Secure Routing in WSNs:

Attacks & Countermeasures

Chris Karlof & David Wagner, UC Berkeley

1st IEEE International Workshop on Sensor Network Protocols & Applications
11 May 2003

Report by Jim Gaskell

CS 577, Prof Kinicki, Fall '11

Overview

- Intro to WSNs
- Security Issues
- Attacks
- Countermeasures
- Summary & Conclusions

Intro

- WSNs (Wireless Sensor Networks)
  - Low power xmits & fixed energy
  - Low computing power
  - Trusting environment
  - Future appears to lead to more sensors at less cost
- Base Station configuration

Security Issues

- WSNs not conducive to security
- No popular protocol addresses issue
- Sensors may lack physical security
- Attackers can have vastly superior resources

Security Issues (cont)

- Usages where security matters:
  - Burglar alarms
  - Building monitoring
  - Emergency response
  - Often lack of physical security
  - MILITARY & POLICE
    - DARPA in-part sponsored paper

General Message Types

- Commands from the Base Station to the Nodes
- Data from the Nodes to the Base Station
- Communication between Nodes to establish routing

Physical Security

Maybe the best way to Attack a mesh:

- Many Nodes distributed over a fairly wide area
- Obtain one and take it apart
- Compromise it and, perhaps, return it to the field

Protocols & their Attacks

Protocol	Relevant attacks
TinyOS beaconing	Bogus routing information, selective forwarding, sink-holes, Sybil, wormholes, HELLO floods
Directed diffusion and its multipath variant	Bogus routing information, selective forwarding, sink-holes, Sybil, wormholes, HELLO floods
Geographic routing (GPSR, GEAR)	Bogus routing information, selective forwarding, Sybil
Minimum cost forwarding	Bogus routing information, selective forwarding, sink-holes, wormholes, HELLO floods
Clustering based protocols (LEACH, TEEN, PEGA-SIS)	Selective forwarding, HELLO floods
Rumor routing	Bogus routing information, selective forwarding, sink-holes, Sybil, wormholes
Energy conserving topol-ogy maintenance (SPAN, GAF, CEC, AFECA)	Bogus routing information, Sybil, HELLO floods

Fig. 1. Summary of attacks against proposed sensor networks routing protocols.

Attacks

- #1 - Aggregation issues
- #2 - Sink Holes
- #3 - Worm Holes
- #4 - Sybil
- #5 - ACK Spoofing
- #6 - HELLO Flooding

#1 - Aggregation Issues

- "Aggregation" definition
- Selective forwarding
- Other Nodes can be discouraged from sending data

#2 - Sink Holes

- Attacker looks attractive to other Nodes for relaying
- May be far away
- May be near to Nodes & far from BS
  - If another node, it's a "selfish" node
- Selective Forwarding

#3 - Worm Holes

- Messages from one area of the Network appear in a different area of the Network
- Even encrypted Messages can be relocated

#4 - Sybil

- Have a single Node act as though it is many
- Perhaps inducing bogus Routing info

#5 - ACK Spoofing

- Sends overheard ACKs to other Nodes (can be encrypted)
- Keeps routes alive and/or redirects path

#6 - HELLO Flooding

- Attacker tells many Nodes that it's an excellent connection to the BS
- Nodes then (attempt to) send their data to the Attacker – perhaps indirectly via hops

Countermeasures

- Public key protocol too costly for Nodes
- Symmetric key protocol OK for Node data, but not for Routing (no cit.)
- "Selfish" nodes can be dealt with by some protocols, but "Blackmailers" can still be used as an attack.

Countermeasures (cont)

- SNEP (Sensor Network Encryption Protocol) has many security features
- μTESLA is a reduced functionality off-shoot of a Workstation authentication protocol

Summary & Conclusions

- This paper is at least 8 years old
- It deals only in theory; not field tests
- It deals only with protocols available at the time
- By their very nature, current Nodes are not very robust against attacks

Conclusions (cont)

- New protocols or hardware need only be compatible with other nodes in the mesh
- Applications can vary markedly in their requirements; choosing hdwr & software must be done with care beginning at the start of the Project

Jim Gaskell

Questions?

or

Comments!