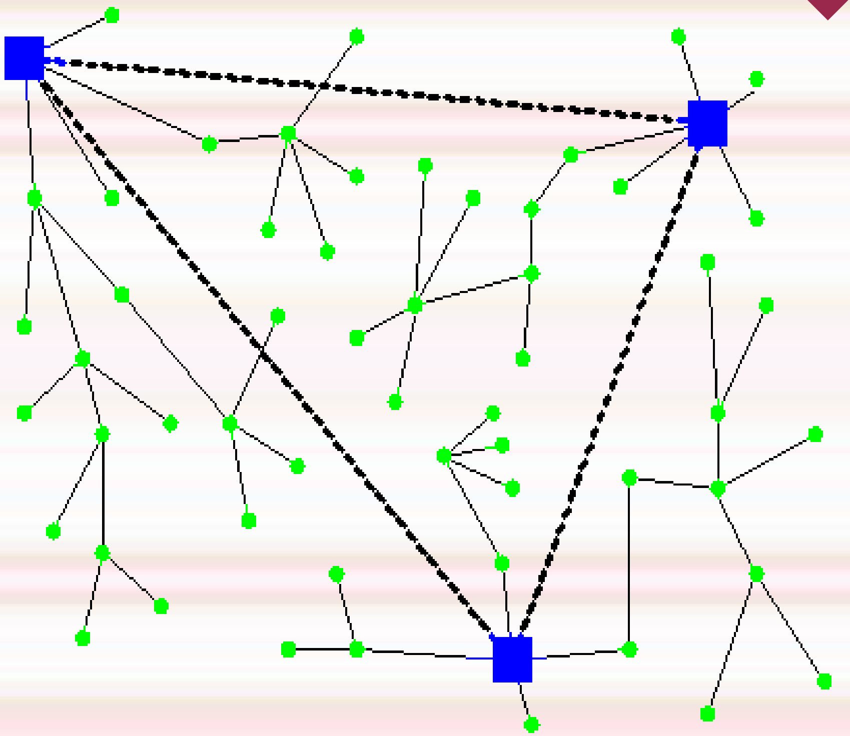
Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

Presented by:

Ivor Rodrigues

Worcester Polytechnic Institute

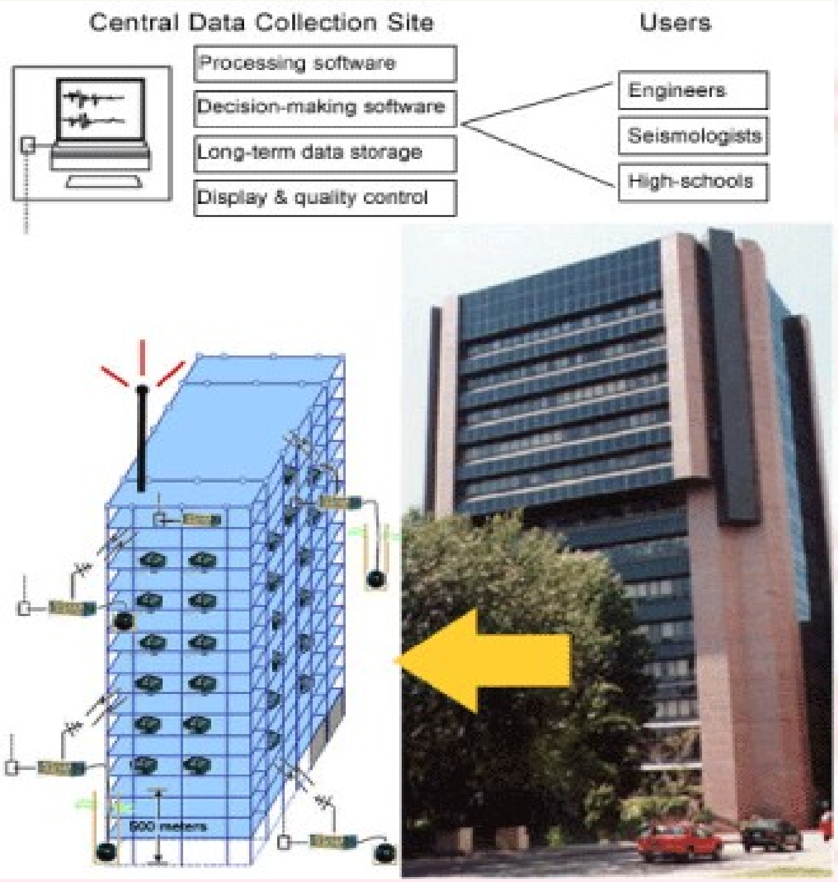
What is a Sensor network?



- A heterogeneous system combining tiny sensors and actuators with general purpose computing elements.

Sensor Network

- 38 strong-motion seismometers in 17-story steel-frame Factor Building.
- 100 free-field seismometers in UCLA campus ground at 100-m spacing



Central Data Collection Site

Processing software

Decision-making software

Long-term data storage

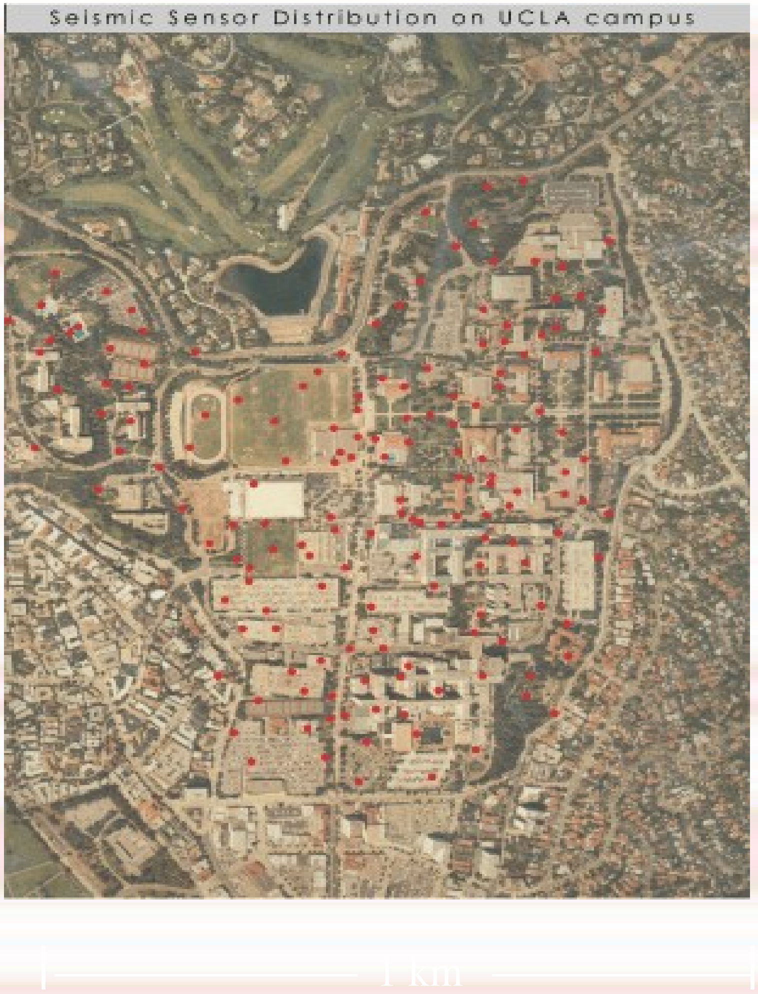
Display & quality control

Users

Engineers

Seismologists

High-schools



Mobicom 2002 Wireless Sensor Networks-Deborah Estrin

Sensors

- Passive Nodes: seismic, acoustic, infrared, strain, salinity, humidity, temperature, etc.
- Active sensors: radar, sonar
  - High energy, in contrast to passive elements
- Small in Size- IC Technology

Use of Sensor Networks?

Wireless Communications and Computing:

Interacting with the physical world

Security and surveillance applications Monitoring of natural habitats

Medical Sensors such as Body Id

This Paper

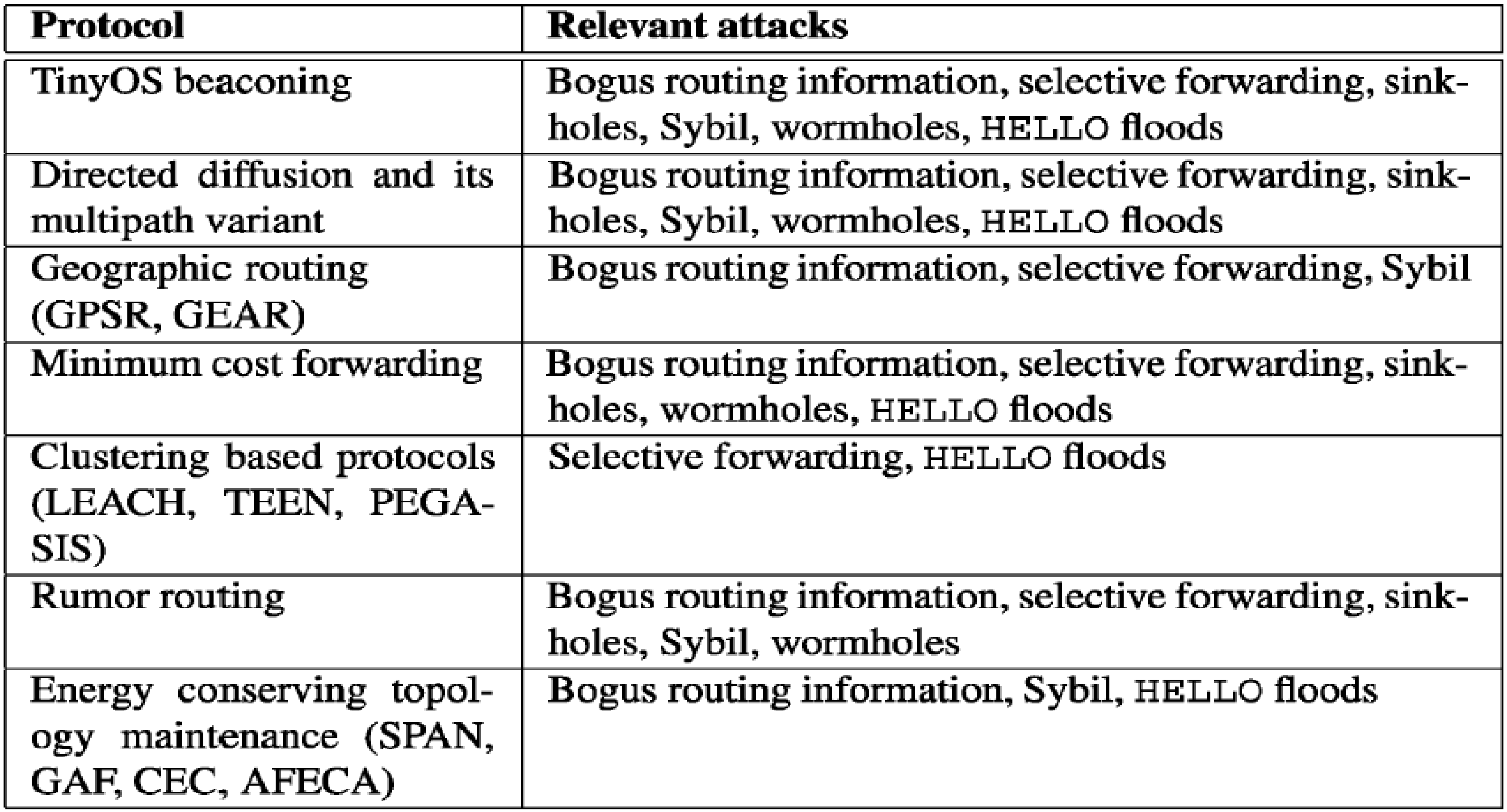
- Propose threat models and security goals for secure routing in wireless sensor networks
- Discuss the various kinds of attacks
- Show how attacks against ad-hoc wireless networks and peer-peer networks can be adapted as powerful attacks against sensor networks.
- Discuss counter measures and design considerations

Motivation

- Security for Routing using Sensor Networks

- Security is not considered as a top priority
- So we see, why sensor networks are so prone to attacks.

Sensor network protocols and Possible 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

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

Requirements for Sensor Networks

- Nodes and network
- Central information processing Unit
- Power
- Memory
- Synchronization, co-operabibility

Definitions

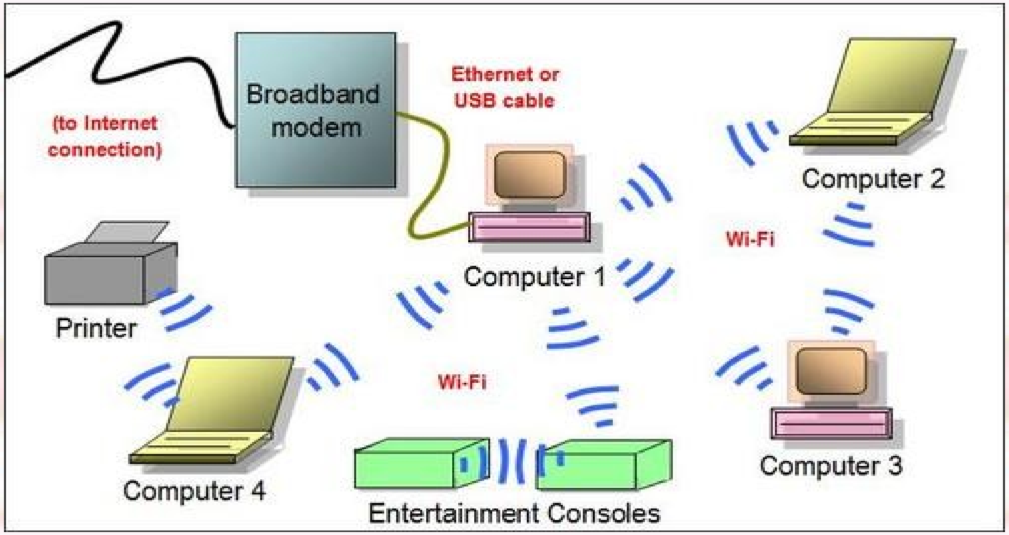
- BS- Base Stations or Sinks
- Nodes
- Aggregate Points
- Sources

Requirements for Sensor Networks

- Power restrictions
- Number of nodes required for deployment
- Duty cycle depends on longevity
- Data rate-Power relation
- Security
- Memory
- Simplicity

Ad-hoc vs. WSN Ad - hoc

- Multi-hop
- Routing between any pair of nodes
- Somewhat resource constrained



Ad-hoc vs. WSN

WSN

- Routing Patterns
  - Many-to-One
  - One-to-Many
  - Local

- Extremely resource constrained

- Trust Relationships to

  prune redundant messages
  - In-network processing
  - Aggregation
  - Duplicate elimination

Mica Mote

- 4 MHz 8-bit Atmel ATMEGA103 Processor
- Memory
  - 128KB Instruction Memory
  - 4 KB RAM / 512KB flash memory
- 916 MHz radio
  - 40 Kbps single channel
  - Range: few dozen meters
- Power
  - 12 mA in Tx mode
  - 4.8 mA in Rx mode
  - 5 µA in sleep mode
- Batteries
  - 2850 mA on 2 AA

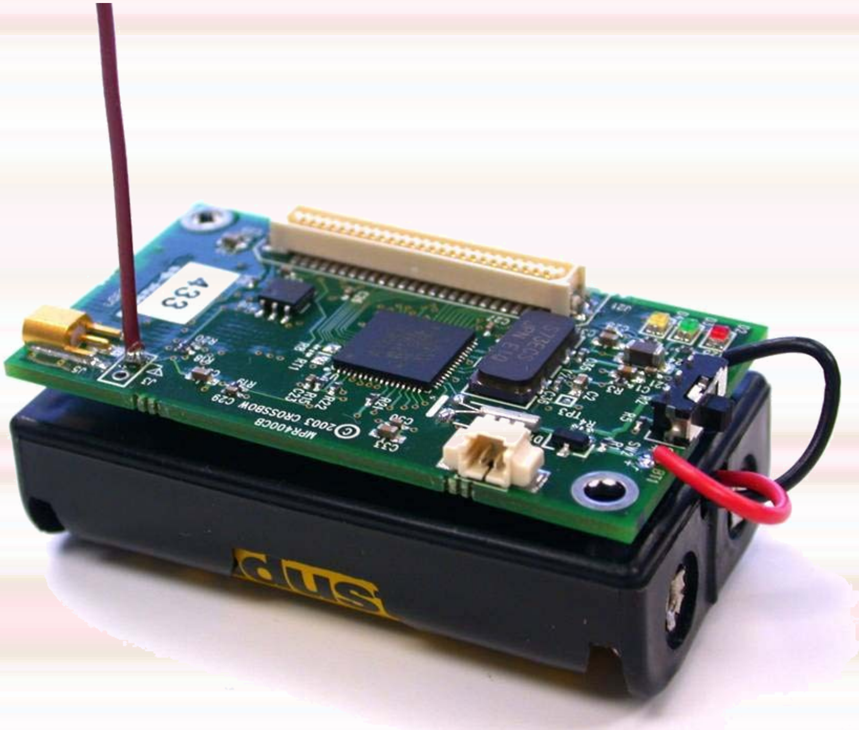


Image source: www.btnode.ethz.ch

Mote Class vs Laptop Class Attacker

- Small
- Less Powerful
- Fewer Capabilities

- Large
- like laptops, highly powerful
- Large capabilities

Outsider Attacker vs Insider Attacker

- Less access
- Does not include compromised nodes

- Big threat
- May or may not include compromised nodes

- Authentication
  - Public key cryptography
    - Too costly
    - WSN can only afford symmetric key

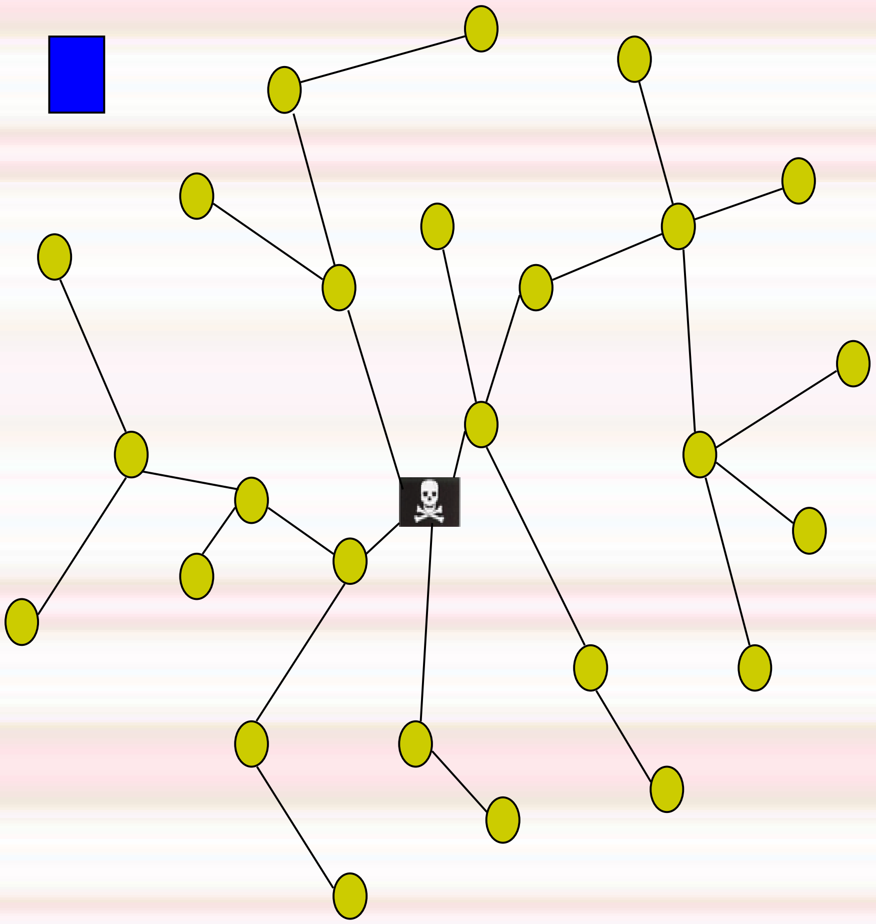
- Secure Routing
  - Source routing / distance vector protocols
    - Require too much node state, packet overhead
    - Useful for fully connected networks, which WSN are not

- Controlling Misbehaving Nodes
  - Punishment
    - Ignore nodes that don’t forward packets
    - Susceptible to blackmailers
- Security protocols
  - SNEP – provides confidentiality, authentication
  - µTESLA – provides authenticated broadcast

Assumptions

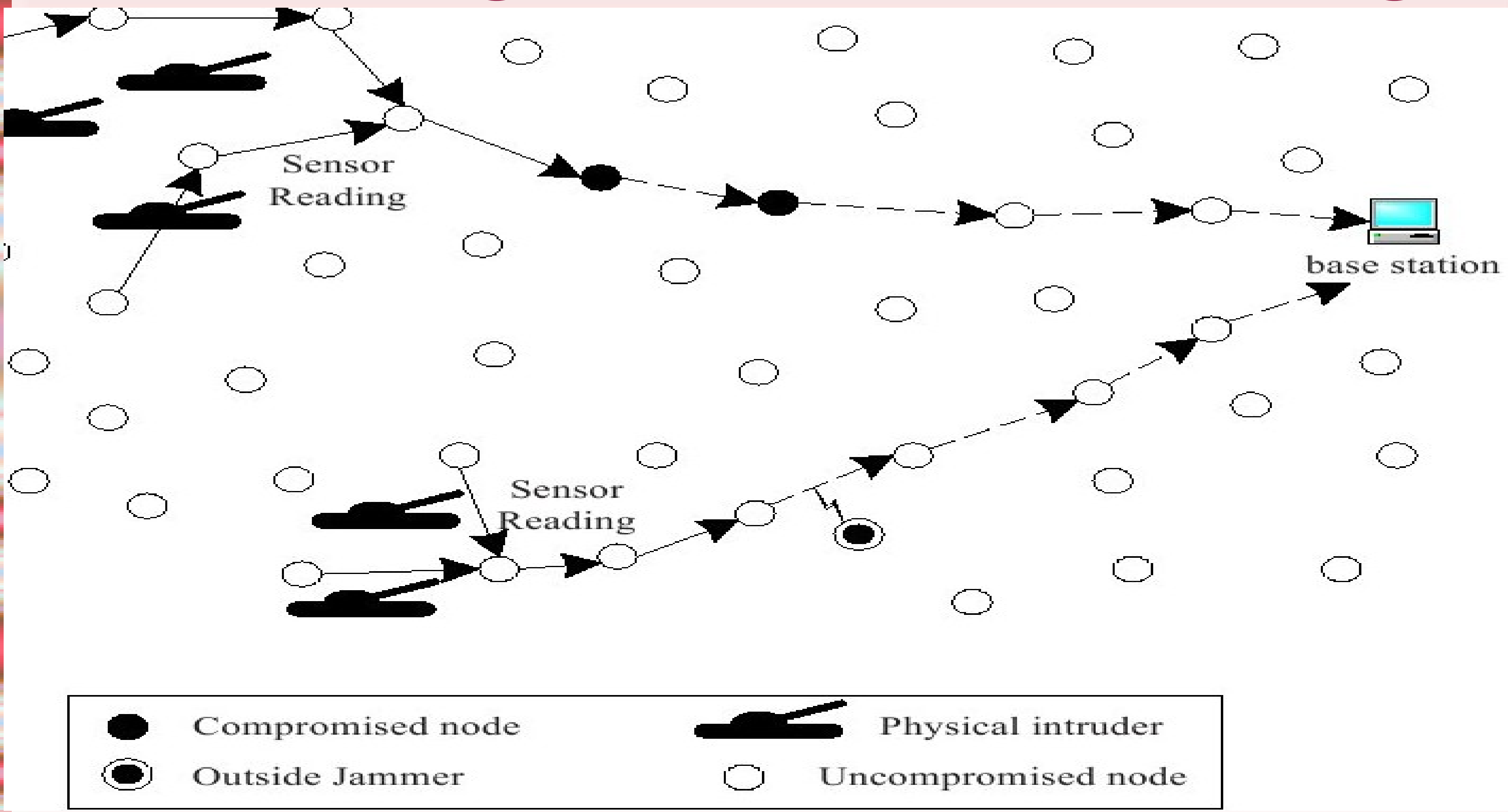
- Network Assumptions
- Trust Requirements
- Threat Models
- Security Goals

Attacks on Sensor Network Routing



- Spoofed, Altered or replayed routing information

Attacks on Sensor Network Routing- Selective forwarding



Attacks on Sensor Network Routing

On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks-Edith C. H. Ngai,1 Jiangchuan Liu,2 and Michael R. Lyu1

- Sinkhole Attack

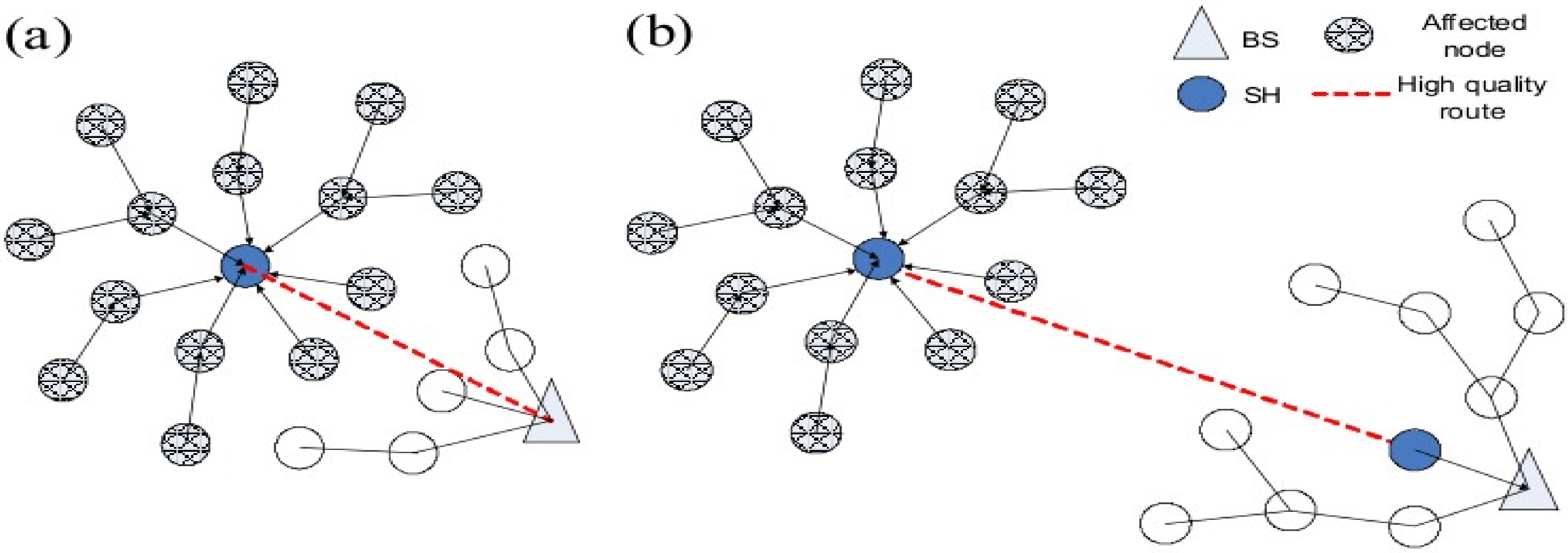
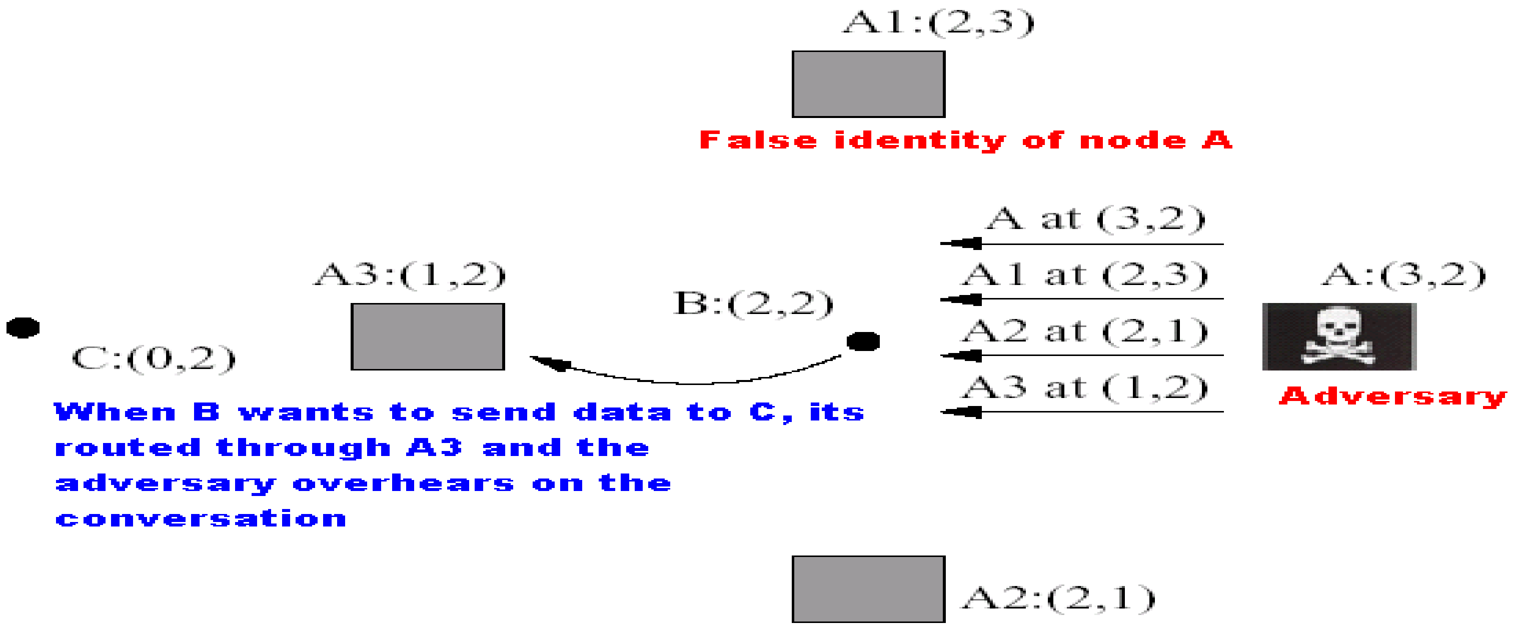


Fig. 1. Two examples of sinkhole attack in wireless sensor networks. (a) Using an artificial high quality route; (b) Using a wormhole.

Attacks on Sensor Network Routing

- Sybil Attack

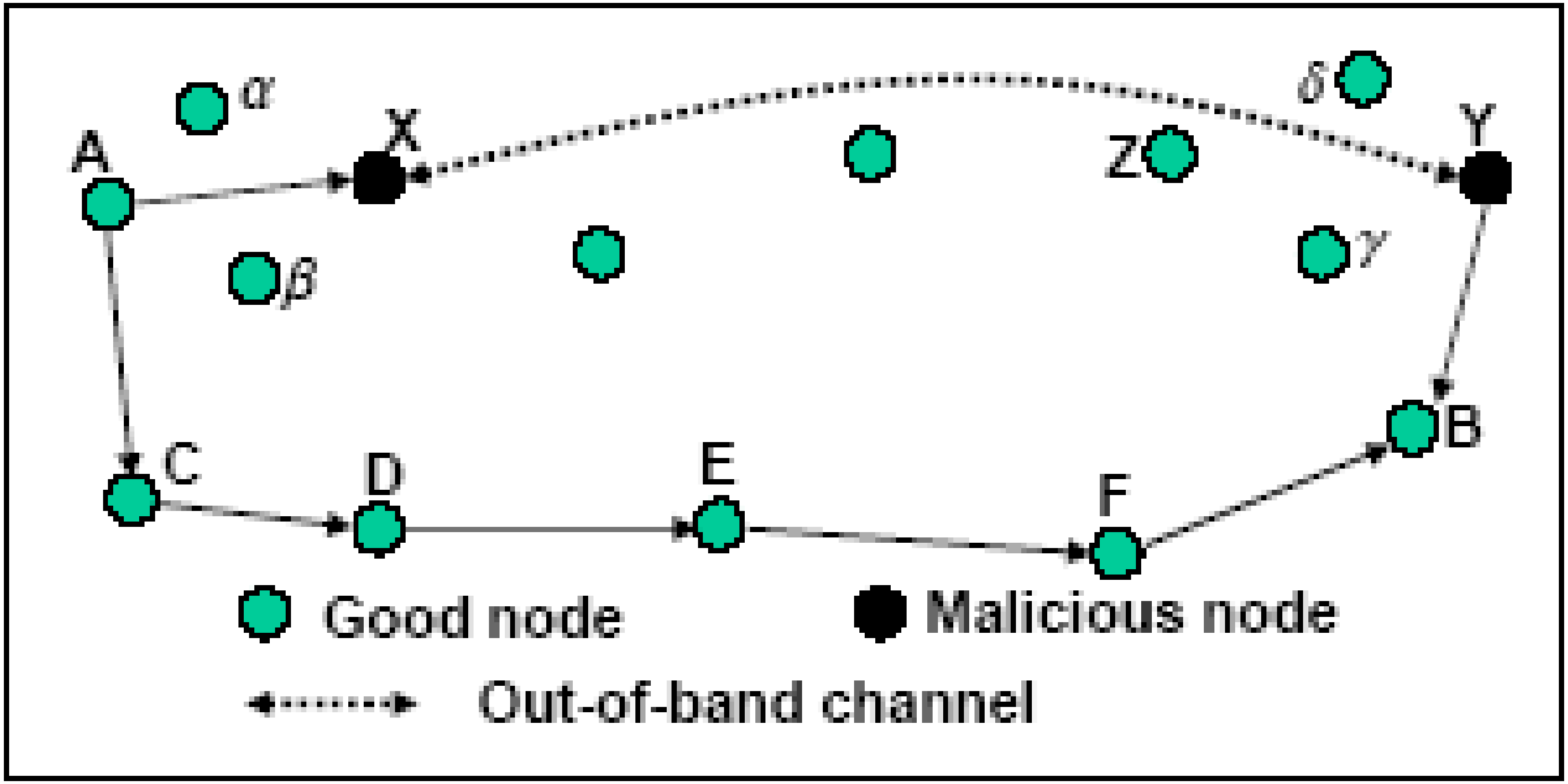


When B wants to send data to C, its routed through A3 and the adversary overhears on the conversation

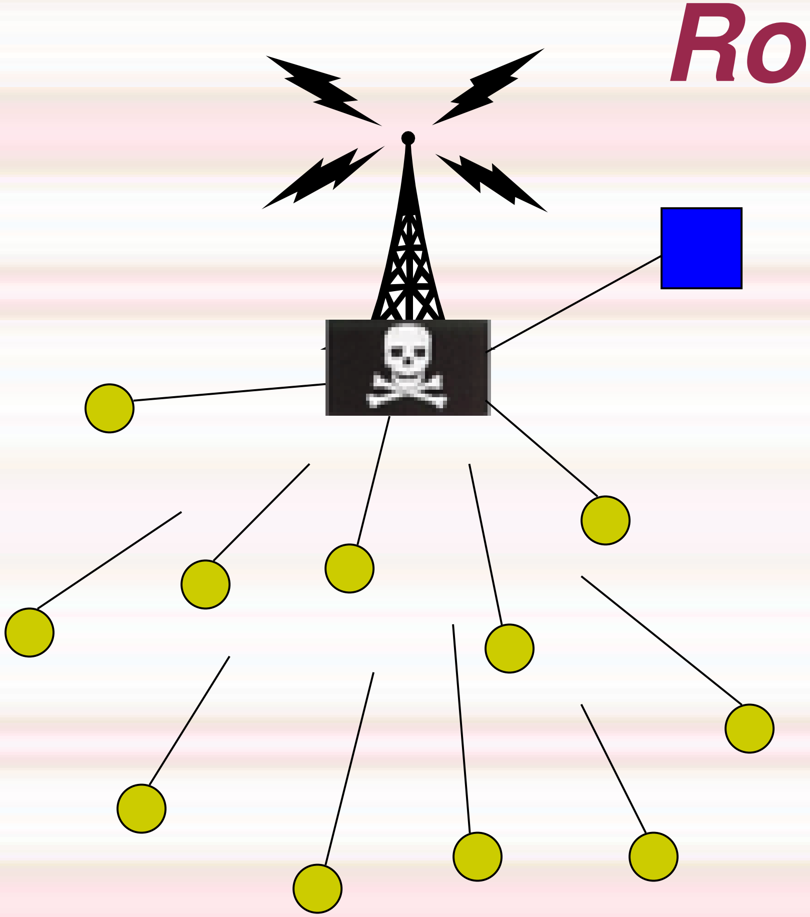
Adversary at (3,2) forges location advertisements of nodes A1,A2 and A3 which are non-existent and its own location

Attacks on Sensor Network Routing

- Wormholes



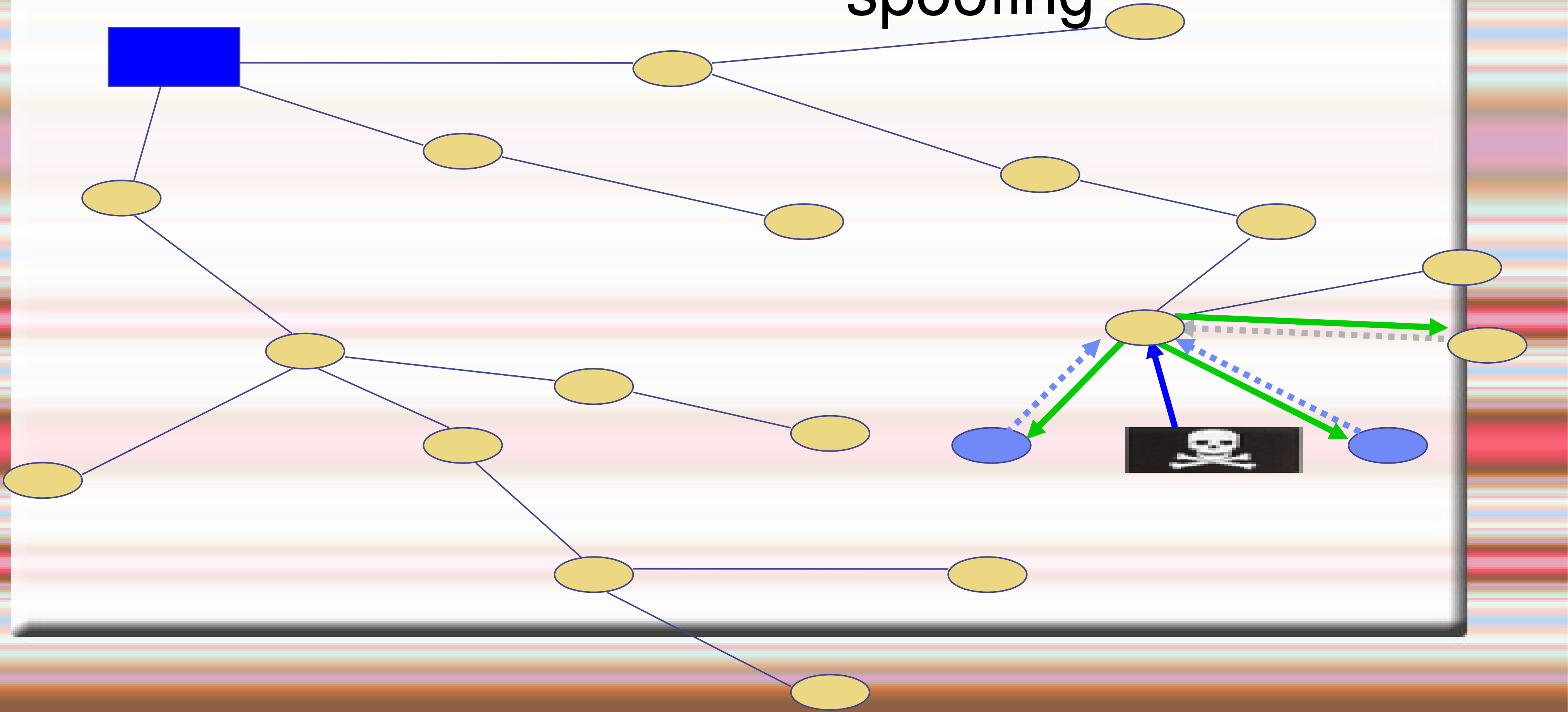
Attacks on Sensor Network Routing



- Hello Flood Attack

Attacks on Sensor Network Routing

- Acknowledgment spoofing



Acknowledgment Spoofing

- If a protocol uses link-layer acks, these acks can be forged, so that other nodes believe a weak link to be strong or dead nodes to be alive.
- Packets sent along this route are essentially lost
- Adversary has effected a selective forwarding attack

Hello flood attack

- In a HELLO flood attack a malicious node can send, record or replay HELLO-messages with high transmission power.
- It creates an illusion of being a neighbor to many nodes in the networks and can confuse the network routing badly.
- Assumption that sender is within normal range
- A laptop class attacker could trick all nodes in network into thinking it's a parent/neighbor

Hello flood attack

- End result can be a feeling of sinkhole, wormhole, selective forwarding symptoms.
- Adversary is my neighbor
- Result: Network is confused

Neighbors either forwarding packets to the adversary

Attack primarily on protocols that require sharing of information for topology maintenance or flow control.

Wormholes

- The wormhole attack usually needs two malicious nodes.
- The idea is to distort routing with the use of a low-latency out-of-bound channel to another part of the network where messages are replayed.
- These can be used, for example, to create sinkholes and to exploit race conditions.
- Useful in connection with selective forwarding, eavesdropping
- Difficult to detect when used in conjunction with Sybil attack
- Wormholes are difficult to detect.

Sybil Attack

- The Sybil attack is targeted to undermine the distributed solutions that rely on multiple nodes cooperation or multiple routes. In a Sybil attack, the malicious node gathers several identities for posing as a group of many nodes instead of one. This attack is not relevant as a routing attack only, it can be used against any crypto-schemes that divide the trust between multiple parties. For example, to break a threshold crypto scheme, one needs several shares of the shared secret.

Sybil Attack

- Affects geographic routing.
- Sending multiple (fictitious) results to a parent
- Sending data to more than one parent

Sinkhole Attack

- A malicious node uses the faults in a routing protocol to attract much traffic from a particular area, thus creating a sinkhole
- Tricking users advertising a high-quality link
- Use a laptop class node to fake a good route
- Highly Attractive and susceptibility due to communication pattern.
- Sinkholes are difficult to defend

Selective Forwarding

- A malicious node can selectively drop only certain packets.
- Especially effective if combined with an attack that gathers much of the traffic via the node, such as the sinkhole attack or acknowledgment spoofing.
- The attack can be used to make a denial of service attack targeted to a particular node. **If all packets are dropped, the attack is called a “black hole”.**

Selective Forwarding

- An Insider attacker included in the routing path

  An Outsider attacker causes collisions on an overheard flow.

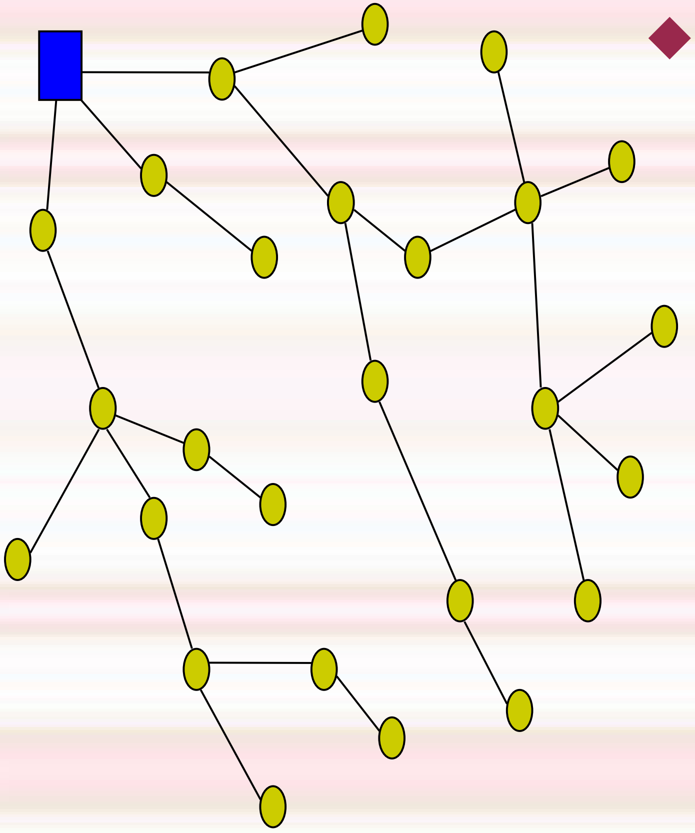
Spoofed, Altered or replayed routing information

- An unprotected ad hoc routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly affect routing information.
- Create routing loops
- Extend or shorten service routes
- Generate false error messages
- Increase end-to-end latency

Attacks on Specific Sensor Network Protocols

- TinyOS Beaconing
- Directed diffusion
- Geographic routing
- Minimum cost forwarding
- LEACH
- Rumor routing
- SPAN & GAF

TinyOS Beaconing



- In TinyOS beaconing, any node can claim to be a base station. If routing updates are authenticated, a laptop attacker can still do a wormhole/sinkhole attack: Laptop attacker can also use a HELLO flood attack to the whole network: all nodes mark it as its parent, but their radio range will not reach it. Mote-class attackers can also create routing loops.

TinyOS Beaconing

- Routing algorithm constructs a breadth first spanning tree rooted at the base station
- The Nodes mark base station as its parent, then inform the base station that it is one of its children node.
- Receiving node rebroadcasts beacon recursively
- Threat Level: Orange

Directed diffusion

- Data Centric
- Sensor Node don’t need global identity
- Application Specific
- Traditional Networks perform wide variety of tasks.
- Sensor Networks are designed for specific task.
- Data aggregation & caching.
- Positive reinforcement increases the data rate of the responses while negative reinforcement decreases it.

Directed diffusion

- Suppression
- Cloning
- Path Influence

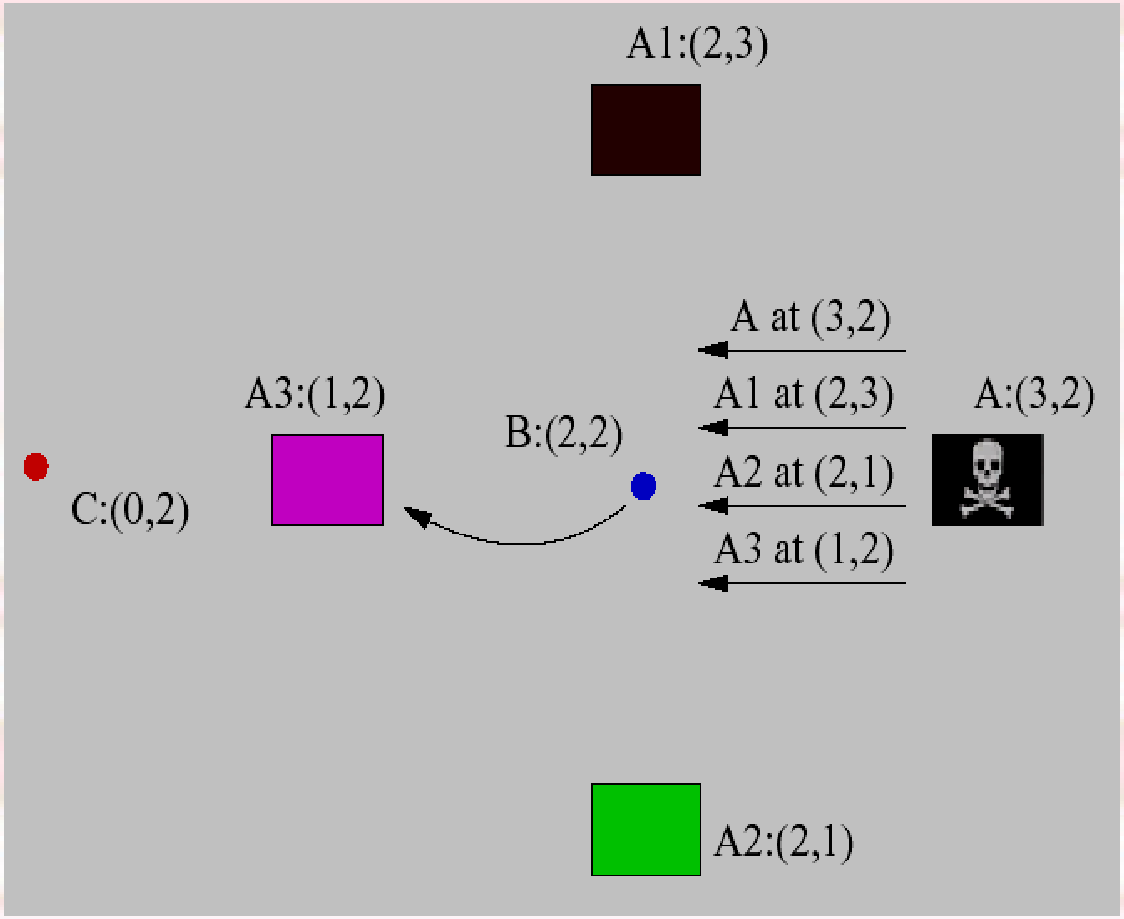
Selective Forwarding

- Worming and Sybiling on directed diffusion WSN's

GEAR and GPSR

- GPSR: unbalanced energy consumption
- GEAR: balanced energy consumption
- GPSR: routing using same nodes around the perimeter of a void
- GEAR: weighs the remaining energy and distance from the target
- GPSR: Greedy routing to Base station
- GEAR: distributed routing, energy and distance aware routing.
- Construct a topology on demand using localized interactions and information without initiation of the base station

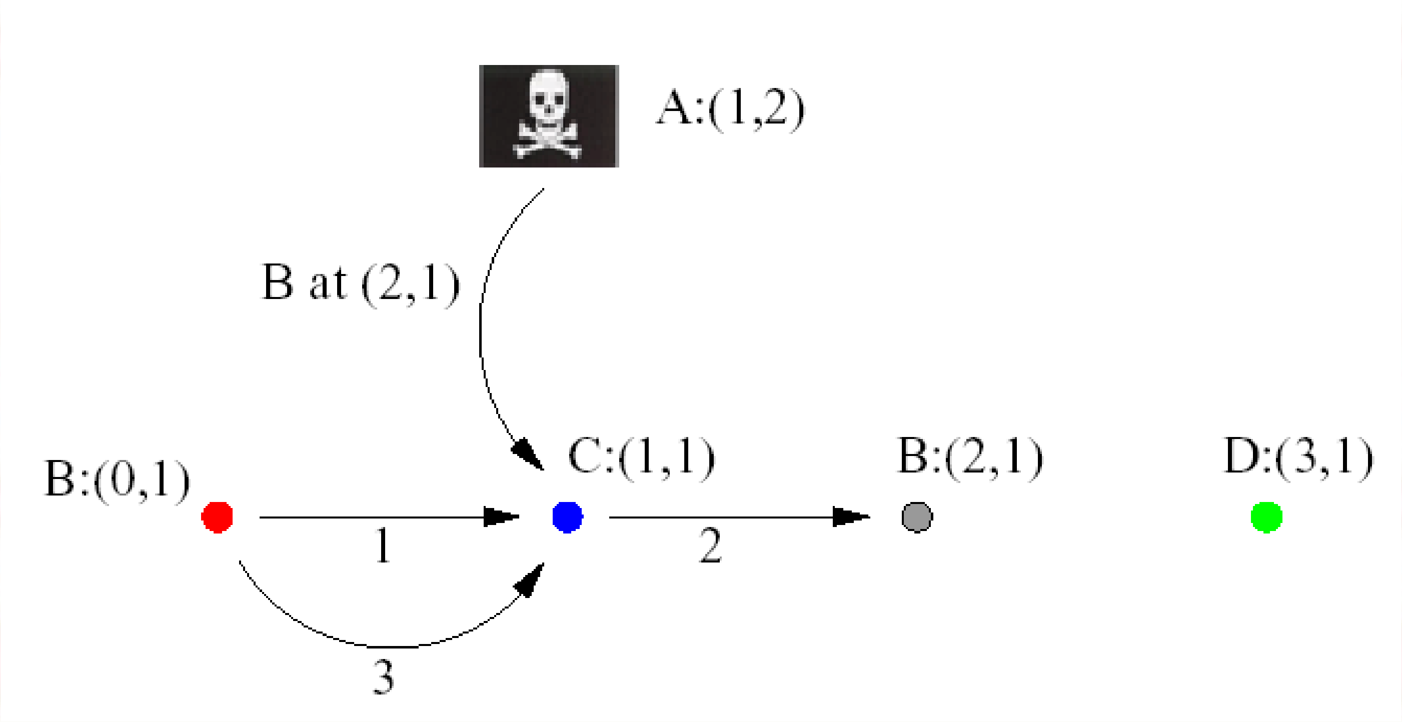
Geographical Attacks and Attackers



- Forging fake nodes to try to plug itself into the data path.

Geographical Attacks and Attackers

- GPSR.



Countermeasures

- Sybil attack

- Unique symmetric key
- Needham-Schroeder
- Restrict near neighbors of nodes by Base station

Countermeasures

- Hello Flooding

- Bi-directionality
- Restricting the number of nodes by the base station

Countermeasures

- Wormhole and sinkhole attacks

- Use time and distance
- Thus Geographic routing protocols like GPSR and GEAR work against such attacks
- Traffic directed towards Base station and not elsewhere like sinkholes

Leveraging Global knowledge

- Fixed number of nodes
- Fixed topology.

Selective Forwarding

- Messages routed over n disjoint paths protected from n compromised nodes

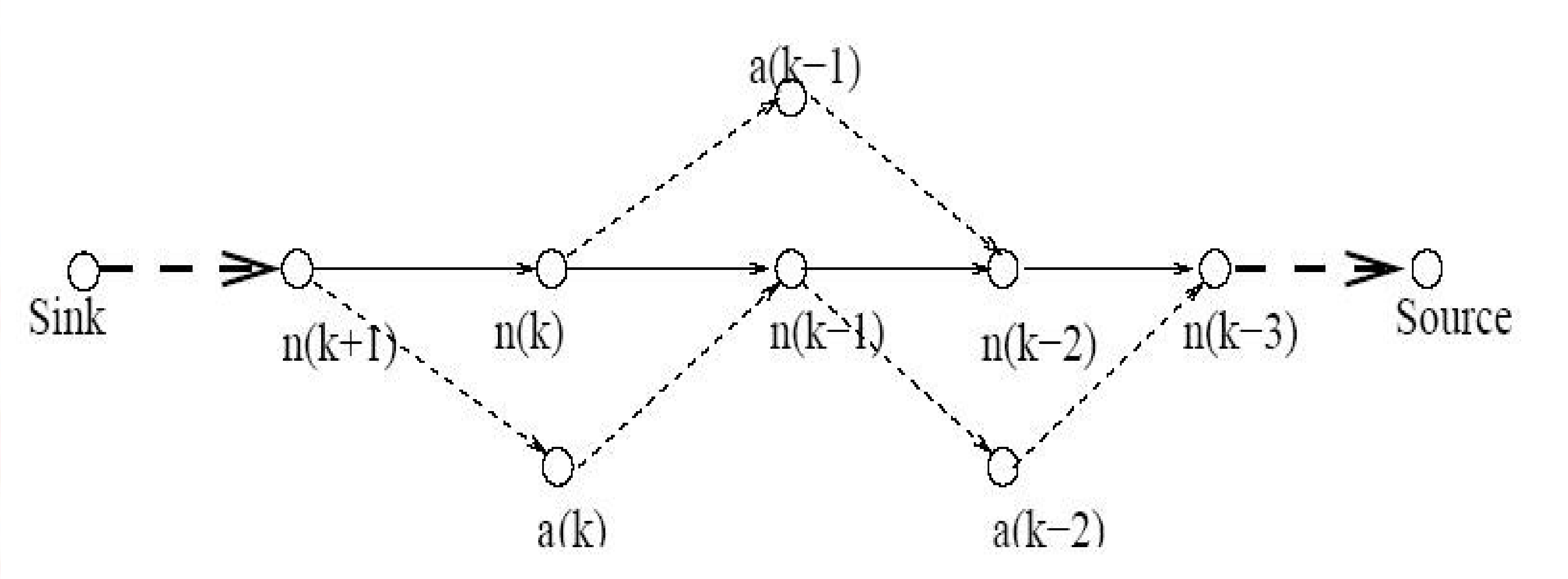


Image Source: http://wiki.uni.lu/secan-lab/Braided+Multipath+Routing.html

Conclusions

- The Authors state that for secure routing, networks should have security as the goal
- Infiltrators can easily attack, modify or capture vulnerable nodes.
- Limiting the number of nodes, using public/global/local key are some of the ways to counter being attacked by adversaries.

Few Observations

- More insight on capturing packets of the air
- Foes or Friends?
- What happens when data is captured, copied and forwarded unnoticed?
- Real issues not stated?
- Real attacks not described, analyzed or observed

Few Observations

- Paper was presented at IEEE Workshop Conference.
- What happens if someone spoofs a legitimate node identity and paralyze it. What are the countermeasures. Can it be detectable
- Should sensor networks provide security or is it their goal to be secure?

References

- Securities in Sensor networks-Yang Xiao
- Mobicom 2002 Wireless Sensor Networks-Deborah Estrin
- On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks-Edith C. H. Ngai Jiangchuan Liu, and Michael R. Lyu
- The Sybil Attack – John Douceur (Microsoft)

e