# Secure Routing in wireless sensor networks: attacks and countermeasures

Chris Karlof and David Wagner
University of California at Berkeley
1st IEEE International Workshop on Sensor Network Protocols and Applications, 2003

Patrick Emaase

# Contents

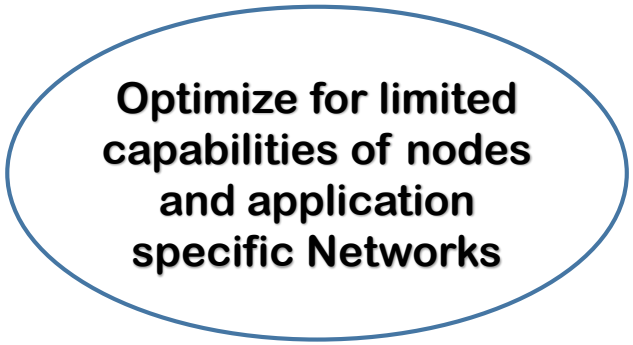
- Focus of the Paper
- Introduction: wireless sensor network; Background
- Comparison of SNs and Ad-Hoc Networks
- Related Work
- Problem statement
- Attacks on sensor network routing
- Attacks on specific sensor network protocols
- Countermeasures
- Conclusion

# Focus of the Paper

- Paper proposes security goals for routing in sensor networks as a design goal from start by:
  - Adapt attack against ad-hoc and peer-to-peer to Powerful attack against sensor network
- Analyze sinkholes and `HELLO` floods for attacks

# Introduction

- Current proposal vs Future or real life





- Contributions of the paper
  - Threat models and security goals for WSN routing
  - Two novel classes of attacks – sinkhole & `HELLO` floods
  - Adapt ad-hoc wireless and P2P networks attacks to sensor security goals
  - Analysis of major routing protocols and energy conserving topology maintenance algorithms for sensor networks
  - Counter-measures and design considerations

# Background

- SNs: Heterogeneous system, combines tiny sensors and actuators
  - Consists many low power low cost, fixed sensors
  - Deployed en masse – monitor and affect environment
- Have Base station (sinks) - Central control, gateway to data processing, storage
  - Steady stream of data to satisfy query (data flow) and sending nodes (sources)
- Aggregation Points – process data, reduce # of messages, sensors
  - Chosen dynamically, management of incoming and outgoing messages
- Restricted resources: Power management, bandwidth, computation
  - Security challenge, public key cryptography expensive, symmetric ciphers sparingly

# Sensor Node Specification

<Mica mote>

| Component | Spec |
|---|---|
| Processor | 4 MHz 8-bit CPU |
| OS | TinyOS |
| RAM | 4 KB |
| Storage | 512 KB flash memory |
| Radio | 916 MHz, 40Kbps<br>Range of a few dozen meters |
| Power supply | AA battery |
| Sensors | Optional |

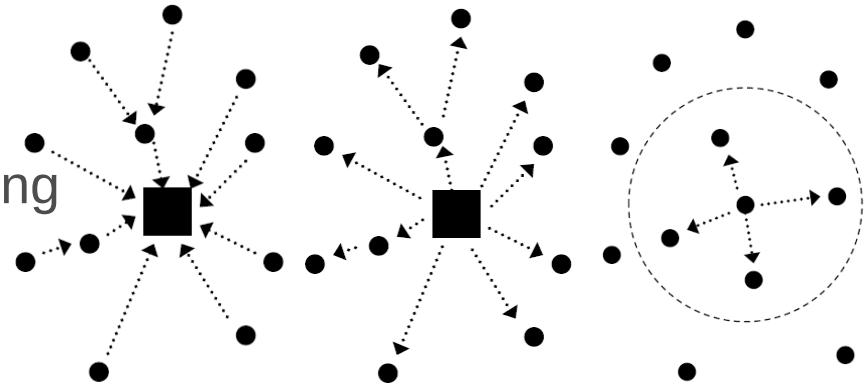
| CPU | Consumption |
|---|---|
| Active | 5.5 mA |
| Sleep | 100 magnitude less power |

| Radio | Consumption |
|---|---|
| Receiving | 4.8 mA |
| Transmit | 12 mA |
| Sleep | 5 μA |

**Optimal sensor: temperature sensor, magnetometer, accelerometer, Microphone, sounder**

<Power consumption>

# SN vs. Ad-hoc Wireless Networks



- Similarity
  - Both Support Multi-hop networking
- Differences
  - Sensor : Supports Specialized communication patterns
    - Many-to-One – multiple sensors to base station or APs
    - One-to-Many – base station to several sensors
    - Local Communication – discover and coordinate with others
  - Sensor nodes more resource constrained than Ad-hoc nodes
    - Public key cryptography not feasible
  - Higher level of trust relationship among SN than ad-hoc
  - SN: Reduce traffic & save energy - in-network processing, aggregation, duplicate elimination

# Related work

- The security issues in ad-hoc networks are similar to those in sensor networks [Zhou & Hass, ‘99; Habaux et al. ‘01; Kong et al. ’01; Zapata, ‘01; Luo, et al. ‘02; Binkley ‘01]
  - Defense mechanisms developed for ad-hoc networks are not directly applicable to sensor networks
- Ad-hoc Network secure routing based on symmetric key encryption was proposed, [Marti et al. 2000] but:
  - Unstable for SNs; Expensive - node state and packet overhead
  - Designed to find & est. routes betw. nodes but not used in SNs

# Related work

- Problem minimizing effects of misbehaving nodes by punishment, reporting and holding grudges [Marti et al. & Buchegger & Boudec]
  - Promising in SNs but vulnerable to blackmailers
- Two building blocks for security protocols optimized for sensor networks
  - μTESLA (provides authentication for data broadcast) and
  - SNEP (provides data confidentiality, two party data authentication, integrity and freshness between nodes and the sink)

# Problem Statement

- Network Assumptions
  - Radio links are insecure
    - Attackers can eavedrio Radio transmission, inject bit in the channel, replay previous packets
  - Adversary can deploy malicious nodes with similar capabilities as the legitimate nodes
  - Attackers have control of more than one node
    - Nodes may collude
  - None tamper proof System
    - Adversary can extract all key materials, data and code on the node

# Problem Statement

- Trust Requirements
  - Compromise of base stations renders network useless
  - Base stations are trustworthy: trusted and correct
  - Nodes (trusted) and Aggregation Points (trustworthy)
    - Aggregation points may become compromised
  - None tamper proof
    - Adversary can access all key, data, code

# Problem Statement

- Threat Model
  - Based on device capability
    - Mote-class attacker – Access few nodes, limited damage
    - Laptop-class – Access powerful devices - advantage,
      - More battery power, better CPU, sensitive antenna, powerful radio transmitters
  - Based on attacker type/location
    - Outside attacks – External to network
      - Conceivable to achieve ideal goals
    - Inside attacks – authorized, access network
      - Goals are not fully achieved -> Hope for Graceful degradation; Degrade no faster than rate $\alpha$ (compromised : total nodes)

# Problem Statement

- Security Goals
  - Integrity, authenticity and confidentiality – Ideal world
    - Guaranteed by Data link layer protocols
  - Availability - rely on routing protocol
  - Application layer: replay attack protection

# Attack Model

- Spoofed, altered, or replayed routing information
- Selective forwarding
- Sinkhole attacks
- Sybil attacks
- Wormholes attacks
- `HELLO` flood attacks
- Acknowledgement spoofing

- Motivation of attack:
  - Access information by intercepting the data flows
  - Disrupt or completely halt the functionality of the sensor network

# Attack Model

- Spoofed, altered or replayed routing information
  - May be used for loop construction, attracting or repelling traffic, extend or shorten source route
  - Goal: Generate false error messages, partitioning the network, increase end to end latency

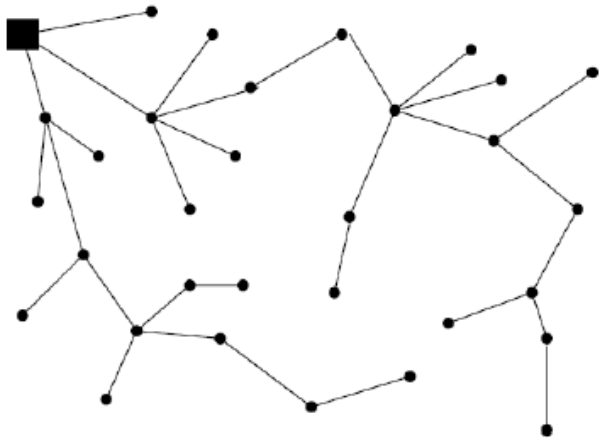
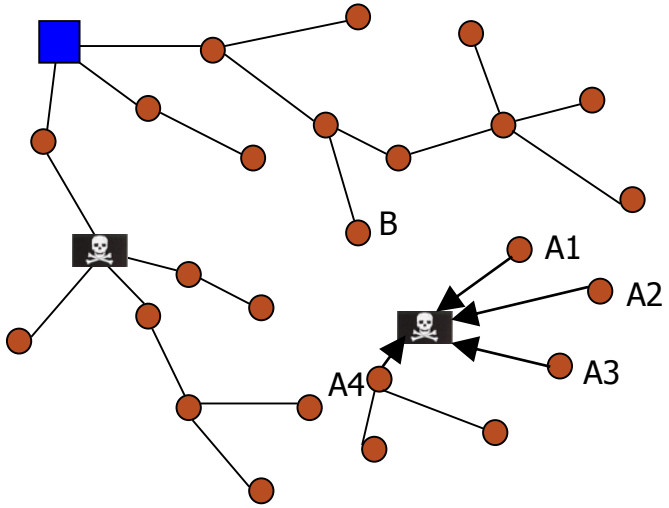
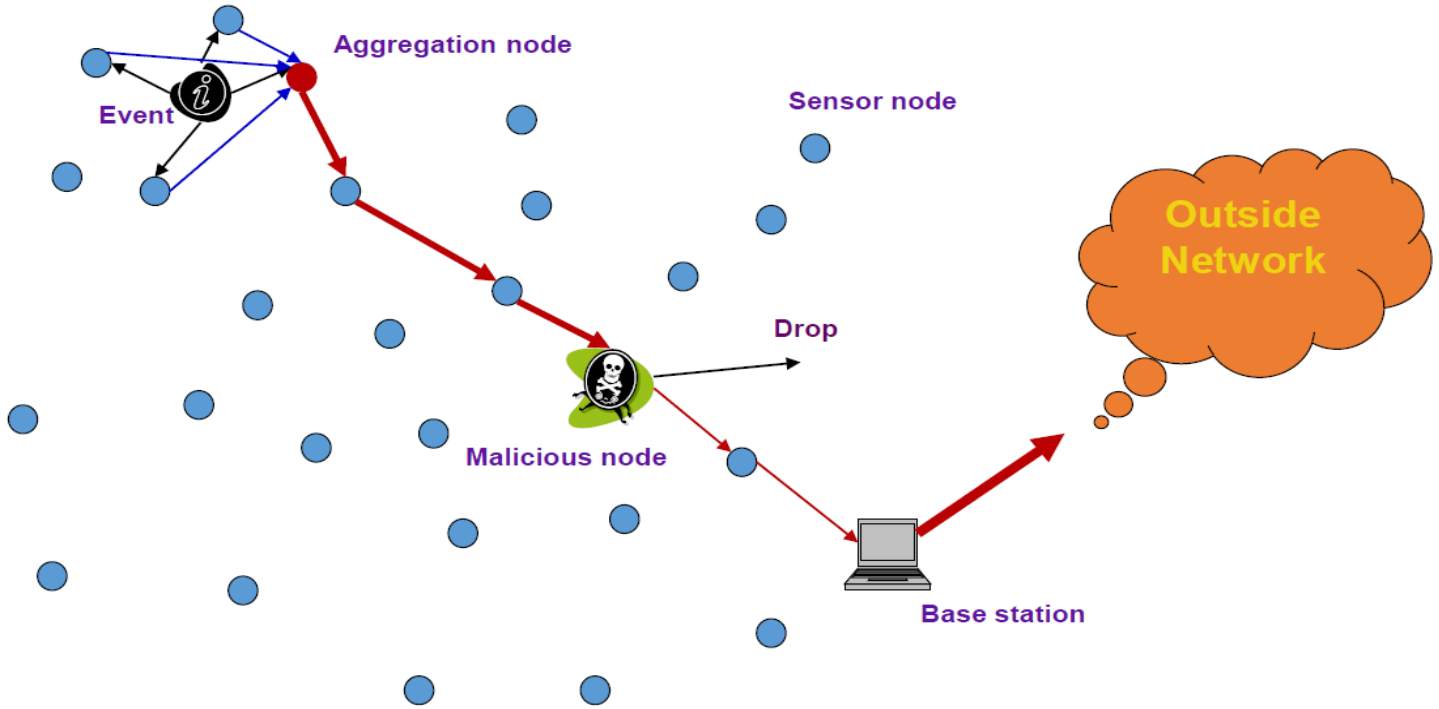


Fig. 4. A representative topology constructed using TinyOS beaconing with a single base station.



# Attack Model

- Selective forwarding
  - A malicious node behaves like a black hole
  - Refuse to forward certain messengers, selective forwarding packets or simply drop them
- Goal: Attempts to include itself on the actual data flow path

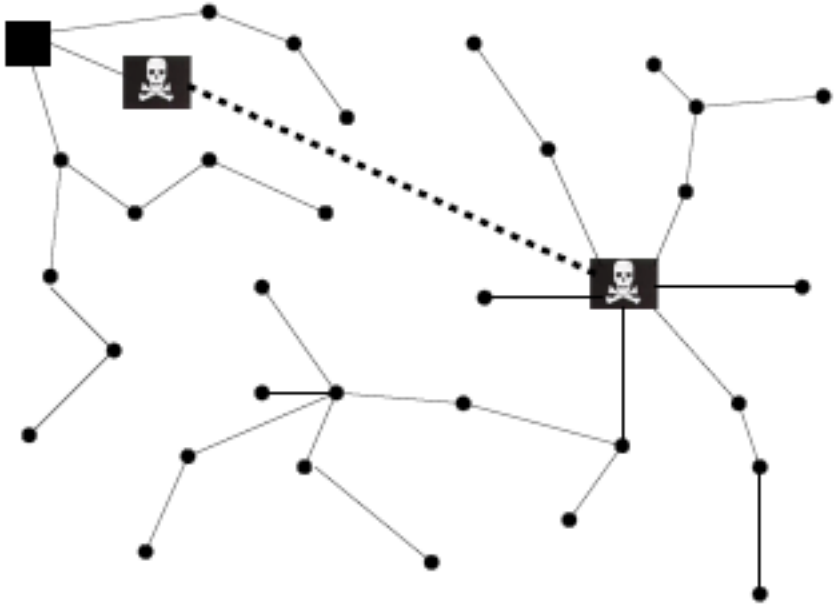


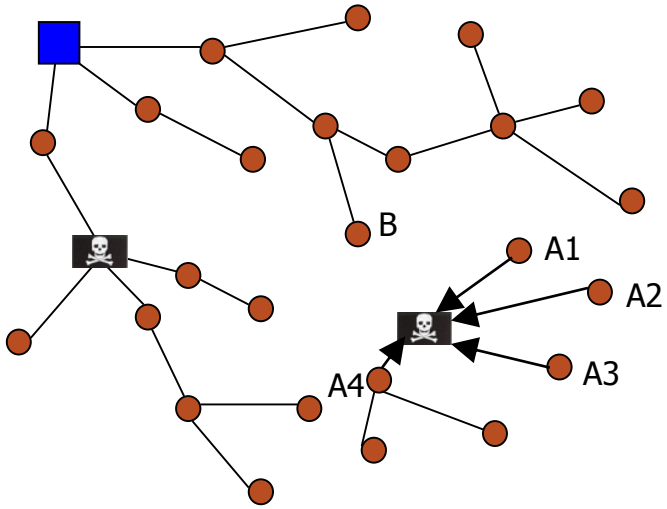
# Attack Model

- Sinkhole attacks
  - Attacker creates metaphorical sinkhole

by advertising for example high quality route to a base station

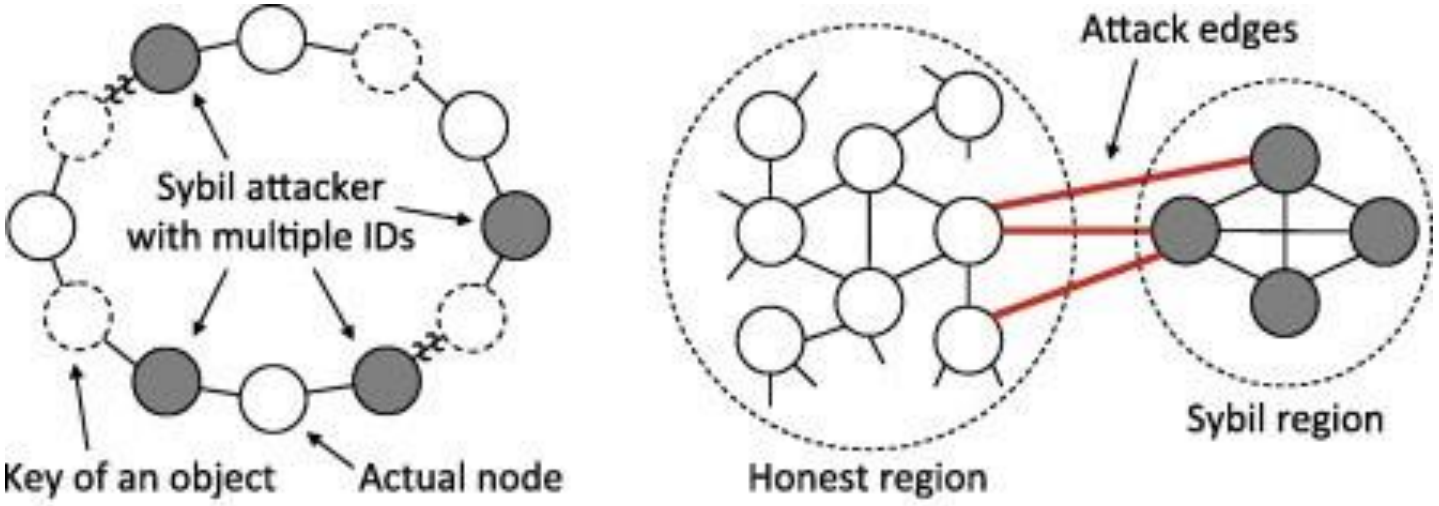
    - Almost all traffic is directed to the fake sinkhole,





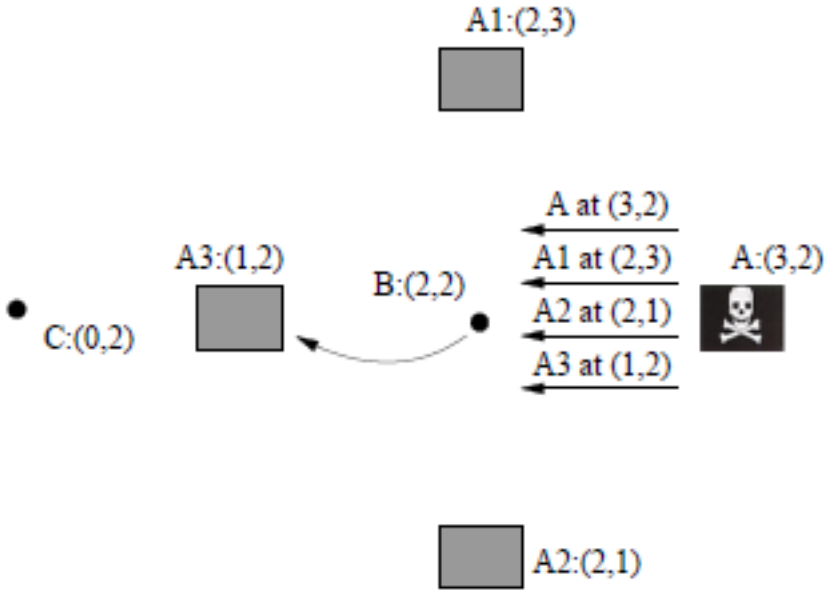
# Attack Model

- The Sybil Attack
  - Forging of multiple identities - having a set of faulty entities represented through a larger set of identities. Falsification
  - Significant threat to location aware routing protocols
    - An adversary node can be in more than one place at once



# Attack Model

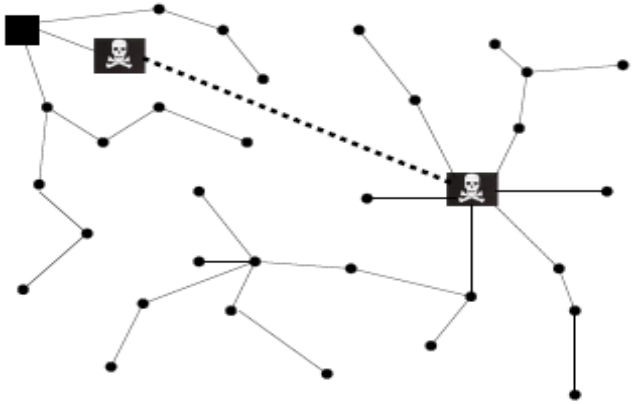
- The Sybil Attack
  - Single node presents multiple identities to others in network
- Goal:
  - Reduce effectiveness of fault tolerant schemes

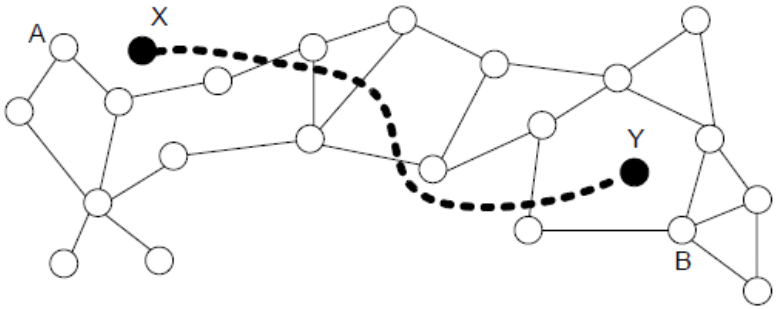



- The Sybil attack
  - Adversary at A at actual location (3,2) forges location advertisements for non-existent nodes A1, A2, and A3 as well as advertising her own location
  - After hearing these advertisements, if B wants to send a message to destination (0,2), it will attempt to do so through A3.
  - This transmission can be overhead and handled by adversary A

# Attack Model

- Wormholes
  - Tunneling of messages over alternative low-latency links,
  - e.g. confuse the routing protocol, create sinkholes.
- Goals
  - Completely disrupt routing if adversary is close to base station
  - Enable sinkhole attack – “providing high quality route to BS”
  - Traffic drawn through wormholes
  - Exploits routing race condition – convinces distant nodes they are neighbours

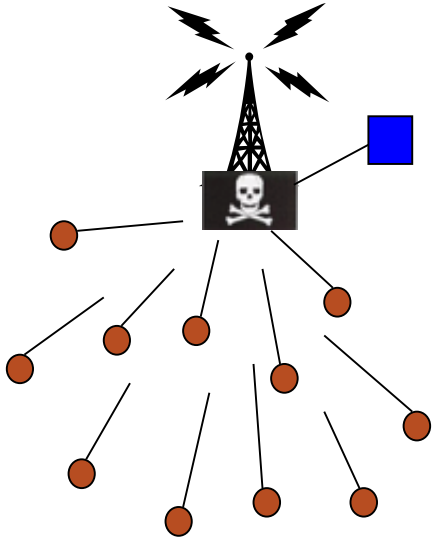




# Attack Model

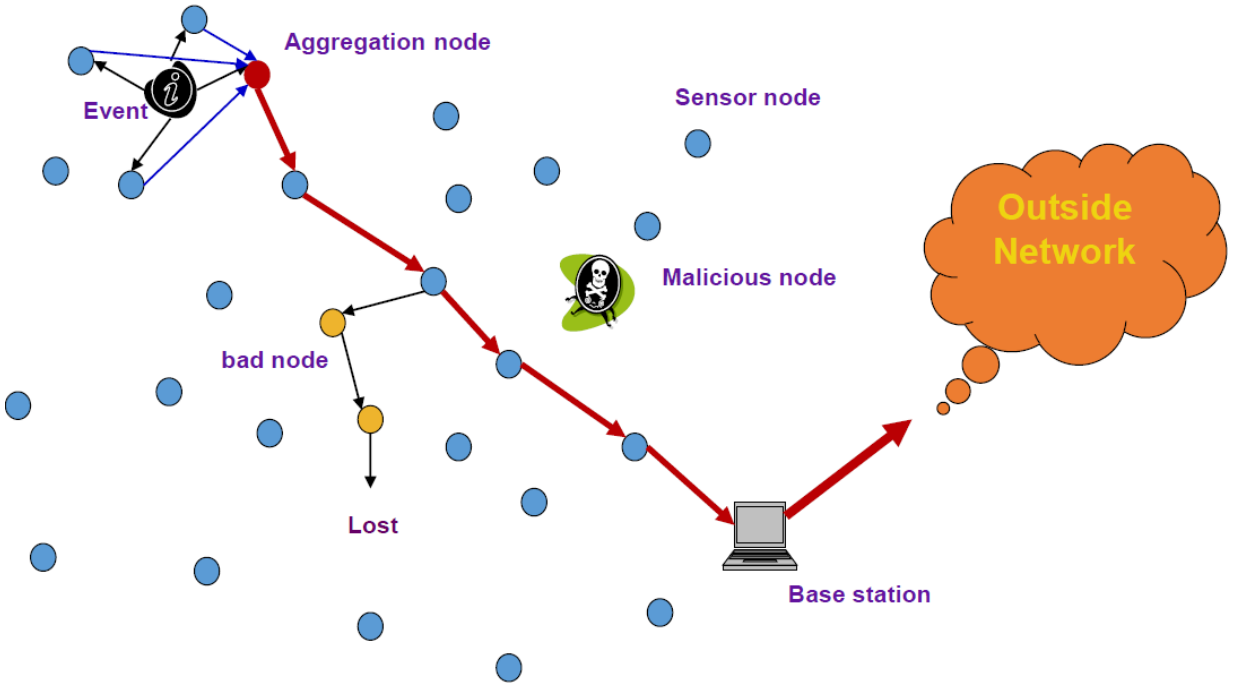
- HELLO flood attack
  - An attacker sends or replays a routing protocol's HELLO packets with more energy able to convince every node in the network that adversary is a good neighbor
  - Goal
    - Enable wormhole attack by broadcasting wormholes
    - Flood the network,

- Adversary re-transmits routing update with power to be received by all nodes
  - Leaves nodes stranded



# Attack Model

- Acknowledgement spoofing
  - Adversary can spoof link layer acknowledgement for “overheard” packets addressed to the nearby nodes
  - Goal: Convince sender weak link is strong or dead/disabled node is alive



# Summary: Attacks on SN Routing

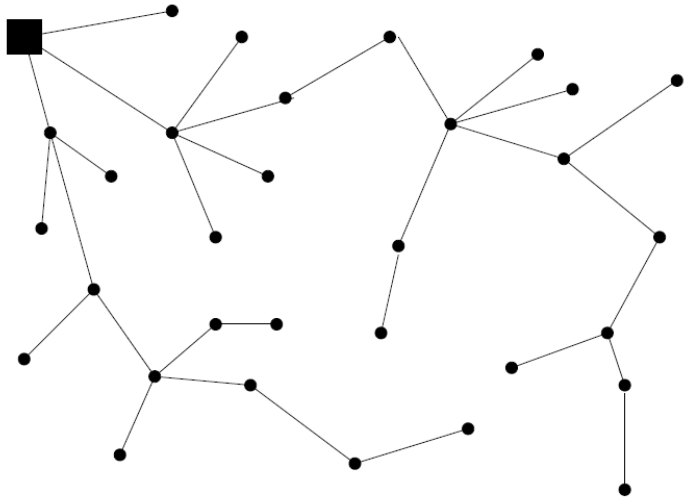
| Attack Category | Attack type | Characteristics |
|---|---|---|
| Spoofed, altered, or relayed routing info | Affects routing topology | Create routing loops, attract, or repel network traffic; extend/shorten source routes, generate false messages, partition network, increase latency |
| Selective attacks | Manipulate user data directly | Malicious nodes refuse to forward some messages or drop them; selectively forwards packets; |
| Sinkhole attacks | Affects routing topology | Lures all traffic from particular area (attractive) to a compromised node, creating ‘sinkhole’ with adversary at the center, most susceptible; |
| Sybil attacks | Manipulate user data directly | Node presents multiple identities to other nodes (forging identity), wrongly exchanging coordinates |
| Wormholes | Affects routing topology | Malicious nodes collude to understate their distance relay packets along out of bound channel |
| HELLO flood attack | Affects routing topology | Adversary pretends good near neighbor, receiving HELLO broadcasts – sent to oblivion; rebroadcast flooding network |
| Acknowledgement spoofing | Affects routing topology | Adversary spoof link layer acknowledgement for “overheard” packets; convinces sender weak link is strong or dead/disabled node is alive |

# Attacks on specific protocols

- TinyOS beaconing
- Directed Diffusion
- Geographic routing
- Additional routing Protocols
  - Minimum Cost forwarding
  - LEACH – Low Energy Adaptive Clustering Hierarchy
  - Rumor routing
  - Energy Conserving Topology Maintenance [GAF, SPAN]

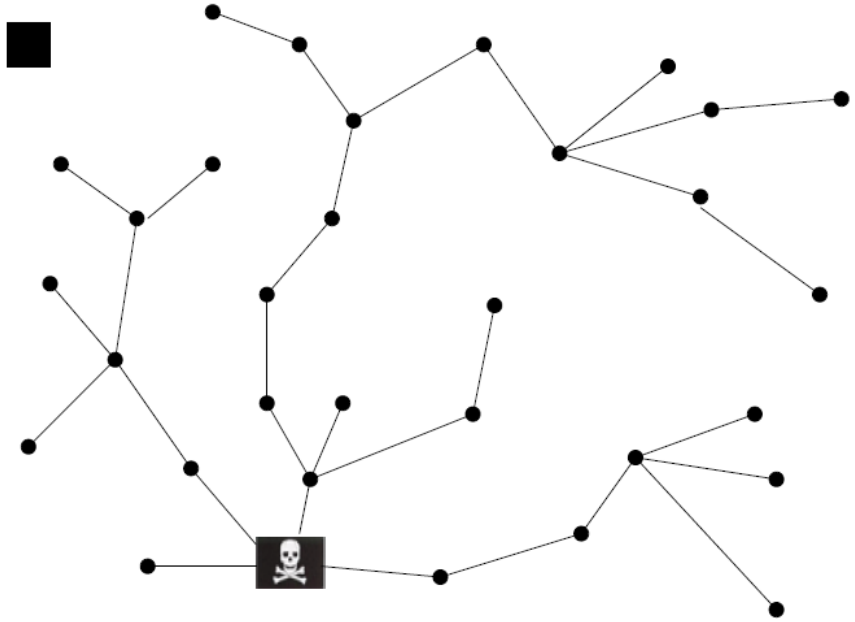
# Tiny OS Beaconing (1/4)

- TinyOS beaconing
  - Constructs a Breadth First Spanning Tree rooted at base station
  - Base station broadcast Route update (beacon) periodically, Nodes receive the update, mark the base station as parent and broadcast it
  - Routing updates are not authenticated



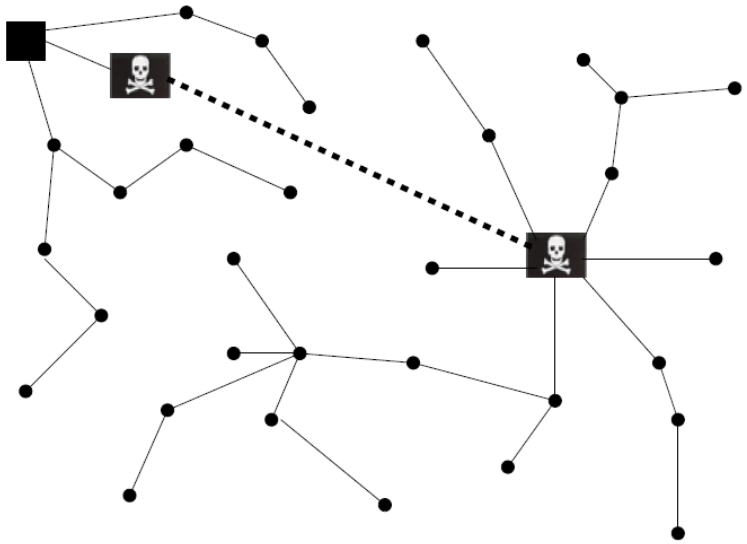
# Tiny OS Beaconing (2/4)

- Spoofing a routing update
  - Spoof – a trick or hoax on routing cost and efficiency
  - Bogus and replayed routing information (such like “I am station”) send by an adversary can easily pollute the entire network
  - Routing loops can easily be created by mote-class adversaries



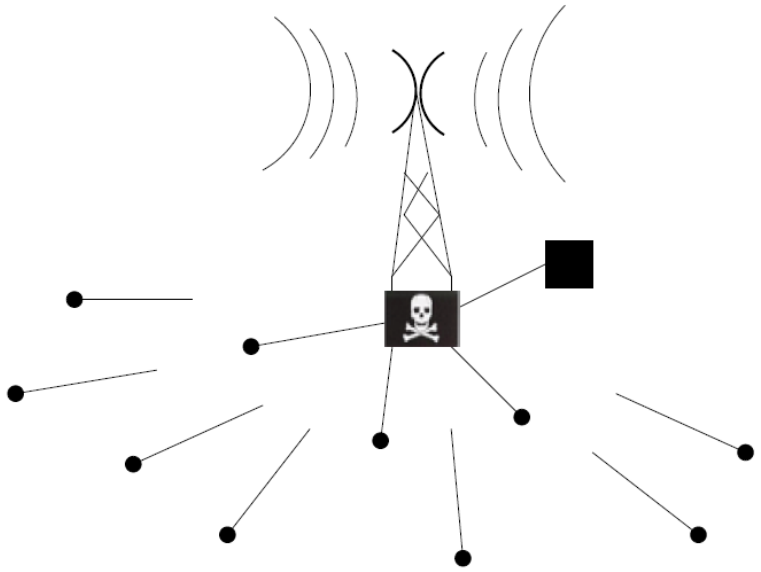
# Tiny OS Beaconing (3/4)

- Wormhole / Sinkhole attack
  - Two colluding powerful laptop-class nodes, one near the base station and one near the targeted area
  - The first node forwards routing updates through wormhole
  - The second node create sinkhole by rebroadcasting the routing update in the targeted area
    - Combination



# Tiny OS Beaconing (4/4)

- HELLO Flood Attack
  - Broadcast a routing update loud enough to reach the entire network by using a powerful transmitter
  - Every node marks the adversary as its parent
  - Most nodes will be likely out of normal radio range. Why?



**Comment**

**Protocol simple – Recovery is difficult**

**Creates a defective flood of packets**

# Directed Diffusion

- Directed diffusion
  - A data-centric routing algorithm for extracts data from SNs
  - BS flood interests for named data setting up gradients in network
  - Interest distribution:
    - Interests are injected into the network from base station
    - Interval specifies an event data rate
    - Interest entry also maintains gradients
    - Data flows from the source to the sink along the gradient
  - Data Propagation and reinforcement
    - Reinforcement to single path delivery
    - Multipath delivery with selective quality along different paths

# Directed Diffusion

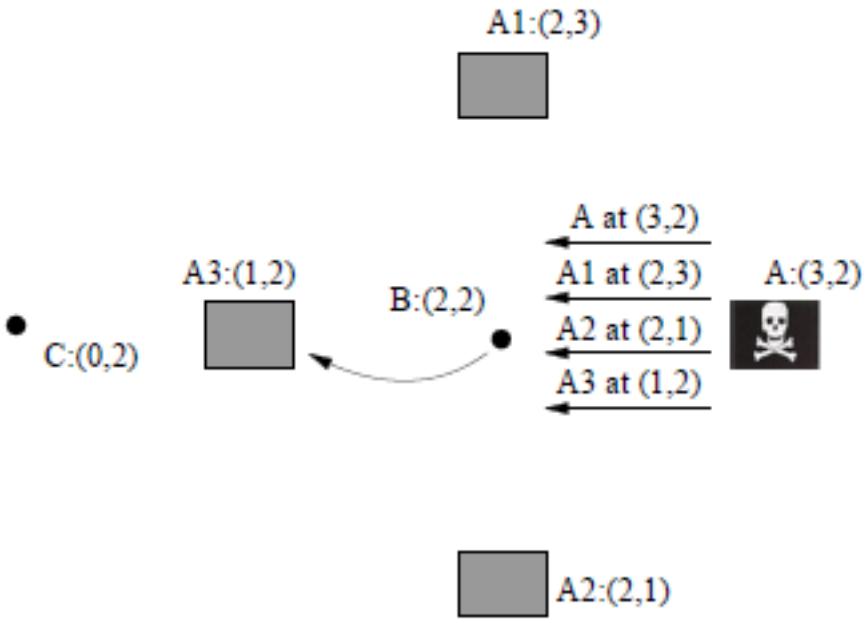
- Directed diffusion Attacks
  - Suppression – Instance of denial of service (DoS)
    - Example: spoof negative reinforcement
  - Cloning – Enables eavesdropping
    - Adversary replay interest with herself as listed in BS
    - Matching interests sent to adversary and legitimate BS
  - Path Influence – Adversary influence path by spoofing positive and negative reinforcement and bogus data events; causes:
    - Data drawn thro adversary due strong positive reinforcement
    - Alternate event flow negatively reinforced
    - Adversary node will be positively reinforced
  - Selective forwarding and data tampering – inserts herself onto data flow path, taking control of the flow

# Geographic routing

- Protocols Used – Leverage nodes' positions and explicit geographic packet end – send queries & route replies
  - GPSR (Greedy Perimeter Stateless Routing)
    - Greedy forwards each hop, routes packet to neighbor closest to the destination.
      - Packets use the same nodes for routing – uneven energy consumption
  - GEAR (Geographic and Energy Aware Routing)
    - Weighs choice of next hop by remaining energy & distance from target
      - Routing flow evenly distributed

# Attacks on Geographic Routing protocols

- The Sybil Attack
  - Surrounding each target using non-existent nodes. Adversary maximizes chances for placing herself on the path of data flow
  - Goal: Circumvent GEAR protocol and attack



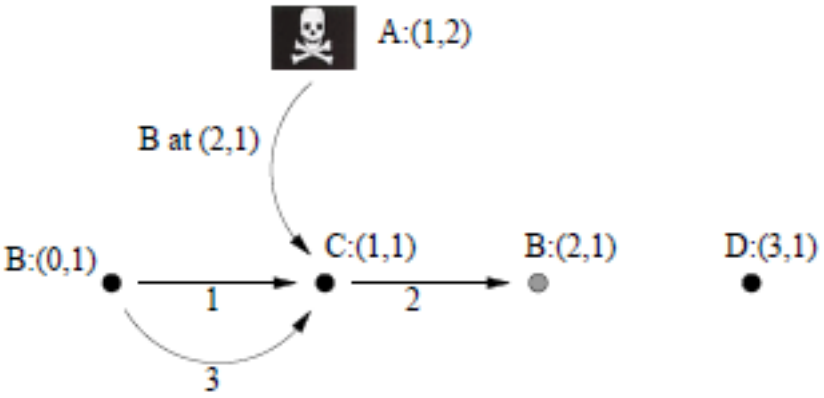

Adversary A at location (3,2) forges location advertisement for non-existent nodes A1, A2, A3 and its own location;

Hears B's intention to send message to C (0,2), will attempt to do so using A3(1,2).

Transmission is overheard and handled by adversary A.

# Attacks on Geographic Routing protocols

- Creating routing loops in GPSR
  - Advertise her location in a way to place herself on the path of a known flow; Forge other node's location to create routing loops
  - Goal: Circumvent GPSR protocol




By forging a location advertisement claiming B is at (2,1), an adversary can create a routing loop.

B forward packets destined for D (3,1) to C, will send back to B since it believes B is closer, creating a loop forever

# Additional routing Protocols

- Minimum Cost forwarding
- LEACH – Low Energy Adaptive Clustering Hierarchy
- Rumor routing
- Energy Conserving Topology Maintenance [GAF, SPAN]

# Countermeasures

- Outsider attacks and Link layer security
  - Authentication and encryption
    - Prevents the majority of outsider attacks
      - Prevents joining the network
      - False routing information, selective forwarding, sinkhole attacks, sybil attacks, ACK spoofing
    - Can’t prevent tunnel packets sent by legitimate nodes or by amplifying an overheard broadcast packets
      - Wormhole attacks, `HELLO` flood attacks
    - More sophisticated mechanism provide protection against wormholes and insider attacks

# Countermeasures

- The Sybil attack
  - Insiders participate in network using compromised nodes IDs
  - Verification of insiders identities done using Public key cryptography may prevent insiders attacks
    - but this is beyond the capabilities of sensor nodes
  - Share a unique symmetric key with a trusted base station
    - Two nodes verify each other by using some protocol (e.g Needham –Schroeder) and establish a shared key
    - Using that key, pair of noes can implement authenticated and encrypted link between them
    - Base station reasonably limit the number of allowed neighbors
  - Restricted communication
    - Compromised nodes to communicate only with verified neighbors

# Countermeasures

- HELLO flood attacks
  - Verify the bidirectionality of a link before taking meaningful action
    - Verify identities
  - Trusted base station limits number of verified neighbors
- Wormhole and Sinkhole attacks
  - Wormholes hard to detecting; Sinkholes difficult to defend in protocols that use advertised information
  - Best solution is to carefully design routing protocols
  - Geographic routing protocol: can be used as a countermeasure
    - Resistant to wormhole and sinkhole attacks
    - Topology constructed on demand using localized interaction without initiation
    - Difficult to create

# Countermeasures

- Leveraging global knowledge
  - Possible if network size is limited/topology well-structure/controlled
    - SNs are inherently self-organizing and decentralized
  - To account for topology changes due to radio interference or node failure, nodes periodically update BS.
    - Suspicious changes indicate node compromise, action be taken
  - Sufficiently restricting the structure of the topology eliminate the requirement for nodes to advertise their locations

# Countermeasures

- Selective Forwarding
  - Multipath routing can counter selective forwarding attacks
  - Messages routed over *n* paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most *n* compromised nodes
  - Allowing nodes to dynamically choose a packet's next hop probabilistically from a set of possible candidates reduces selective forwarding

# Countermeasures

- Authenticated broadcast and flooding
  - Required to ensure level of asymmetry – No node spoof messages from BS, yet verify them. All broadcasts authenticated
  - Achieved through μTESLA – a protocol for efficient, authenticated broadcast and flooding using symmetric key and requires minimal packet overhead
    - Also requires loose time synchronization – no need to know exact real time diff btw. sender & receiver
  - Flooding information in hostile environment
    - SPIN and Gossip algorithms – reduce messaging costs

# Summary of attacks

| 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 |

# Conclusion

- Proposed routing protocols for SNs are insecure
- Link layer encryption and authentication provide first defense against mote-class outsiders.
- Cryptography is not enough for insiders and laptop-class adversaries, careful protocol design is needed.
- SNs Security protocols are feasible

# SNEP

- SNEP offers the following nice properties:
  - Semantic security:
    - Since the counter value is incremented after each message, the same message is encrypted differently each time. The counter value is long enough that it never repeats within the lifetime of the node.
  - Data authentication:
    - If the MAC verifies correctly, a receiver can be assured that the message originated from the claimed sender.
  - Replay protection:
    - The counter value in the MAC prevents replaying old messages. Note that if the counter were not present in the MAC, an adversary could easily replay messages.

# SNEP

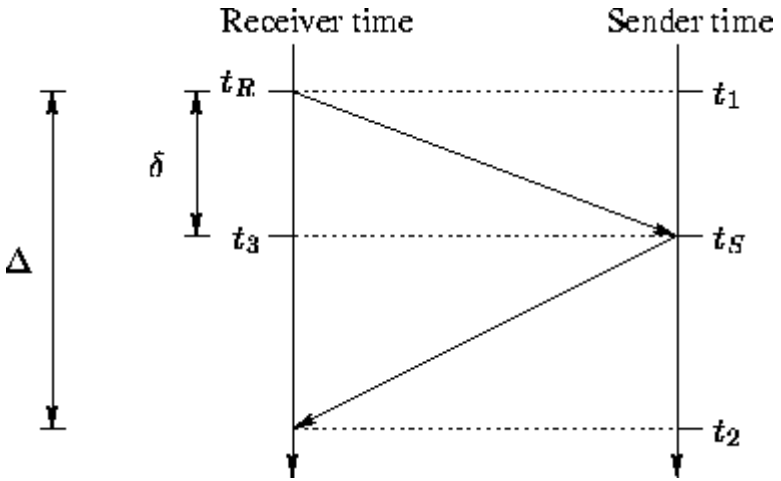
- SNEP offers the following nice properties:
  - Weak freshness:
    - If the message verified correctly, a receiver knows that the message must have been sent after the previous message it received correctly (that had a lower counter value). This enforces a message ordering and yields weak freshness.
  - Low communication overhead:
    - The counter state is kept at each end point and does not need to be sent in each message

# μTESLA

- Designed to solve the following inadequacies of TESLA sensor networks
  - TESLA authenticates the initial packet with a digital signature, which is too expensive for our sensor nodes. μTESLA uses only symmetric mechanisms.
  - Disclosing a key in each packet requires too much energy for sending and receiving. μTESLA discloses the key once per epoch.
  - It is expensive to store a one-way key chain in a sensor node. μTESLA restricts the number of authenticated senders.

# μTESLA

- Loose time synchronization



# Additional Routing Protocols

- Minimum cost forwarding
  - Leverages clustering to efficiently disseminate queries and gather sensor readings to and from all nodes in the network
    - Assumes every node can directly reach a base station
  - LEACH organizes nodes into clusters – one node is cluster-head

  - Attack
    - HELLO Flood - transmitting advertisement all or selectively

# Additional Routing Protocols

- LEACH: Low Energy Adaptive Clustering Hierarchy
  - Algorithm for efficiently forwarding packets from sensor nodes to a base station
  - Does not require nodes to maintain explicit path information or even unique node identifiers
    - Works by constructing a cost field starting at BS
  - Attack
    - Sinkhole - advertising cost zero anywhere in the network
    - Wormhole – Help synchronize this attack with BS-initiated cost updates
    - HELLO Flood - disable entire network by transmitting advertisement with cost zero powerful enough to be received by every network node

# Additional Routing Protocols

- Rumor routing
  - Probabilistic protocol for matching queries with data event
  - Rumor routing offers a energy efficient alternative when the high cost of flooding cannot be justified

  - Attack
    - Denial of service – removing event information or not forwarding
    - Sinkhole – Selective forwarding, create many copies of agents received

# Additional Routing Protocols

- Energy conserving topology maintenance
  - More sensors than needed deployed, use redundant nodes to extend network lifetime. SPAN and GAF decide which nodes to be active
    - Replacement is hard or impossible
  - GAF – Places nodes into virtual “grid squares” adj. nodes communicate
    - Nodes in: sleeping (off), discovery (probe), and active (routing) states.
  - Attack
    - Sinkhole – Selective forwarding, create many copies of agents received
    - Selective forwarding attack or choose to ignore all incoming packets.
    - The Sybil and HELLO flood - target individual grids by broadcasting a high ranking discovery message from a bogus, non-existent node in each grid

# Additional Routing Protocols

- Energy conserving topology maintenance
  - SPAN - Nodes sleep or join backbone of coordinator of “coordinators” that attempt to maintain routing fidelity in the network
  - Coordinators always awake others go into “power saving” mode periodically send and receive HELLO messages to determine to become coordinators
  - GAF – Places nodes into virtual “grid squares” adj. nodes communicate
    - Nodes in: sleeping (off), discovery (probe), and active (routing) states.
  - Attack
    - Spoofing – Sends bogus packets