# Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

**Chris Karlof, David Wagner**

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

**Presented by Michael Putnam**

**(Some images and slides taken from author’s presentation, others as noted)**

# Author Bio's

- University of California - Berkeley
  - **Chris Karlof**

    Grad Student in CS

    Researches:

    Computer Security
    Web Security
    Electronic Voting

  - **David Wagner**

    Associate Professor in CS

    Researches:

    Computer Security
    Electronic Voting
    Program Analysis for Security reasons

# Motivationally Speaking

Biographies
INTRODUCTION
Background
WSN v. Ad-hoc
Related Work
Problem Statement
Routing Attacks
Protocol Attacks
Countermeasures
Conclusions

- **Focus is on routing security in Sensor Networks**

- **Many protocols have been proposed, but for none has security been a goal.**

- **Since none of the protocols were designed with security as a goal, not unsurprising to find they’re insecure.**

# Historically Speaking

Biographies

INTRODUCTION

Background

WSN v. Ad-hoc

Related Work

Problem Statement

Routing Attacks

Protocol Attacks

Countermeasures

Conclusions

- **Security is non-trivial to fix in existing protocols**
- **Typically adding security on after the fact leads to poor results**
- **Not likely that simply adding a security mechanism will make them secure**

# Security in Sensor Networks

- Security is critical
  - Military apps
  - Building monitoring
  - Burglar alarms
  - Emergency response

Image taken from author’s slides

- Yet security is hard
  - Wireless links are inherently insecure
  - Resource constraints
  - Lossy, low bandwidth communication
  - Lack of physical security

# Contributions

- Propose threat models and security goals for secure routing in wireless sensor networks.

- Introduce two novel classes of previously undocumented attacks
  - Sinkhole Attacks
  - HELLO Floods.

**Image source: jedicraft.blogspot.com**

**Image source:  www.burkhardagency.com**

# Contributions

- Show how attacks against ad-hoc wireless networks and P2P networks can be adapted against sensor networks.

- Present security analysis of all the major routing protocols and topology maintenance algorithms for sensor networks. We describe practical attacks against all of them that would defeat any reasonable security goals.

- Discuss countermeasures and design considerations for secure routing protocols in sensor networks.

# Mica Mote

Biographies
Introduction
BACKGROUND
WSN v. Ad-hoc
Related Work
Problem Statement
Routing Attacks
Protocol Attacks
Countermeasures
Conclusions

- 4 MHz 8-bit Atmel ATMEGA103 Processor
- Memory
  - 128KB Instruction Memory
  - 4 KB RAM / 512KB flash memory
- 916 MHz radio
  - 40 Kbps single chann
  - Range: few dozen me
- 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.btnode.ethz.ch

# Resource Constraints

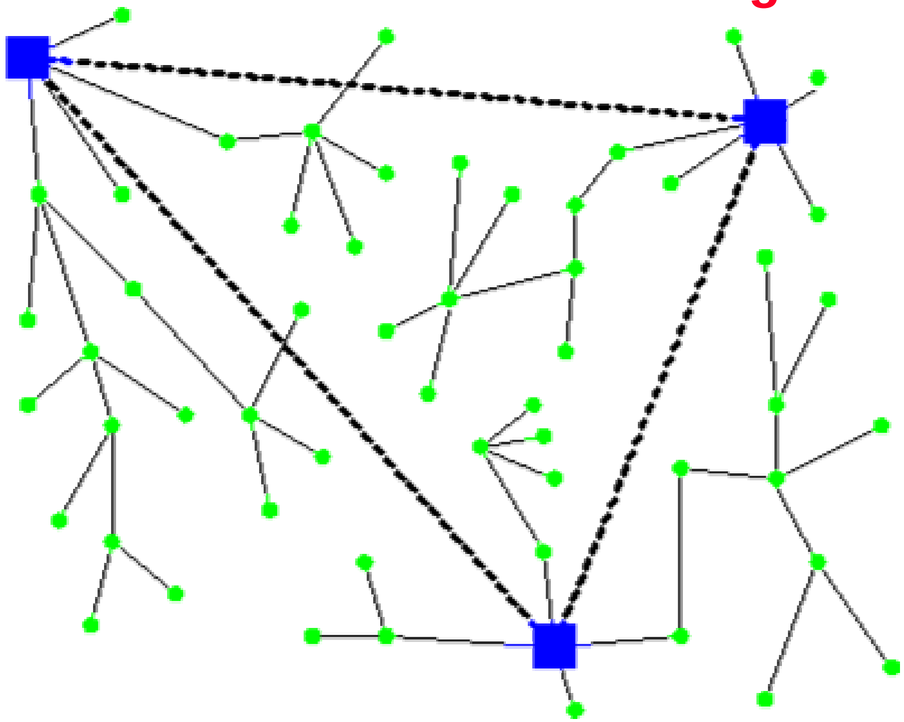
Biographies
Introduction
BACKGROUND
WSN v. Ad-hoc
Related Work
Problem Statement
Routing Attacks
Protocol Attacks
Countermeasures
Conclusions

- **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

# Routing in sensor networks

Biographies
Introduction
BACKGROUND
WSN v. Ad-hoc
Related Work
Problem Statement
Routing Attacks
Protocol Attacks
Countermeasures
Conclusions

- **Base stations and sensor nodes**
- **Low overhead protocols**
- **Specialized traffic patterns**
- **In-network processing**
- **These differences necessitate new secure routing protocols**



■ base station

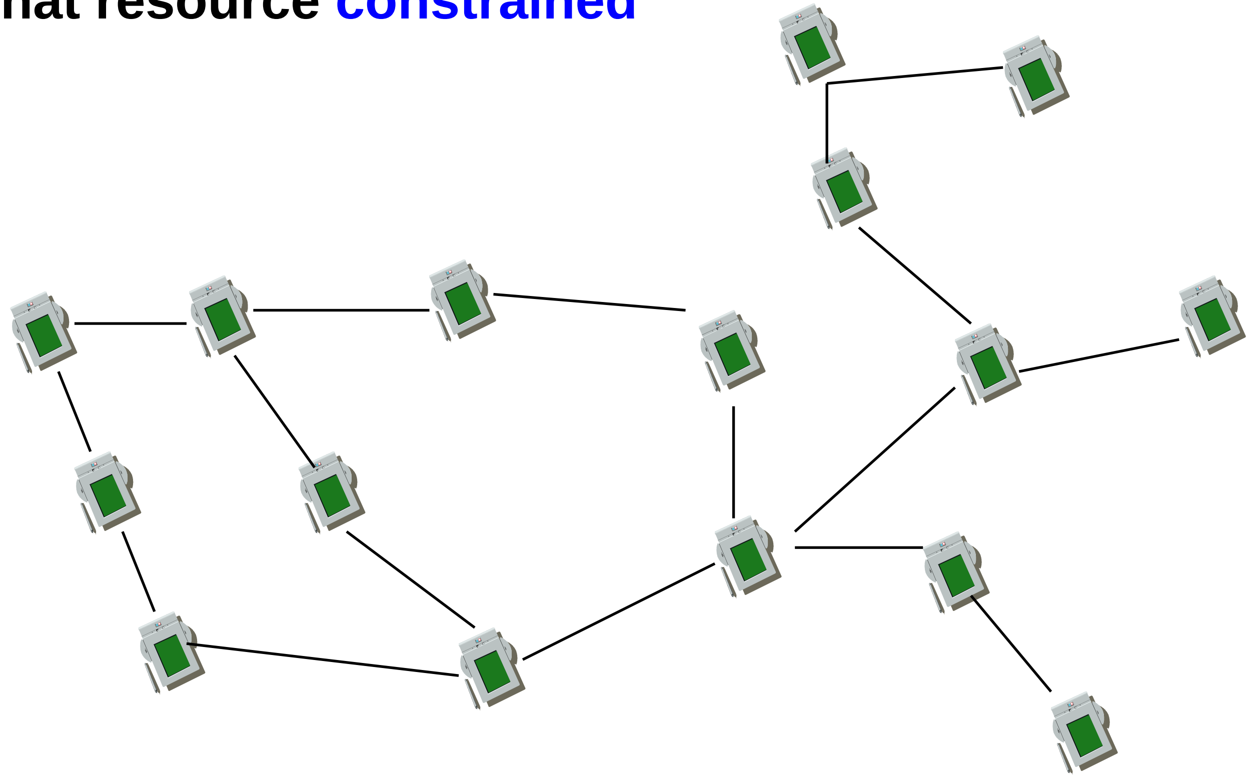
● sensor node

# Ad-hoc vs. WSN

Biographies
Introduction
Background
**WSN v. AD HOC**
Related Work
Problem Statement
Routing Attacks
Protocol Attacks
Countermeasures
Conclusions

- **Multi-hop**
- **Routing between any pair of nodes**
- **Somewhat resource constrained**

**Ad - hoc**



# Ad-hoc vs. WSN

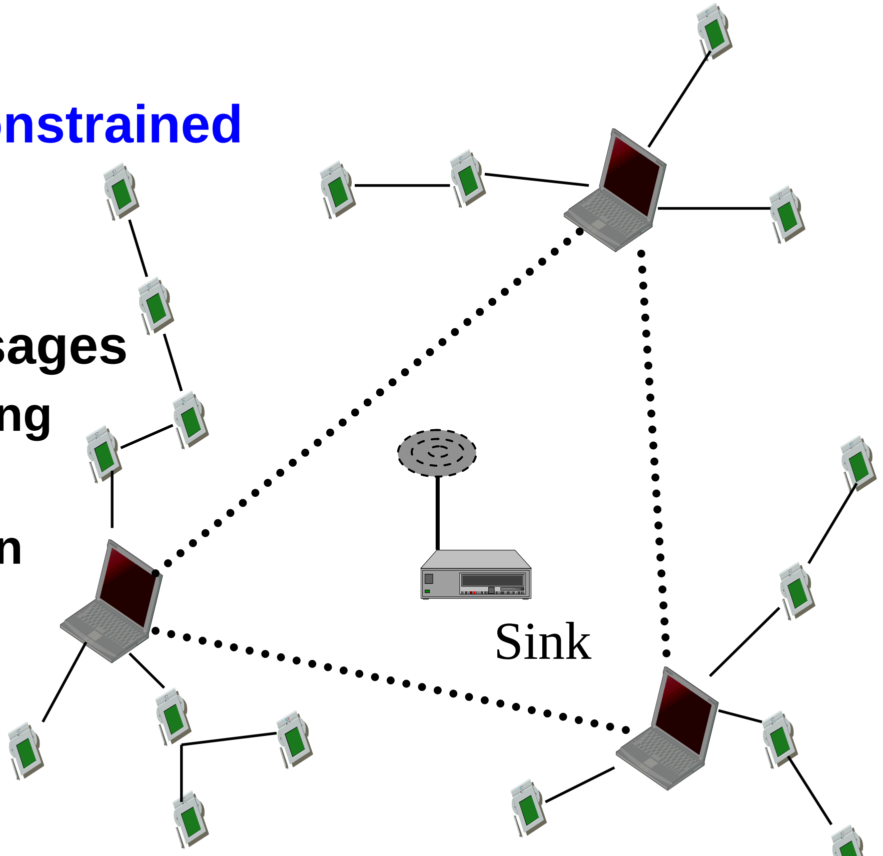
Biographies
Introduction
Background
**WSN v. AD HOC**
Related Work
Problem Statement
Routing Attacks
Protocol Attacks
Countermeasures
Conclusions

- **Routing Patterns**
  - **Many-to-One**
  - **One-to-Many**
  - **Local**

- **Extremely resource constrained**

- **Trust Relationships to prune redundant messages**
  - **In-network processing**
  - **Aggregation**
  - **Duplicate elimination**

**WSN**



# Research

Biographies
Introduction
Background
WSN v. Ad hoc
**RELATED WORK**
Problem Statement
Routing Attacks
Protocol Attacks
Countermeasures
Conclusions

- **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**

# Network Assumptions

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
PROBLEM STATEMENT
Routing Attacks
Protocol Attacks
Countermeasures
Conclusions

- Radio links are insecure
  - Injected bits
  - Replayed packets
- Malicious nodes / neighbors
  - Added to the network
  - Good ones “turned” bad
  - Many could lead to a mutiny
- Sensors are not tamper-proof
  - Processed Data
  - Stored Code

# Trust Requirements

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
PROBLEM STATEMENT
Routing Attacks
Protocol Attacks
Countermeasures
Conclusions

- Assumption that 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

# Threat Models

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
PROBLEM STATEMENT
Routing Attacks
Protocol Attacks
Countermeasures
Conclusions

Image source: news.bbc.co.uk

Image source: www.planetware.com

- **Mote-class attackers vs. Laptop-class attackers**
  - **Capabilities (Battery, Transmitter, CPU)**
  - **Local vs. Network radio link**
  - **Local vs. Network eavesdropping**

- **Outsider attacks vs. Insider attacks**
  - **Outsider: DDos**
  - **Insider: Malicious code, stolen data**

# Security Goals

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
PROBLEM STATEMENT
Routing Attacks
Protocol Attacks
Countermeasures
Conclusions

- 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)

# Spoofed, altered, replayed routing

- 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

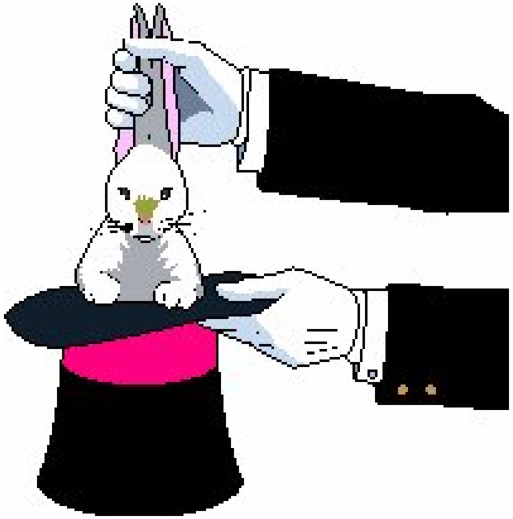
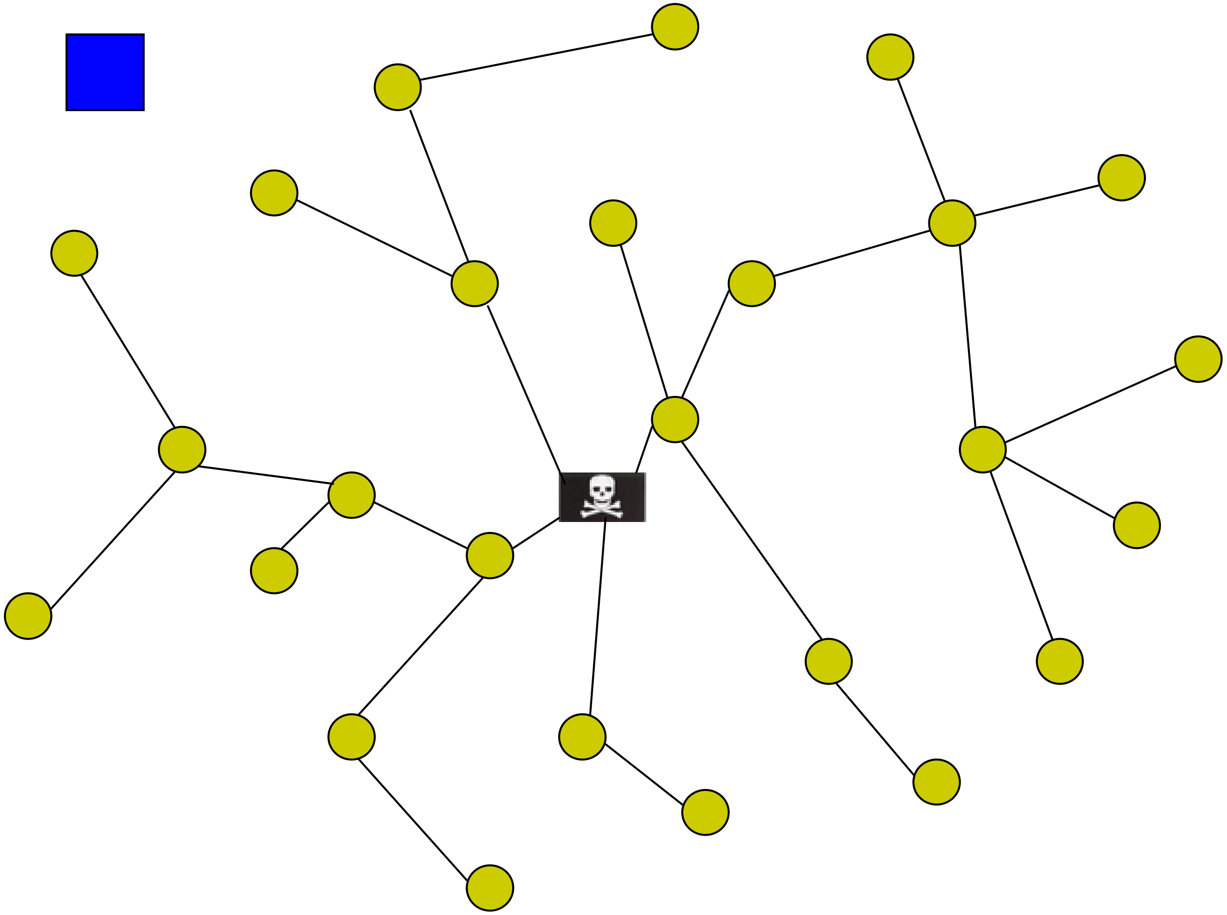


Image source: poganka.splinder.com

# Spoofed, altered, replayed routing

- **Example: spoof routing beacons and claim to be base station**



# Selective Forwarding

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
ROUTING ATTACKS
Protocol Attacks
Countermeasures
Conclusions

- **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**

**Image source: sunny.moorparkcollege.edu**

# Sinkhole Attack

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
ROUTING ATTACKS
Protocol Attacks
Countermeasures
Conclusions

- Malicious node tries to get traffic to pass through it
  - Lots of opportunities to tamper with traffic
- Bad guy tricks base station and nodes into thinking it provides a high-quality link
  - Lies about its quality,
  - Use a laptop class node *fake* a good route
- False perception makes it likely to attract flows
- High susceptibility due to communication pattern of WSN

Image source: http://www2.gsu.edu/~geowce/sinkholes.htm

# Sybil Attack

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
ROUTING ATTACKS
Protocol Attacks
Countermeasures
Conclusions

- 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

Image source: thecinema.blogia.com

# Wormholes

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
ROUTING ATTACKS
Protocol Attacks
Countermeasures
Conclusions

- Tunneling messages in one part of the network to distant parts of the network

- Great setup for a sinkhole
  - Useful in connection with selective forwarding, eavesdropping
  - Difficult to detect with Sybil

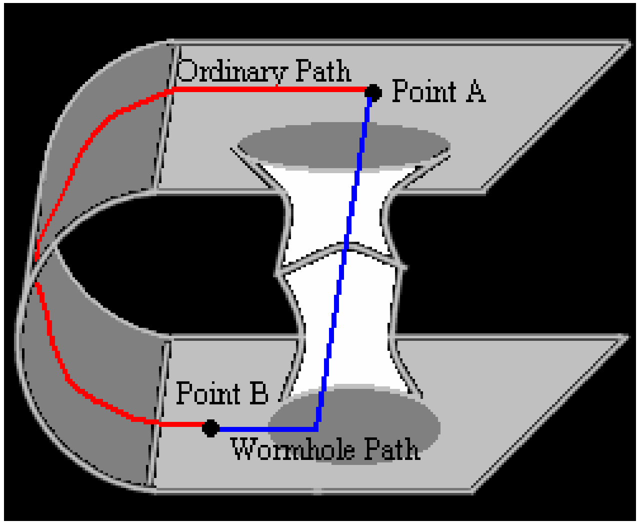


Image source: library.thinkquest.org

# HELLO Flood

- HELLO packets to announce presence to neighbors
  - Assumption that sender is within normal range
  - A laptop class attacker could trick all nodes in network into thinking it’s a parent/neighbor
- 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

Image source: www.lamission.edu

# ACK Spoofing

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
ROUTING ATTACKS
Protocol Attacks
Countermeasures
Conclusions

- 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

Image source: www.americansforprosperity.org/blog/

# TinyOS Beaconing

Biographies

Introduction

Background

WSN v. Ad hoc

Related Work

Problem Statement

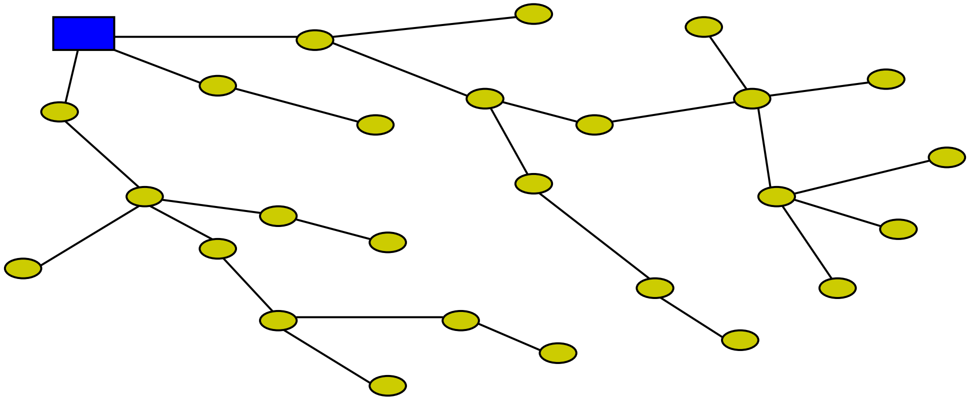
Routing Attacks

PROTOCOL ATTACKS

Countermeasures

Conclusions

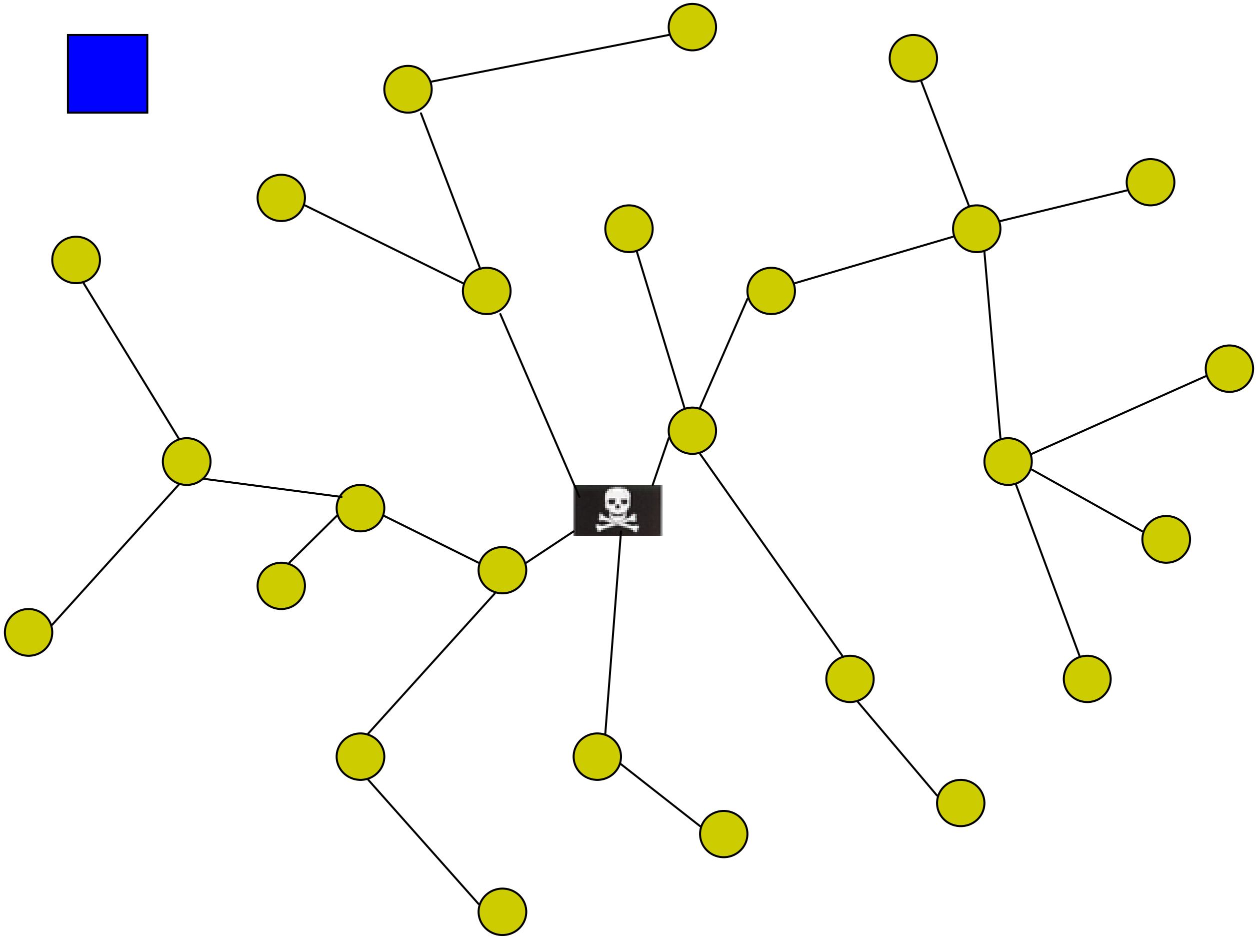
- **Routing algorithm - constructs a spanning tree rooted at base station**
- **Nodes mark base station as its parent, then inform the base station that it is one of its children**
- **Receiving node rebroadcasts beacon recursively**
- **Included with the TinyOS distribution**



# TinyOS Beaconing

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
Routing Attacks
**PROTOCOL ATTACKS**
Countermeasures
Conclusions

- **Any node can claim to be the base station**



# Directed Diffusion

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
Routing Attacks
PROTOCOL ATTACKS
Countermeasures
Conclusions

- Data-centric routing algorithm
- Base Station floods request for particular information
- Nodes with that information respond to the request in reverse path direction
- Positive reinforcement increases the data rate of the responses while negative reinforcement decreases it.

# Directed Diffusion

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
Routing Attacks
**PROTOCOL ATTACKS**
Countermeasures
Conclusions

- **Suppression**
  - **Achieved with negative reinforcements**
  - **Type of DoS**
- **Cloning**
  - **Replaying an overheard interest**
  - **Enables eavesdropping**
- **Path Influence**
  - **Creates sinkhole using positive/negative reinforments**
  - **Adversary can influence topology**
  - **Leads to data tampering and selective forwarding**

# Geographic Routing

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
Routing Attacks
PROTOCOL ATTACKS
Countermeasures
Conclusions

- **Greedy Perimeter Stateless Routing (GPSR)**
  - **Forwards data to the next closest neighbor at each hop**
  - **Leads to subset of nodes being used more**

- **Geographic and Energy Aware Routing (GEAR)**
  - **Like GPSR, but weights each hop with energy info**
  - **Tries to balance out energy usage**

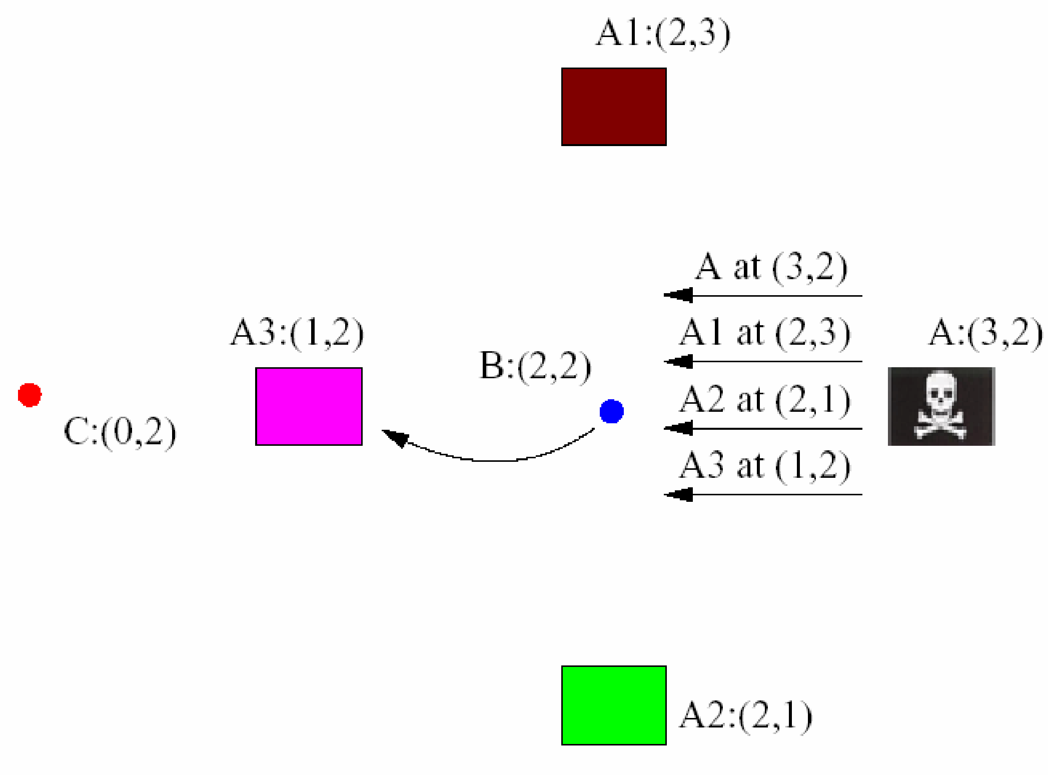
- **Both require nodes to exchange positioning info**

- **GEAR requires nodes to share energy info**

# Geographic Routing

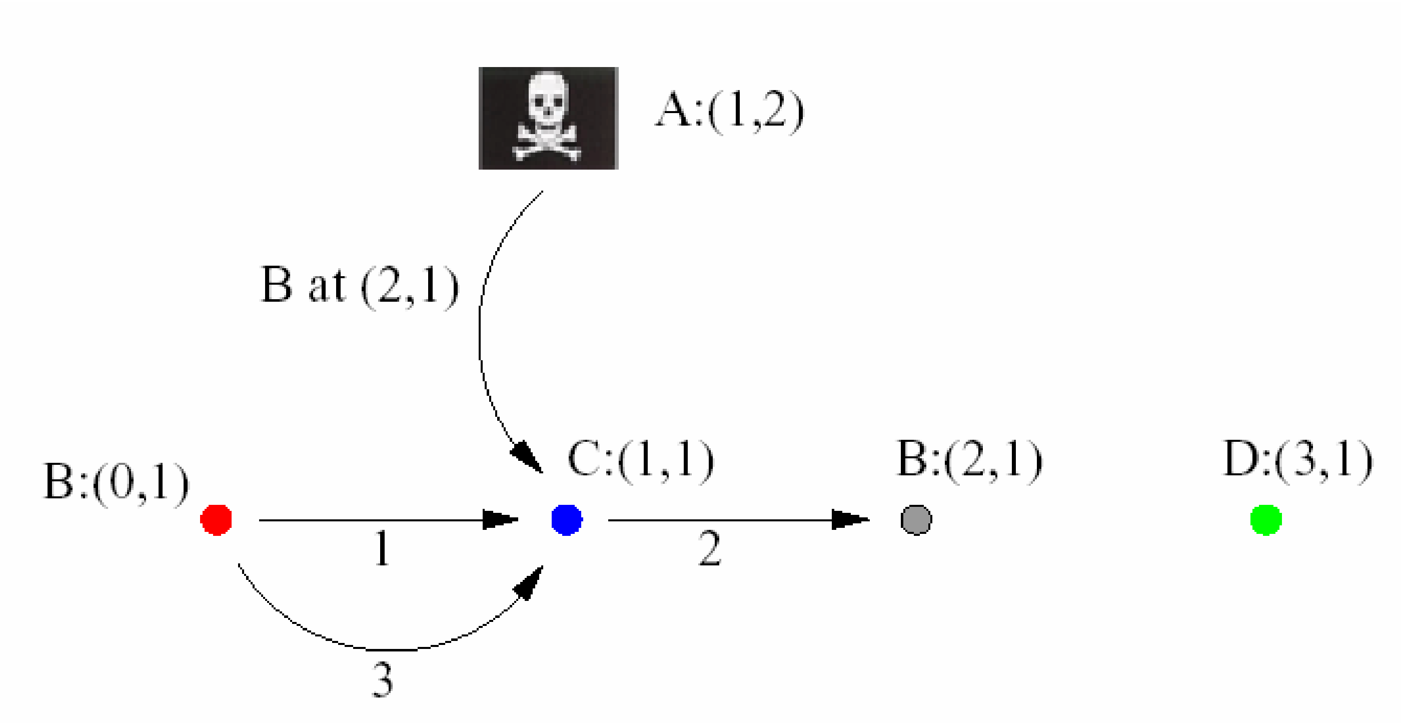
Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
Routing Attacks
**PROTOCOL ATTACKS**
Countermeasures
Conclusions

- **Fake location / energy information**



# Geographic Routing

- **Create Routing Loops**



# Additional Routing Protocols

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
Routing Attacks
**PROTOCOL ATTACKS**
Countermeasures
Conclusions

- **Minimum Cost Forwarding**
- **Low Energy Adaptive Clustering Hierarchy (LEACH)**
- **Rumor Routing**
- **Topology Maintenance Algorithms**
  - **SPAN**
  - **GAF**
- **15 protocols studied,**
  - **nearly all the proposed WSN routing protocols.**

# Outsider Attacks

- **Link Layer Security**

- **Prevention by encryption and authentication**
  - **using global shared key**

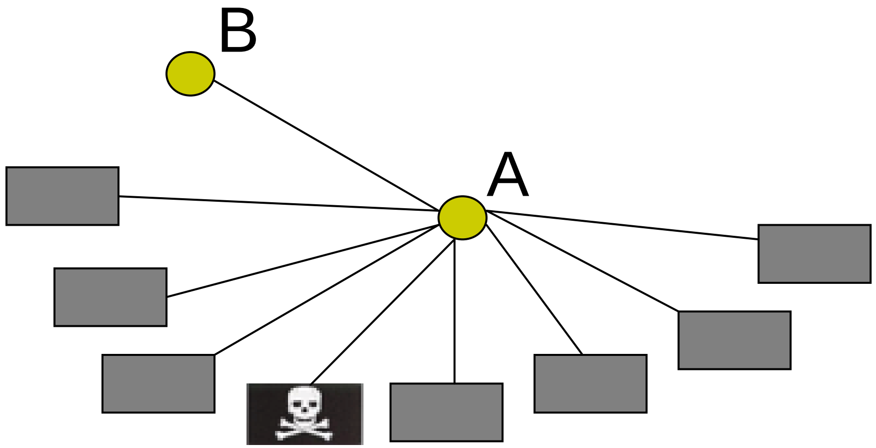
- **ACK's can be authenticated**

- **Defeats Sybil, Selective Forwarding, Sinkhole**
  - **Adversary cannot join the topology**

# Sybil Attack

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
Routing Attacks
Protocol Attacks
COUNTERMEASURES
Conclusions

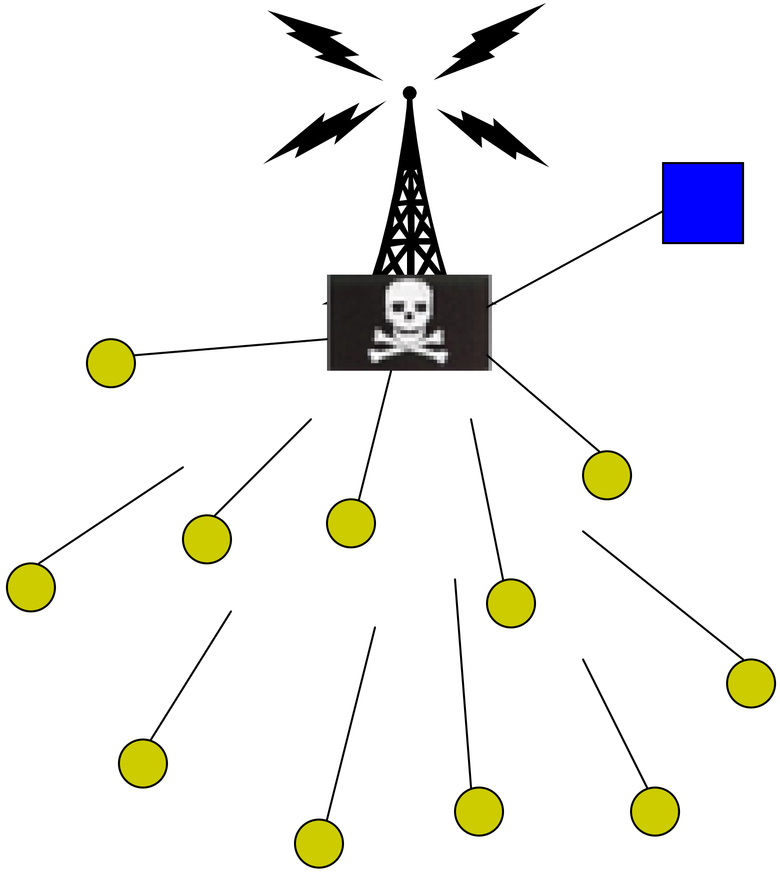
- **Verify Identities**
  - **Share a unique key with the base station**
  - **Nodes create encrypted link using this key**
- **Prevent nodes from creating too many links**
  - **Limit number of neighbors a node can have**
- **Wormholes are still possible**
  - **but adversary will not be able to eavesdrop or modify messages**



# HELLO Flood Attack

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
Routing Attacks
Protocol Attacks
COUNTERMEASURES
Conclusions

- Verify bi-directionality of the link
  - Same as with Sybil, using shared key protocol

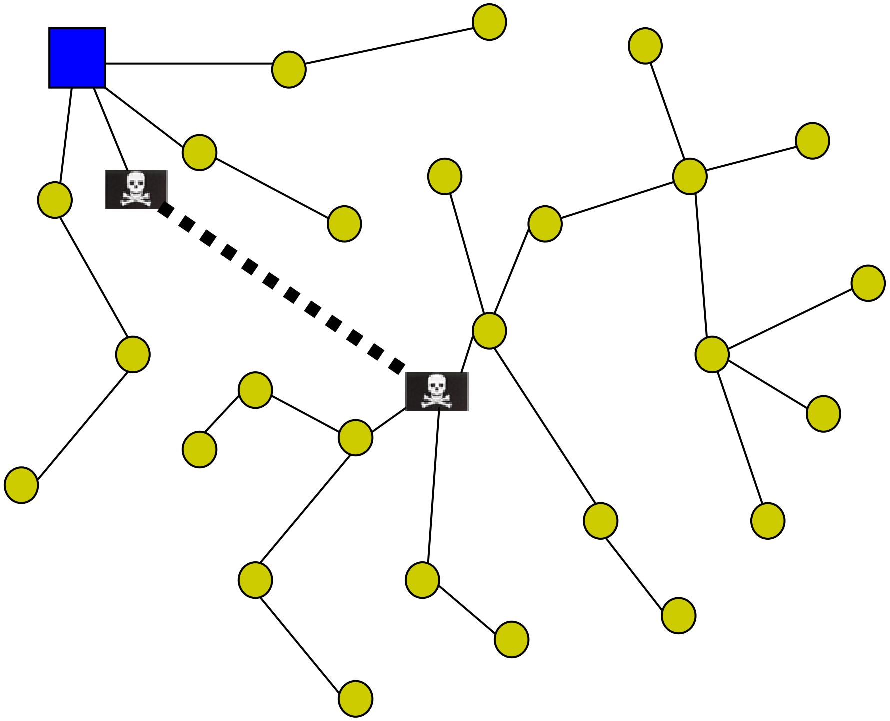


# Wormholes

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
Routing Attacks
Protocol Attacks
COUNTERMEASURES
Conclusions

- Hard to detect
  - Private, out-of-band channel used to transmit messages

- Invisible to underlying sensor network



# Sinkholes

- Protocols that use advertised information are most susceptible
  - Remaining energy
  - End-to-end reliability estimates
  - Unverified routing information

Image source: http://www2.gsu.edu/~geowce/file/cave02.jpg

# Wormholes / Sinkholes

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
Routing Attacks
Protocol Attacks
COUNTERMEASURES
Conclusions

- **Design routing protocols that neutralize these attacks**
  - **Topology created by base station is most vulnerable**
- **Geographic routing offers better protection**
  - **Topology on-demand**
  - **Based on local interactions**
  - **Neighboring nodes keep bad guys honest**

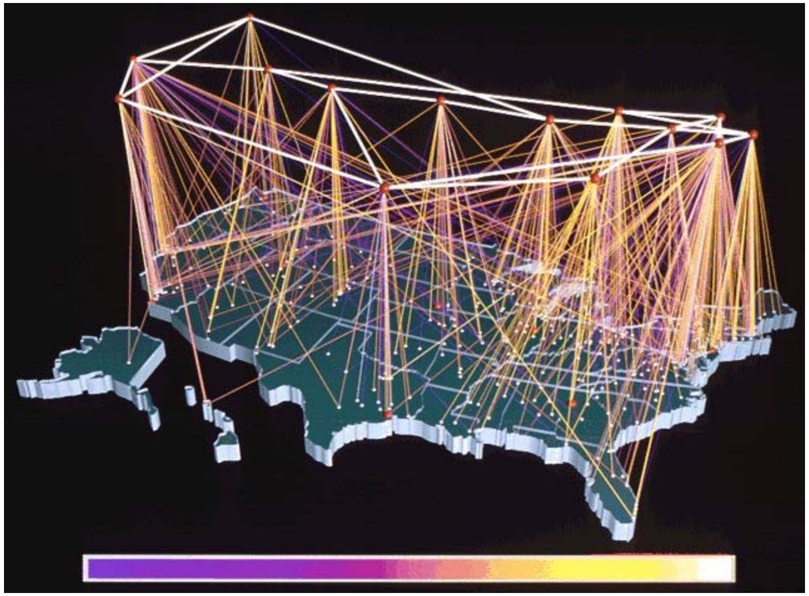
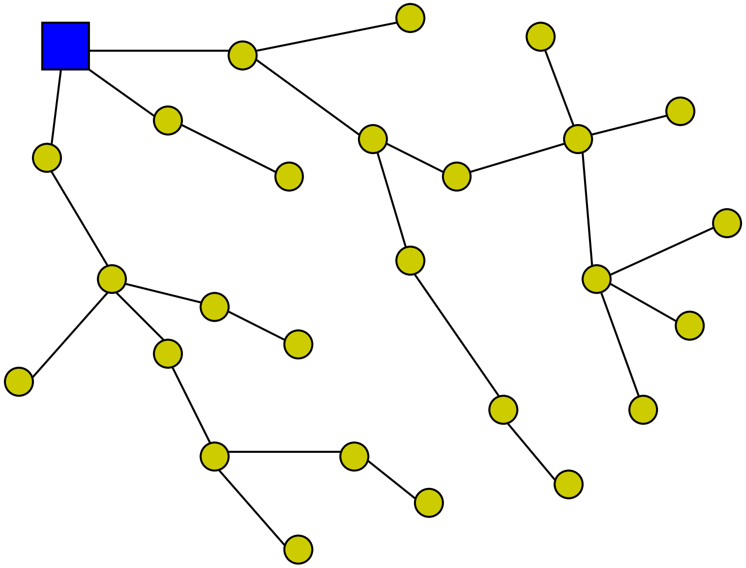


**Image source: http://www.cybergeography.org/spanish/geographic.html**

# Leveraging Global Knowlege

- **Fixed network size**
  - Keeps bad guys from joining

- **Fixed network topology**
  - Prevents sinkholes and wormholes
  - Location information must be trusted
  - Probabilistic varying of the next-hop can help



# Selective Forwarding Attack

- Best chance is multi-path routing
  - Messages routed over *n* disjoint paths protected from *n* compromised nodes

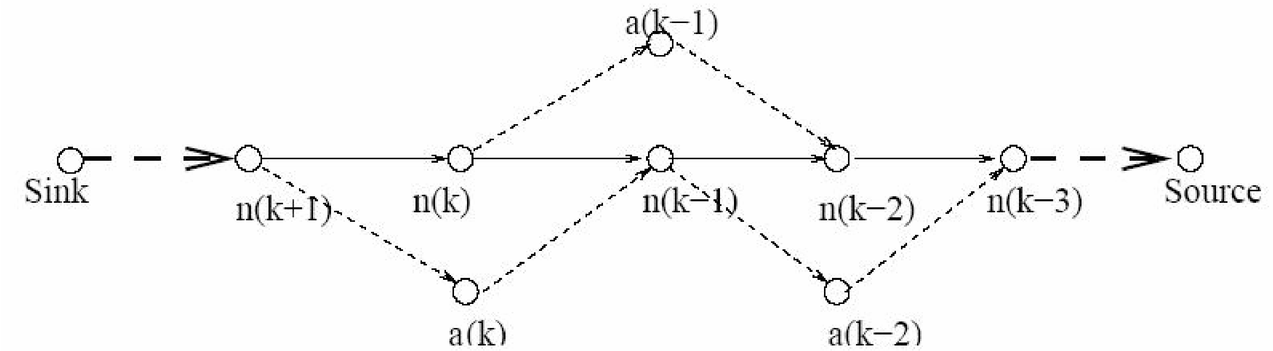


Image Source: http://wiki.uni.lu/secan-lab/Braided+Multipath+Routing.html

- Probabilistically choosing next-hop

# Authenticated Broadcast  and Flooding

- Base Station
  - Trustworthy
  - Nodes should not be able to spoof these messages
  - Authentication protocols
    - Digital signatures, excessive packet overhead
    - µTESLA
      - Uses symmetric key cryptography
      - Minimal packet overhead
      - Prevents replay by discarding old keys

# Authenticated Broadcast and Flooding

- **Flooding**
  - **Used to get information to all nodes**
  - **Adversaries need to form a vertex cut**

- **Downsides**
  - **High energy cost**
  - **Increased collisions**
  - **Congestion**

- **Proposals**
  - **Spin**
  - **Gossiping algorithms**

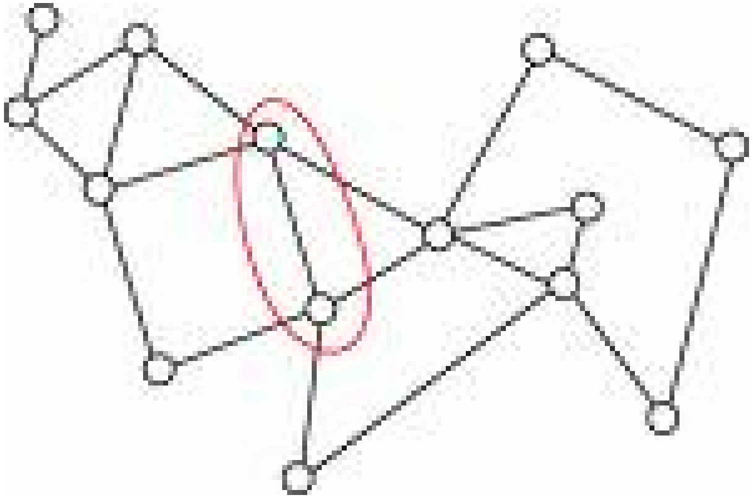


**Image source: http://www.elet.polimi.it**

# Countermeasure Summary

Biographies
Introduction
Background
WSN v. Ad hoc
Related Work
Problem Statement
Routing Attacks
Protocol Attacks
Countermeasures
CONCLUSIONS

- Link layer encryption and authentication
- Multi-path routing
- ID verification
- Bidirectional link verification
- Authenticated broadcast

**Protects against**

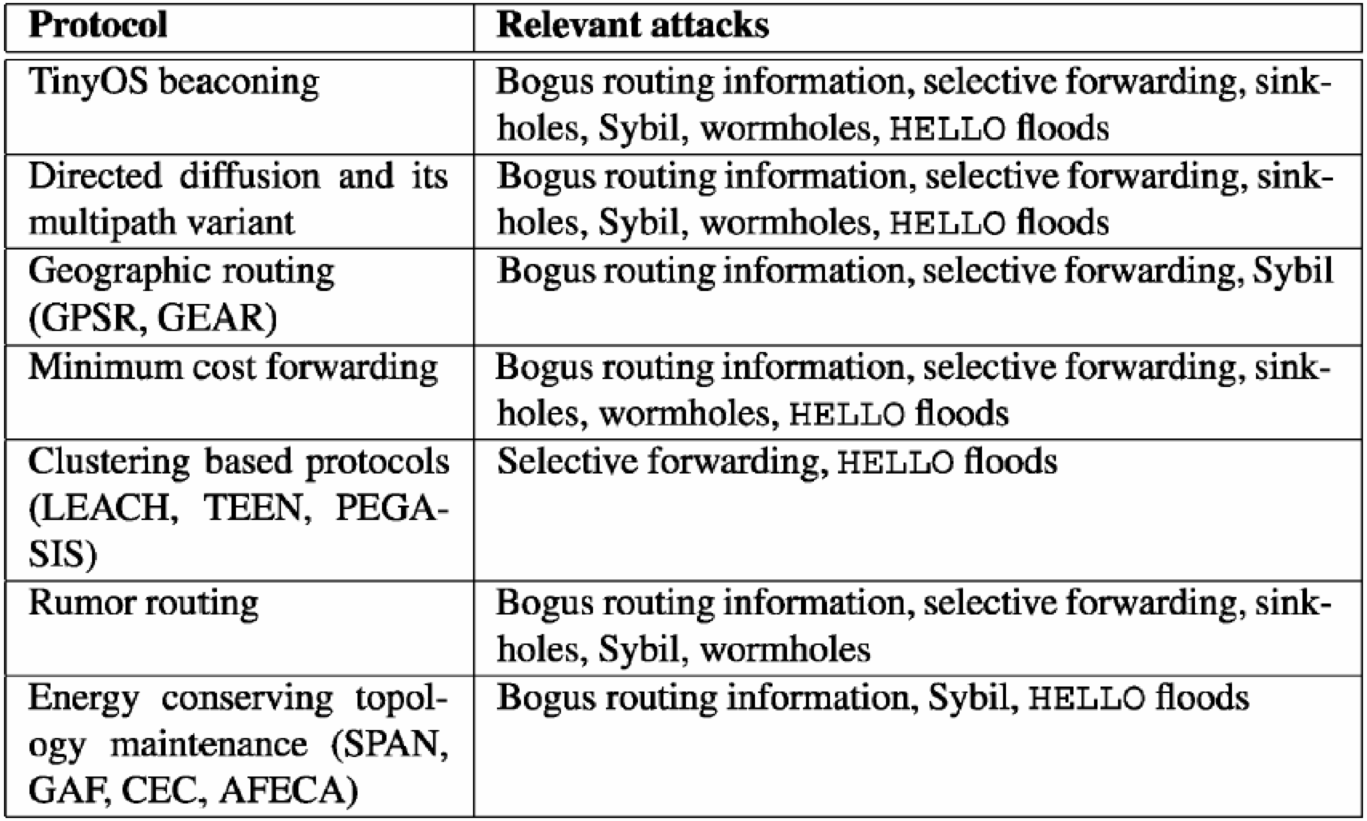
- Outsiders
- Spoofed routing info
- Sybil
- HELLO flood
- ACK spoofing

- Sinkhole
- Wormhole

**Requires special routing**

Geographic is promising

# Attack Summary



| **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.