Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

Chris Karlof and David Wagner

Bharath Ramesh

Inherent Limitations in Wireless Sensor Networks

- Insecure wireless communication
- Limited node capabilities
- Possible insider threats.
- Every aspect designed with power in mind
- End-to-end security mechanisms harder to deploy, intermediate nodes need direct access to the content of the messages.
- Adversaries can use powerful laptops with high energy and long range communication to attack the network

Basic Terminology

- Base station / sinks
- Data flow
- Sources / nodes / motes
- Aggregation points

Traffic Pattern

- Many-to-one
- One-to-many
- Local Communication

Previous Proposed Methods

- SEAD, Secure pebblenets: Secure routing for ad-hoc network using symmetric key cryptography.
- Punishment, reporting and grudges against selfish nodes.
- SNEP: Confidentiality, authentication and freshness between nodes and sink
- µTESLA: Authenticated broadcast

Security Considerations – Network assumptions

- Wireless communication, radio links are insecure
- Malicious nodes installed by adversary
- Access to all data and code from compromised nodes
- Physical and MAC layer susceptible to direct attacks

Security Considerations – Trust Requirement

- Base station are trustworthy, they interface with outside world
- Aggregation point combine message correctly and forward to base station

Security Considerations – Threat Models

Classes of attackers

- Mote class
- Laptop class

Types of attackers

- Outsider attacks
- Insider attacks

Security Considerations – Security goals

Ideal world goals

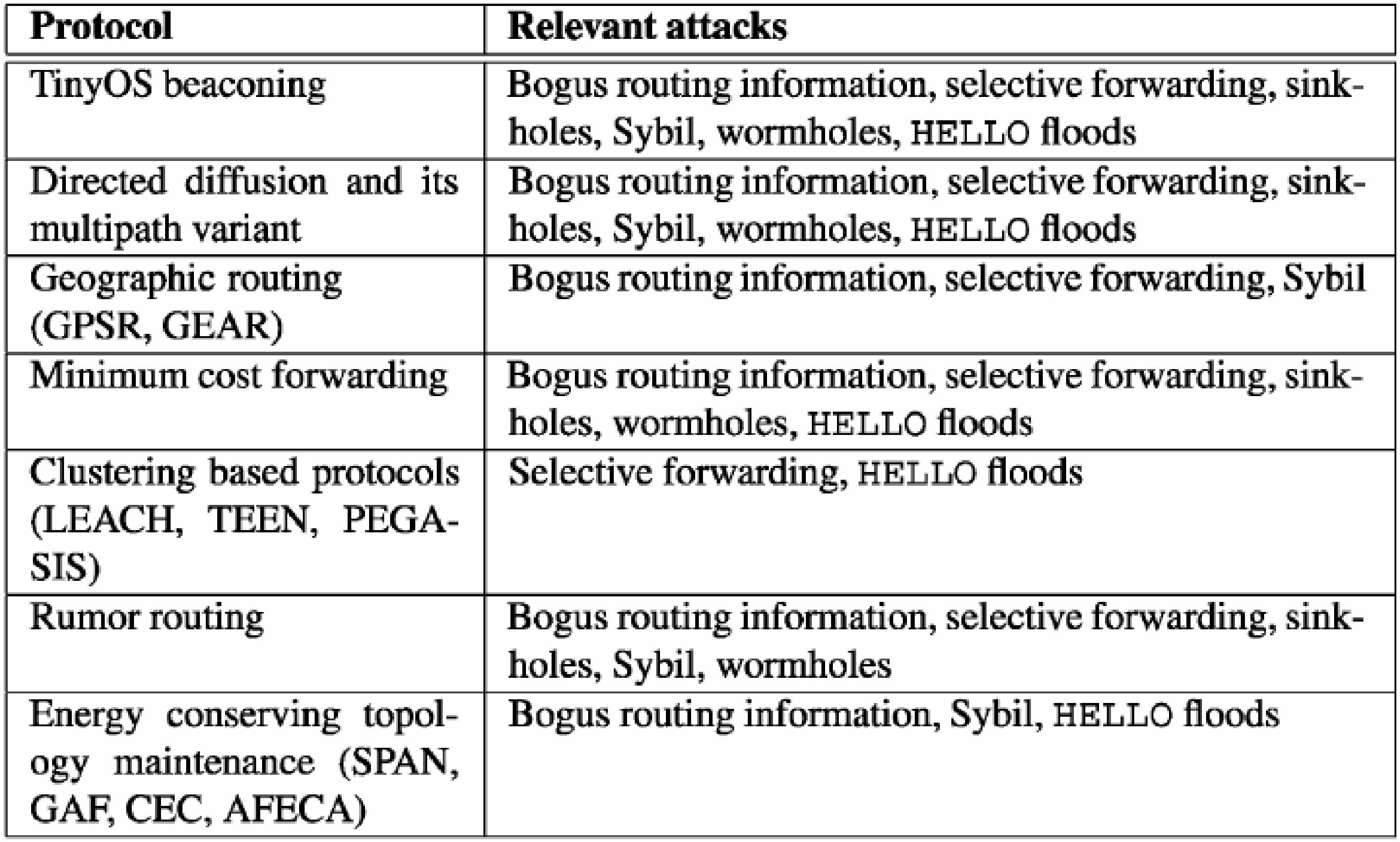
- Confidentiality
- Integrity
- Authenticity
- Availability of messages

The best goal – graceful degradation in presence of inside attacker

Possible Attacks

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

Summary of 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

Countermeasures

- Outsider and Link layer security – simple link layer encryption and authentication using globally shared keys
- Sybil attack – unique shared key with base station
- HELLO flood attack – verify bidirectionality of link, authenticate neighbors with identity verification protocol
- Wormhole and sinkhole attacks – very difficult to defend against, geographical protocols can do a good job

Countermeasures – contd.

- Leveraging global knowledge – limited network size, well structured/controlled topology
- Authenticated broadcast and flooding – HELLO messages to be authenticated

Conclusion

- Secure routing is vital to the acceptance and use of sensor networks
- Left open to the designed of sensor network routing protocol
- Link layer encryption and authentication
- Security issues to be addressed during routing protocol designs