Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

Chris Karlof and David Wagner

Presenters: Hyowon Lee & Yongbae Bang

Contents

Introduction

- Sensor networks
  - Heterogeneous system with tiny sensors and actuators
  - Consist of many low-power, low-cost nodes at fixed location
  - Route messages using multi-hop wireless communication
- Current routing protocols in sensor networks
  - Optimize for the limited capabilities of the nodes and application specific nature of the networks
  - Do not design with security as a goal
- Secure routing protocols in sensor networks
  - Many SNs are deployed in open, physically insecure, or hostile environments
  - Wireless communication itself is also insecure
  - Routing protocols in SN must be designed with security in mind

Introduction

- Contributions
  - Propose threat models and security goals for secure routing in wireless sensor networks
  - Introduce two new attacks against sensor networks
    - Sinkhole attacks & HELLO floods
  - Discuss the relevance of attacks of the ad-hoc wireless networks and P2P networks to sensor networks
    - Wormhole attack & Sybil attack
  - Analyze the security of major routing protocols and energy conserving topology maintenance algorithms for sensor networks
  - Suggest a set of countermeasures and considerations for the design of secure routing protocols

Background

- SNs have one or more base stations (sinks)
  - Centralized control point: gateway, data processing and storage
  - Request steady stream of data to satisfy a query
  - Aggregation points are used for reducing the total message sent and saving energy
    - Forward an aggregate of sensor readings from nodes to a base station
    - Chosen dynamically
- SNs are resource constrained
  - Low power, low bandwidth, little computational power
  - Security challenge
    - Public key cryptography is expensive to use in SN
    - Symmetric key cyphers can be used sparingly
    - Secure routing mechanisms in ad-hoc networks are inadequate for SN

Sensor Networks vs Ad-hoc Wireless Networks

- Similarity
  - Both support multi-hop networking
  - Security issues in both networks are similar
- Differences
  - SNs have a more specialized communication pattern
    - Many-to-one : multiple sensors to a base station
    - One-to-many : single base station to multiple sensors
    - Local communication : discover and coordinate neighboring nodes
  - SNs are more resource constrained than ad-hoc networks
    - Public key cryptography is not feasible in SN
  - Higher level of trust relationships in SN
    - To reduce the network traffic and save energy

Problem Statement

- Network assumptions
  - Radio links are insecure
    - Eavesdrop radio transmissions, inject bits in the channel, replay previous packets
  - Attacker can deploy a few malicious nodes with similar capabilities
  - Attacker may have control of more than one node
    - Malicious nodes may collude to attack
  - No tamper resistant
    - Attacker can extract all key materials from the node

Problem Statement

- Trust requirements
  - Compromise of base stations can render the entire network useless
    - Base stations are trustworthy (can be trusted and assumed to behave correctly)
    - Most routing protocols trust messages from base stations
  - Aggregation points may become compromised
    - Aggregation points is not necessarily trustworthy

Problem Statement

- Threat models
  - Based on capability
    - Mote-class attackers
      - Access fewer nodes with similar capabilities
      - Limited damage
    - Laptop-class attackers
      - Access to more powerful nodes
      - Jam the entire sensor network, eavesdrop on an entire network
  - Based on location of attacker
    - Outsider attackers
      - Attacker has no special access to sensor network
    - Insider attackers
      - Attacker is an authorized participant in the sensor network

Problem Statement

- Security goals
  - Integrity, Authenticity, Availability – Ideal routing protocol

  - Protection against eavesdropping
    - Confidentiality should be provided through link layer encryption
    - Consider eavesdropping achieved by the cloning of a data flow

  - Protection against the replay of data packets
    - Can be fully detected at the application layer

  - Presence of insider attackers
    - Goals are not fully achieved
    - Graceful degradation: degrade no faster than a ratio of compromised nodes to total nodes

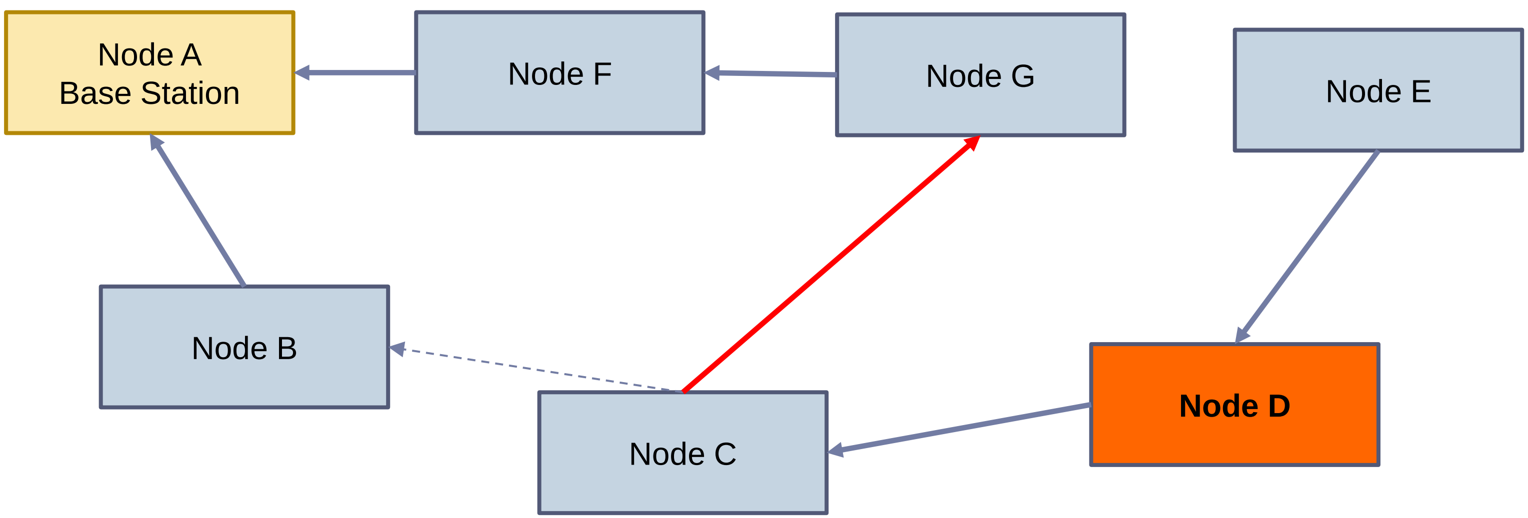
Attacks on Sensor Network Routing

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

- Difference between attacks
  - Manipulate user data directly
  - Affect the underlying routing topology

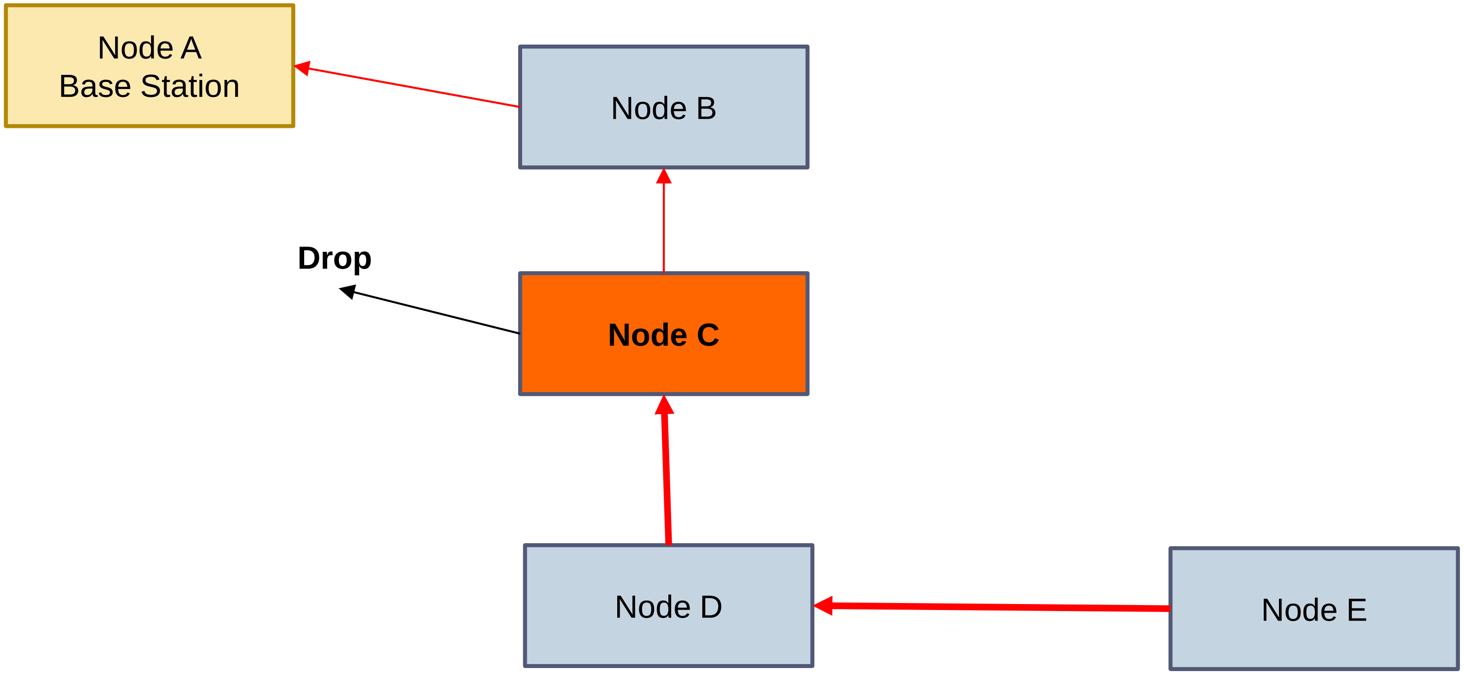
Spoofed, Altered, or Replayed Routing Information

- Directly spoofing routing information exchanged between nodes
- Create routing loops, generate false error messages, partition network, increase end-to-end latency, and so on



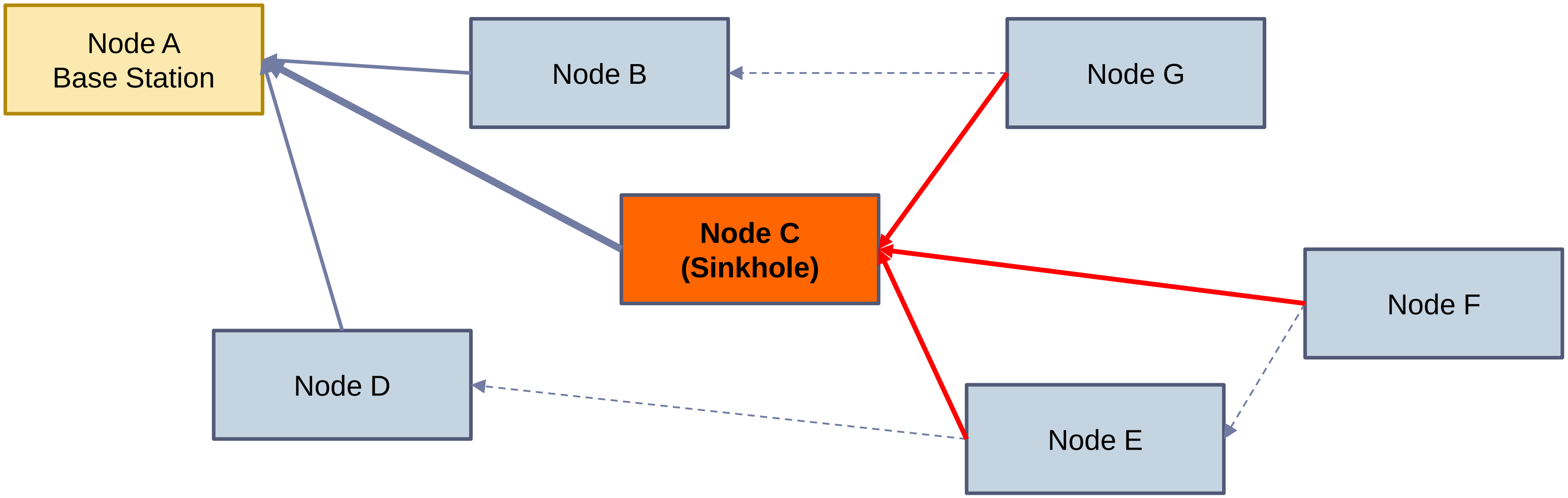
Selective Forwarding

- Malicious nodes refuse to forward certain messages
- Selectively forwards packets or drops packets



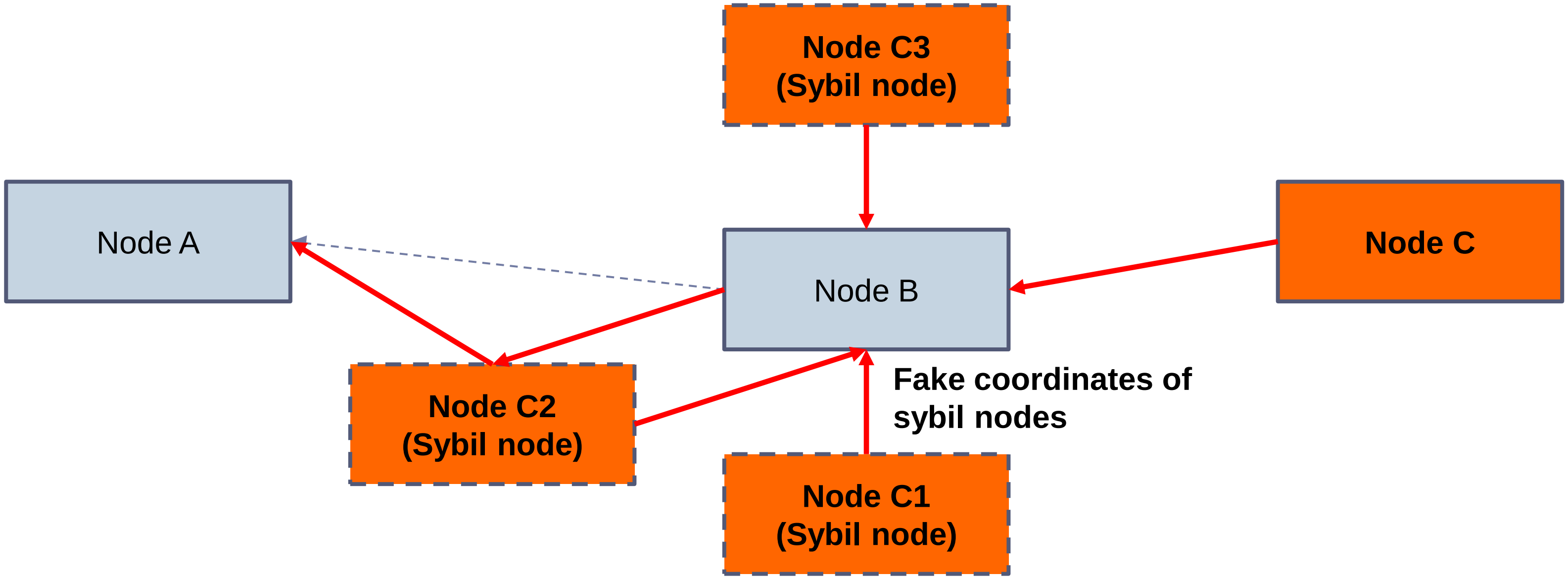
Sinkhole Attacks

- Create a metaphorical sinkhole with the adversary at the center
- Make a compromised node look attractive to surrounding nodes
  - Laptop-class adversary with high quality route to a base station
  - Almost all traffic is directed to the fake sinkhole



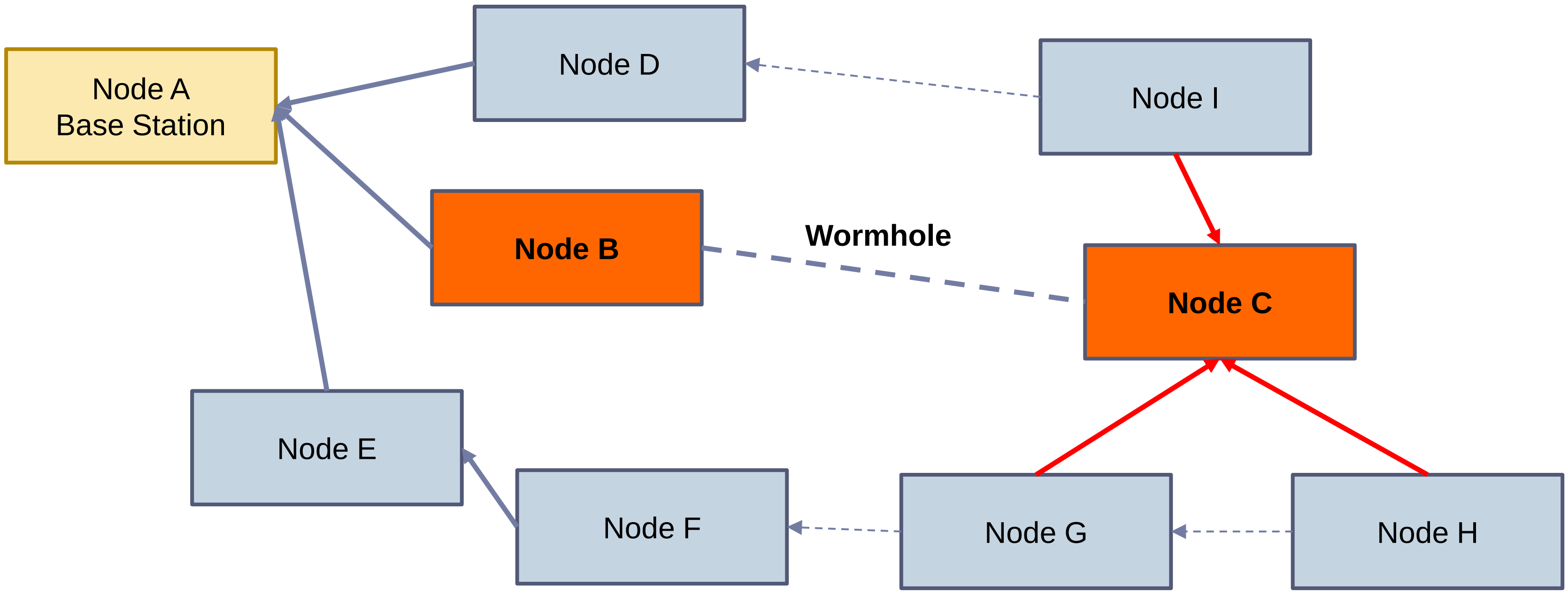
Sybil Attacks

- Single node presents multiple identities to other nodes in the network
- Significant threat to geographic routing protocol
  - An adversary node can locate on more than one place at once



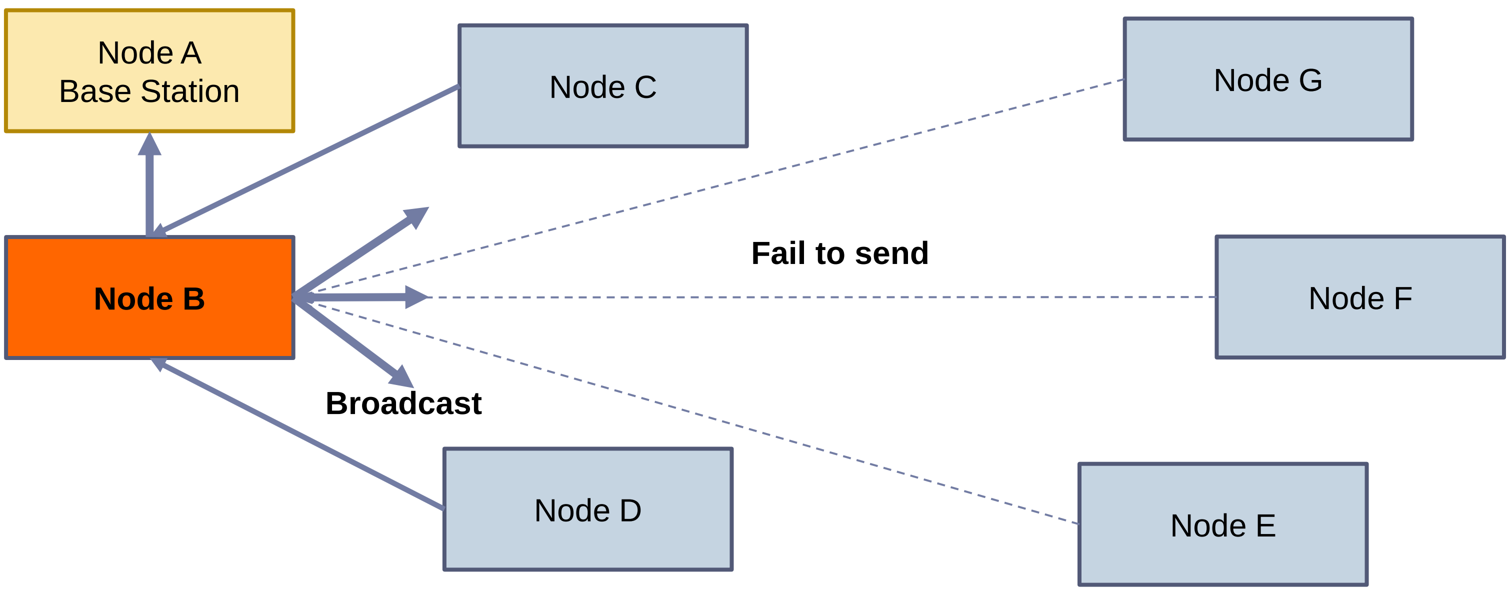
Wormholes

- Tunnels messages over a low latency link
- Disrupt routing by creating a wormhole close to a base station
- Convince two distant nodes that they are neighbors



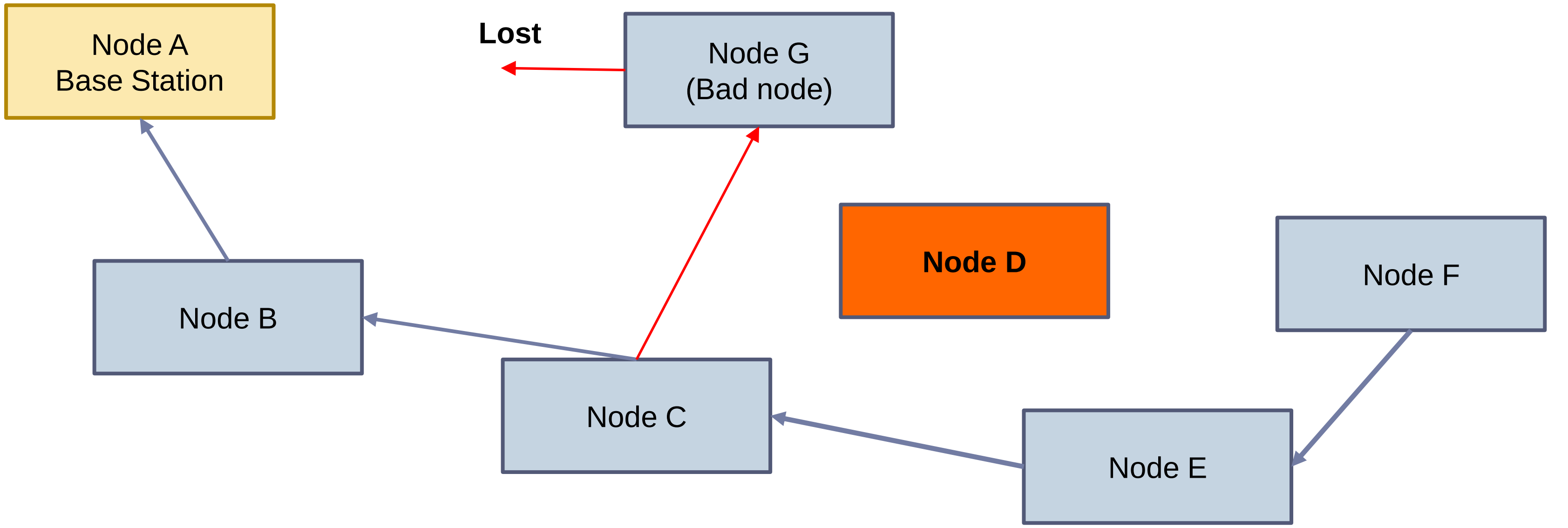
HELLO Flood Attacks

- Laptop-class attacker sends or replays HELLO packet with more energy to convince every node in the network that the adversary is a neighbor
- Protocols with information exchange between nodes for topology maintenance or flow control is subject to this attack



Acknowledgment Spoofing

- Spoof link layer acknowledgments for overheard packets
- Convince the sender that a weak link is strong or a dead node is alive
  - Can use selective forward attack by encouraging the target node to transmit packets on a weak or dead link



Attacks on Specific Sensor Network Protocols

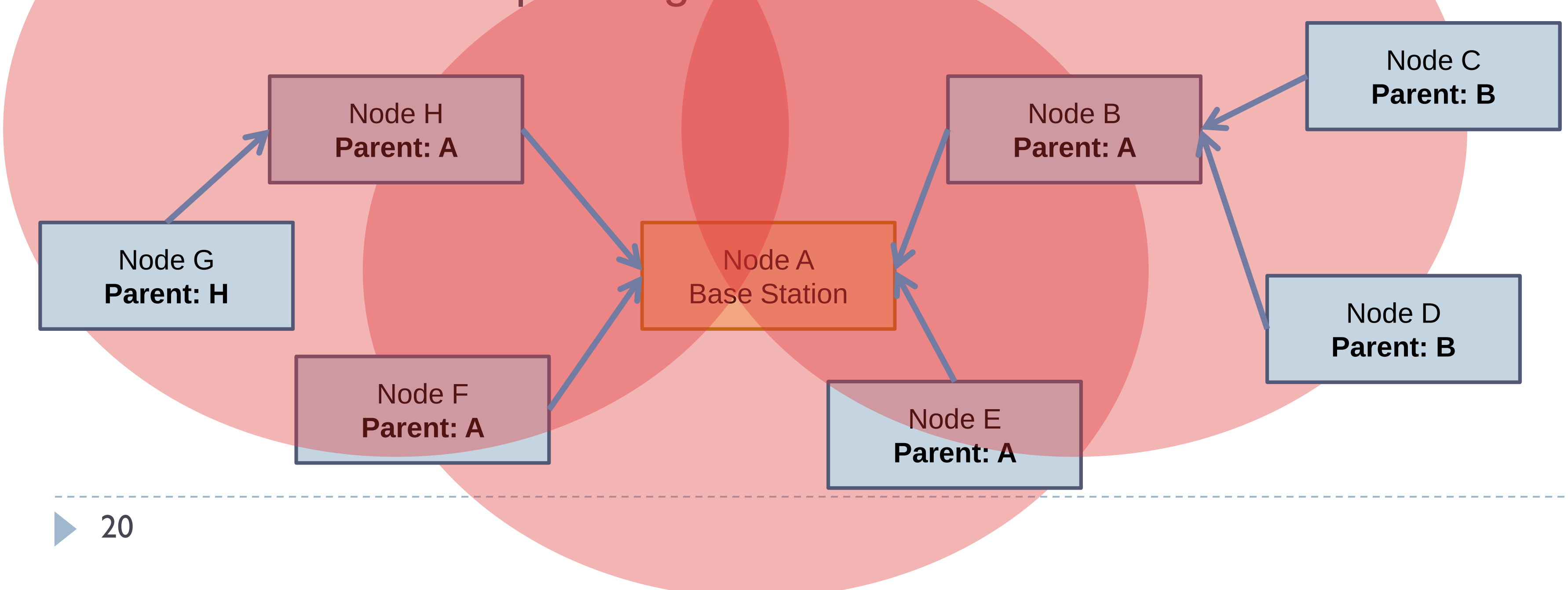
Protocol	Insecure?	Relevant Attacks
Tiny OS beaconing	Yes	B, SF, SH, SY, W, H
Directed Diffusion	Yes	B, SF, SH, SY, W, H
Geographic Routing	Yes	B, SF, SY
Minimum Cost Forwarding	Yes	B, SF, SH, W, H
Clustering Based Protocols (LEACH, TEEN, PEGASIS)	Yes	SF, H
Rumor Routing	Yes	B, SF, SH, SY, W
Energy Conserving Topology Maintenance	Yes	B, SY, H

Abbreviations of Attacks

- B: Bogus routing information
- SF: Selective forwarding
- SH: Sinkholes
- SA: Sybil Attack
- W: Wormholes
- H: HELLO floods

TinyOS Beaconing

- A lightweight, event-driven operating system for sensor networks
- Widely used in research due to its simplicity
- Beaconing Algorithm
  - A breadth first spanning tree

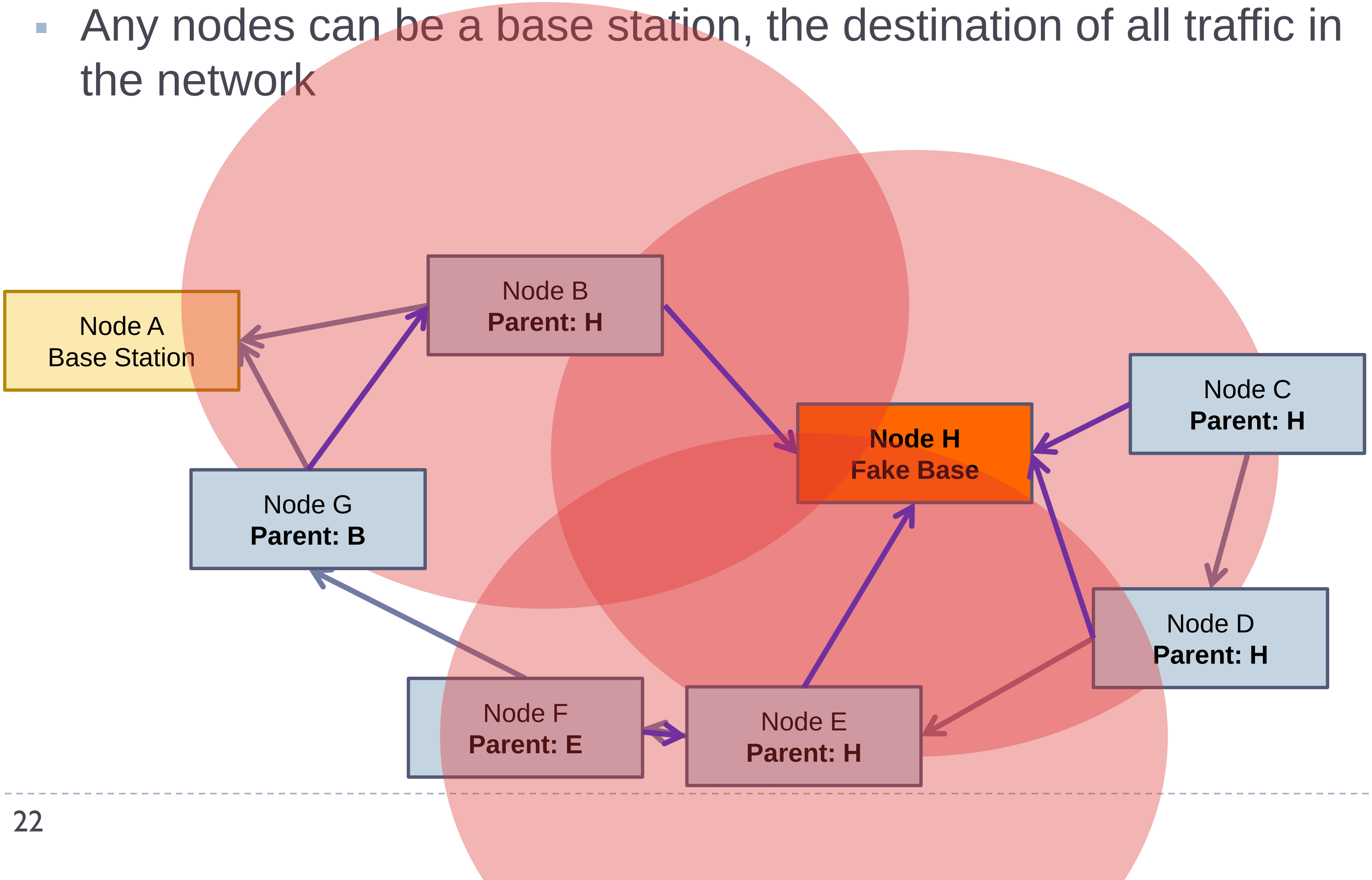


TinyOS Beaconing - Attack

- It is highly susceptible to attack
- Attacks
  - Fake base station
  - A combined wormhole/sinkhole attack
  - HELLO flood attack
  - Routing Loop

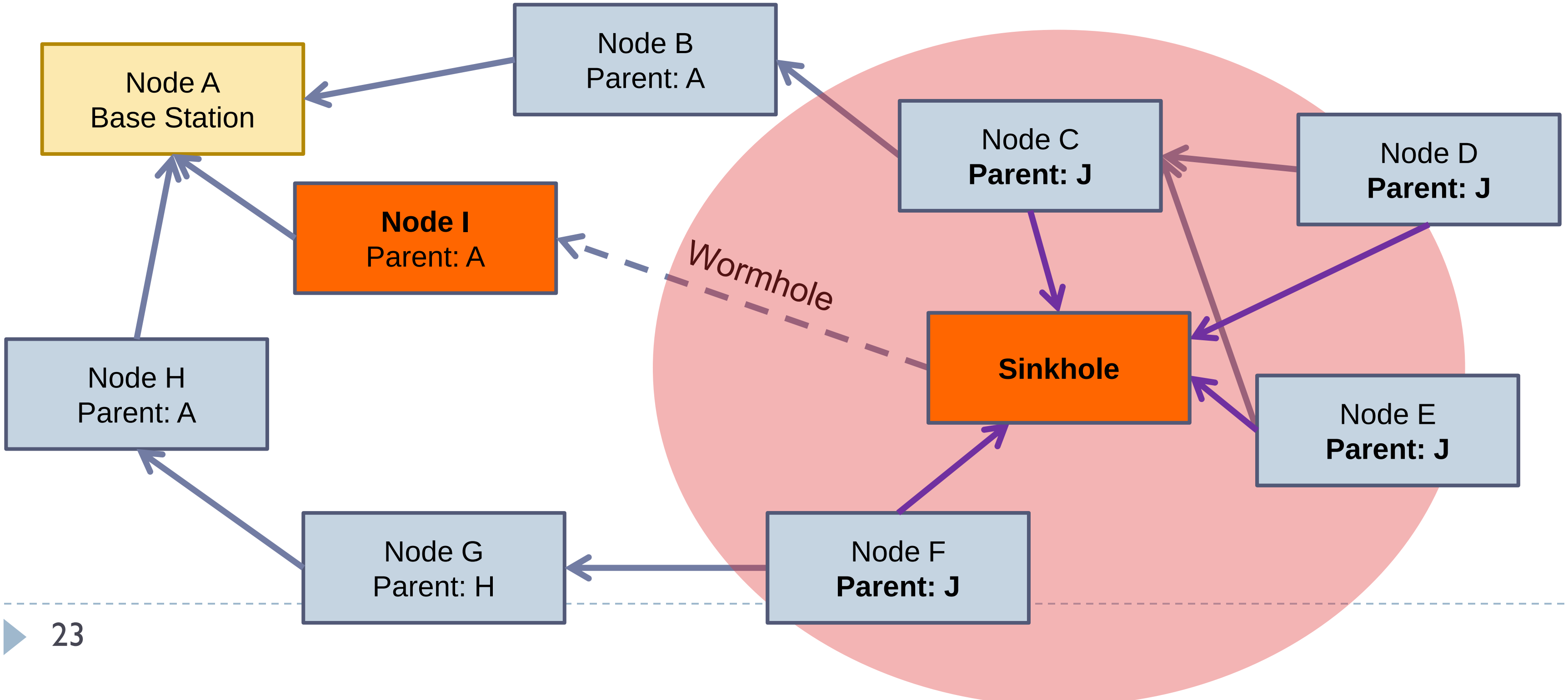
TinyOS Beaconing - Attack - Fake Base Station

- The routing updates are not authenticated
  - Any nodes can be a base station, the destination of all traffic in the network



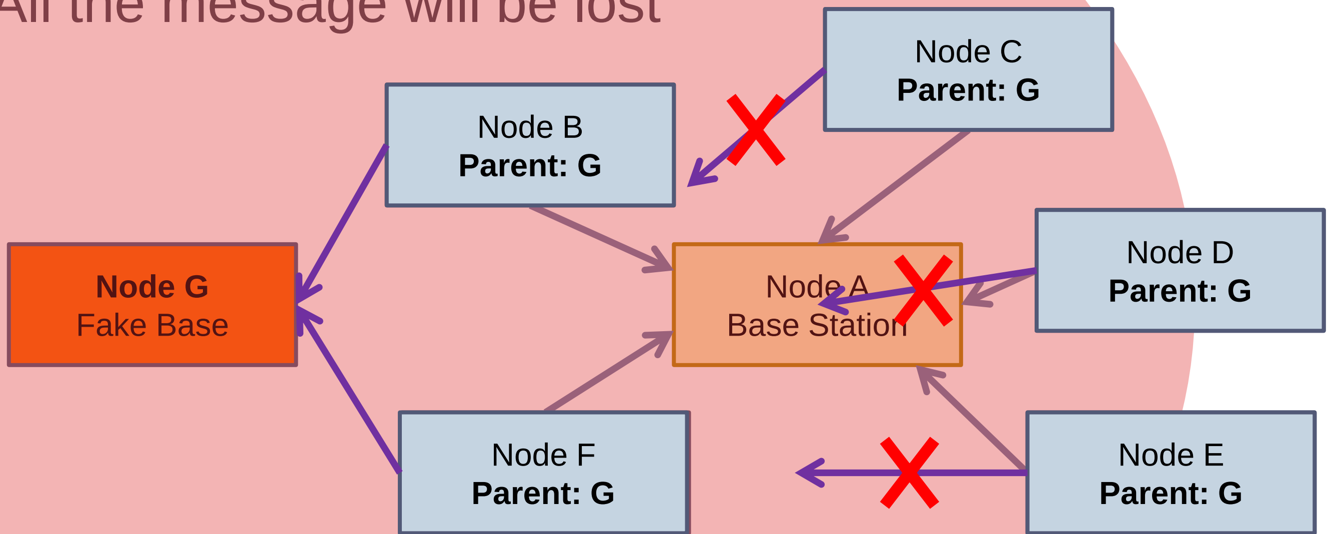
TinyOS Beaconing - Attack - Wormhole/Sinkhole Attack

- Even if authenticated, laptop-class adversary can do
  - Create wormhole to make a sinkhole
- Enable a potent selective forwarding attack



TinyOS Beaconing - Attack - HELLO Flood Attack

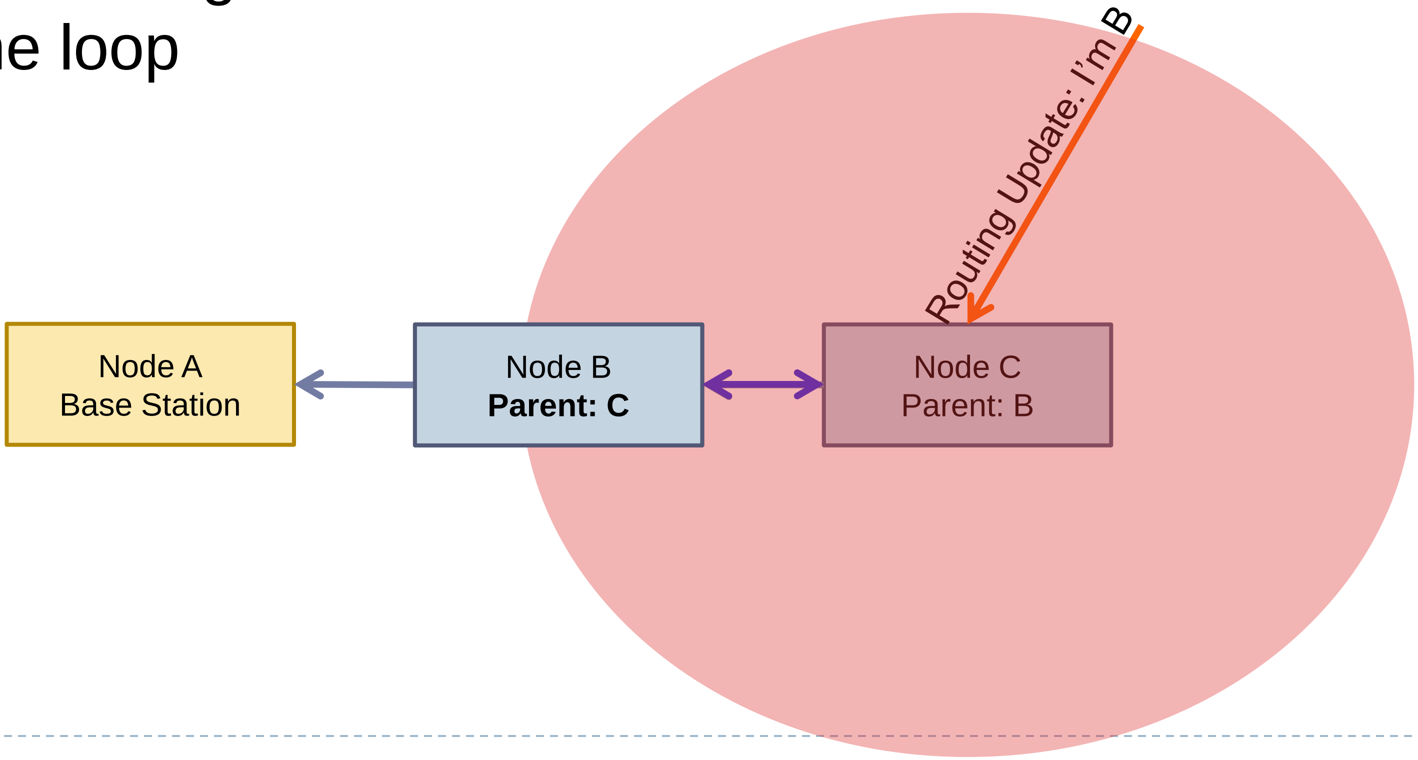
- Laptop-class adversary with a powerful transmitter
  - Broadcast a routing update loud to the entire network
  - All the message will be lost



- Hard to recover
  - Even though a node realizes its parent is not in its range, each of its neighbors likely marked the adversary as its parent

TinyOS Beaconing - Attack - Routing Loop

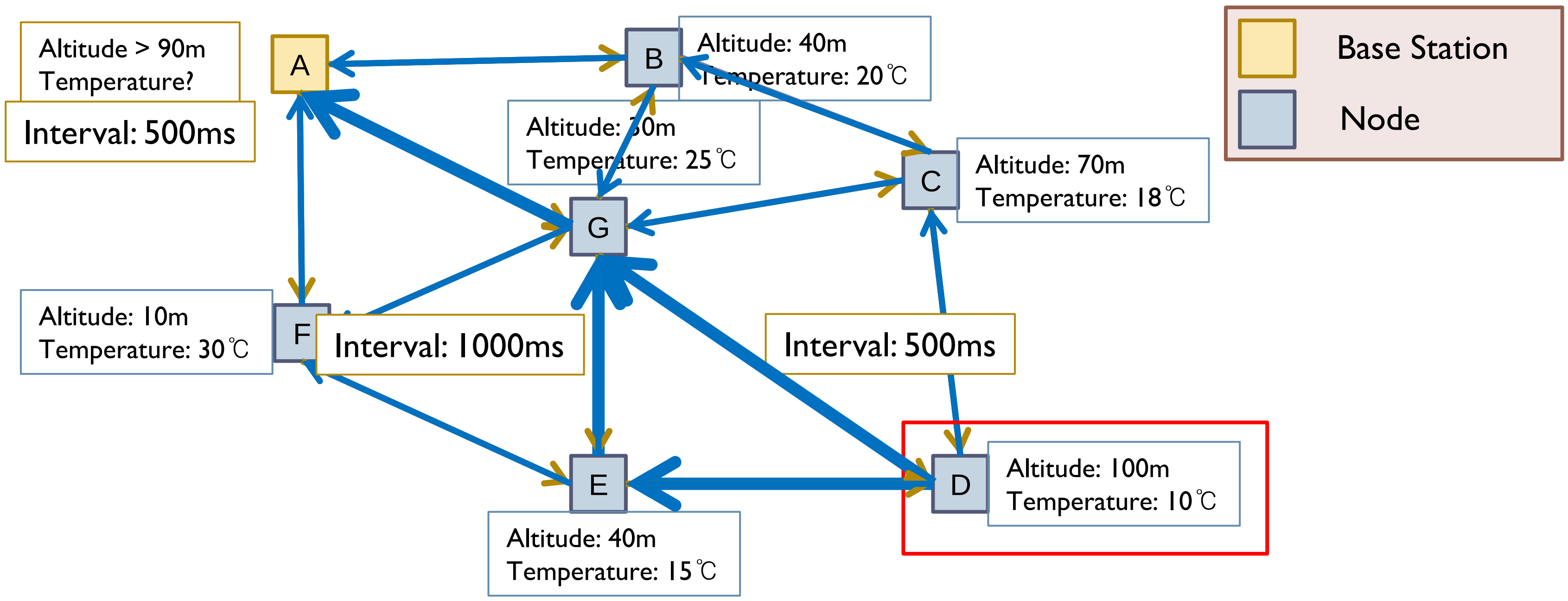
- Mote-class adversary
- Spoof routing updates to make node B and C mark each other as parent
- The message from either B or C will be forever forwarded in the loop



Directed Diffusion

- Data-centric communication paradigm for drawing information out of a sensor network
- Interest Dissemination
  - Base stations flood interests for named data
  - They set up gradients within the network designed to draw events
  - Nodes satisfy the interest disseminate information along the reverse path of interest propagation
- Data rate of link reinforcement
  - Positive when the base station starts receiving events
  - Negative
- Multipath variant of directed diffusion is proposed

Directed Diffusion - Example

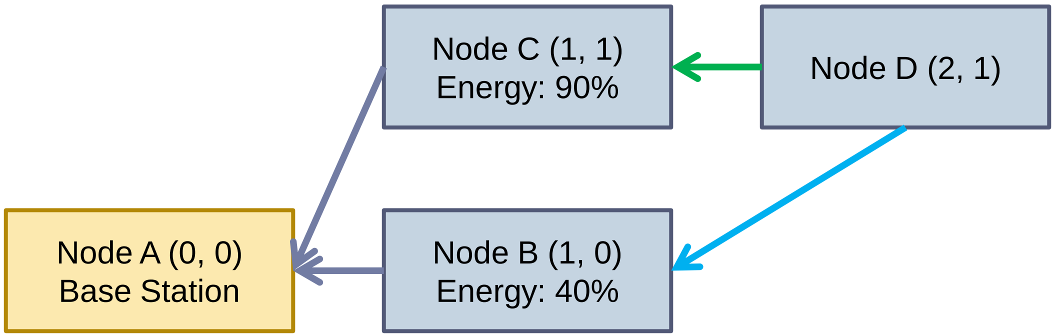


Directed Diffusion - Attack

- Suppression
  - DoS: Spoof negative reinforcements to suppress a flow
- Cloning
  - Eavesdropping: Duplicate same interest to listen
- Path Influence
  - Modify any flow of events propagates through the adversary
- Selective Forwarding and Data Tampering
  - If adversary in the path, it can modify and selectively forward packets
- Wormhole attack
  - to make data flows away from the base station and make sinkhole
- Sybil attack
  - For the multipath version

Geographic Routing

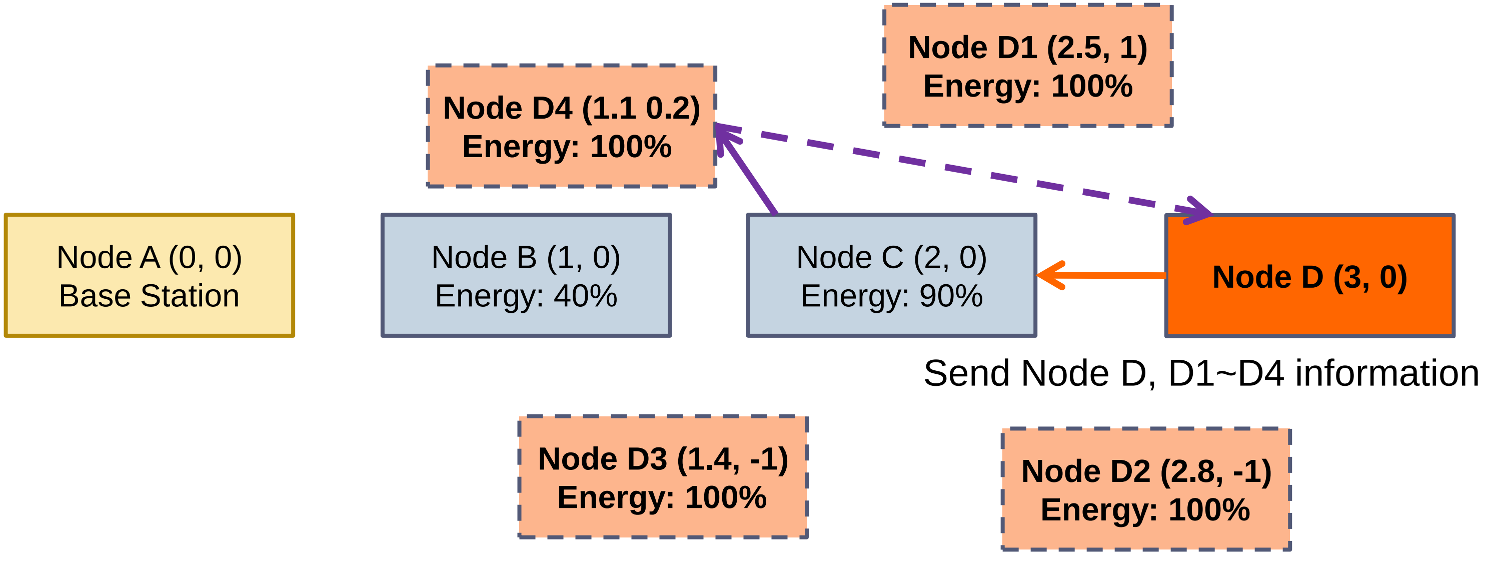
- To efficiently disseminate queries, the geometric location data is used



- Greedy Perimeter Stateless Routing (GPSR) →
  - Routing each packet to the neighbor **closest** to the destination
  - Uneven energy consumption due to the fixed path
- Geographic and Energy Aware Routing (GEAR) →
  - Weighting the choice of the next hop by both **remaining energy** and **distance** from the target

Geographic Routing - Attack - Sybil Attack

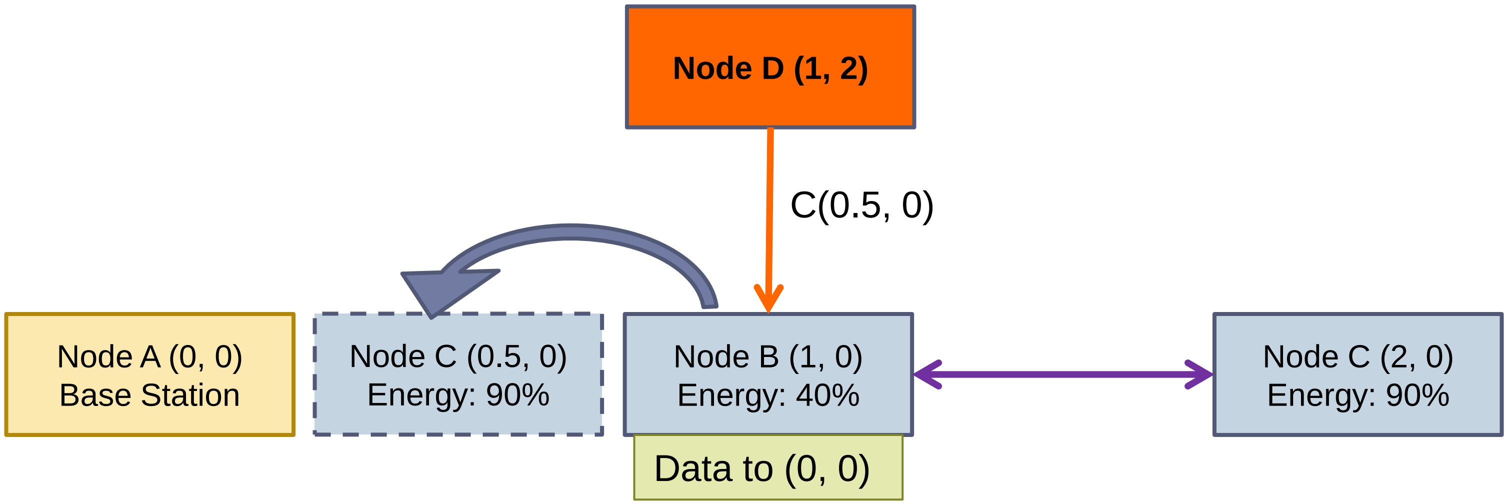
- Fake location on the path to intercept the event
- Report maximum energy to make it always be selected



- Selective forwarding attack can be mounted

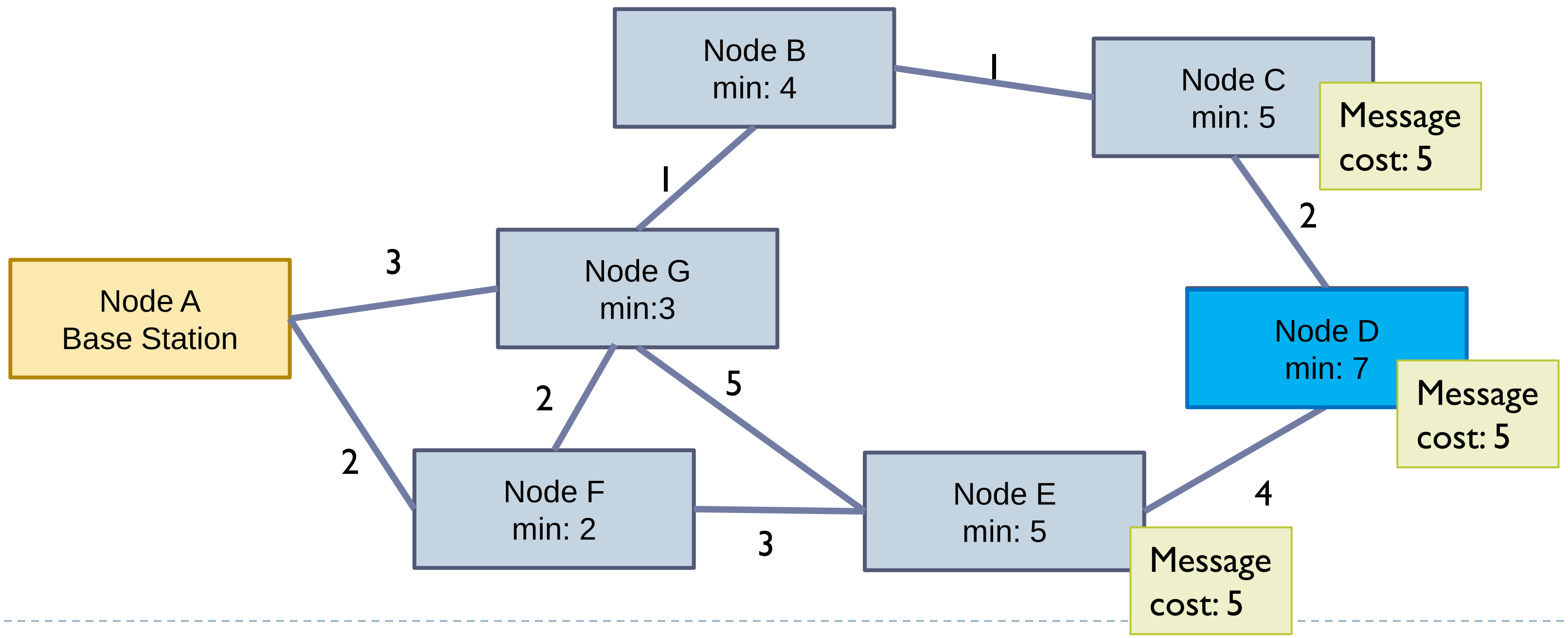
Geographic Routing - Attack - Routing Loop

- In GPSR, routing loop can be made without active participation in packet forwarding
- Fake location of C makes the packet will be forwarded forever between B and C



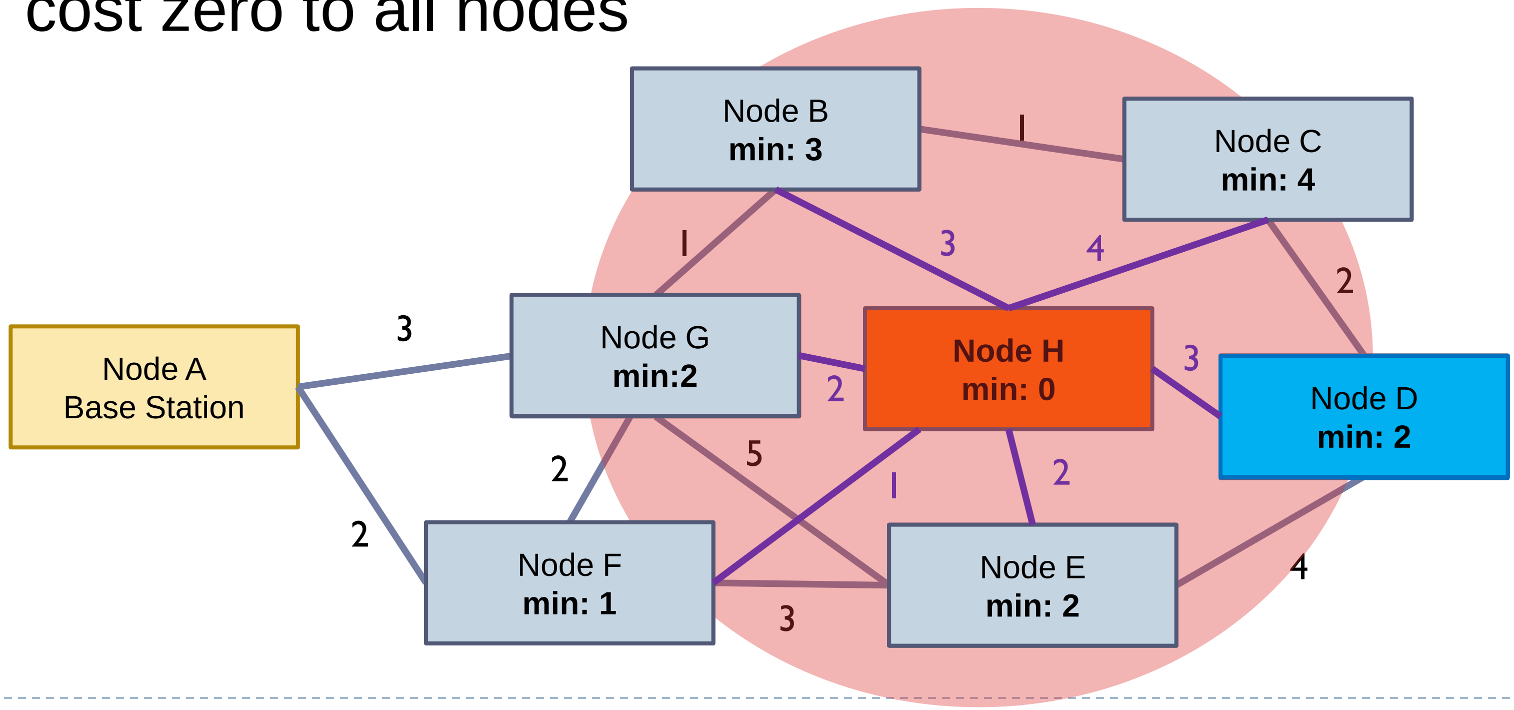
Minimum Cost Forwarding

- Every nodes maintain the cost of each link and its minimum total cost to the base station
  - Distributed shortest-paths algorithm
- Cost: hop count, energy, latency, loss, etc.



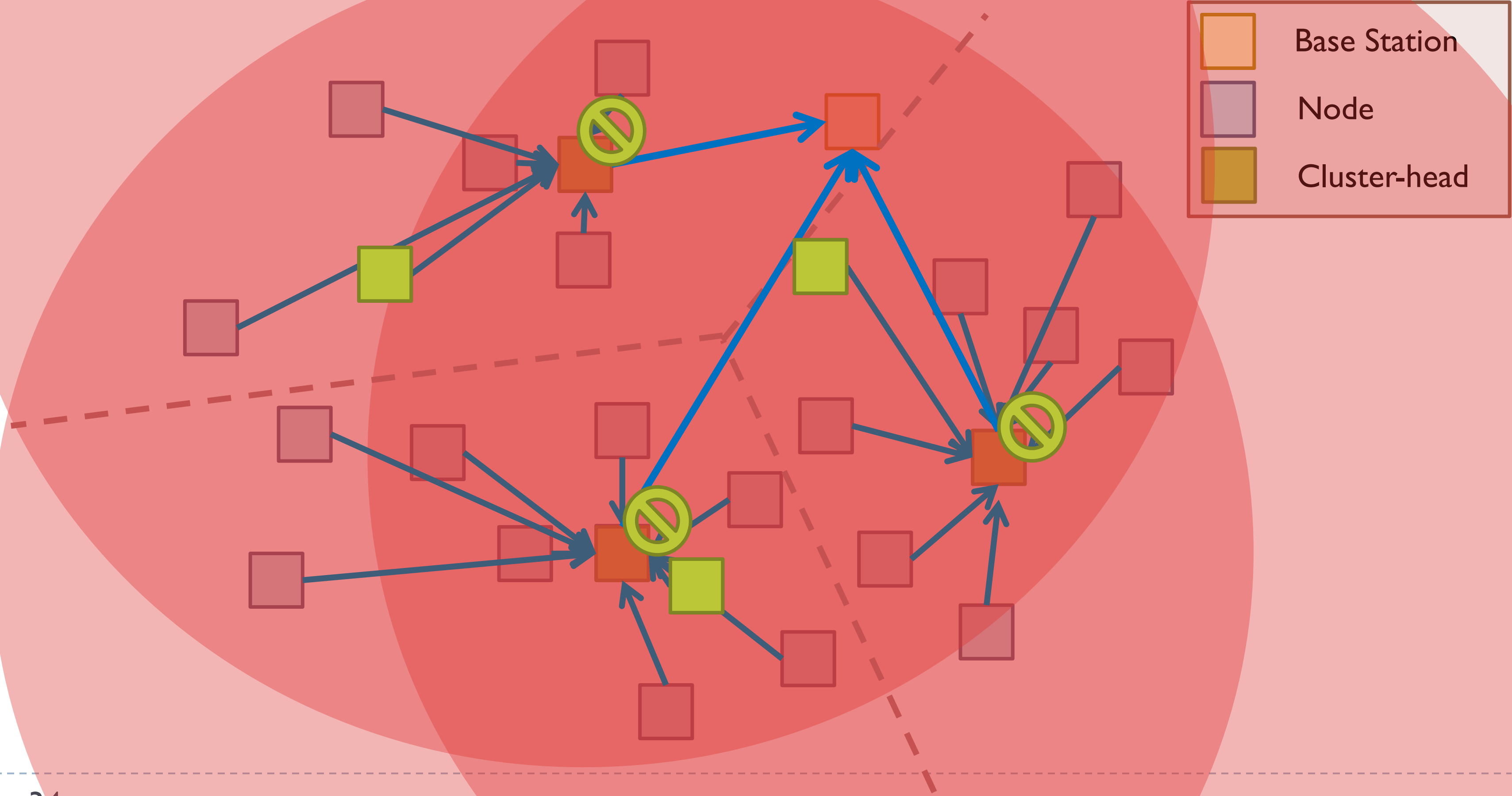
Minimum Cost Forwarding - Attack

- Sinkhole attack: adversary can advertise cost zero
- Wormhole attack: to synchronize the base station-initiated cost updates
- HELLO flood attack: disable entire network by advertising cost zero to all nodes



LEACH: Low-Energy Adaptive Clustering Hierarchy

- When every node can reach the base station directly, cluster the network to reduce the power consumption



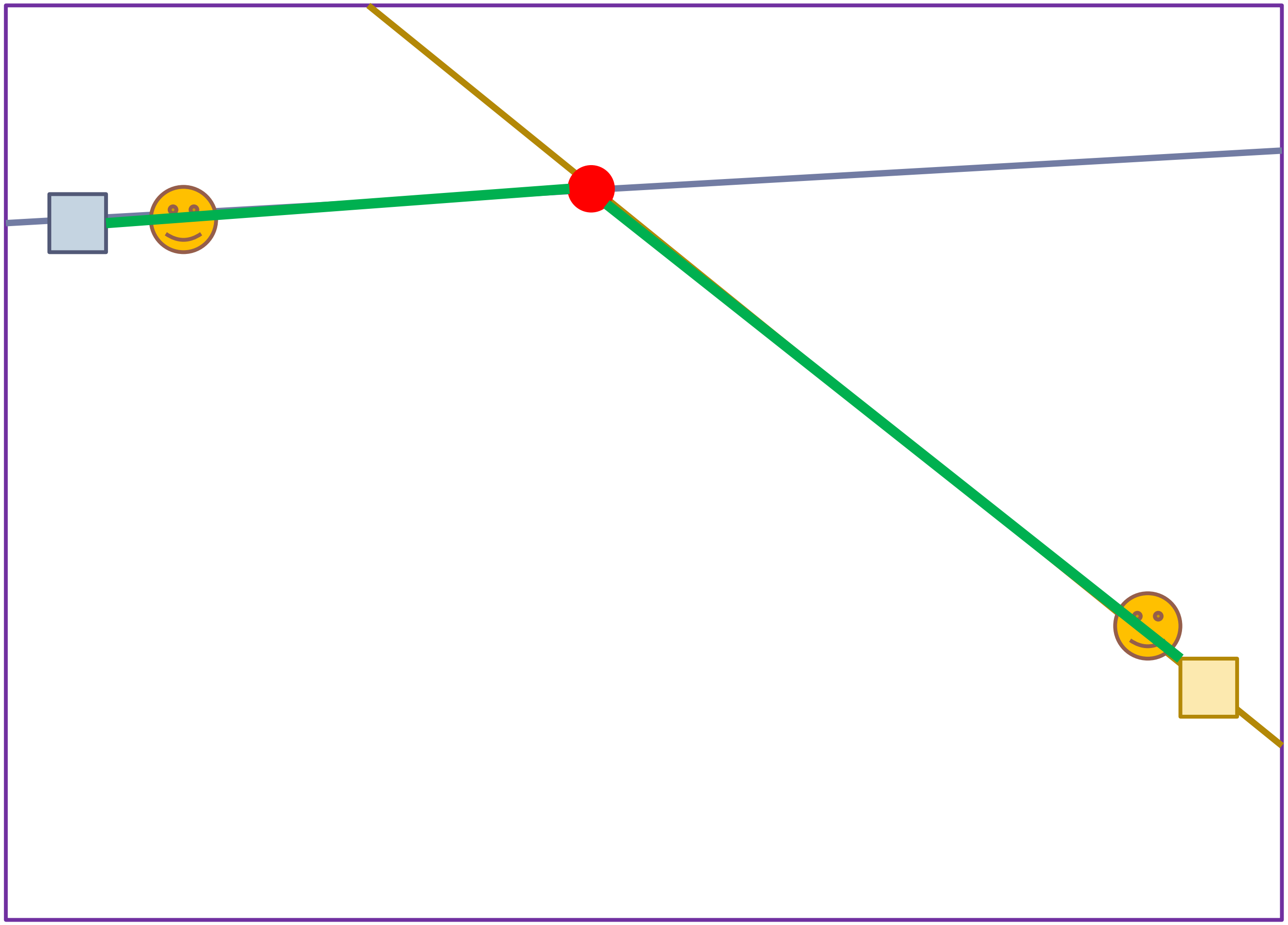
LEACH - Attack

- Nodes choose the largest signal power
- HELLO flood attack
  - A powerful advertisement to all nodes
  - Every nodes choose the adversary as its cluster-head
  - If some data reached, the adversary can selectively forward
  - Others that can not reach the adversary → disabled
- Selective forwarding attack
  - Using small number of nodes with same technique
- Sybil attack
  - To counter the refusing to use the same cluster-head
- Other cluster protocols (TEEN, PEGASIS) are also susceptible

Rumor Routing

- A probabilistic protocol for matching queries with data events
- Offers an energy-efficient alternative when the high cost of flooding cannot be justified
- An agent is sent to find the way
  - When sensor observe some events
  - When base station wants to disseminate a query
- Agent carries information
  - a list of events, the next hop of paths to those events, the corresponding hop counts of those paths, TTL, a list of previously visited nodes and those nodes' neighbors

Rumor Routing - Example

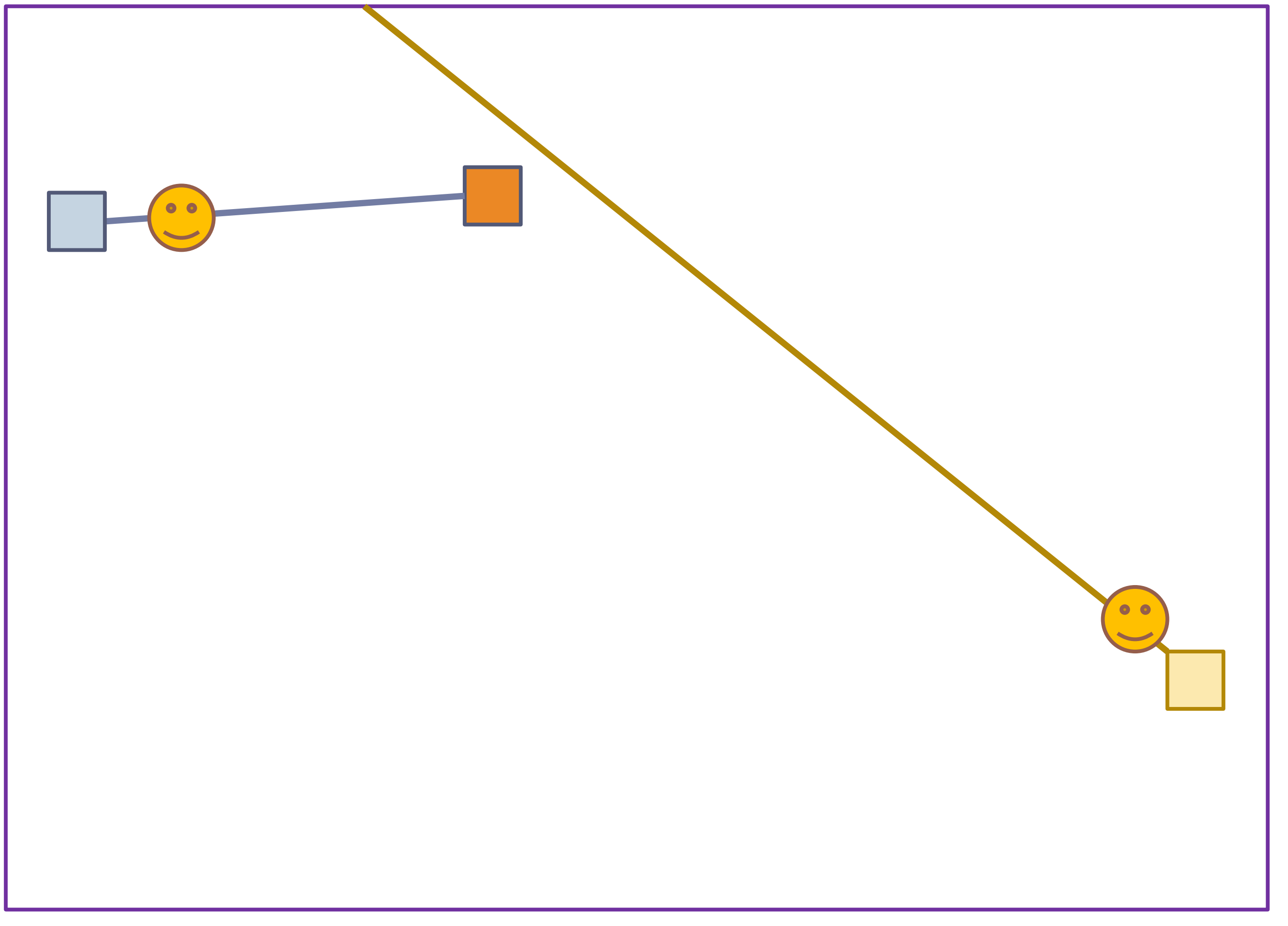


Rumor Routing - Attack

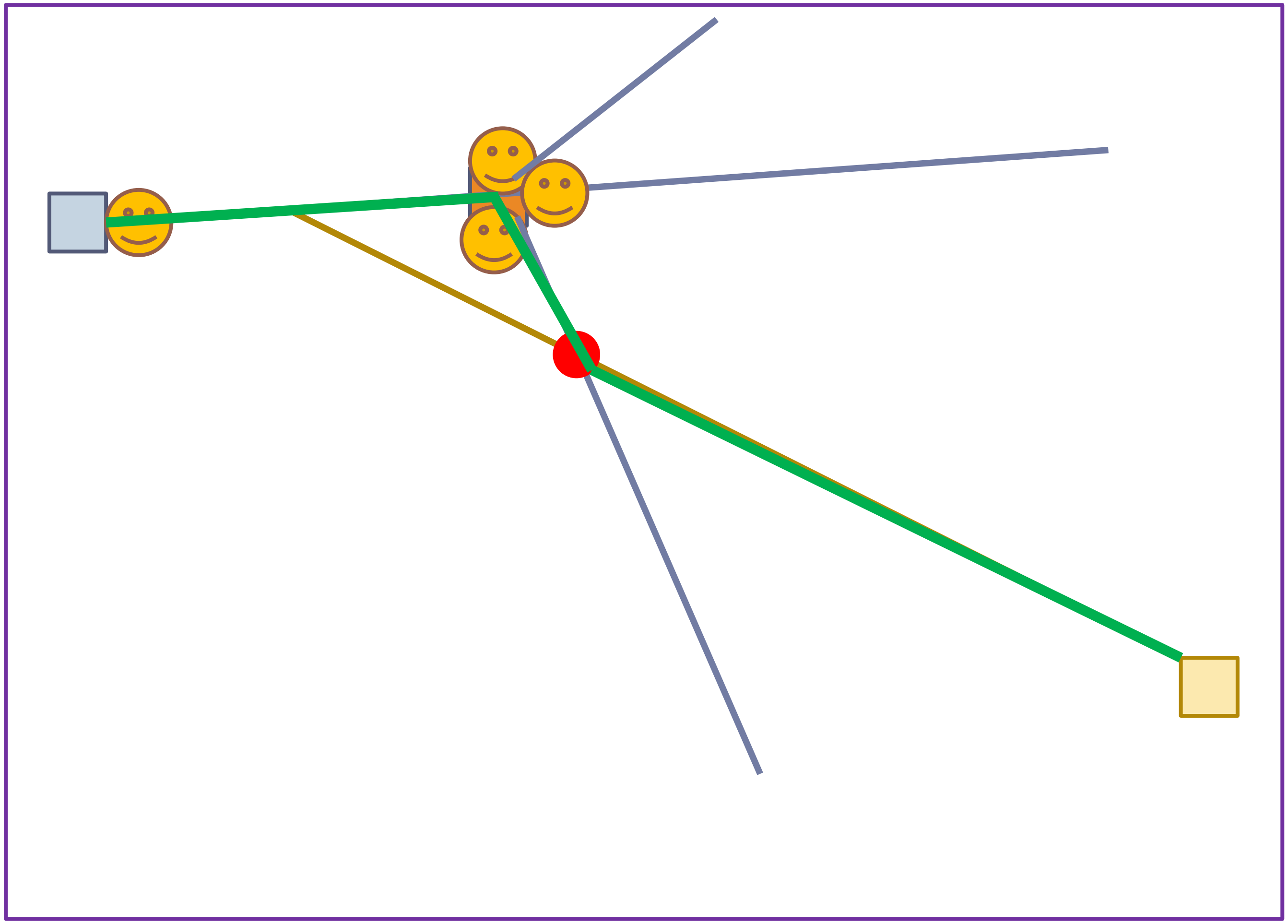
- Denial-of-service attack
  - Remove the event information carried by the agent
  - Refuse to forward agents entirely
  - Modify the query or event information in agents

- Selective forwarding attack
  - The intersection must occur between the adversary and BS
  - Make tendrils that make many routes via the adversary
  - To make it, forward multiple copies to multiple neighbors
  - To enlarge it, change TTL to max and hop count to 0
  - Create wormhole and use Sybil attack to maximize the probability

Rumor Routing - Attack - DoS

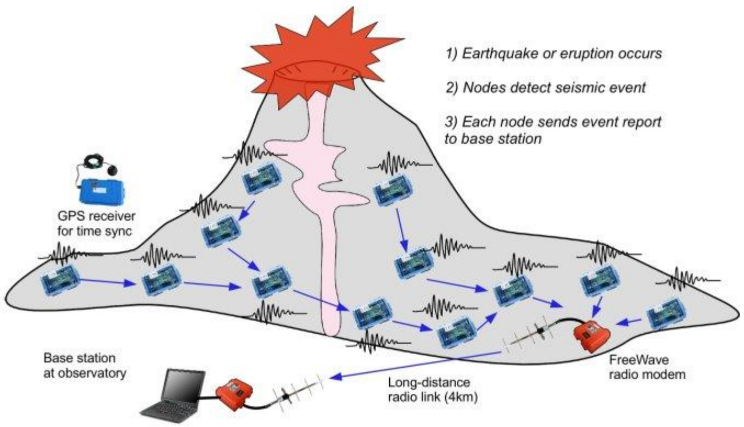


Rumor Routing - Attack - Selective Forwarding



Energy Conserving Topology Maintenance

- Sensor networks in hard to reach areas (ex: volcano)
  - Difficult to replace the batteries
  - Difficult to add new ones



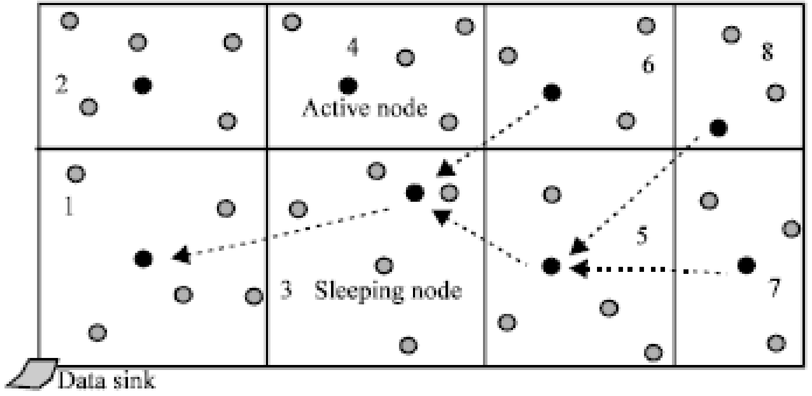
- Solution: deploy more sensors than needed

- Protocols that adaptively decide which nodes are active
  - Geographic Adaptive Fidelity (GAF)
  - SPAN

Geographic Adaptive Fidelity (GAF)

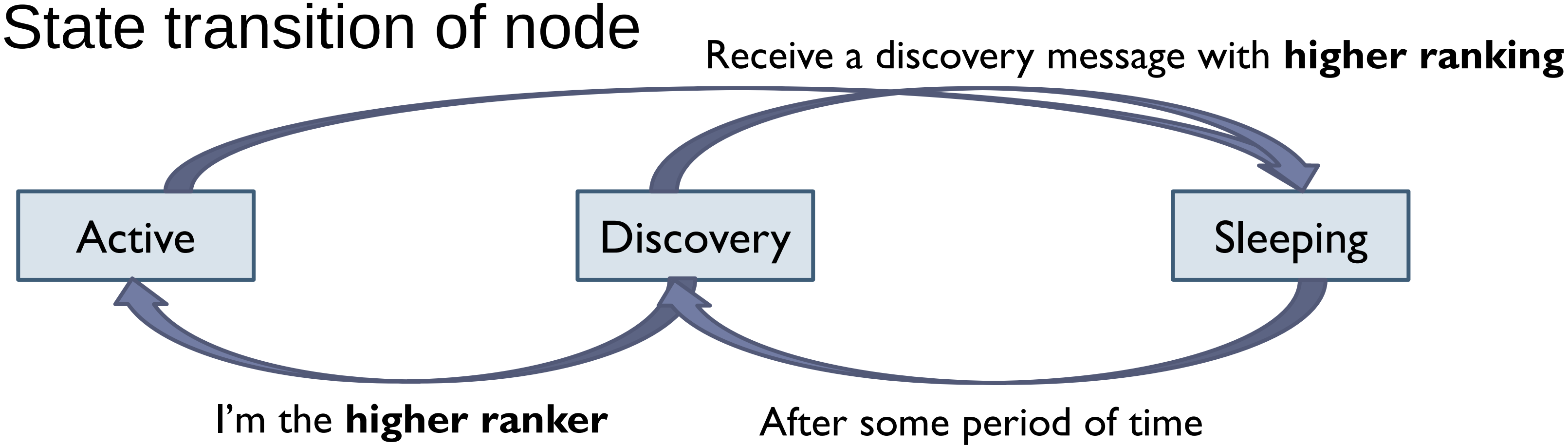
- Place nodes into virtual "grid squares"

- Grid Square
  - according to geographic location and expected radio range
  - Any pair of nodes in adjacent grid squares are able to communicate
  - Attempt to reach a state: only one active node in each grid square



Three States of Nodes in GAF

- Three States of node
  - Sleeping: turn off the radio
  - Discovery: probe the network to determine the node is needed
  - Active: participate in routing
- Rank
  - Nodes are ranked with **current state** and **expected life time**
  - Higher ranker will be in **active** state and **participate** in routing
- State transition of node



GAF - Attack

- Selective forwarding attack
  - periodically broadcasting high ranking discovery messages
  - Other nodes in its grid will be disabled

- Sybil attack + HELLO flood attack
  - With a loud transmitter, all grid will choose non-existent node

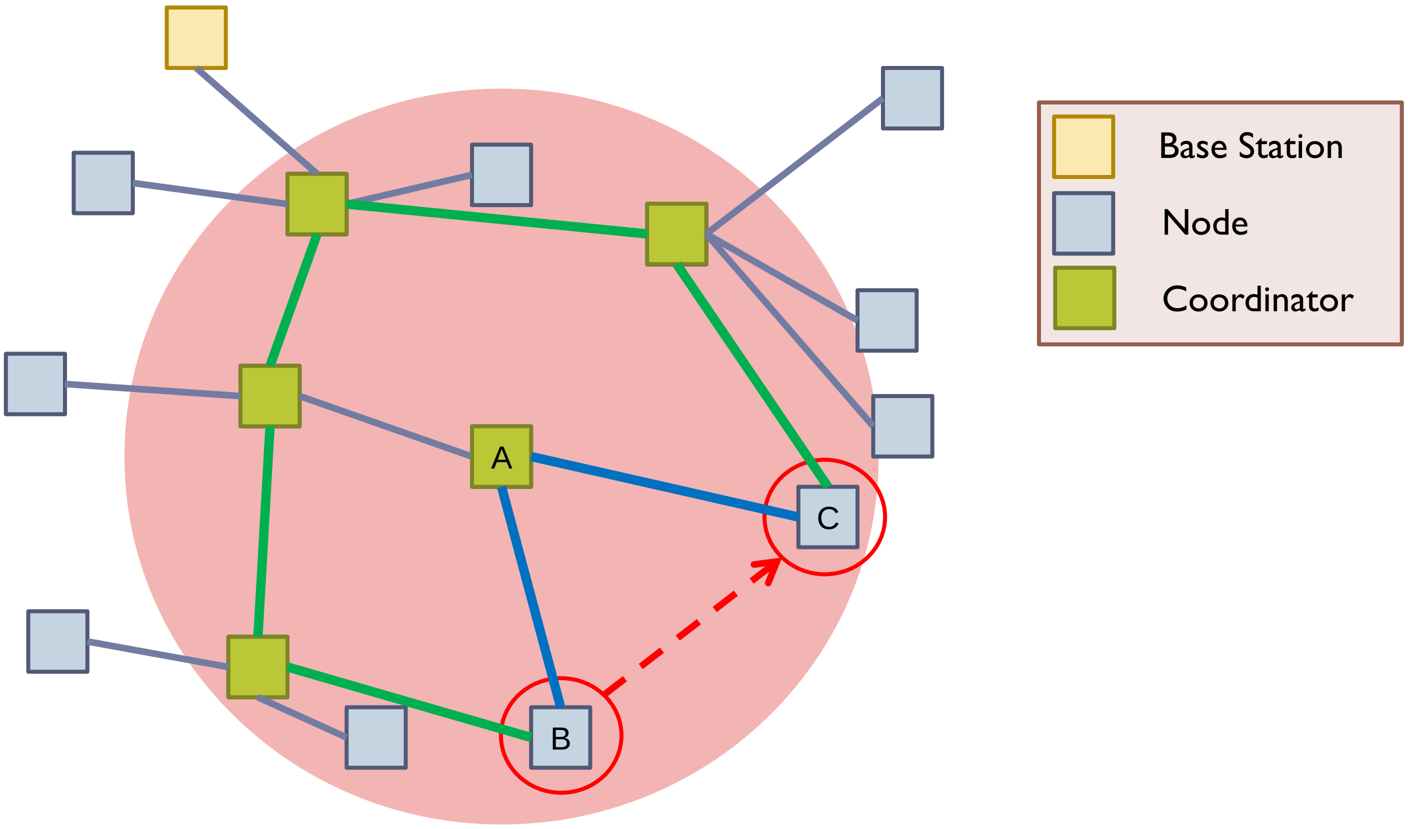
SPAN

- Coordinators maintains the routing fidelity

- States of node
  - Sleep: power saving mode
  - Coordinator: stay awake continuously while the remaining nodes go into sleep mode
    - Periodically send HELLO message to determine the new state
      - HELLO message: current status, current neighbors, current coordinators

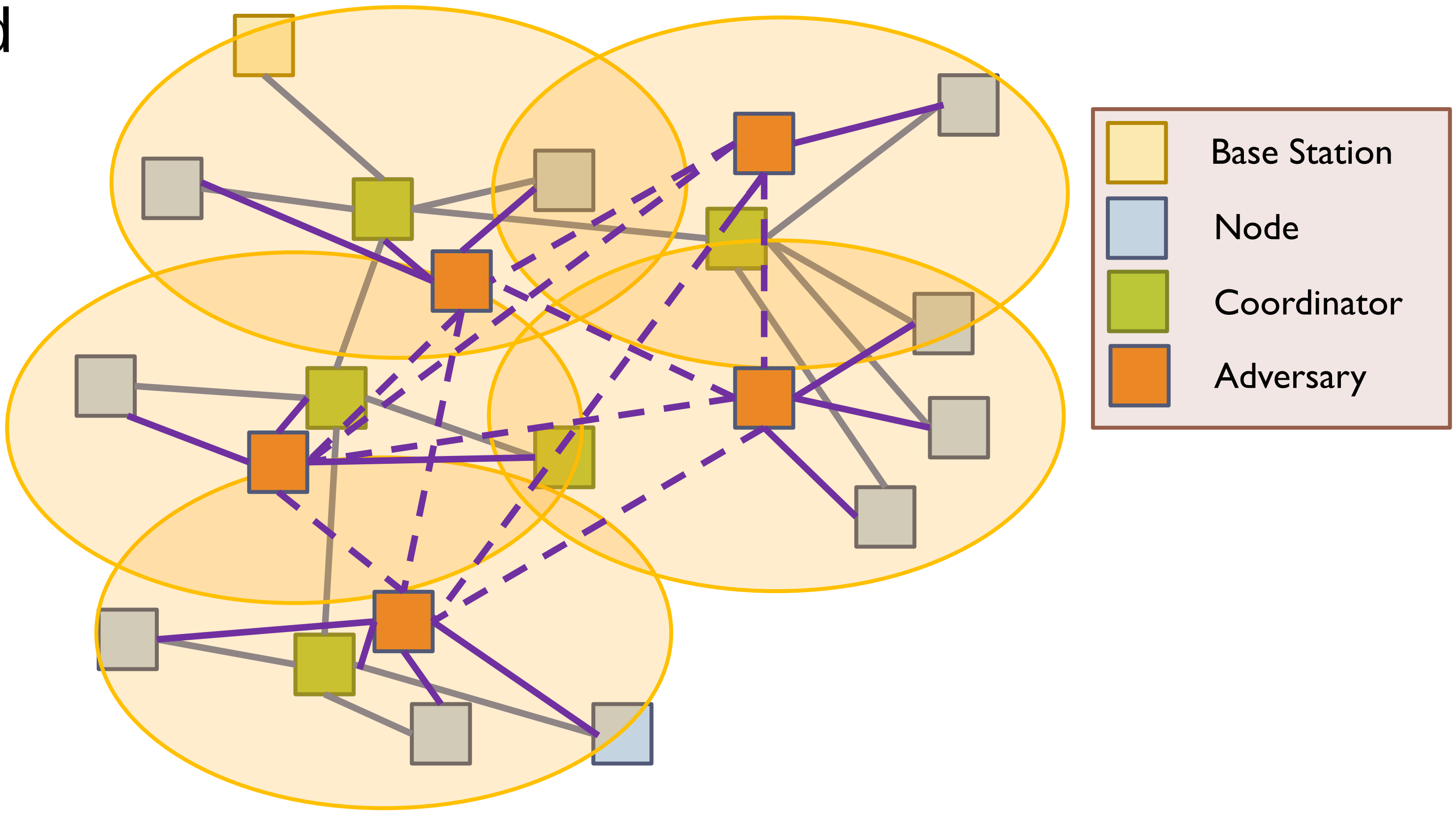
- Eligible to become a coordinator
  - When two of its neighbors cannot reach other directly or via one or two coordinators
  - High utility and energy has prior to become a coordinator

SPAN - Example



SPAN - Attack

- Prevent nodes from becoming coordinators when they should



- To enable a selective forwarding attack, just scale down

Countermeasures

- Outsider attacks and link layer security
- The Sybil attack
- Hello flood attacks
- Wormhole and sinkhole attacks
- Leveraging global knowledge
- Implementation considerations for Sybil attack defenses
- Selective forwarding
- Authenticated broadcast and flooding
- Ultimate limitations of secure multi-hop routing

Outsider Attacks and Link Layer Security

- To prevent the majority of outsider attacks
  - Link layer encryption
  - Authentication mechanisms using a globally shared key
  - Monotonically increasing counter for each link
- Prevents
  - Spoofing, altering, replaying, Sybil attack
  - Selective forwarding, sinkhole attacks
- Not countered
  - Wormhole attacks, HELLO flood attacks
  - Black hole selective forwarding
  - Insider attacks or compromised nodes

The Sybil Attack

- Using a globally shared key allows an insider to masquerade as any node
- To prevent
  - Verify the identities of all nodes
    - All nodes share a unique symmetric key with a trusted base station
    - Two nodes can verify other's identity and establish a shared key
      - Needham-Schroeder protocol
  - Allow the communication with the verified neighbors only
  - Restrict the number of neighbors a node is allowed
- Prevents
  - Sybil Attack, eavesdrop, modify any future communications

HELLO Flood Attacks

- Verify the bi-directionality of a link before taking actions

- To prevent
  - The identity verification protocol is sufficient
    - It verifies the bi-directionality of the link
    - The limitation of the # of neighbors reduces the compromised nodes

Wormhole and Sinkhole Attacks

- Difficult
  - Wormhole: private, out-of-band channel is invisible
  - Sinkhole: advertised information(ex: energy) is hard to verify

- Protocols that construct a topology initiated by a base station are most susceptible

- To prevent
  - Design routing protocols carefully
    ex) Geographic routing protocols

Leveraging Global Knowledge

- When the network size is limited, global knowledge helps the security

- Examples
  - Topology Monitor
    - All nodes report their neighbors to the base station, it can map the topology
    - Nodes report periodically to account for small changes (radio interference or node failure)
    - Drastic or suspicious changes might indicate a node compromised
  - No advertise location (using restricted structure …)
    - If neighbors' locations can be derived easily without advertisement, the fake location is prevented

Implementation Considerations for Sybil Attack Defenses

- How can each node get the unique key from the base station?
  - Flood
    - Denial-of-Service attack is available
  - Increase base station tx power to reach every node in a single hop
    - Used for efficient authenticated end-to-end acknowledgements
    - Global time synchronization

Selective Forwarding

- A compromised node near the source or base station has high chances to launch a selective forwarding attack

- To prevent
  - Multipath routing: route over n paths with completely disjoint
    - Difficult to create
  - Multiple Braided paths: no two consecutive nodes on in common
  - Dynamically choose next hop: reduce the chances of an adversary gaining complete control of a data flow

Authenticated Broadcast and Flooding

- Broadcast and flooding must be authenticated
- **µ**TESLA is suitable
  - Efficient / Authenticated broadcast and flooding
  - Uses only symmetric key cryptography
  - Minimal packet overhead
  - Requires loose time synchronization

- Flooding
  - Robust: it is hard to prevent a message from reaching every nodes
  - High energy cost, potential losses (by collision)
    - SPIN, gossiping algorithms can help the downsides

Ultimate Limitations of Secure Multi-hop Routing

- Near the base stations are attractive for compromise

- To prevent
  - Clustering protocol
    - Cluster-heads communicate directly with the base station
  - Randomly rotating set of virtual base stations
    - A multi-hop topology is constructed using the set
    - Virtual base station communicate directly with the real base station
    - The set should be changed frequently

Conclusion

- Secure routing is vital on sensor networks
- Currently proposed routing protocols are insecure
- Careful protocol design is needed
  - **Mote-class outsiders** can be counteracted easily
    - Link layer encryption
    - Authentication
  - Defense against **laptop-class adversaries** and **insiders** are hard