

Security Topics in Networking and Distributed Systems CS 590D

Lecture 20: Secure Routing in Wireless Sensor Networks

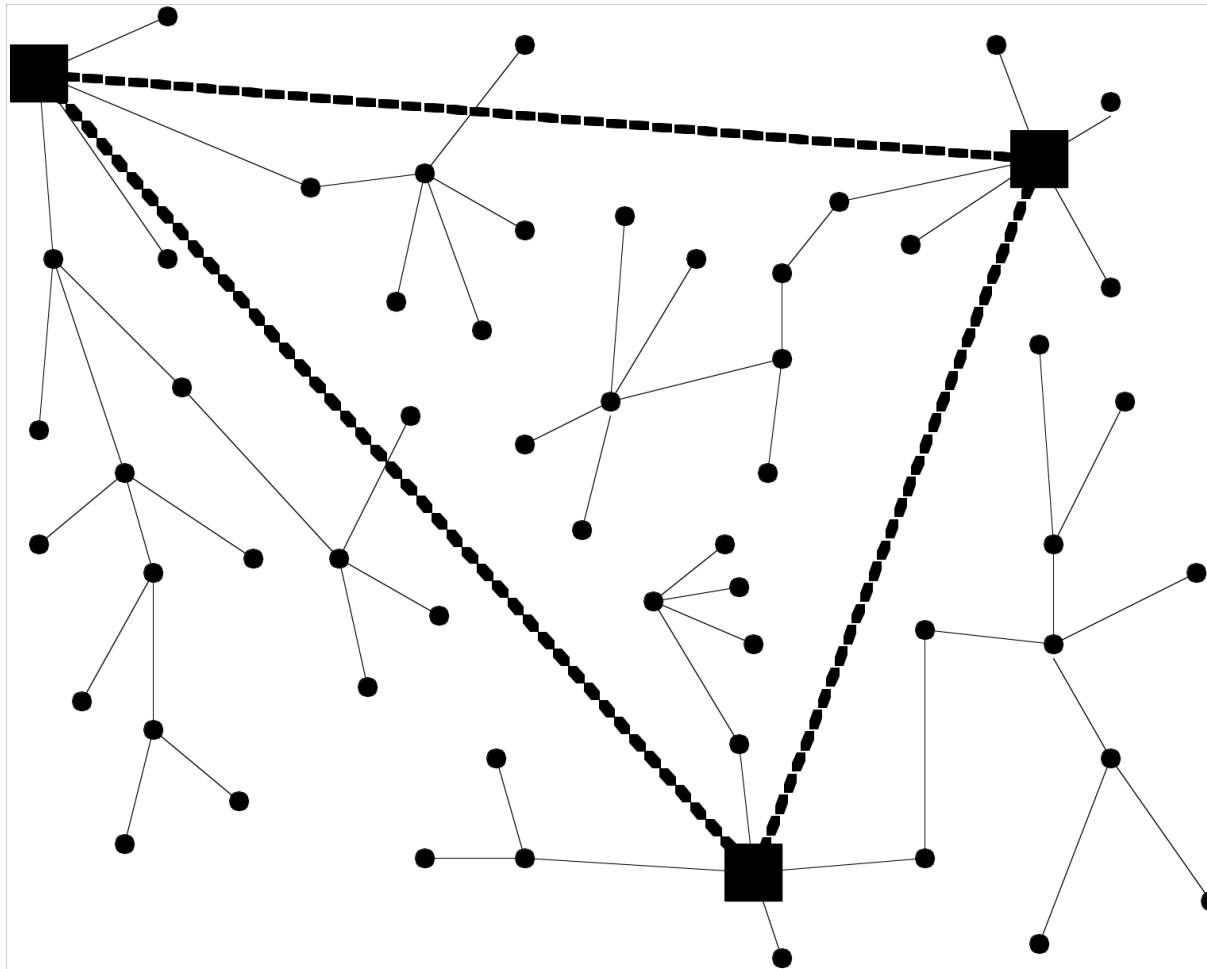
Department of Computer Sciences
Purdue University

References

- SPINS: Security Protocols for Sensor Networks Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar MOBICOM 2001.
- Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures Chris Karlof, David Wagner, First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.



Sensor Network Architecture



Challenges

- Limited memory, battery, and bandwidth
- Vulnerability of nodes to physical capture
- Nodes not tamper resistant (neighbor distrust)
- For some applications, there is no knowledge of post deployment configuration

Particularities of Sensor Networks

- Aggregation
- Traffic patterns
- Trust relationships

Aggregation

- Aggregation: aggregation points process data from several sensors and send only one aggregated value
- WHY AGGREGATION?
- How expensive is sending vs. processing?
- Transmitting 1 bit consumes as much as executing 800-1000 instructions
- Security very difficult to provide under these constraints

Traffic in Sensor Networks

- Many-to-one: multiple sensors report data to an aggregation point
- One-to-many: a single node multicasts a query or control information to several nodes
- Local communication: neighboring nodes send localized messages to discover other nodes and coordinate

Trust

- Base stations are trusted
- If base stations are compromised, the entire network can be compromised
- Aggregation points may be trusted in certain protocols and not trusted in other.
- Sometimes aggregation points are sensors, they can be easily compromised, they should not be trusted

Attack Model

- Based on resources available to an attacker:
 - Mote-class attackers
 - Laptop-class attackers, stronger, more damaging
- Relation with the system
 - Insider attacks
 - Outsider attackers

Security Goals

- Ideal world: integrity, authenticity and availability of messages in the presence of adversaries of arbitrary power
- Real world:
 - graceful degradation in the presence of insider attacks
 - Authenticity and integrity

Attacks

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



TinyOS Beaconing

- Dissemination tree rooted at the base station (breadth first spanning tree)
- Periodically the base station broadcasts a route update
- Nodes receiving the update mark the base station as parent and rebroadcast the update
- All packets received by a node are sent to the parent and propagated till they reach the base station



TinyOS Beaconing: Attacks

- Inject information, create routing loops, partition the nodes, spoof packets
- HELLO attacks: a powerful attacker could reach the entire network and create the impression that he is everybody's neighbor, packets are dropped
- Sybil and wormhole attacks also possible
- Prevent outsider attacks using authentication
- What about replay?
- Insider attacks very challenging to prevent
- Verify that links are bidirectional
- Prove identity and location
- Also solution for wormhole based on directional antenna

Some Observations

- Not all routing protocols are susceptible to the same type of attacks
- Geographical-based protocols less susceptible to wormholes, assuming information is authenticated
- Minimum cost forwarding protocols vulnerable to sinkhole attacks
- LEACH protocol vulnerable to HELLO attack

Countermeasures Summary

- Authentication and data-link encryption can prevent in the presence of outsiders:
 - Sybil
 - Injection and modification prevent
 - NOT PREVENTED: HELLO and sinkhole attacks
- Insider attacks: link-layer security does not prevent the above attacks. Insider attacks and wormhole attacks (coming from either insider or outsiders) are the most difficult to prevent

Countermeasures Summary (cont.)

- Sybil in the presence of insiders, use symmetric keys shared with the base station to minimize the number of identities an attacker can pretend he has
- HELLO attacks: verify that links are bidirectional using a mutual authentication hand-shake protocol
- Wormholes: use location, time constraints or directional antenna
- Selective Forwarding: use multi-path??? What is the cost associated with this?
- Use authenticated broadcast