

# Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

Chris Karlof and David Wagner

NEST Retreat: Winter 2003 UC-Berkeley

## Overview

- Sensor network routing protocols have not been designed with security as a goal
- Analyze current proposals: find attacks and suggest countermeasures and design considerations

## Threat models

- Mote-class vs. laptop-class adversaries
- Insiders vs. outsiders
- Insiders and laptop-class adversaries are the main challenge**

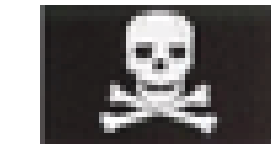
## Security goals

- Integrity, authenticity, and availability of messages
- Not likely to be fully attainable in the presence of insiders or laptop-class adversaries → *graceful degradation* is desirable
- Confidentiality and replay protection of application messages are better handled at a higher layer

Protocol	Relevant Attacks
TinyOS beaconing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Directed diffusion and its multipath variant	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Geographic routing (GPSR, GEAR)	Bogus routing information, selective forwarding, Sybil
Minimum cost forwarding	Bogus routing information, selective forwarding, sinkholes, wormholes, HELLO floods
Clustering based protocols (LEACH, TEEN, PEGASIS)	Selective forwarding, HELLO floods
Rumor routing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes
Energy conserving topology maintenance (SPAN, GAF, CEC, AFECA)	Bogus routing information, Sybil, HELLO floods

Paper to appear in SNPA'03

## Attacks

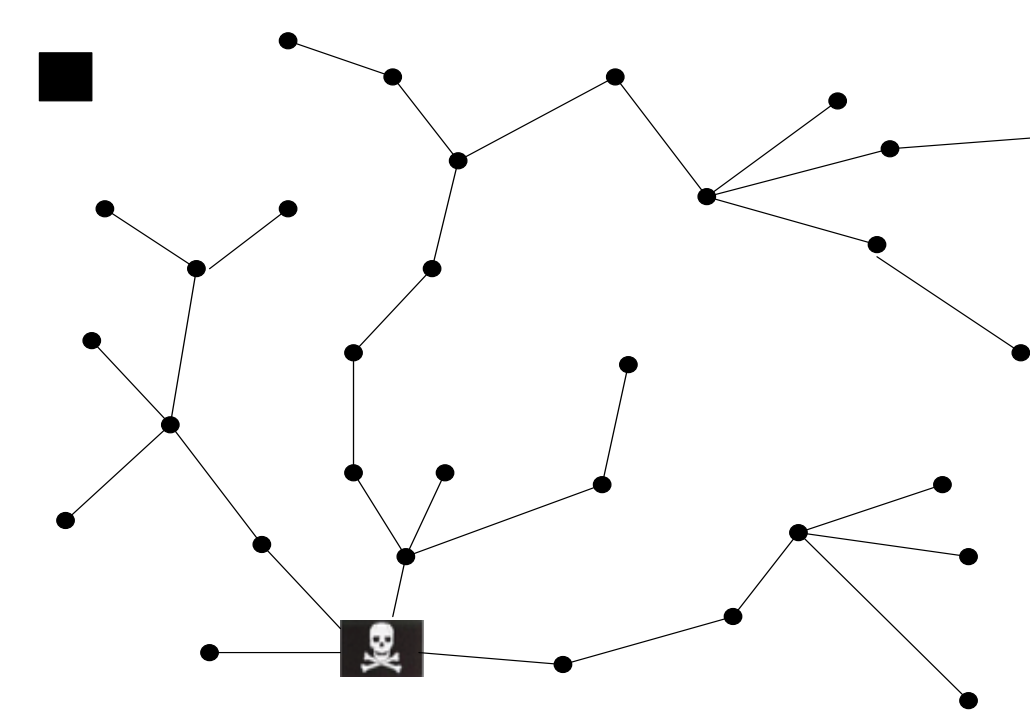


= adversary

■ = base station

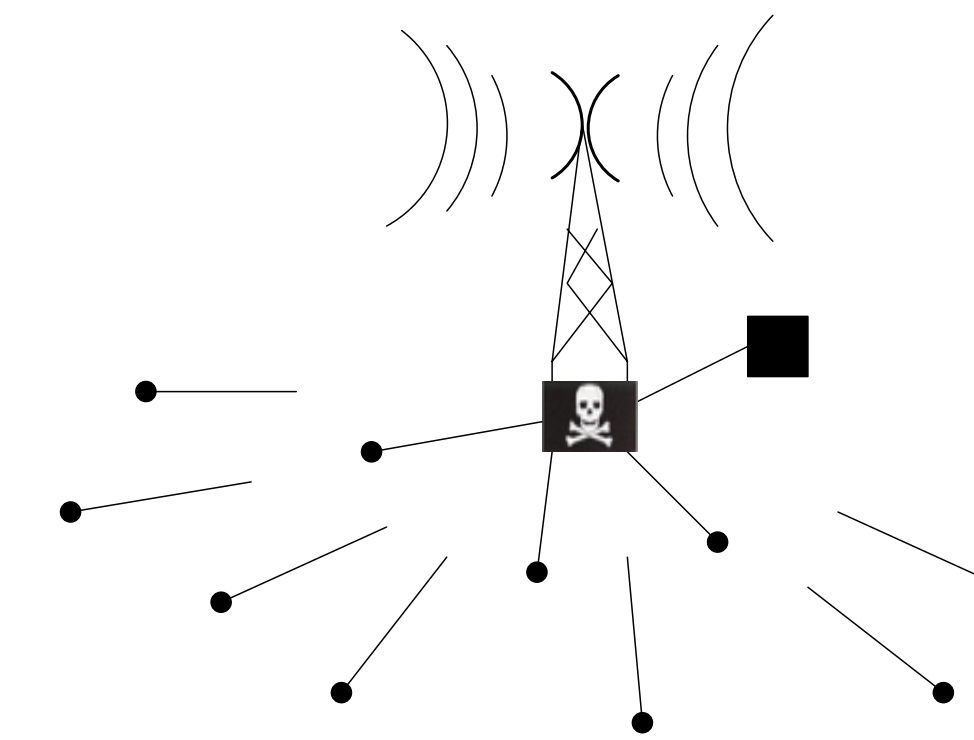
● = sensor node

### Bogus or replayed routing information



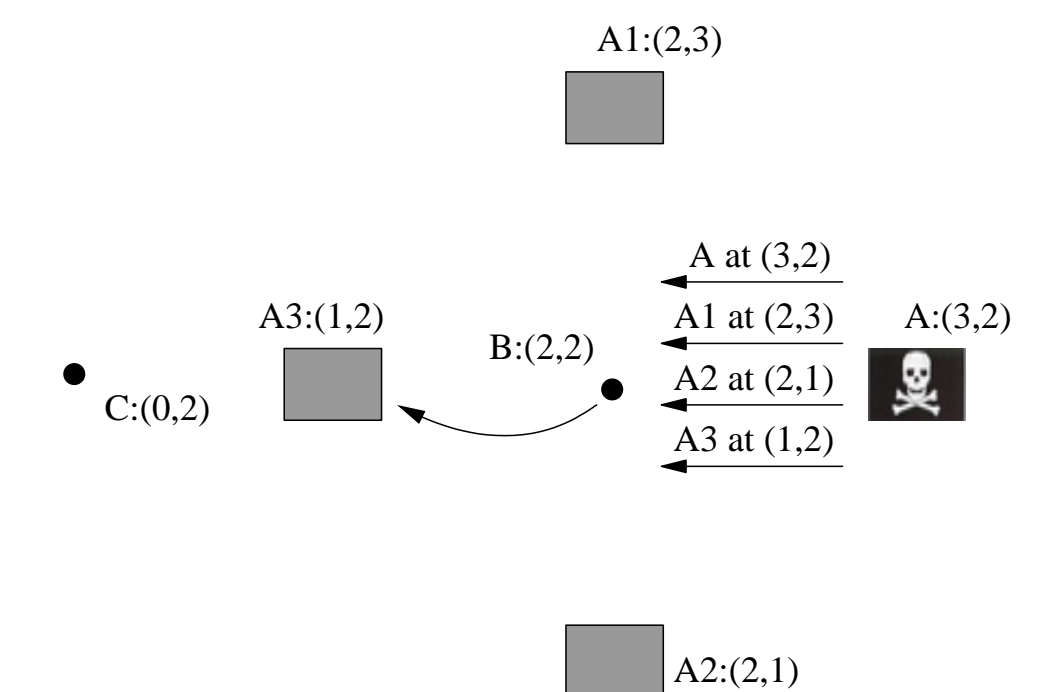
Protocols must detect bogus and replayed routing information. Recursive propagation of information must be used carefully: an adversary can easily pollute the entire network.

### HELLO flood attack



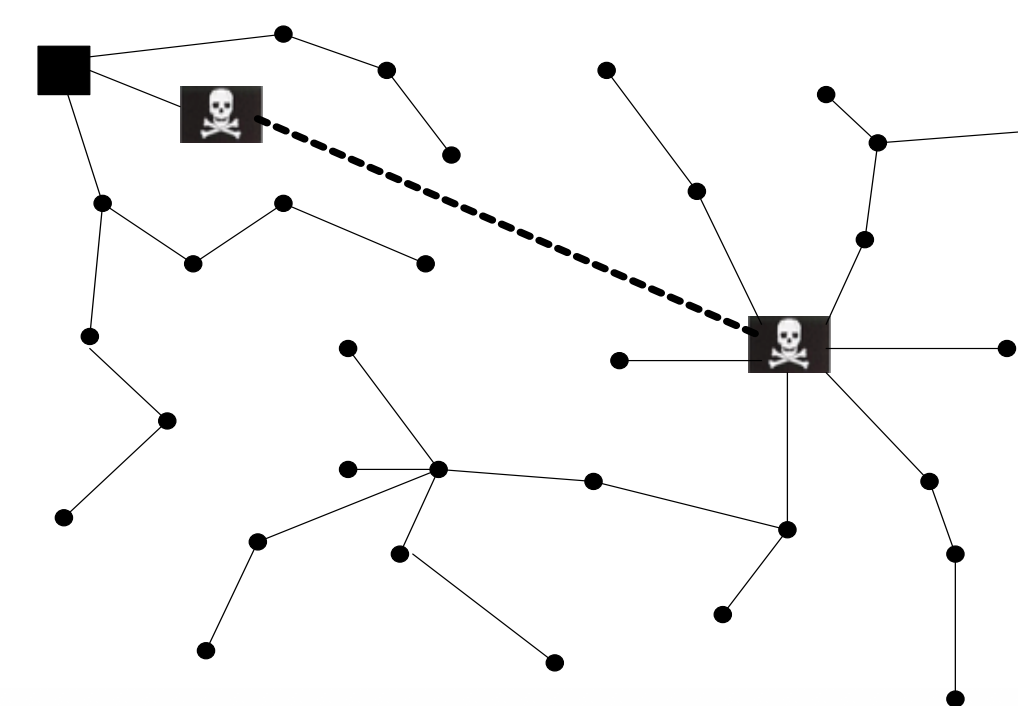
Inferring a node is a neighbor (i.e. within radio range) after receiving a broadcast packet from them may be ill-conceived. An adversary with a powerful transmitter could easily reach every node in the network.

### Sybil attack



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

### Wormholes



An adversary can tunnel messages received in one part of the network over a low-latency link and replay them in a different part. By tunneling routing updates, a *sinkhole* may be created, potentially drawing all traffic in a large area through the adversary. The adversary may then choose to *selectively forward* packets of some nodes while dropping those of others, enabling her to suppress the traffic of particular nodes.

## Countermeasures

- Link layer security with a globally shared key can prevent the majority of outsider attacks: bogus routing information, Sybil, selective forwarding, sinkholes. However, it provides little protection against insiders, HELLO floods, and wormholes.
- Establish link keys using a trusted base station. Verifies the bidirectionality of links and prevents Sybil attacks and HELLO floods.
- Multipath and probabilistic routing limits effects of selective forwarding.
- Wormholes are difficult to defend against. Can be mounted effectively by both laptop-class insiders and outsiders. Good protocol design is the best solution: geographic and clustering-based protocols hold the most promise. Wormholes are ineffective against these protocols.
- Authenticated broadcast and flooding are important primitives.
- Nodes near base stations are attractive to compromise. Clustering-based protocols and overlays can reduce their significance.
- Conclusion: Link layer security is important, but cryptography is not enough for insiders and laptop-class adversaries: careful protocol design is needed as well.