Secure Routing in Sensor Networks: Attacks and Countermeasures

(Authors: Chris Karlof and David Wagner, UC Berkeley)

Presented By- Meixing Le

Introduction

- Current proposals for routing protocols in sensor networks optimize for limited capabilities of nodes and application specific nature of networks but do not consider security.
- The protocols designed for sensor networks are not designed with security as a goal but security is important.
- Different from conventional networks
  - In network aggregation in WSNs
  - Do not access the content of messages (conventional)
    - Routing Protocol handle message availability
    - End to end security mechanism(SSH, SSL)

Introduction

- Propose security goals for routing in wireless Sensor networks
- Show how certain attacks against Ad-hoc networks and peer-to-peer networks can be adapted into more powerful attacks against sensor networks
- Provide a list of attacks and their countermeasures
- Current protocols are vulnerable to attacks.
- Current sensor routing protocols are designed not for security, but for optimizing the limited resources.
- Design secure routing protocols in WSNs are very difficult.
  - WSNs cannot provide resources available to traditional networks for security.
  - WSN's (system constraints) offer the attacker unique attacks that aren't found in traditional networks.

Contributions

- Propose threat models and security goals for secure routing in wireless sensor networks
- Introduce TWO new classes of Attacks for Sensor networks
  - Sinkhole attacks
  - HELLO flood attacks
- Show how the attacks against Ad-hoc networks and peer-to-peer networks can be adapted into powerful attacks against sensor networks
- Give a thorough security analysis of major routing protocols and energy conservation topology maintenance algorithms for sensor networks
- Discuss countermeasures and design considerations for secure routing protocols

Background

- Sensor Network : Heterogeneous system consisting of tiny sensors and actuators having some computing elements.
- Base Station :
  - Point of centralized control
  - Gateway to another network, powerful data processing unit, or point of human interface
  - More processing capability, memory & power
- Aggregation Point
  - collects sensor readings from surrounding and forwards a single message representing an aggregate of values. These are typically regular sensor nodes.
- POWER constrained environment

Berkeley Mica Mote

- 4MHz 8-bit CPU
- 128KB instruction memory
- 4KB of RAM for data, 512KB flash memory
- 40Kbps, a few dozen meters
- 4.8 mA in receive mode, 12mA in transmit mode, 5uA in sleep mode.
- Power: 2850mA hours.
- Run at full power, two weeks
- Each bit transmitted consumes power as executing 800-1000 instructions
- Will not follow Moore's Law

Background

- Sensor nodes in this paper are considered immobile.
- Sink receives a stream of data from nodes, this stream of data is called data flow.
- Nodes that send data are sources.

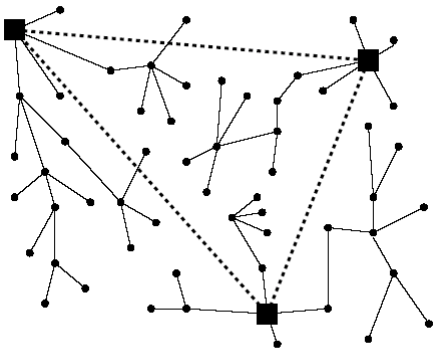


Fig. 3. A representative sensor network architecture.

Sensor Networks VS AD-Hoc Wireless Networks

- They both use multi-hop networking.
- Distinction is that AD-Hoc supports routing between any pair of nodes whereas sensor networks have more specialized communication pattern.
- Most traffic in sensor networks can be of 3 types
  1. Many-to-One- Multiple sensor nodes sends readings to base station of aggregation point.
  2. One-to-Many- A single node typically base station broadcast a message. Query or control information.
  3. Local Communication-Node broadcast or unicast messages to other neighbor nodes.
- Sensor nodes more resource constrained than Ad-hoc nodes.
  - Higher level of trust relationship among sensor nodes : In-network processing, aggregation, duplication elimination

Related Work

- Defense mechanism in developed for ad-hoc networks are not applicable to sensor networks.
- Some Ad-hoc security algorithms are based on Public Key Cryptography which is too costly for sensor networks. Sensor networks use efficient Symmetric Key Cryptography
- Minimizing the effect of misbehaving or selfish nodes: Promising but vulnerable to blackmailers.
- Perrig et al. present two security protocols for sensor networks: SNEP(confidentiality, authentication and freshness between nodes) and uTESLA (provides authenticated broadcast.)

Network Assumption

- Assuming radio links are insecure.
- Attackers can eavesdrop radio transmissions, inject bits and replay previously heard channel.
- Attacker can also deploy some malicious nodes with similar hardware capabilities by purchasing separately or by capturing nodes and physically overwrite.
- Malicious node collude to attack the system
- Sensor nodes are not temper resistant- i.e. adversary compromises a node, she can extract all material, data and code stored in the node.

Trust Requirements

- Base station interface a sensor network to outside world, if significant number of them are compromised it makes entire sensor network useless.
- For this reason we assume base stations are trustworthy.
- Aggregation points may be trusted component in certain protocols.
- Nodes rely on info from aggregation points and trust messages sent to them will be forwarded to the base station.
- Adversary may try to attack Aggregation points as these are nothing but regular sensor nodes so they are not necessarily treated as trustworthy.

Threat Model

- Mote-Class attackers and Laptop-class attackers
- Mote-Class attackers:
  - attackers has access to few sensor nodes.
- Laptop-class attackers:
  - Access to more powerful devices. Have more battery power, better CPU, sensitive antenna, powerful radio Tx, etc
  - can do more damage, can jam radio link in immediate vicinity. It can eavesdrop the entire network.
- Outside attacks & Inside attacks:
  - Outside attacks : attacker external to the network, Mote, Laptop
  - Inside attacks : Authorized node in the network is malicious/ compromised

Security Goals

- Reliable message delivery (one to one) is main concern in routing protocols but this is not the case in Sensor Networks as routing can be many to one.
- In the presence of outsider adversaries:
  - Link layer security mechanisms integrity, authenticity, availability of messages
- In the presence of insider adversaries:
  - Link layer security mechanisms are not enough. Not all of these goals are not fully attainable.
- It is difficult to guarantee integrity, authenticity and confidentiality.
  - The goal of secure routing protocol is to guarantee integrity, authenticity, availability of messages in presence of adversaries

Security Goals

- Data confidentiality
  - Data cannot be reached by outsider
- Data authentication
  - Receiver ensures the data received from a trusted source.
- Data integrity
  - Data is not altered in transition
- Data freshness
  - Not the replayed old message

Attacks On Sensor Networking Protocols

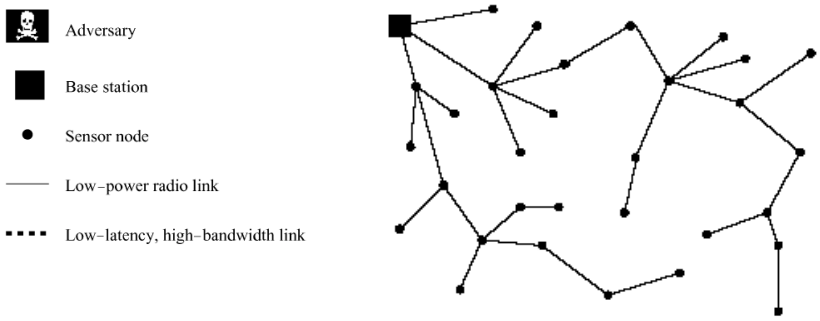
- Most network layer attack in sensor networks fall into one of the following categories

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

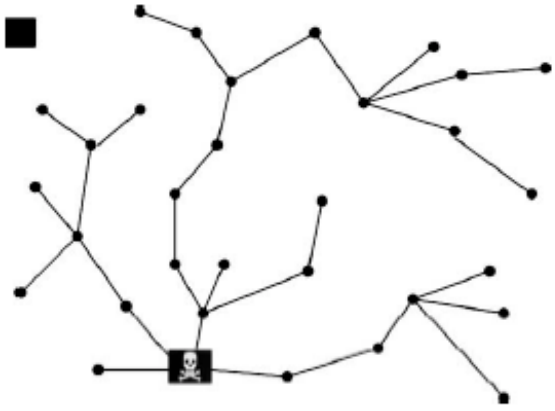
Spoofed, altered, replayed routing information

- Def: Attack against the routing information exchanged between nodes.
- Actions:
  - spoofing,
  - altering,
  - replaying routing information.
- Consequences:
  - create routing loop,
  - attract or repel traffic,
  - extend or shorten source routes,
  - generate false error messages,
  - partition the network,

Example WSN Topology before Attacks

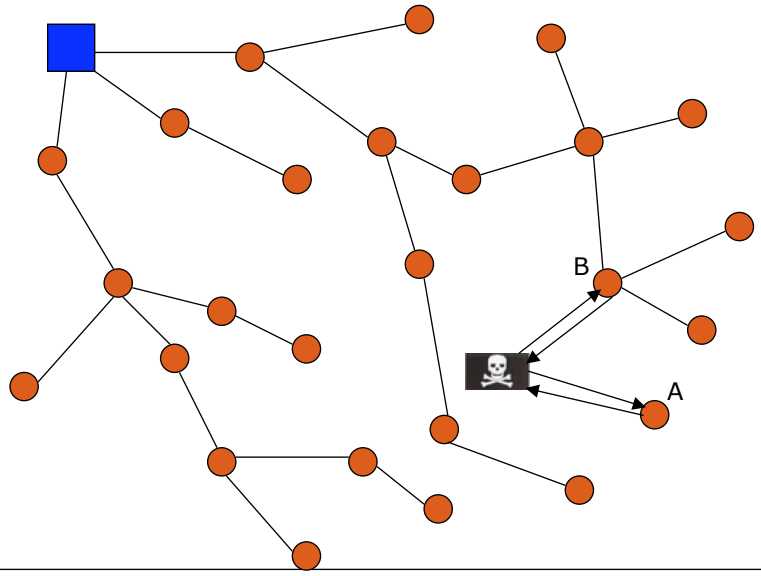


Bogus Routing Information Attack in TinyOS Beaconing

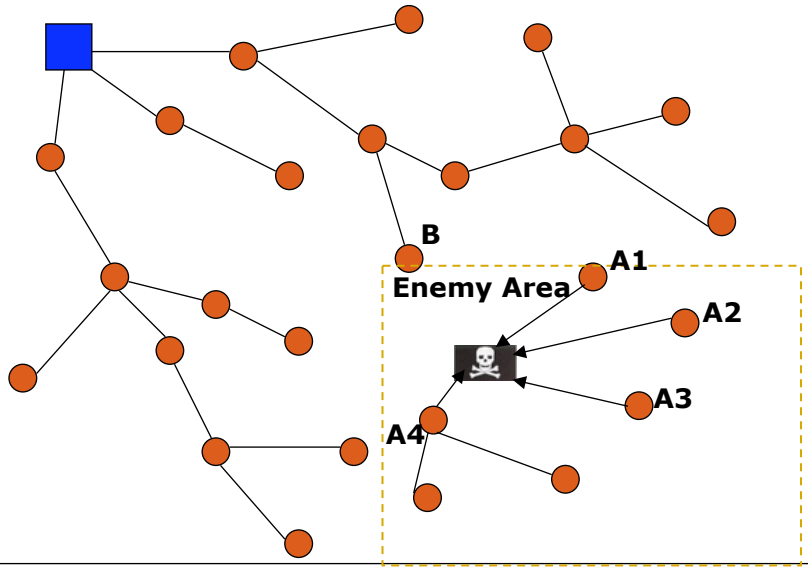


E.g. An adversary **spoofing and replaying** a routing update from a base station in TinyOS beaconing.

Bogus Routing Information Causing Routing Loops



Using Bogus Routing Information to Attracts/Repels Traffic



Attack 2: Selective Forwarding (1)

- Def: Malicious nodes try to stop the propagation of certain messages.
- Condition 1: Adversaries are on the path of a flow.
- Actions:
  - Black hole, drop every packet.
  - refuse forwarding certain messages,
  - drop certain messages,
  - suppressing or modifying packets from a selected few other good nodes.
- Features: Adversaries attempt to follow the path of least resistance and to include itself on the actual data path flow.

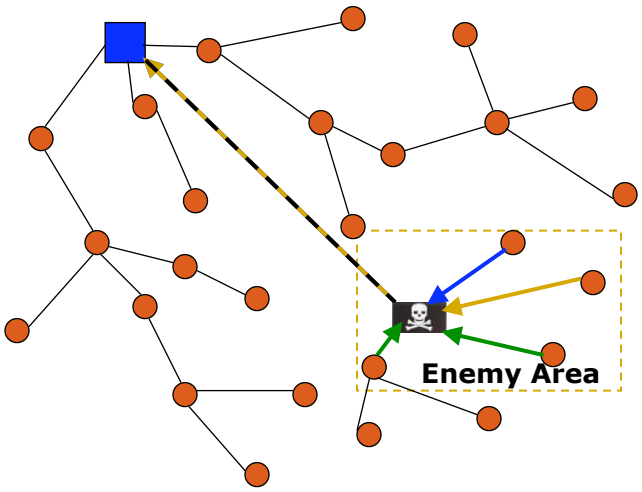
Attack 2: Selective Forwarding (2)

- Condition 2: Adversaries overhear a flow.
- Actions:
  - Jam or cause collision on each forwarded packet.
- Consequences:
  - Suppress certain messages.
  - More tricky.

Attack 3: Sinkhole Attack, a Special Selective Forwarding Attack

- Def: Adversaries lure nearly all traffic from a particular area through a compromised node. Thereby creating sinkhole with adversary at the center.
- Actions:
  - Tamper with application data along the packet flow path. (selective forwarding)
  - Making a compromised node look especially attractive to surrounding nodes.
  - Sending out strong signals with low latencies.
  - Laptop class adversary provide a high quality route to base station by transmitting at high power
  - creating a wormhole using wormhole attack.
- Consequences: Suppressed messages in a certain area.
- Motivation: To enable selective forwarding.

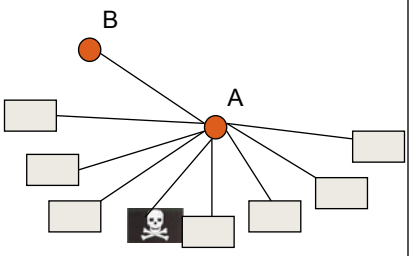
Example of Selective Forwarding/ Sinkhole



CSCE990 - UNL, Fall 2004,
mli@cse.unl.edu

Attack4: The Sybil Attack

- Def: A single node forges multiple identities.
- Geographic routing is very susceptible – exchange of locality information. A set of nodes instead of one.
- Actions:
  - Having a set of faulty entities.
- Overall Effects:
  - Reduces the efficiency of fault-tolerant schemes, such as distributed storage, dispersity and multipath routing, topology maintenance, and etc.

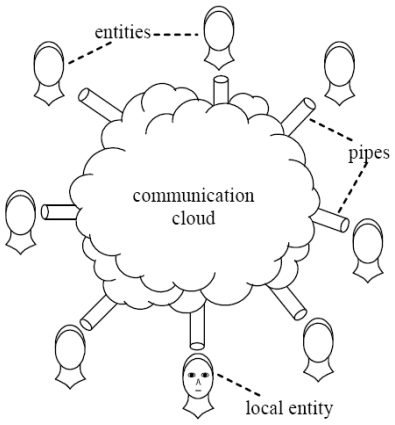


Attacks on sensor network routing cont'd

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]

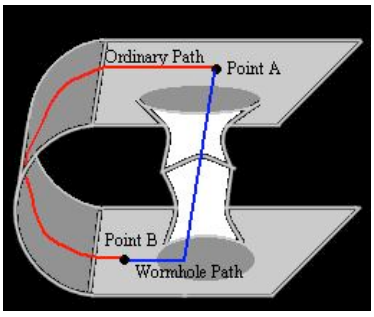
Attack 5: Wormhole Attack

- Def: Adversaries tunnel messages over alternative low-latency links and replay them in a different part of the network.
- Actions:
  - An attacker locates between two nodes and forwards messages between them.
  - Two distant malicious nodes understate their distance. To convince the faraway nodes that they are just one or two hops away from the base station.
- Consequences:
  - Exploits routing race conditions
  - Enables other attacks (eg: create sinkhole)
  - Convince two distant nodes that they are neighbors
  - Combine with selective forwarding or eavesdropping

Attack 5: Wormhole Attack

Wormhole

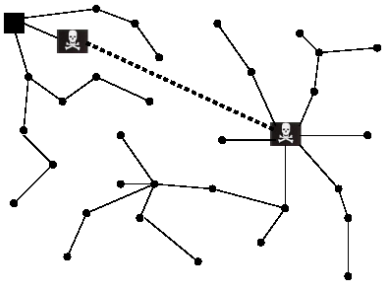
An adversary tunnels packets received in one part of the network over a low-latency link and replays them in a different part of the network



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

Attack 5: Wormhole Attack

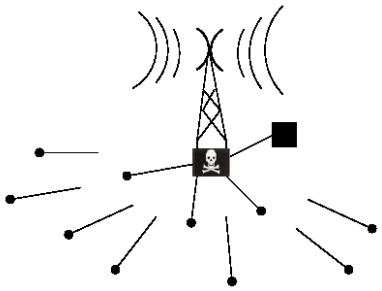
- Adversary creates two wormholes one near Base Station and one near targeted area.
- The first forward routing update to second which rebroadcast to targeted area.



Attack 6: HELLO floods

- Def: An attacker sends or replays a routing protocol's HELLO packets with more energy.
- Attacks on protocols that use HELLO packets to announce to neighbors.
  - These protocols assume that the sender of a received packet is within normal radio range.
- Can be launched by insiders and outsiders.
- Effects:
  - Attract a lot of nodes to use the forged high-quality routes.
  - Leave these nodes sufficiently far away form the attacker sending packets into oblivion.
  - The network is at a state of confusion.

After HELLO Flood Attack

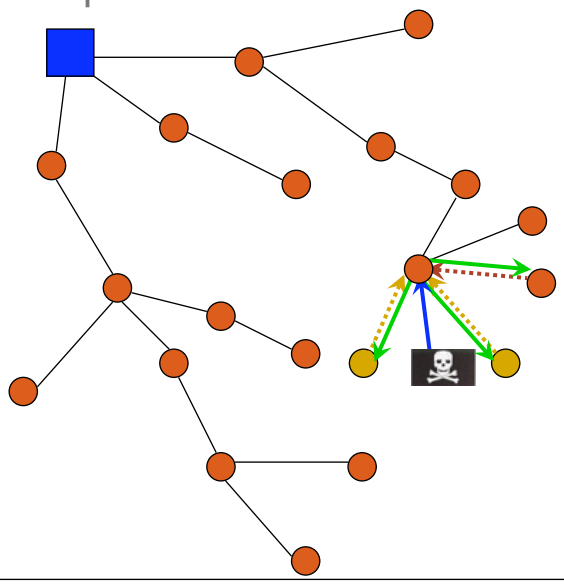


HELLO flood attack against TinyOS beaconing

Attack 7: Acknowledgement Spoofing

- Def: Spoof link layer acknowledgement to trick other nodes to believe that a link or node is either dead (actually alive) or alive (actually dead).
- Attacks on protocols that relay on link layer acknowledgement.
- Actions:
  - Spoof link layer ACK packets of neighbor nodes.
  - Selective forwarding by encouraging sender to send via weak links.
- Effects:
  - Convince the sender that a weak link is strong.
  - Convince the sender that a dead or disabled node is alive.
  - Can mount a selective forwarding attack.

Attack 7: Acknowledgement Spoofing Example

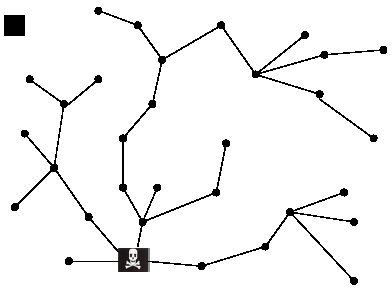


Vulnerability of Current Routing Protocols

Attack	TinyOS	Directed Diff	Geographic Routing	Min Cost Fwding	Cluster Based	Rumor Routing	Energy Conserving
Bogus routing	X	X	X	X		X	X
Selective forwarding	X	X	X	X	X	X	
Sinkholes	X	X		X		X	
Sybil	X	X	X			X	X
Wormholes	X	X		X		X	
HELLO floods	X	X		X	X		X

Attacks on specific sensor network protocols

- TinyOS beaconing
  - It constructs a 'Breadth first' spanning tree rooted at the base station
  - Base station periodically broadcast route updates
  - Marking parent from who they receive the first update during current time interval.
  - Packets travel through the paths along tree



Attacks

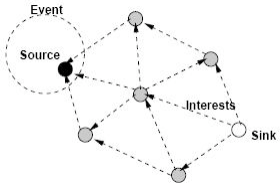
- Unauthenticated route updates
  - Malicious node acts as base station
- Authenticated route updates
  - Prevent claiming base station
  - Two colluding nodes (laptop-class attacker) form wormhole to direct all traffic through them
    - One near base station, one near target area.
    - The link is much faster than the normally links.
  - Laptop-class attacker which is powerful transmitter use HELLO flood attack
    - every node marks attacker as parent
    - Majority node send packets into oblivion.
    - One node realize this has few options
  - Mote-class attacker can cause 'Routing loops' between two nodes
    - Forge routing update indicating A is the parent of B

Directed Diffusion

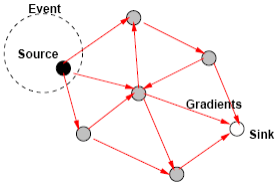
- Protocol description:
  - Data-centric routing algorithm drawing information out of a sensor network
  - Base station send the 'named' data which is flooded as 'interests' throughout the network
  - 'Gradients' are set up to 'draw' events (data matching the interests)
  - Base station positively reinforces high data rates paths
  - There's a multipath variant of directed diffusion

Attacks on specific sensor network protocols cont'd

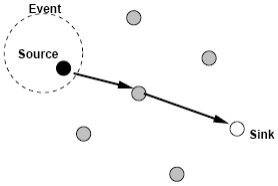
- Directed diffusion



Interest propagation



Initial gradients set up



Data delivery along reinforced path

Pictures from [6]

Attacks

- Difficult for attackers to prevent interests from reaching targets able to satisfy them.
- When sources begin to generate data events, attack a data flow in four goals:
- Suppression
  - Denial of service, spoof negative reinforcements.
- Cloning
  - Enable eavesdropping
  - Adversary receives an interest from BS, replay that interest with herself as base station, events will send to both
- Path influence
  - Spoofing positive and negative reinforcement, bogus event
  - Change the path, put herself on the path of a data flow
- Selective forwarding and data tampering
  - With above attacks, adversary gain control of the flow

Attacks

- Laptop class adversary creating a wormhole
  - A next to base station, broadcast spoof negative reinforcement to surrounding nodes
  - B close to where events are generated, attract data flow by spoofing strong positive reinforcement to neighbors
  - Interests are sent by wormhole and rebroadcast by B
  - Push data flows away from base station and towards the resulting sinkhole centered at node B
- Multipath version
  - More robust
  - Adversary use Sybil attack against her neighbors

Geographic routing

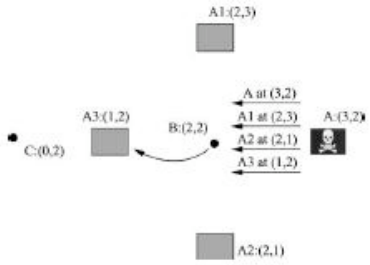
- Leverage nodes' positions & explicit geographic packet destinations to efficiently disseminate queries and route updates
- GPSR (Greedy Perimeter Stateless Routing)
  - Greedy forwarding at each hop, routing packet to the neighbor closest to the destination.
  - Drawback: a single flow will always use the same nodes ,Uneven energy consuming
- GEAR (Geographic and Energy Aware Routing)
  - Remedy the problem, choose next hop by remaining energy and distance from the target.
- Require exchange of location information
  - Except well structured topologies(grid)

Attacks

- Location information can be misrepresented
- Regardless of actual location, advertise spoof location information, place herself on the path of a data flow
- GEAR: advertise maximum energy
- Adversary forge location advertisements creating routing loops
- Two figures

Attacks

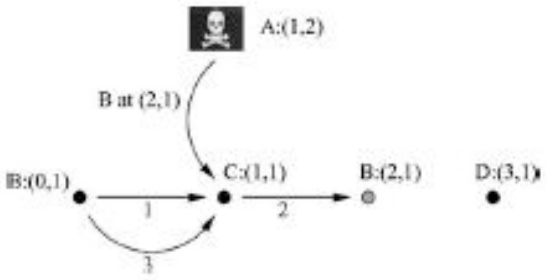
- Geographic routing
  - Attacks
    - Sybil attack



Picture from [7]

Attacks

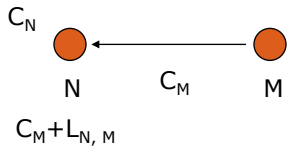
- Attacks
  - Creating routing loops in GPSR



Picture from 7

Minimum cost forwarding

- Two nodes M, N. M will send a message to N that its cost is
- C(M)+L(N, M). N compares this with C(N).
- If C(N)<C(M)+L(N, M) then N sets its new cost as C(N) =C(M)+L(N, M) and broadcast declaring its new cost.
- In essence this is distributed shortest-paths algorithms.
- Message initiated by a source contain cost budget which is the minimum cost. At each hop, link cost is subtracted from the budget.



Attacks

- Susceptible to sinkhole attacks
  - Mote-class: Advertising cost zero
  - Laptop-class: use wormhole to synchronize the attack
- HELLO flood attack
  - Laptop class: advertising cost zero powerful enough to be received by every node in the network.
  - The adversary will be the sole destination of messages from nodes within radio range, nodes outside radio range are stranded

LEACH: low-energy adaptive clustering hierarchy

- Nodes organized into clusters with one node serving as a cluster-head
- Nodes send data to cluster heads
- Cluster-heads aggregate data for transmission to a base station
- Randomized rotation of cluster heads to evenly distribute energy consumption.
- Set up phase
  - Each node decide whether or not to be a head based on its energy and the global desired percentage of heads
  - Broadcast intention, non head nodes pick one cluster
- Steady state
  - Heads wait to receive data in its cluster, and send them

Attacks

- Choosing head based on received signal strength, laptop class adversary using HELLO flood attack.
- Adversary will be the only head, selective forwarding, rest of the network disabled
- Can be applied in a small number of nodes
- Simple countermeasure:
  - Refuse to use same heads in consecutive rounds
  - Random select head instead of the signal strength
- Sybil attack can defeat the countermeasures
- Hierarchical cases: attack against top-most layer cluster

Rumor routing

- Probabilistic protocol for matching queries with events
- When a source observes an event, sends an agent on a random walk through the network.
- Agent: list of events, next hop on path, corresponding hop counts, time to live(TTL), list of visited nodes.
- Arriving a new node, exchange their knowledge of the data events, decrements TTL
- Base station also create an agent in similar way to query data
- A route from base station to a source is established when a query agent arrive a node traversed by event agent which satisfied the query.

Attacks

- Establishment of routing depends on properly handling agents
- Adversary mount Dos attack by removing event information carried by the agent or refusing to forward agents. Information in the agents can also be changed
- Mote-class:
  - create a sinkhole by extending tendrils in all directions. Forward multiple copies of the received agents, maximize the chance on the path of a flow.
  - TTL is set to maximum, hop counts reset to zero
  - Count set to zero can turn other agents information

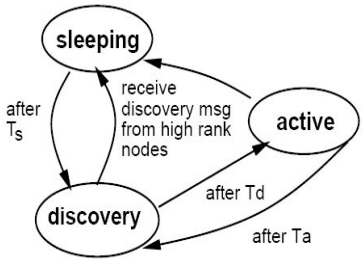
Attacks

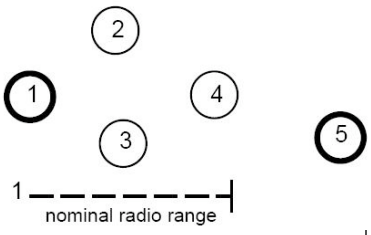
- Laptop-class:
  - Create a wormhole, one node near source and the other node near base station.
  - Using Sybil attack to maximize the chance of being chosen.
  - Queries match the events quickly via wormhole
  - Can add selective forwarding attack

Energy conserving topology maintenance

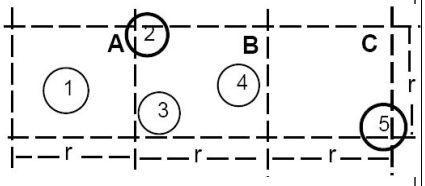
- Add more nodes than needed to extend network lifetime
  - Geographic Adaptive Fidelity (GAF)

State transitions





Node redundancy



GAF

- Virtual grid squares, according to geographic location and expected radio range
- Three states: sleeping, discovery, active.
- active node participate in routing
- Discovery nodes probe to decide active or not
- Sleeping node turn radio off
- Nodes are ranked with respect to current state and expected lifetime
- Discovery messages are used to exchange state
- Attempt to reach a state each grid has only one active

Attacks

- Nodes receive a discovery message from higher rank will transition to sleeping. After some time to wake up and back to discovery
- Disable other nodes in her grid by broadcasting high rank discovery message. Can add selective forwarding
- Laptop class can disable whole network,
- Sybil attack & HELLO flood attack, broadcasting high rank discovery message from a non existing node in each grid
- Frequently do it, keep the entire network sleeping

SPAN

- Nodes decide to sleep or be coordinators.
- Power saving node periodically send and receive HELLO message to decide become a coordinator.
- HELLO message: current status, current coordinators, current neighbors
- Node becomes eligible to be a coordinator if two of its neighbors can't reach other directly or via one or two coordinators
- Such nodes send announcement with delay.
- Delay is based on the function of utility and energy.
- After some time, announce intention to withdraw.

Attacks

- Laptop-class adversary prevent nodes from becoming coordinators when they should
- Partition the area into cells
- For each cell, there's a bogus coordinator
- Broadcast powerful HELLO messages
- All the node in the cell and other bogus coordinator are its neighbors.
- Other nodes choose the bogus coordinator to routing
- No real nodes works in the routing
- Selective forwarding, compromise a small area

Countermeasures

- Outsider attacks and link layer security
  - Shared key and link layer encryption
  - Outside attacks can be prevented by simple link layer encryption and authentication using a globally shared key.
  - Sybil attack won't work because attacker should know the global key to participate.
  - Similarly selective forwarding and sinkhole attacks are not possible because the key is necessary which attacker do not know.
  - Ineffective against Wormhole, Hello floods attacks
  - Completely ineffective in the presence of insider attacks
    - Bogus routing information
    - Create sinkholes
    - Selectively forward packets
    - Sybil attacks
    - HELLO floods

countermeasures

- Countermeasure to Insider Sybil attacks
  - Every node shares a unique symmetric key with the base station
  - A pair of neighbor nodes use the resulting key to implement an authenticated, encrypted link between them. (Pairwise Key)
  - Base station limit the number of neighbors a node is allowed to have – prevent an insider attacker establishing shared keys with every node in the network.
- Not perfect
  - Malicious nodes can still communicating with its verified neighbors
  - wormhole attack by create an artificial link between two nodes to convince them they are neighbors

Countermeasures

- Countermeasure to HELLO flood attacks
  - Verify the bidirectionality of the link between two nodes
- Less effective if the adversary have highly sensitive receivers as well as powerful transmitter.
- Every node authenticate each of its neighbors with an identity verification protocol using base station
  - The compromised node has to authenticate itself to a lot of nodes
  - Base station can detect the HELLO flood

Countermeasures

- Wormhole and Sinkhole attacks
  - These are very difficult to defend especially when used in combination.
  - Protocols that construct a topology initiated by a base station are the most vulnerable
  - Geographic routing protocol can be one solution to defend these attacks because topology in geographic protocol is constructed using localized interaction.

Countermeasures

- Leveraging global knowledge
  - Global knowledge can be leveraged in security mechanism
  - Geographical Routing protocols.
    - Problems: How to get the location information – attackers may disseminate spoofed location information
    - Solution: Restrict the structure of topology to eliminate the need for location information by the node. Use fixed topology like square, triangular or Hex Grid structure. However, it also restrict its application.

Countermeasures

- Selective Forwarding
  - Node has great chance to be on the flow, and close to source or base station is most likely to launch
  - Multipath routing can be used to counter these types of selective forwarding attacks.
  - Messages routed over n paths whose nodes are completely disjoint are completely protected against selective forwarding.
  - Allowing nodes dynamically choose a packet's next hop from a set of possible candidates.

Countermeasures

- Authenticate Broadcast and flooding
  - Base station is trustworthy.
  - Adversaries must not be able to spoof broadcast or flooded messages from any base station.
  - HELLO message from neighbor nodes should be authenticated and impossible to spoof.
- Attention: public key cryptography and digital signatures is beyond the capabilities of sensor.
- μTESLA protocol to prevent replay of broadcast messages issued by the base station
  - Replay is prevented because messages authenticated with previously disclosed keys are ignored

Countermeasure Summary

- Link layer encryption and authentication, multipath routing, identity verification, bidirectional link verification and authenticated broadcast can protect against outsiders, bogus routing information, Sybil attacks, HELLO floods, and acknowledgement spoofing.
- Sinkhole and Wormhole pose significant challenges to protocol design. It unlikely exists countermeasures against these attacks if the protocol design is completed.
- Geographic routing protocols are one class of protocols that holds promise against these.

Conclusion

- Secure routing is vital to the acceptance and use of sensor networks for many application. Link layer encryption and authentication mechanism may be reasonable first approximation for defense.

THANKS

HAVE A NICE DAY

QUESTIONS ?