Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

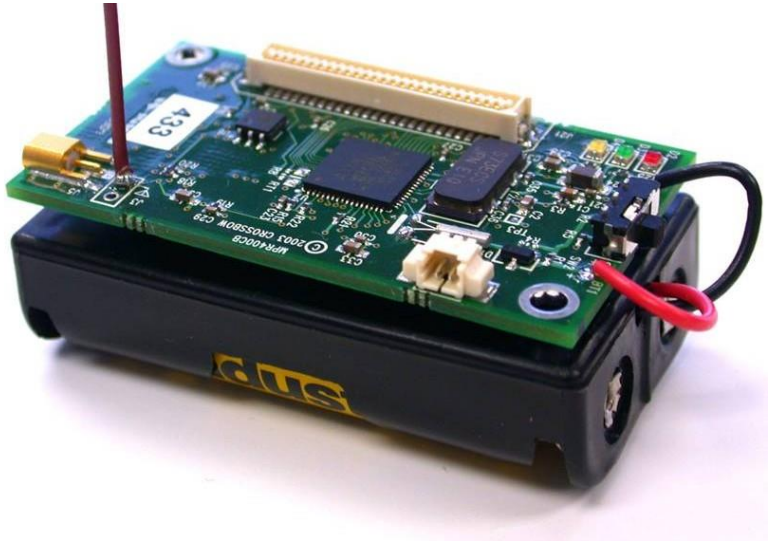
By Chris Karlof and David Wagner

Lukas Wirne – Anton Widera – 23.11.2017

Table of content

Background

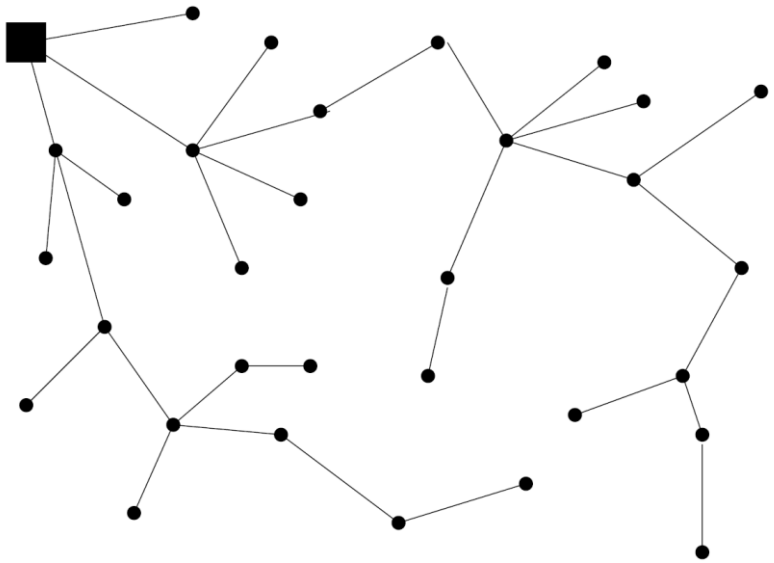
- Wireless sensor networks are everywhere
- Spread out over an area
- Sensors have only small capacities
  - Mica mote:
    - 4MHz 8 Bit Processor
    - 4KB of RAM
    - 512KB of flash memory
    - Radio that reached few dozen meters
    - Two AA Batteries around 2850mA
    - Running only two weeks on full power



Source: http://www.eecs.harvard.edu/~konrad/projects/motetrack/mica2.jpg

Background

- Nodes have Base Station
  - Accessible to human
  - Powerful center with power access
  - Extracting data from network or broadcasting it
- Multi-hop network to base station
  - Aggregation Nodes
  - Summarize Data and forward it
  - Assignment random and dynamic



Sensor networks vs. Ad-hoc wireless networks

- Ad-hoc Networks can route between any pair or nodes
- Wireless Sensor Network traffic:
  - May to one: all Nodes report to base station
  - One to many: base station broadcasts to all nodes
  - Neighboring nodes send data to each other
- Nodes in WSN are not moving
- Ad-hoc Networks have 2-3 order of magnitude more power and rechargeable big battery

-> Security Protocols for Ad-hoc networks cant be used on WSN

Security in Wireless Sensor Networks

- Security is important, but security overhead is expensive
- Transmitting one Bit = 800 instructions of power
- In TinyOS packet overhead is only 4 bytes
- Asymmetric encryption has to be ruled out due to restricted components
- Symmetric encryption should be used sparsely

Problem Statement

- Network Assumption:
  - Radio links are insecure
    - Eavesdrop conversation possible
    - Injecting bits in the channel possible
    - Replay previous heard packets possible
  - Attacker has control over more than one node
    - Either purchasing them separate or hijacking friendly nodes
  - If node highjacked then all keys and data can be extracted from it
- Trust Requirement:
  - Base stations are trustworthy
  - Aggregation points may be trusted components on some protocols

Problem Statement – Threat Models

- Mote class attack:
  - Attacker has only access to few sensor nodes with similar capabilities
- Laptop Class attack:
  - Attacker has access to more powerful devices like laptops
  - Might be able to eavesdrop on entire network or jam it due to good antennas

- Outside Attack:
  - Attacker has no special access to the network
- Insider Attack:
  - Authorized participant gone bad
  - Either malicious nodes running bad code or new nodes stolen code

Problem Statement – Security Goals

- Traditional Security Goals:
  - Integrity of message,
  - Authentication and
  - Availability of message delivery

- Eavesdropping should not be cared about on routing level, but on application layer
- Same with replay of packets

- Hard to obtain these goals again Laptop Class Attacks

Attack on sensors

- 1. Spoofed, altered, or replayed routing information
- 2. Selective forwarding
- 3. Sinkhole attacks
- 4. Sybil attacks
- 5. Wormholes
- 6. HELLO flood attacks
- 7. Acknowledgement spoofing

Spoofed, Altered, or Replayed Routing Information

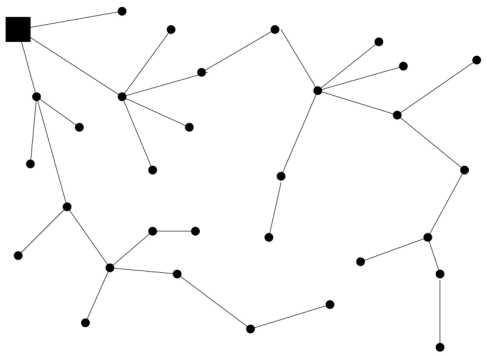
- Most direct Attack
- By Spoofing, Altering and Replaying Information attacker can:
  - Create routing loops
  - Affect or repel network traffic
  - Alter source routes
  - Generate false error messages
  - Partition the network
  - Increase end to end latency
- Included in most Attacks

Selective Forwarding

- Malicious nodes drops traffic and doesn’t forward it
- Black hole behavior(dropping all packets)
  - But detection is simple and other route selected by neighbors

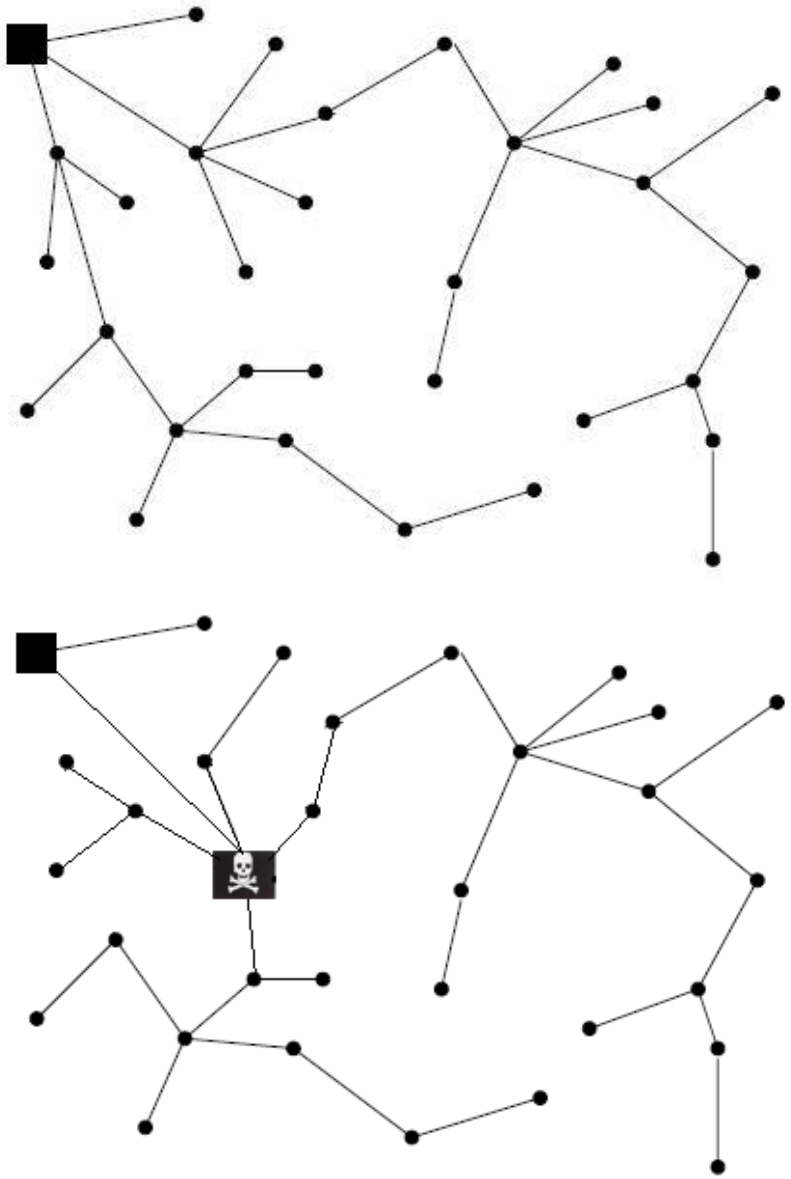
-> Only forward selected ones

- But only effective if malicious node is on a data flow route
  - Combined with many attacks



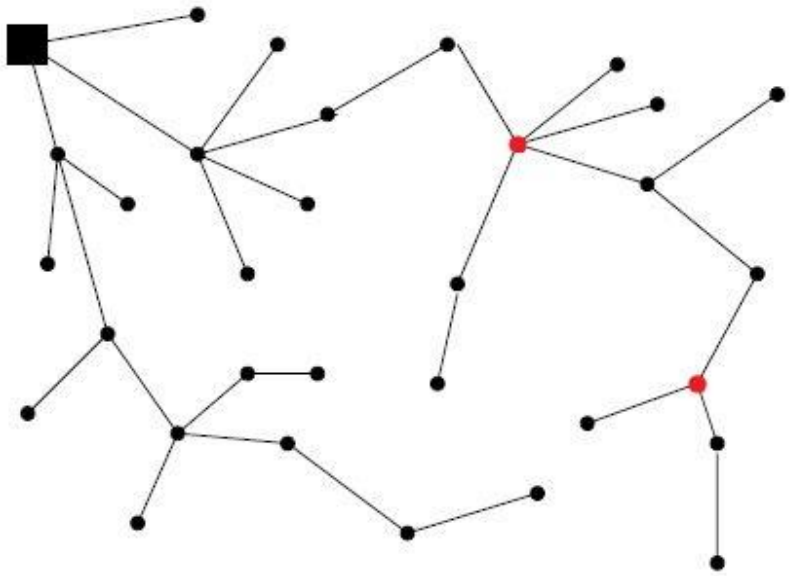
Sinkhole attacks

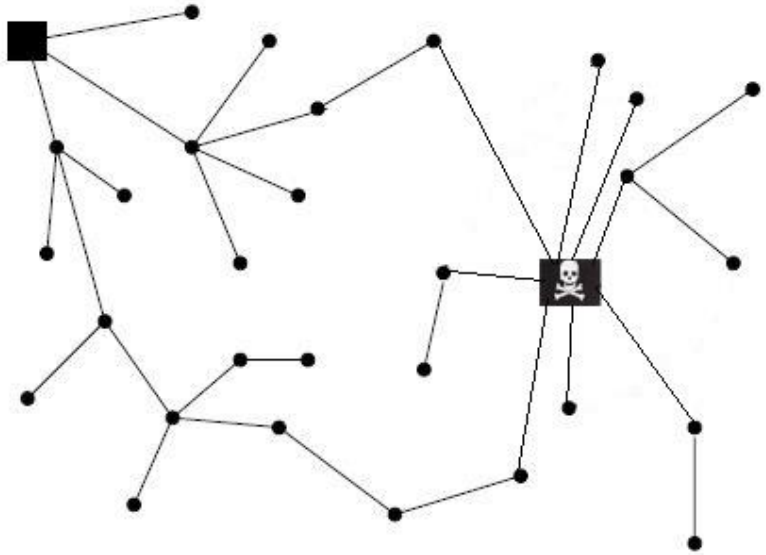
- Lure the traffic through compromised node by looking more attractive
- Can influence the route for nodes several hops away by amplified signal
  - Works against ack-based protocols
- Controls the flow of data
  - Selective forwarding
- Change message information



The sybil attacks

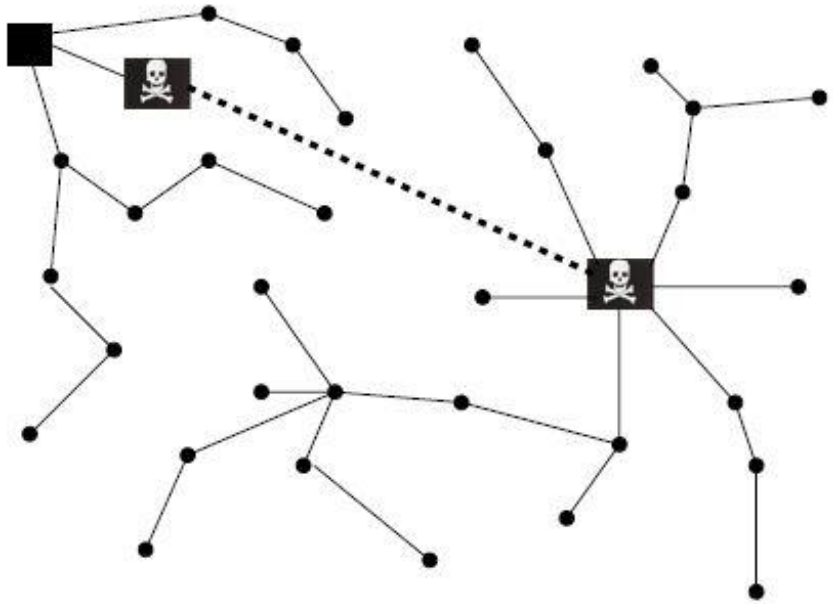
- A single node presents multiple identities to other nodes in the network
- Threatening to fault-tolerant schemes
  - Distributed storage
  - Dispersity and multipath routing
  - Topology maintenance





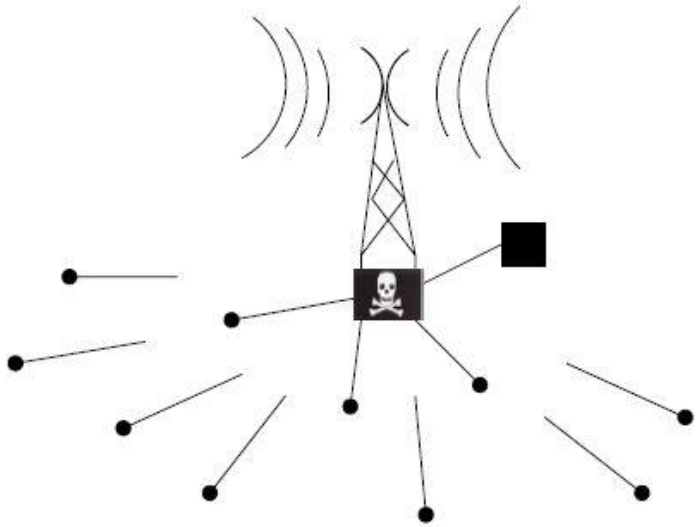
Wormholes

- "Tunnels" messages over a low latency link to other parts of the network
  - Tunnel only available to the attacker
- Usually two distant nodes working together
- Well-placed wormhole could create sinkhole
  - Neighbors tells about the good route to other nodes in the system



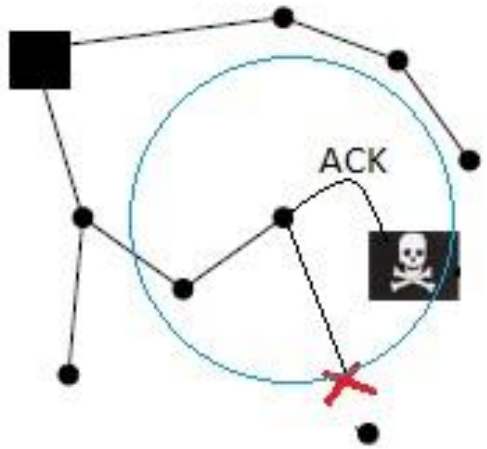
Hello flood attacks

- Some protocols uses broadcast HELLO packets to announce themselves to their neighbors
- Attacker broadcasts HELLO packets with strong signal
- Neighbors may assume that the sender is in range
  - Adjusts route to compromised node, results in lost packages



Acknowledgement spoofing

- Several sensor network routing algorithms rely on link layer acknowledgements
- Compromised node can spoof acks from dead/disabled node
- Sending node continue sending to that
- Dead/disabled node/route



Attacks on specific sensor network protocols

TinyOS beaconing

- Lightweight, event-driven operating system
  - TinyOS is under development at UC Berkeley
  - Routing mechanism widely used in research and experimental platform
- Base station is the final destination of all data packets
  - All packets received or generated by a node are forwarded to its parent
- Routing mechanism works by constructing a breadth first spanning tree rooted at the base station
- No scheme for query dissemination
  - Flooded, no query, constant send rate, or only when they occur(rare)

TinyOS attacks

- Routing updates are not authenticated
  - Anyone can claim to be the base station
- Fragile to attacks
  - Combined wormhole/sinkhole attack
  - HELLO floods
  - Infinite loop attack

Directed diffusion

- Data-centric communication paradigm
  - drawing information out of a sensor network
- Interest Broadcast
  - Base stations flood interests for named data
  - They set up gradients within the network designed to draw events
  - Nodes satisfy the interest by broadcasting information along the reverse path of interest flow
- Multipath variant of directed diffusion is proposed

Directed diffusion attack

Suppression

- Spoof negative reinforcements to suppress a flow

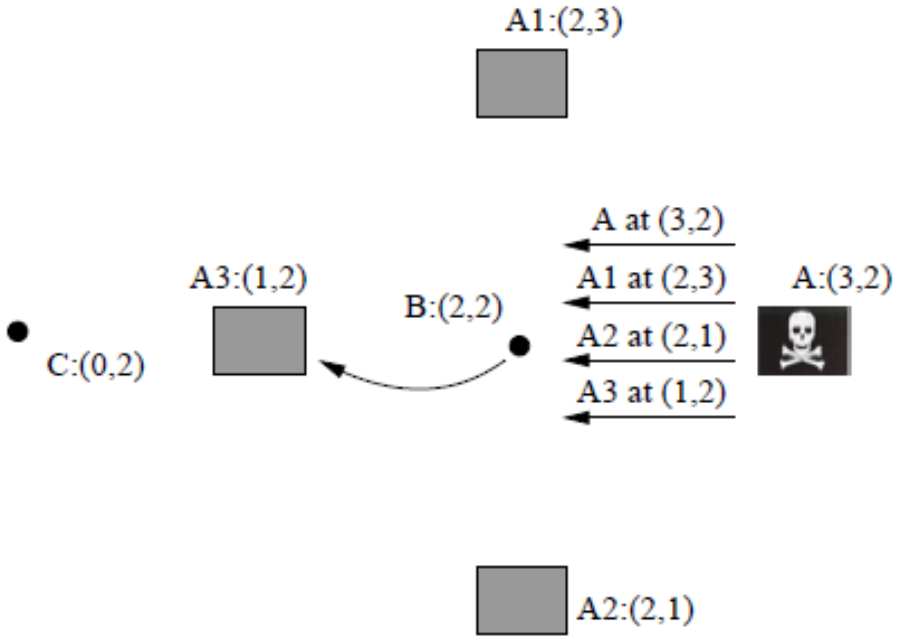
- Cloning
  - Clone an interest and replay it as the base station
- Path Influence
  - Can influence by spoofing reinforcements and bogus data
- Selective Forwarding and Data Tampering
  - Using above attack, an adversary can be in the path
    - Can modify, selectively forward packets
- Wormhole attack
  - Spoofing reinforcements to make the data flow through the wormhole
- Sybil attack
  - Reinforce to the adversary

Geographic routing

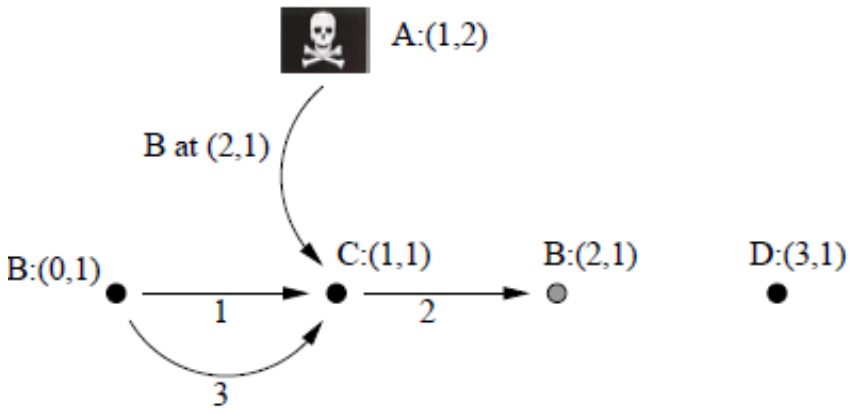
- Greedy Perimeter Stateless Routing (GPSR)
  - Greedy forwarding, but recovers if a hole is found and goes around it
  - Need distance information between nodes
  - Drawback: Unevenly power consumption
- Geographic and Energy Aware Routing (GEAR)
  - Greedy forwarding calculated on distance + power information
  - Need distance information between nodes and power information

Geographic routing attack

- Compromised node can advertise wrong location/remaining power
  - More success with combining with sybil Attack, preferable circle or sphere



- Compromised node creates routing loop between C and B



Countermeasures

Outsider attacks and link layer security

- Link layer encryption and authentication with globally shared key
  - Lets every node authenticate messages
  - Prevents adversaries from spoofing or altering routing and data packets
- Prevent replay of packets with counter
  - Nodes remember most recently increased counter and discards old packages

- Prevents from most attacks, but not all. Secure against:
  - Sybil attacks
  - Selective forwarding
  - Sinkhole attacks

Insider attacks

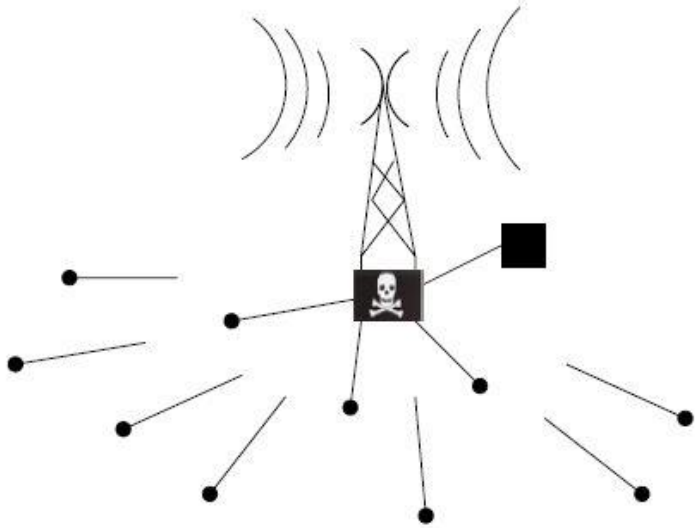
- Globally shared key are completely ineffective against insider attacks
  - Compromised node has the shared key and can change data and routing information, take identitys of nodes, or create new identities
- Public key cryptography is a solution, but:
  - generating and verifying digital signatures is beyond the capabilities of sensor nodes

Prevent Sybil insider attacks

- Every node share a unique symmetric key with a trusted base station
  - Two nodes can then use a Needham-Schroeder like protocol to verify other's identity and establish a shared key
- Prevent compromised node from creating shared keys with everyone
  - Base station can limit the number of neighbors a node is allowed to have and send an error message when a node exceeds it
- Compromised node is left communicating only with its neighbors

Prevent HELLO floods insider attacks

- Verify the bidirectionality of a link
  - Good defence combined with unique symmetric key



Wormhole and Sinkhole insider attacks

- Wormhole and sinkhole attacks are very difficult to defend against
- Best solution is to carefully design routing protocols in which wormholes and sinkholes are meaningless
- One class of protocols resistant to these attacks are geographic routing protocols
- Artificial linksare easily detected in geographic routing protocols because the “neighboring” nodes will notice the distance between them is well beyond normal radio range

Leveraging global knowledge

- Nodes sends information about neighbor/geographic location to base station. Base station can then calculate the topology of the network
  - Base station locates wormholes
  - Harder with big networks
- A compromised node with location between the targeted node and a base station will guarantee it's the destination for all forwarded packets from that node
  - Multipath routing can help with this problem with topology in mind
    - When a node must route around a“hole”, an adversary can “help” by appearing to be the only reasonable node to forward packets to. Solution, more multipathing?

Conclusion

- Secure routing is vital
- Demonstrated that currently proposed routing protocols for these networks are insecure
- Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against moteclass Outsiders
- Cryptography is not enough to defend against laptop-class adversaries and insiders: careful protocol design is needed as well.

Questions?