Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

by

Chris Karlof, David Wagner

Presented by
William Scott
December 01, 2009

- **Note:** all material taken from Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures by Chris Karlof, David Wagner

Table of Contents

What is This Study?

- **History:**
- Chris Karlof Grad Student in CS at University of California – Berkeley
- David Wagner Associate Professor in CS at University of California - Berkeley
- First IEEE International Workshop on Sensor Network Protocols and Applications May 11, 2003
- Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols Vol I, No.2-3 September 2003
- Analysis continues..

- **What is the study about?**
  - The authors focus on secure routing issues in WSNs
    - Show how they are different from ad hoc networks
    - Introduce two new classes of attacks
      - Sinkhole attack
      - Hello flood attack
  - Analyze security aspects of major routing protocols
  - Discuss countermeasures & design considerations for secure routing in WSNs

- **What are the study findings:**
  - Demonstrate that currently proposed routing protocols for these networks are insecure.
  - Networks should have security as the goal.
  - Infiltrators can easily attack, modify or capture vulnerable nodes.
  - Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote-class outsiders, but cryptography alone is not enough.
  - Protocol design must take into account the possible presence of laptop-class adversaries and insiders and the limited applicability of end to end security mechanisms.

Real world attacks not described, analyzed or observed. The paper is theoretical.

The Studies Findings

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

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

Background

MICA MOTE

- 4 MHz 8-bit Atmel ATMEGA103 Processor
- Memory
  - 128KB Instruction Memory
  - 4 KB RAM / 512KB flash memory
- 916 MHz radio
  - 40 Kbps single channel
  - Range: few dozen meters
- Power
  - 12 mA in Tx mode
  - 4.8 mA in Rx mode
  - 5 µA in sleep mode
- Batteries
  - 2850 mA on 2 AA

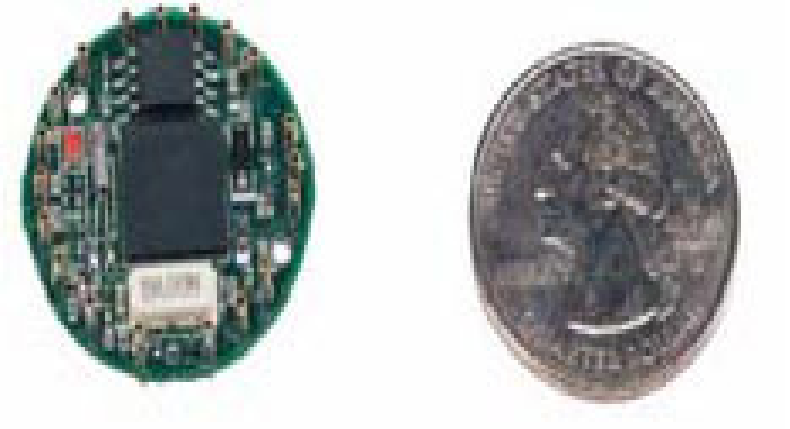


Image source:www.zess.uni-siegen.de/.../smart_sen.jpg

Background

- Power
  - Two weeks at full power
  - Less than 1% duty cycle to last for years
  - Sleep mode most of the time
- Security
  - Public key cryptography too computationally expensive
  - Symmetric key to be used sparingly
  - Only 4KB RAM →maintain little state
- Communication
  - Each bit Tx = 800-1000 CPU instructions

Background

- **Context:**
  - WSNs consist of hundreds or thousands of low-power, low-cost nodes having a CPU, power source, radio, and other sensing elements
  - Have one or more points of centralized control called base stations or sinks
  - Sensor readings from multiple nodes processed at aggregation points
  - Power is the scarcest resource

Background

- **Context:**
  - A representative sensor network architecture

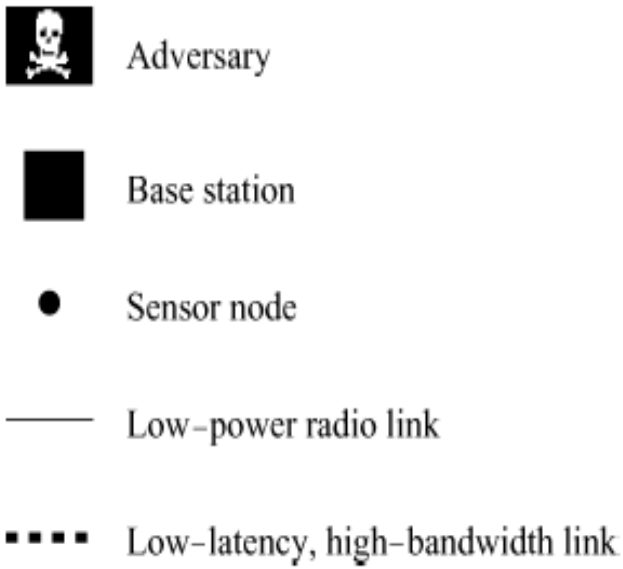
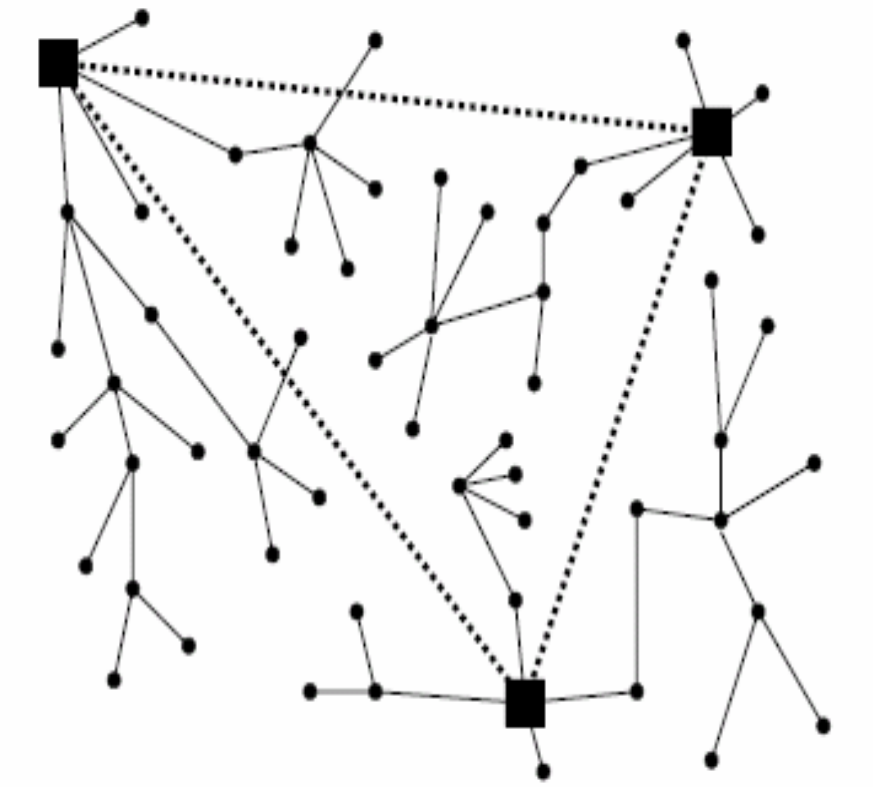


Fig. 2. Sensor network legend. All nodes may use low-power radio links, but only laptop-class adversaries and base stations can use low-latency, high-bandwidth links.



Sensor networks vs. ad-hoc wireless networks

- **Wireless Sensor Networks (WSNs) vs. Ad-hoc Wireless Networks (WNs)**

WSNs

- Communication method - multihop networking
- One or more points of centralized control such as base stations
- Routing - specialized communication pattern
- Resource-starved nature
- Trust relationships between nodes assumed
- Public key cryptography not feasible

AD-hoc WNs

- Communication method - multihop networking
- There is no fixed infrastructure such as base stations
- Routing - any pair of nodes
- Limited resources
- Trust relationships between nodes not assumed
- Public key cryptography possible

Related Work

- Authentication
  - Public key cryptography
    - Too costly
    - WSN can only afford symmetric key
- Secure Routing
  - Source routing / distance vector protocols
    - Require too much node state, packet overhead
    - Useful for fully connected networks, which WSN are not
- Controlling Misbehaving Nodes
  - Punishment
    - Ignore nodes that don't forward packets
    - Susceptible to blackmailers
- Security protocols
  - SNEP – provides confidentiality, authentication
  - µTESLA – provides authenticated broadcast

Problem Statement

- Network assumptions
  - Insecure radio links
    - Injected bits
    - Replayed packets
  - Malicious nodes may collude to attack the network
    - Added to the network
    - Good ones “turned” bad
    - Many could lead to a mutiny
  - Sensor nodes not temper resistant
    - Processed Data
    - Stored Code
  - Physical and MAC layers vulnerable to direct attacks

Need a better discussion of pulling packets out of the air or injecting.

Problem Statement

- Trust Requirements
  - Assume base stations are trustworthy
    - Behave correctly
    - Messages from base stations are assumed correct
  - Nodes are not assumed trustworthy
    - Regular nodes
    - Aggregation points
      - Provide routing information,
      - Collect and combine data
      - Valuable component of the network
      - Bad guys would love to control an aggregation point

If each node were marked with an RFID chip then they would be marked as friend anything else would be considered a foe

Problem Statement

- 2 types of threat models:
  - Based on type of attacking devices
    - Mote-class attackers vs. Laptop-class attackers
      - Capabilities (Battery, Transmitter, CPU)
      - Local vs. Network radio link
      - Local vs. Network eavesdropping
  - Based on attacker location
    - Outsider attacks vs. Insider attacks
      - Outsider: Distributed Denial of Service
      - Insider: Malicious code, stolen data

I would think denial of service through jamming would be practically impossible to defend.

Problem Statement

- Security Goals:
  - Every receiver should be able to:
    - Receive messages intended for it
    - Verify integrity of the message
    - Verify identity of the sender
    - Achieve security in the presence of adversaries of arbitrary power
  - Eavesdropping
    - Application Responsibility
      - Secrecy
      - Replaying data packets
    - Protocol Responsibility
      - Rerouting
  - Achievability (Insider vs. Outsider)

Should sensor networks provide security? Is security the goal or is it gathering data?

Attacks on sensor network routing

- Spoofed, altered, or replayed routing information:
  - Create routing loops
  - Attract or repel network traffic
  - Extend or shorten service routes
  - Generate false error messages
  - Partition the network
  - Increase end-to-end latency

What happens when a real node identity is spoofed and paralyzed? What are the countermeasures? Is it detectable?

Attacks on sensor network routing

- Selective forwarding:
  - Malicious nodes may drop packets
    - Dropping everything raises suspicion
    - Instead, forward some packets and not others
  - Insider
    - Bad guy included in the routing path
  - Outsider
    - Bad guy causes collisions on an overheard flow

Attacks on sensor network routing

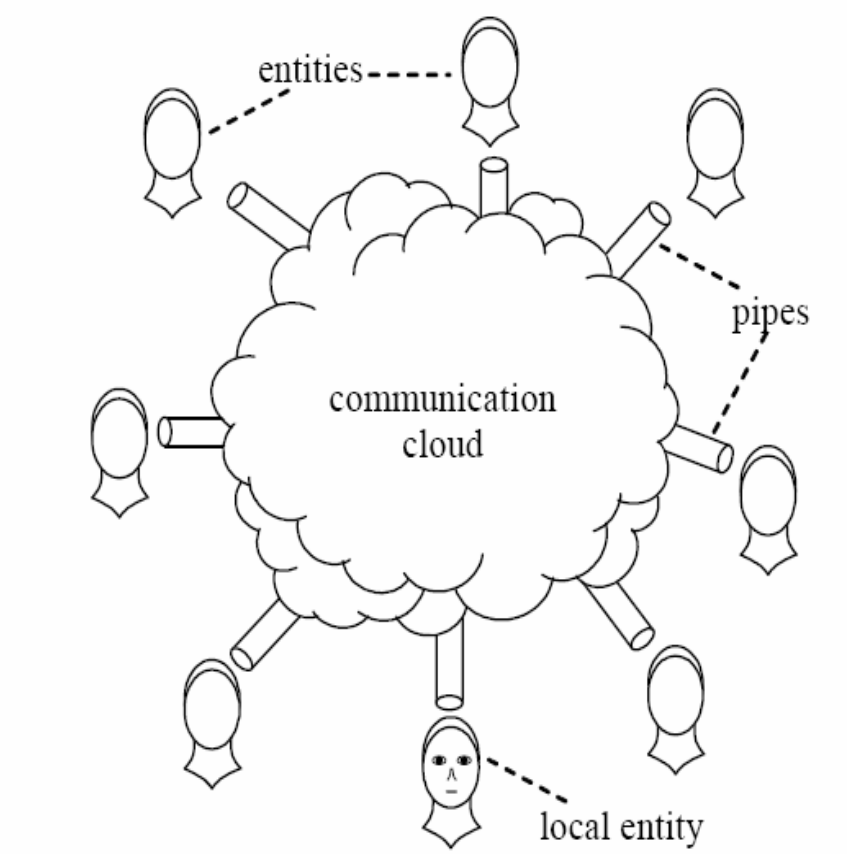
- Sinkhole attacks:
  - Adversary's goal is to lure traffic through a compromised node
  - Bad guy tricks base station and nodes into thinking it provides a high-quality link
    - Lies about its quality,
    - Use a laptop class node to fake a good route
  - Work by making the compromised node look attractive
  - High susceptibility due to communication pattern of WSN

Attacks on sensor network routing

Sybil Attack:

"One can have, some claim, as many electronic personas as one has time and energy to create."

Judith S. Donath [1]



Picture from [2]

Attacks on sensor network routing

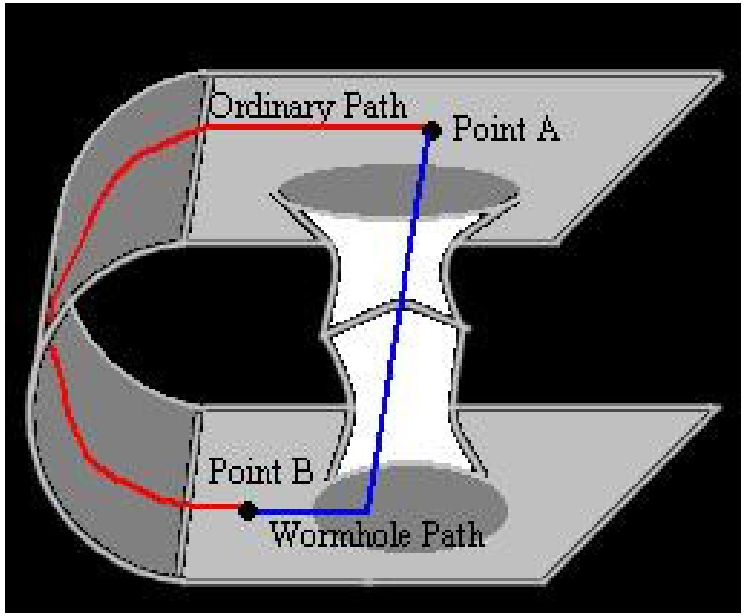
- Sybil Attack:
  - A single node presents multiple identities to other nodes in the network
  - Threat to geographic routing
    - Being in more than one place at once
  - Threat to aggregation processing
    - Sending multiple (fictitious) results to a parent
    - Sending data to more than one parent

Attacks on sensor network routing

- Wormholes:

Wormhole

An adversary tunnels packets received in one part of the network over a low-latency link and replays them in a different part of the network



Picture from http://library/thinkquest.org/27930/wormhole.htm

Attacks on sensor network routing

- HELLO flood attack:
  - Many protocols require that nodes broadcast HELLO packets to announce themselves to their neighbors
    - Assumption that sender is within normal range
    - Laptop-class attacker can convince all nodes that it is their neighbor by transmitting at high power
  - Deceived nodes would try to send packets to this node
    - Packets would instead go out into oblivion
  - False routing information leaves network in state of confusion
  - Protocols that rely on local coordinated maintenance are susceptible

Attacks on sensor network routing

- Acknowledgement spoofing:
  - Adversary sends link-layer ACKs for overheard packets
  - Fools node into sending traffic through a weak/dead link
    - Packets sent along this route are essentially lost
    - Adversary has effected a selective forwarding attack

Attacks on specific sensor network protocols

- TinyOS beaconing:
  - Routing algorithm - constructs a spanning tree rooted at base station
  - Nodes mark base station as its parent, then inform the base station that it is one of its children
  - Receiving node rebroadcasts beacon recursively
  - Included with the TinyOS distribution

Attacks on specific sensor network protocols

- TinyOS beaconing:
  - Protocol is highly susceptible to attack.
  - Routing updates are not authenticated, so it is possible for any node to claim to be a base station and become the destination of all traffic in the network.

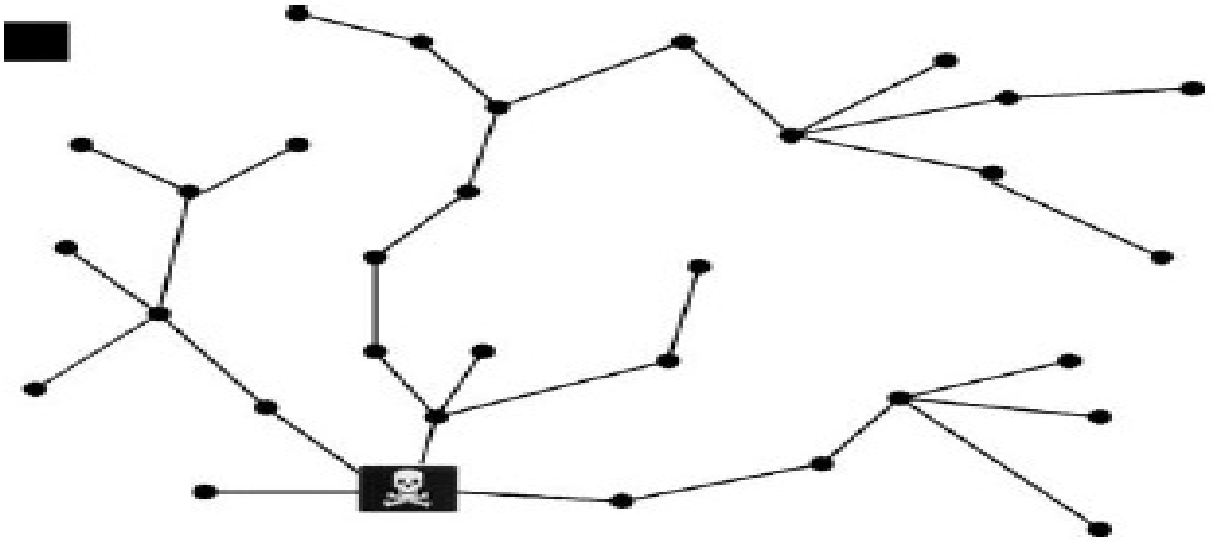


Fig. 5. An adversary spoofing a routing update from a base station in TinyOS beaconing.

Attacks on specific sensor network protocols

- TinyOS beaconing:
  - Combined wormhole/sinkhole attack

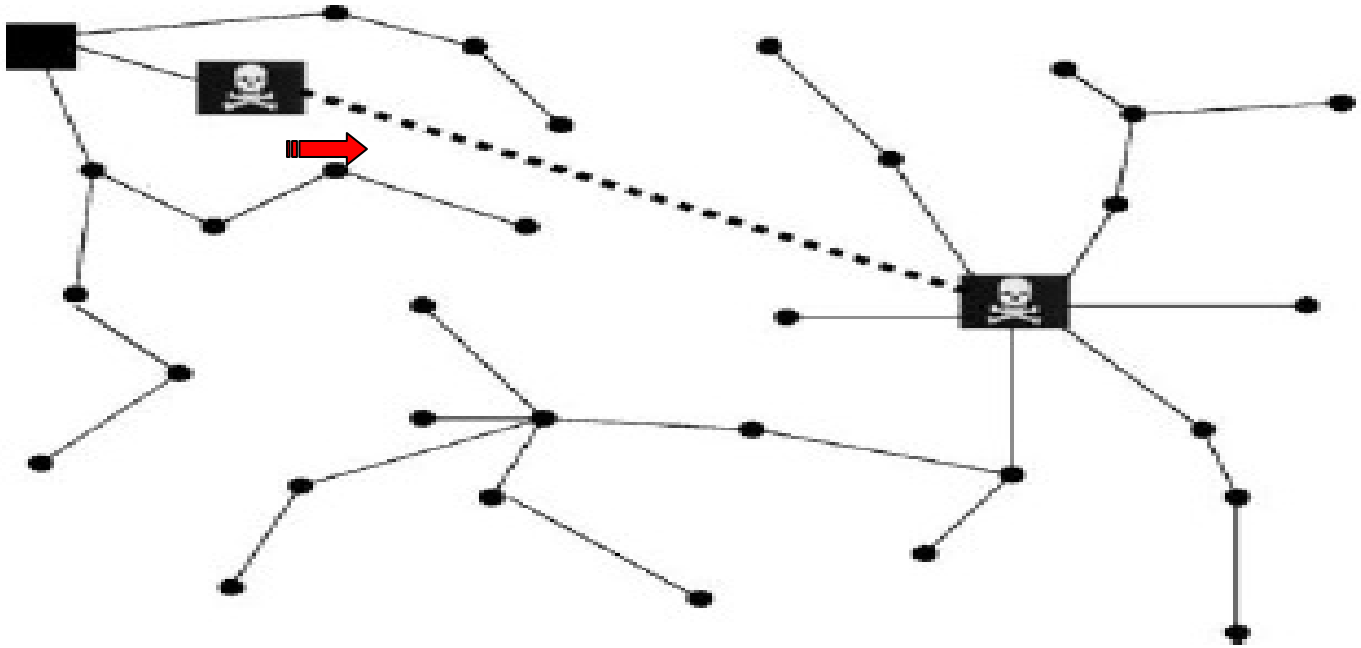


Fig. 6. A laptop-class adversary using a wormhole to create a sinkhole in TinyOS beaconing.

Attacks on specific sensor network protocols

- TinyOS beaconing:
  - A laptop-class adversary has a powerful transmitter.
  - It uses a HELLO flood attack to broadcast a routing update loud enough to reach the entire network, causing every node to mark the adversary as its parent.
  - Most nodes will be likely out of normal radio range of both a true base station and the adversary.
  - As shown below the network is crippled: the majority of nodes are stranded, sending packets into oblivion. Due to the simplicity of this protocol, it is unlikely there exists a simple extension to recover from this attack.

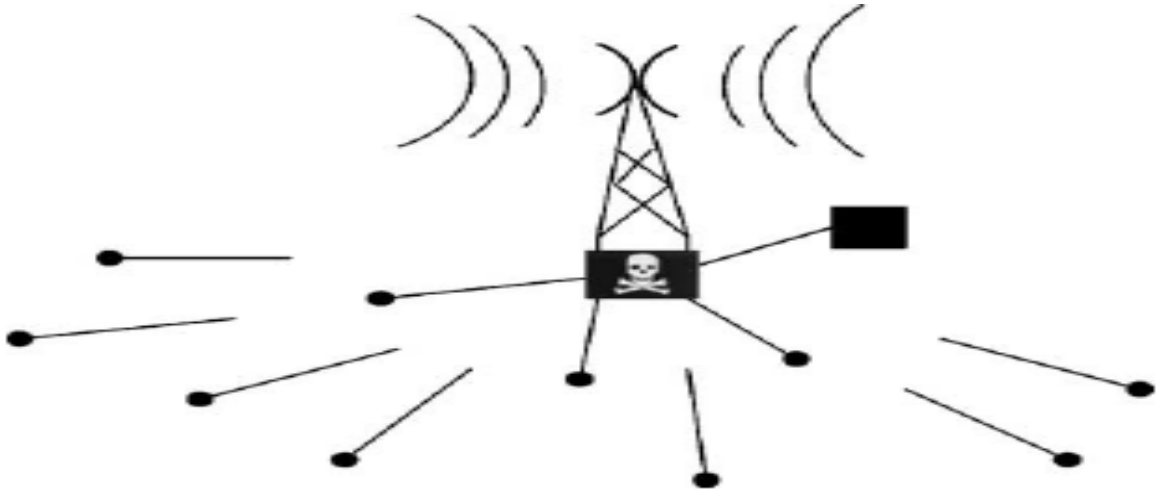


Fig. 7. HELLO flood attack against TinyOS beaconing. A laptop-class adversary that can retransmit a routing update with enough power to be received by the entire network leaves many nodes stranded. They are out of normal radio range from the adversary but have chosen her as their parent.

References

1. J. S. Donath, “Identity and Deception in the Virtual Community”, *Communities in Cyberspace*, Routledge, 1998.
2. J.R. Douceur, The Sybil attack, in: 1st International Workshop on Peer-to-Peer Systems (IPTPS 02), 2002.
3. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," in IEEE SPNA, 2002