tr>
</tbody>
</table>
Countermeasures

• Outsider attacks and link layer security
• Sybil attack
• HELLO flood attacks
• Wormhole and sinkhole attacks
• Selective forwarding
• Authenticated broadcast and flooding
Outsider attacks and link layer security

• Solution
  • Global share key: link layer encryption and authentication

• Limitation
  • Ineffective
  • Wormhole and HELLO flood attack
  • Insider attack or compromised node
Sybil attack

• Solution
  • Every node share a unique symmetric key with base station
  • Two node establish a shared key and verify each other’s identity
  • Base station limit the number of neighbors around a node
  • When a node is compromised, it is restricted to communicating only with its verified neighbors

• Limitation
  • Adversary can still use a wormhole to create an artificial link between two nodes to convince them
HELLO flood attacks

• Solution
  • Verify the bidirectionality of a link before taking meaningful action
  • Every node authenticate each of its neighbors with an identity verification protocol using a trusted base station
Wormhole and sinkhole attacks

• Solution
  • Design routing protocols which avoid routing race conditions and make these attacks less meaningful
  • Geographic routing protocols: construct a topology on demand using only localized interactions and information
Selective forwarding

• Solution
  • Multipath routing: message routed over n paths whose nodes are completely disjoint
  • Nodes dynamically choose a packet’s next hop probabilistically from a set of possible candidates

• Limitation
  • Completely disjoint paths is difficult to create
Authenticated broadcast and flooding

• μTESLA protocol to prevent replay of broadcast messages issued by the base station
  • Replay is prevented because messages authenticated with previously disclosed keys are ignored

• Flood the information about the malicious nodes in the network
## Countermeasure summary

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Countermeasure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outsiders</td>
<td>Link-layer encryption and authentication,</td>
</tr>
<tr>
<td>Sybil</td>
<td>Multipath routing,</td>
</tr>
<tr>
<td>HELLO floods</td>
<td>Identity verification,</td>
</tr>
<tr>
<td>ACKs spoofing</td>
<td>Bidirectional link verification,</td>
</tr>
<tr>
<td></td>
<td>Authenticated broadcast</td>
</tr>
<tr>
<td>Sinkhole attack</td>
<td>Geographic routing protocols</td>
</tr>
<tr>
<td>Wormhole attack</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

• Demonstrate current routing protocols for wireless sensor networks are insecure

• Provide several countermeasures to against attacks

• Link layer encryption, authentication and so on