Secure routing in Wireless sensor Networks: Attacks and Countermeasures

AUTHORS: CHRIS KARLOF AND DAVID WAGNER

UNIVERSITY OF CALIFORNIA AT BERKELEY, BERKELEY, CA 94720, USA

PRESENTED BY CHUNG TRAN

Outline

- Introduction
- Background
- Sensory Network vs. ad-hoc wireless network
- Related Work
- Problem Statement
- Attack on Sensor network routing
- Attacks on specific sensor network protocols
- Countermeasures
- Ultimate limitations of Secure multihop routing
- Conclusion
- Comments

Introduction

- Focus on routing security in wireless sensor networks.
- Current proposals for routing protocols in sensor networks optimize for the limited capabilities of the nodes and the application specific nature of the networks, but does not consider security
- When this paper was written they consider that security is something they can design after the maintain the limited resources of the sensor networks been in place

Authors Contributions

- Authors five main contributions
  1. Propose threat models and security goals for secure routing in wireless sensor networks
  2. Introduce and document attacks against sensor network
     i. Sinkhole
     ii. HELLO floods
  3. Show how attack work for ad-hoc wireless network and peer-to-peer and adapt for sensor network
  4. Analysis of major routing protocols and energy conserving topology maintenance algorithms for sensor networks. Summary in Fig.1
  5. We discuss countermeasures and design considerations for secure routing protocols in sensor networks

Figure 1

Protocol	Relevant attacks
TinyOS beaconing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Directed diffusion and its multipath variant	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Geographic routing (GPSR, GEAR)	Bogus routing information, selective forwarding, Sybil
Minimum cost forwarding	Bogus routing information, selective forwarding, sinkholes, wormholes, HELLO floods
Clustering based protocols (LEACH, TEEN, PEGASIS)	Selective forwarding, HELLO floods
Rumor routing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes
Energy conserving topology maintenance (SPAN, GAF, CEC, AFECA)	Bogus routing information, Sybil, HELLO floods

Fig. 1. Summary of attacks against proposed sensor networks routing protocols.

Background

- **Sensor network**: refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements.
- **Hardware**: Berkeley TinyOS
  - Small(several cubic inch) sensor/actuator unit with a CPU, power source, radio, and several optional sensing elements
  - Processor: 4 MHz 8-bit Atmel ATMEGA 103 CPU with 128 KB of instruction memory, 4KB of RAM for data and 512 KB of flash memory
  - 5.5 mA when active, two orders of magnitude less power when sleeping
  - Radio 916 MHz low-power radio from RFM, 40 Kbps bandwidth range few dozen meters, consume 4.8 mA receive mode, 12 mA in transmit mode, 5μA in sleep mode
  - Two AA batteries provide 2850 mA h at 3 V

Background

- Base Station: is typically a gateway to another network, a powerful data processing or storage center or access point for human interface
  - Can request a steady stream of data, such as a sensor reading every second. This is refer to as a data stream
  - If all of the nodes are require to do this then they will never be able to go to sleep mode to conserve power. Therefore, an access points are created.
  - Access point are often time where 1 node relate and send such information to the base station from all surrounding neighbors. So in sensor network there maybe many of these. This allow it neighbor more time to spend in sleep mode to conserve power.

Figure 2

Adversary

Base station

Sensor node

Low–power radio link

Low latency, high bandwidth link

Fig. 2. **Sensor network legend.** All nodes may use low power radio links, but only laptop-class adversaries and base stations can use low latency, high bandwidth links.

Figure 3

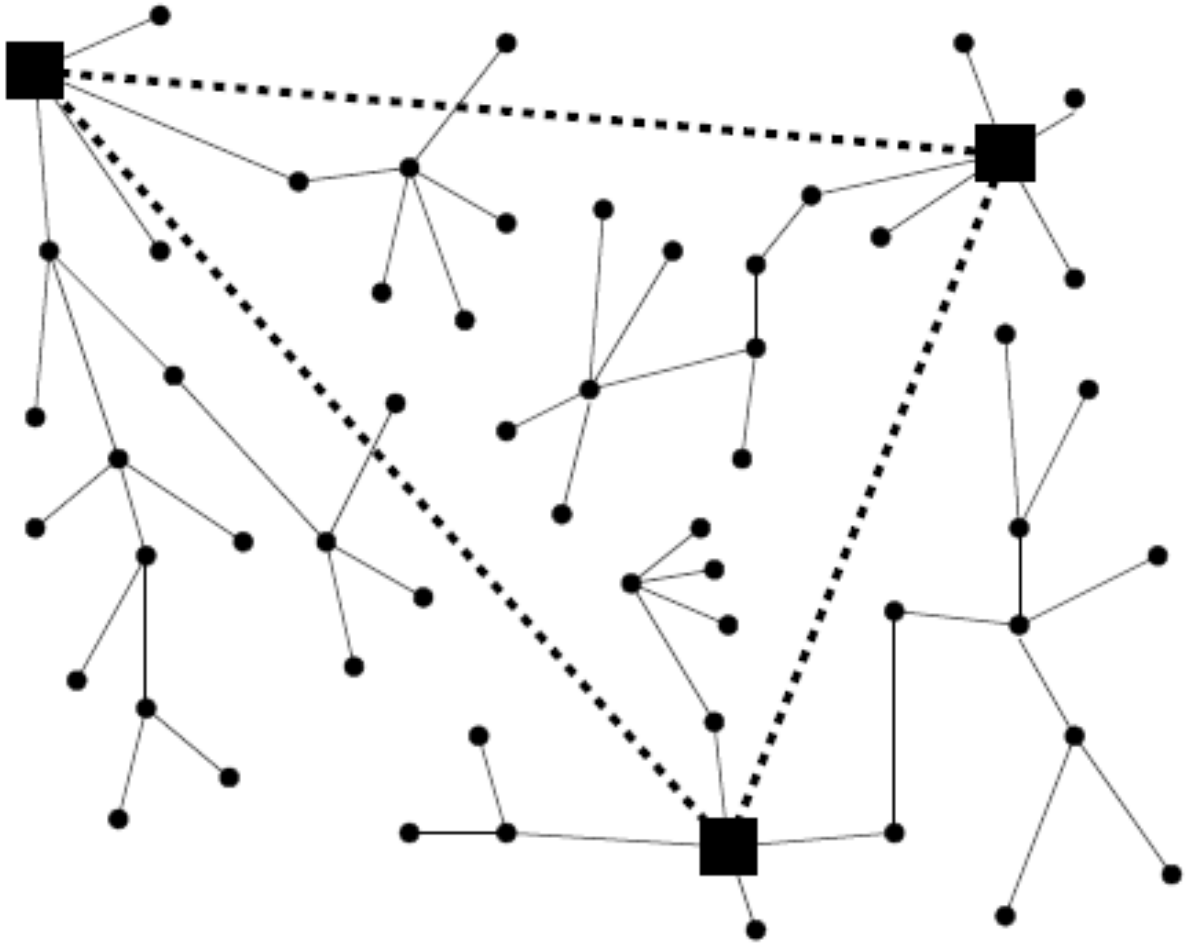

Fig. 3. A representative sensor network architecture.

Resources limitation

- A Berkeley Mica running on active mode will last for about two weeks. In order for it to last a year it need to run at 1% or less of a duty cycle. This is still the scarcest resources so design of sensor network often time would focus on this
- Memory is also a limited resource with only 4KB of RAM so this limit security that can be build into sensor network

Sensor Network vs. Ad-Hoc Wireless Network

- Ad-hoc and Sensor network but are dominated by the fact they uses multihop networking to communicate
- Some major differences;
  - Ad-Hoc network typically support routing between any pair of nodes whereas sensor networks have a more specialized communication pattern, here are some way sensor network communicate
    - Many-to-one: Multiple sensor nodes send sensor readings to a base station or aggregation point in the network
    - One-to-many: a Single node(base station) multicasts to several sensor nodes
    - Local Communication: Neighboring nodes send localized messages to discover and coordinate with each other. A node may boardcast message intended to a received by all neighboring nodes or unicast messages intended for a single neighbor

Related work

- Because of the limitation of sensor networks they cannot adopt ad-hoc security and uses it. The paper point out in ad-hoc they would uses public key cryptography, but with sensor node having such limited memory constrain that would be impossible so it rely exclusively on efficient symmetric key cryptography
- Symmetric key cryptography are based on source routing or distance vector protocols and are unsuitable for sensor networks
  - Too expensive in term of node state and packet overhead and it base on communication between a pair of node—not how sensor node communication protocols

Related work (continue)

- Some studies propose of dealing with misbehavior or selfish node through negative actions such as punishment, reporting, and holding grudge. The authors said this might work but it vulnerable to blackmailers. I have no idea what this mean, but this propose way to maintenance sensor node seems very bias. I just want to say here that the authors seems very bias against women. All the attackers from the article are refer to as her(feminine)
- Authors mention Perrig researches into this area and Perrig came up with SNEP and µTESLA.
  - SNEP provide confidentiality, authentication, and freshness between nodes and the sink
  - µTESLA provides Authenticated broadcast

Problem Statement

- Network Assumptions
- Trust requirements
- Threat models
- Security Goals

Network Assumptions

- Wireless communication mean radio links are insecure.
- Attackers can eavesdrop on our radio transmissions, inject bits into the channel, and replay previously overhead packets.
- Since the defender can deploy many sensor nodes, the adversary can do the same either buy purchasing with the same hardware capacity or by turning some node that was deploy. Once the adversary done this the node become a malicious node and be working for the adversary against the defender
- Sensor nodes are design to be cheap and easy to deploy so they are not design to have tamper proof. You can of course buy some model that are tamper proof, but that would defeat the inexpensive cost of sensor nodes

MAC and Physical Layer: Direct Attack

- MAC protocol using Clear-to-send/receive-to-send(CTS/RTS) frames, adversaries can send frequent CTS frames with long "duration" fields, effectively preventing other nodes from using the channel.
- MAC using randomized backoff are susceptible to attack if node have poor entropy management or predictable pseudo-random number generation. Adversary can predict the backoff time and can cause long backoff times or collisions
- Physical Layer just uses a radio jam, by transmitting without stop

Trust requirement

- Base Station are assume to be trustworthy because if too many does not work the whole communication with outside world will stop
- However Access point are not consider trustworthy. They are often just simple node that was elected to communicate with the Base Station so they can be compromise. We mention when we said an adversary can either deploy their own node or change a node.

Threat Models

- Mote versus laptop attackers
- With Mote-class attacker they have the same kind of node as the sensor network and not able to do much
- However, with a laptop they can do much more and we will see this in later attack on well known algorithm
- There are 2 type of attacks; outside versus inside
- Outside attack have no special access to the sensor network
- Insider attack is often someone who been given authorization and have access

Security goals

- Is to guarantee the network is working properly
  - It must have confidentiality
  - Integrity
  - Authenticity
  - Availability of all messages in the presence of resourceful adversary

  The question is where does the security need to be focus when we working with sensor network; Application layer, Link Layers, or others

  With outside Adversaries Link Layer is the best it will deny outsiders access to the network. However, with insiders Link Layer is not enough. So the authors propose security be build into the routing protocols

Attacks on sensor network routing

- Here is a list of type of attacks
  - Select forwarding
  - Sinkhole attacks
  - Sybil attacks
  - Wormholes
  - HELLO flood attacks
  - Acknowledgement spoofing

Spoofed, altered, or replayed routing information

- Target routing information being exchange between nodes
  - Route loop
  - Attract or repel network traffic
  - Extend or shorten source routes
  - Generate false error messages
  - Partition the newwork
  - Increase end-to-end latency
  - etc

Selective Forwarding

- Malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further
- Black hole-one form of selective forwarding where no packets are forward and all packets are drop, neighbor might just ignore this node and route around it
- A more subtle approach is to suppress or modify packets origination from a few nodes and forward the rest to keep from detection
- Best to make sure it on a path that well uses so the adversary can just put selective forwarding on the path to cause malicious intention

Sinkhole Attacks

- Lure all of nearby nodes to compromised node creating a sinkhole where the adversary have all the data
- Sinkhole are often uses in conjunction with other attacks to create much more devastating attack on the network
- Combine this with a laptop and wormhole attack an adversary can cause the whole sensor network to tunnel all data stream to it
- We will see further example of this when we example some of the attacks later
- This in my opinion is the dangerous form of attack in sensor network because it can combine well with any of the other attack and sensor network can be completely compromise

Sybil Attack

- Name taking from a book call Sybil, in the book the woman have multiple personality it base on a case study
- Sybil attack is where a node can represent multiple identities to other node in the network
- It can broadcast that it closest to the Base station and all traffic will flow through it
- With Sybil attack it able to broadcast so many identities change the architect of sensor network

Wormholes

- The Adversary tunnels messages received in one part of the network over a law-latency link and replays them in a different part
- Simplest instance of this attack is a single node situated between two other odes forwarding messages between the two of them
- Basically in a wormhole attach the adversary make other nodes think their nodes is shortcut to the base station so traffic will be routed through their node
- Uses against route race conditions where the sensor node are instructed to find the shortest route to the base station
- When uses with Sybil attack detection can be almost impossible

HELLO flood attack

- In Sensor network node need to send out HELLO packets to tell it neighbor that it still there so traffic can goes through it
- With a laptop an adversary can broadcast this HELLO message and all nodes in the sensor network might believe that the closest hop it through the laptop. The laptop does not need to be the closest but with enough signal strength it can fool all the other nodes to believe so and send all packets through the laptop
- Let say a node might realize that an adversary have done this still it left with very few options because it neighbors might have not realize this and if any packets was to forward to them will still end up at the laptop

Attacks on specific sensor network protocols

- TInyOS beaconing
- Directed Diffusion
- Geographic routing
- Minimum cost forwarding
- LEACH
- Rumor Routing
- Energy conserving topology maintenance
- GAF
- SPAN

TinyOS Beaconing

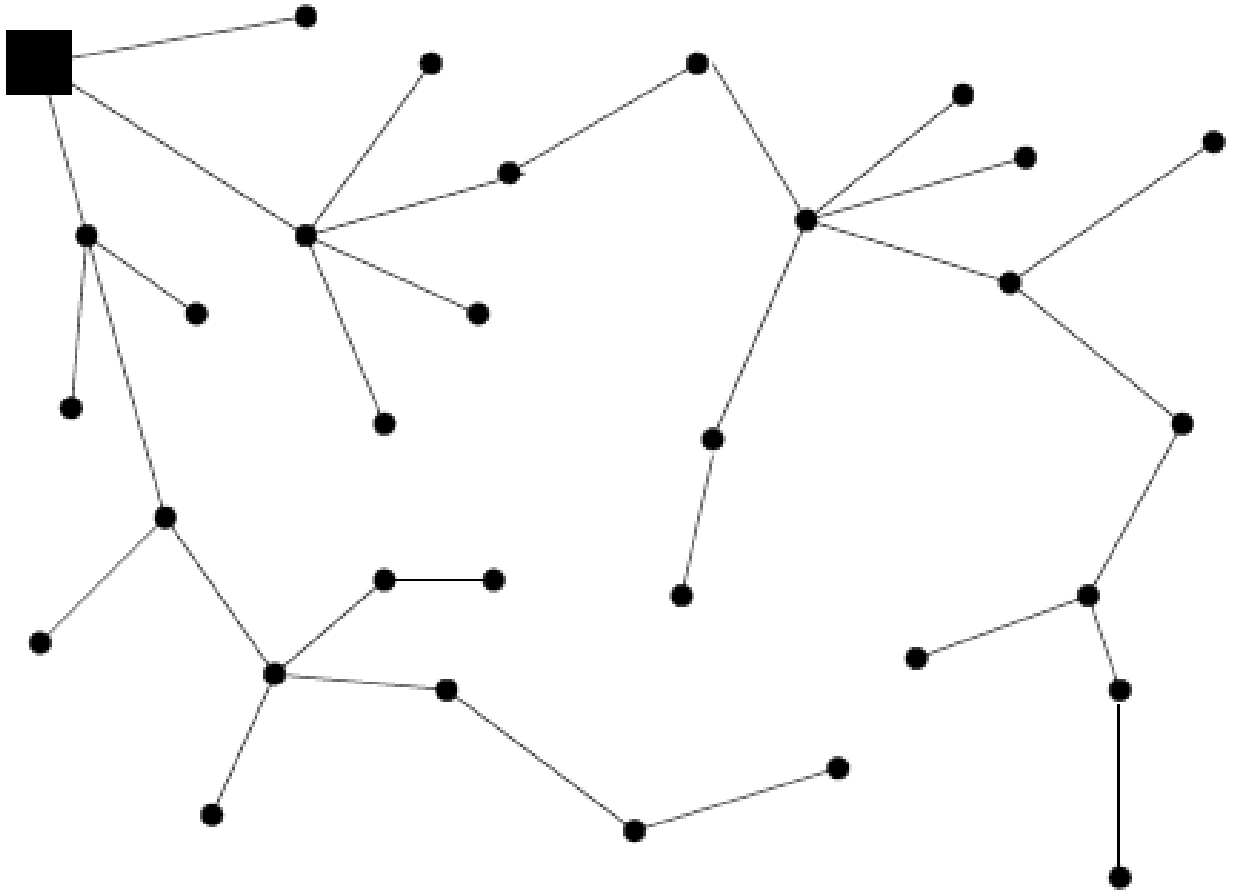

Fig. 4. A representative topology constructed using TinyOS beaconing with a single base station.

TinyOS Beaconing

- Constructs a breadth first spanning tree rooted at a base station
- Periodically the base station broadcasts a route update
- As the broadcast get updated at each node it will send it to it children so they can update it as well

TinyOS Beaconing attack

- Since it not authenticated this can be attack quite easily
- The idea is where the adversary from the figure will begin by broadcasting itself as the parent(base station)
- Once it reach the nodes they will begin to form a spanning tree around the adversary node and will cut itself off from the original base station. This can be done with spoofing
- They can achieve a lost in oblivion by using HELLO flood attack
- Let us take a look at some of these attacks

TinyOS Beaconing attack spoofing

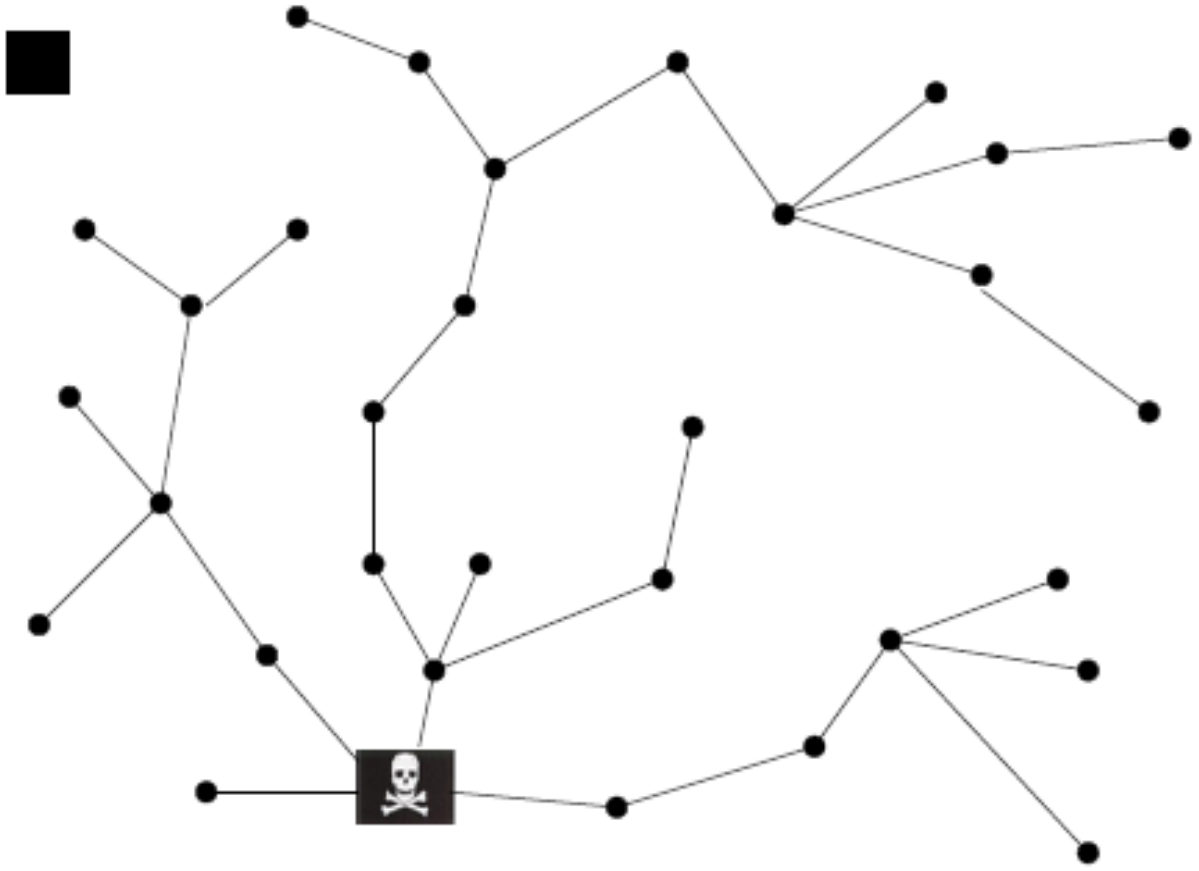

Fig. 5. An adversary spoofing a routing update from a base station in TinyOS beaconing.

TinyOS wormhole and sinkhole attacks

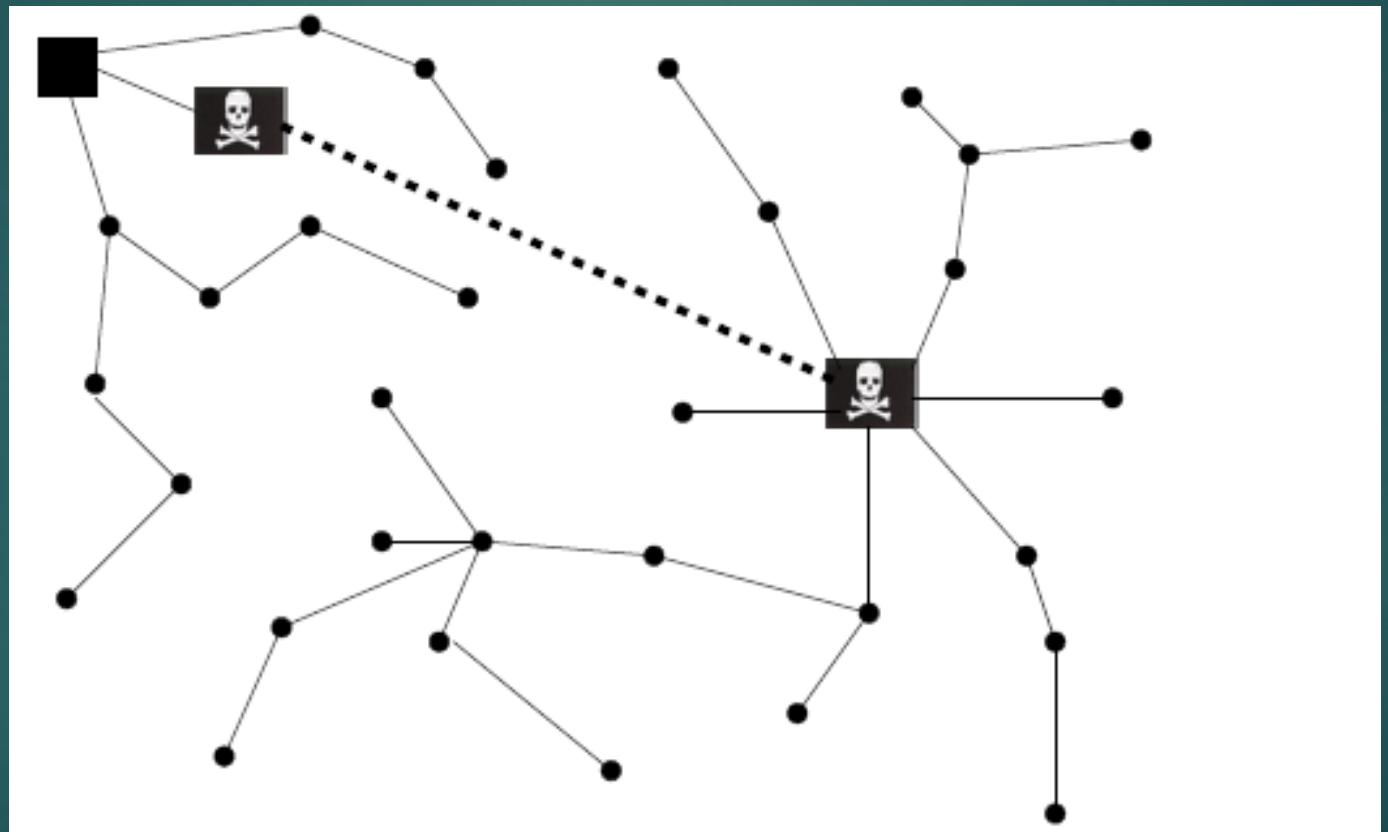

Fig. 6. A laptop-class adversary using a wormhole to create a sinkhole in TinyOS beaconing.

TinyOS HELLO flood attack

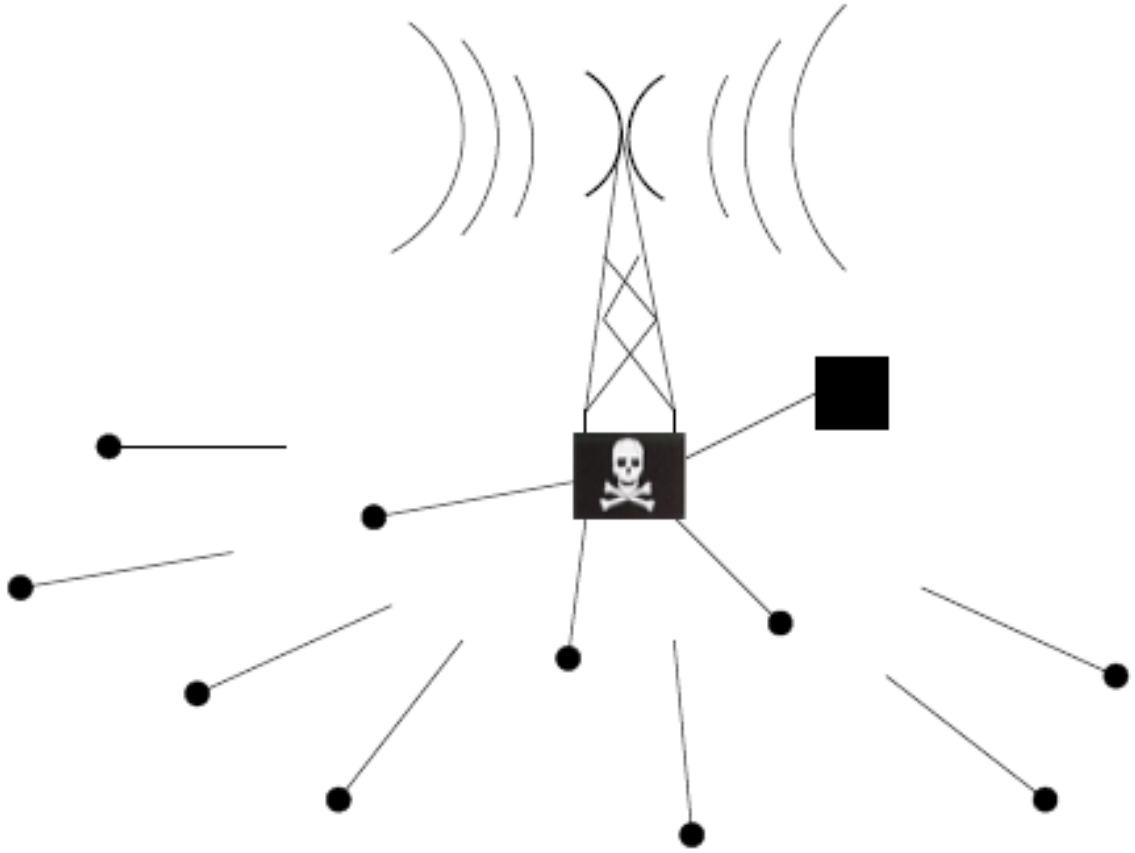

Fig. 7. HELLO **flood attack against TinyOS beaconing.** A laptop-class adversary that can retransmit a routing update with enough power to be received by the entire network leaves many nodes stranded. They are out of normal radio range from the adversary but have chosen her as their parent.

Directed diffusion

- Data –centric routing algorithm for drawing information out of a sensor network
- Base stations flood interests for named data, setting up gradients within the network designed to draw events (i.e. data matching the interest
- When a node satisfy this interest it will reverse and send back the data until it reach the base station
- A node might have multiple request from it neighbor so it will send a copy to all of those who request it

Directed Diffusion attacks

- Since multiple copy of the data can exist on the network stopping the base station from getting the data might not be possible, but the adversary might have other goals
  - Suppression: Flow suppression is an instance of denial-of-service. Spoof negative reinforcements. Example make the normal path seems more costly to take by advertise it as longer we see this in another example
  - Cloning: A flow enables eavesdropping. Once an adversary know of an interest request the adversary can just replay it and make the node send the adversary the data
  - Path influence: Influence the path taken by a data flow by spoofing positive and negative reinforcements. Changing what adversities through positive and negative reinforcements allow for the adversary to get the data

Directed Diffuse attacks continue

- Finally we have Selective forwarding and data tampering
  - Here instead of getting just the data from the other three goals the adversary modify the data and send it back to the base station, or just select with packets get send

  The author said to uses Wormholes attack to cause more damage to the sensor network

  For multipath uses Sybil this is where a node will Broadcast to neighbors that it need the information. So the neighbor node will send the data to the malicious node instead to where it need to go

Geographic routing

- Geographic and Energy Aware routing (GEAR)
- Greedy perimeter stateless routing (GPSR)
- GPSR uses greedy forwarding at each hop, routing each packet to the neighbor closest to the destination. If holes are encountered greedy forwarding is impossible. GPSR goes around the void of these holes.
- GPSR drawback is that packets along a single flow will always use the same nodes from the routing of each packet, uneven energy consumption
- GEAR remedy this by comparing remaining energy and distance from the target

Geographic routing attack

- Adversaries will adversities it location so it will be on the path of the flow. When it come to GEAR since energy is a metric it uses to determine where the data flow should goes. ALL the adversary have to do is advertise maximum energy.
- To make this attack even more dangerous change it to a Sybil attack which we see with the next figure on the next page

Geographic routing Figure 8

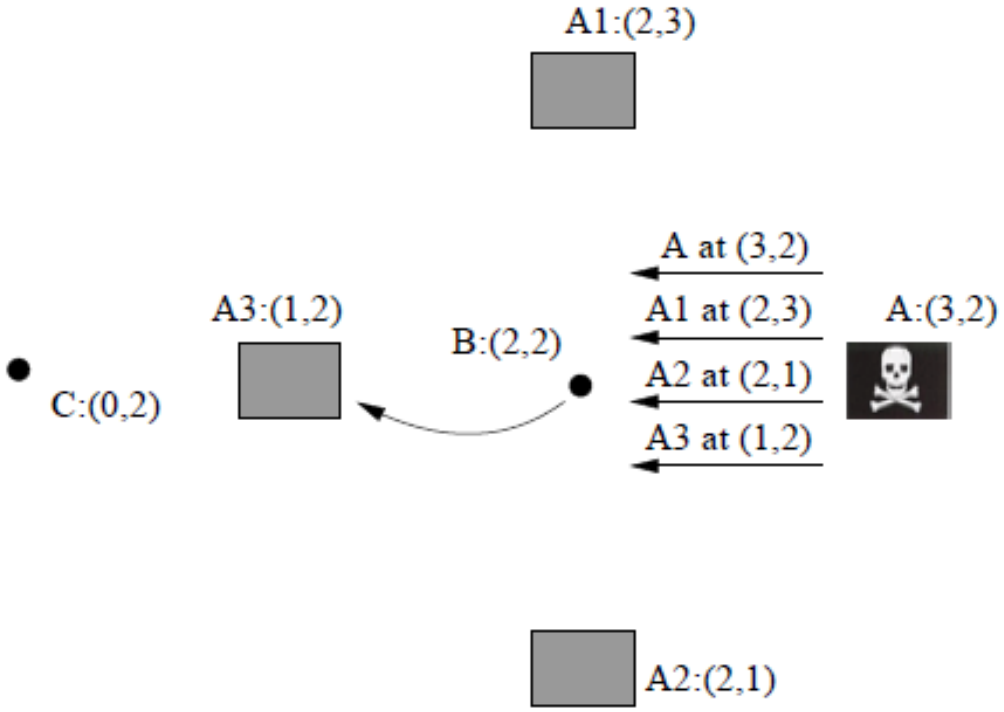

Fig. 8. **The Sybil attack against geographic routing.** Adversary A at actual location (3,2) forges location advertisements for non-existent nodes A1, A2, and A3 as well as advertising her own location. After hearing these advertisements, if B wants to send a message to destination (0,2), it will attempt to do so through A3. This transmission can be overheard and handled by the adversary A.

Geographic routing Figure 9

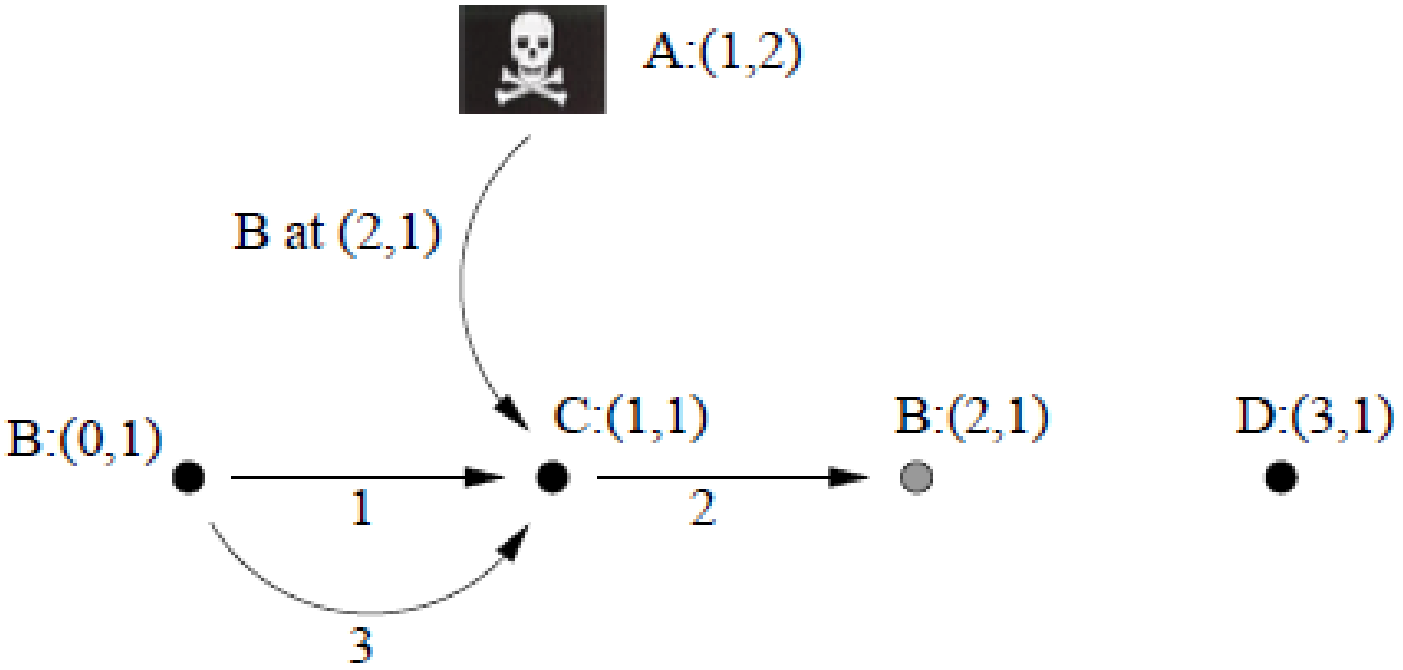

Fig. 9. **Creating routing loops in GPSR.** By forging a location advertisement claiming B is at (2,1), an adversary can create a routing loop as described in Section VII-C.

Minimum cost forwarding

- All node maintain a cost field to the base station
- Base station is always value at 0, all other nodes start at ∞
- Once a flooding beacon start at the base station all other nodes update their cost field and maintain it
- Cn = Cm + Ln,m if the value on the left is smaller it maintain that value else the new Cn is Cm+Ln,m for further explanation please refer to distributed shortest-path algorithm

Minimum cost forwarding

- Sinkhole attack all the adversary have to do is broadcast it node as a cost 0. This is for adversary who uses node to attack sensor network
- With a laptop an adversary can uses wormhole to further this attack on Minimum cost forwarding algorithms by synchronizing attack
- Using a laptop an adversary can uses HELLO flood attack to advertise a cost zero powerful enough to disable the entire network
- This will cause all packets to come to the adversary

LEACH

- Low-Energy adaptive clustering hierarchy
- Assume all nodes can reach the base station with high-power transmission
- Leach organize cluster and 1 node become the cluster-head. This cluster-head will directly send packets to the base station allowing for other nodes in the cluster to save energy.
- To ensure all node have the same amount of energy it uses randomized rotation so all node have a chances to be cluster-head node
- In LEACH the cluster-head will wait to receive data from all nodes than send the data to the base station

LEACH attack

- The adversary can uses a laptop to HELLO flooding attack and disable the entire network
- The adversary can also you selective forwarding and a few compromise nodes to if the adversary nodes are the cluster-head
- When pair it with Sybil attack each node can adversities multiple identities causing it to become the cluster-head more times.
- There are many more attack and algorithms, but I feel LEACH is an important one to mention because it seems like such a good idea
- However, taking from an old saying "A chain is as strong as it weakest link" clearly the best way to attack this one is using that statement

Countermeasures

- Outsider attacks prevented by Link Layer encryption and Authentication globally shared key
  - Sybil attack are no longer relevant nodes in the sensor network will not even acknowledge it
  - Sinkhole and selective forwarding are no good because the adversary cannot join the topology
  - Only Wormhole and HELLO flood attack are a problem left when using the above method

Countermeasure Sybil attack

- Two node can uses Needham-Schroeder to verify each other identity
- If a node become compromise it can only have meaningful conversation with it verify neighbors
- This will help with eavesdropping or modify of data

Countermeasure HELLO flood attacks

- Verify the bidirectionality of a link before taking meaningful action based on a message receive over that link, however, not effective against a highly sensitive receiver as well as a powerful transmitter
- Each node to authenticate each of its neighbors with an identity verification protocol using a trusted station
- The ideas is if an adversary claiming to be neighbor to a lot of node and try to authenticate itself to so many node will raise alarm

Wormhole and sinkhole attacks

- Wormhole are hard to detect because it uses a private out-of-band channel invisible to the underlying sensor network
- Sinkhole are difficult to defend against because in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify
- When combine make it very difficult to detect and defend against
- Best to design routing protocol that resistance to routing race conditions with make these type of attacking meaningless

As the author stated security cannot come after the design because the attacks is aim at the design weakness

Leveraging global knowledge

- I think this is what this section mean
- Let the base station map out the topology of the whole sensor network
- If there is a change drastic the base station need to verify the changes and take appropriate actions
- The rest is node is too trusting, a node come upon a hole and see someone advertise that it part of the network will trust it. However, the authors stated from the beginning base station are trustworthy nodes are not.
- It inexpensive nature allow for easy tampering

Authenticate broadcasting and flooding

- The author argue that only base station can HELLO flood and all node need to be able to authenticate this message
- Node can broadcast HELLO flood message to it neighbor but this can still be authenticated, but a normal node is not all other node neighbor so when one node try to say it everyone neighbor that should raise some red flag

Ultimate Limitation of secure multihop routing

- After a few hop from the base station these node become attractive for compromise, when enough is compromise, all is lost
- LEACH might be the best options against node compromise because it select a cluster-head
- Another options is a virtual base station to create an overlay network, after a set of virtual base station have been selected a multihop topology is constructed using them
- The virtual base station communicate with the actual base station
- The virtual base station need to be change often so the adversary have a hard time choosing the right one

Conclusion

- Security is important, else spending money to set in place a sensor network to let it be compromise by a few simple attack is just a waste of time
- If we start with a stronger design for sensor network we do not have to worry about some of the attacks
- Sensor network is not the same as ad-hoc wireless network, so what work for ad-hoc might not work for sensor network

Comment?