

# Secure Routing in Wireless Sensor Networks

## Introduction to Wireless Sensor Networks

Ida Siahaan / Leonardo Fernandes

DIT

# Outline

- 1 Motivation
- 2 Wireless Sensor Networks Routing
  - Directed Diffusion
- 3 Security in Wireless Sensor Networks
  - Security Requirements
  - Security Threats
- 4 Countermeasures
  - Outsider attacks and link layer security
  - The Sybil attack
  - HELLO flood attacks
  - Wormhole and sinkhole attacks
  - Leveraging global knowledge
  - Selective forwarding
  - Authenticated broadcast
- 5 Example of Secure Sensor Network Routing Protocol
  - Attacked Directed Diffusion
  - Proposed Solution for Directed Diffusion

## Motivation

- Current routing protocols optimize for the limited capabilities of nodes and the application-specific nature of networks, But do not consider security
- Security is a basic requirement of most applications
  - ▶ Industry
  - ▶ Surveillance
  - ▶ Health Systems
  - ▶ Military Applications
- in-network processing makes end-to-end security mechanisms harder to deploy because intermediate nodes need direct access to the contents of the messages

## Wireless Sensor Networks Routing

- WSN's are resource constrained
- Multihop vs single hop topologies
- Routing is usually data-centric rather than address-centric
- Example: Directed Diffusion

# Directed Diffusion

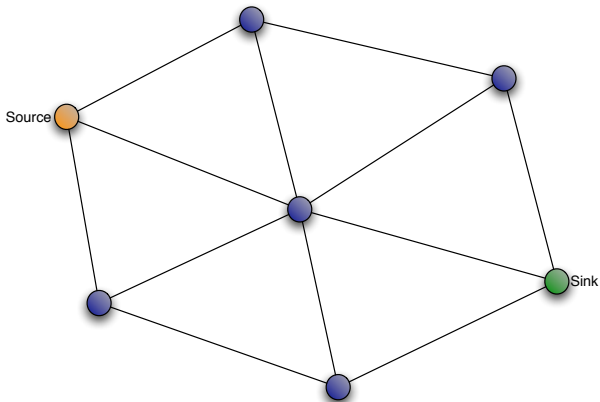


Figure: A simple scenario

# Directed Diffusion

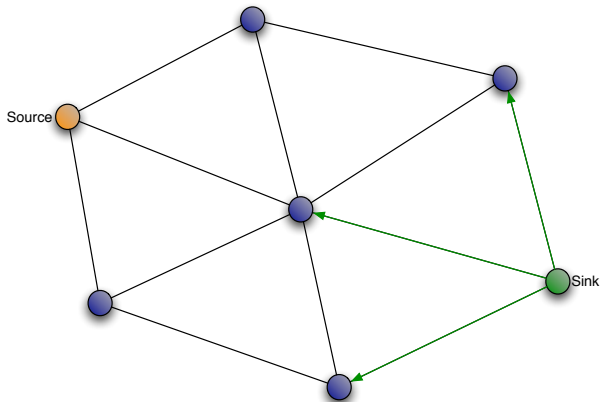


Figure: Interest propagation

# Directed Diffusion

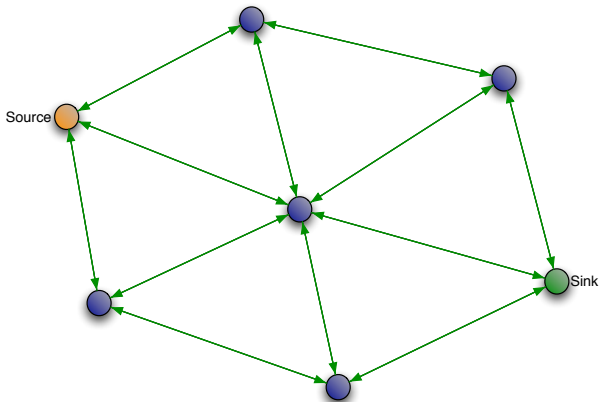
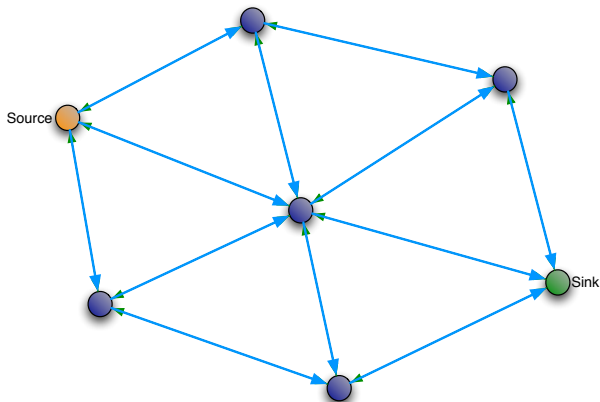


Figure: Interest propagation

# Directed Diffusion



**Figure:** Low Rate Messages: At this point the sink needs to decide which incoming path to reinforce. The directed diffusion description does not specify how this choice should be done, leaving it as a design choice. One simple possibility could be to include in the low rate messages a Hop Count value, so that the sink can choose the shortest path.



# Directed Diffusion

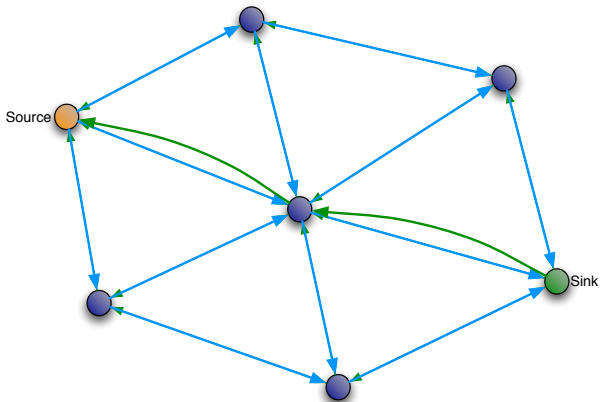


Figure: Reinforcement

# Directed Diffusion

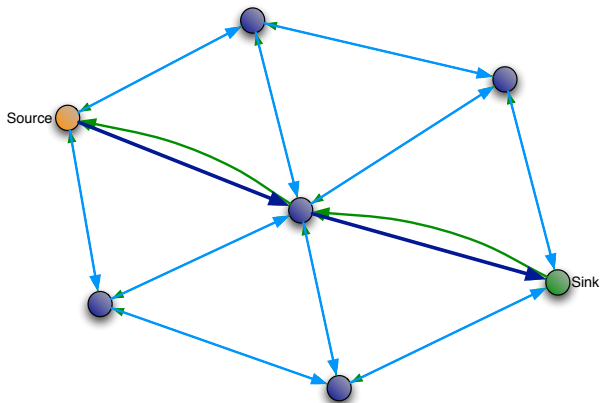


Figure: Data Delivery Along Reinforced Path

# Directed Diffusion

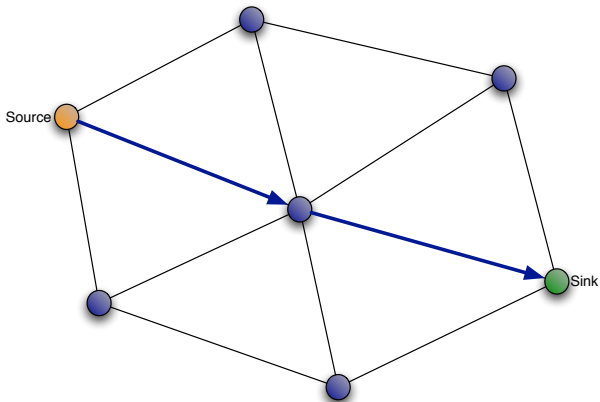


Figure: Data Delivery Along Reinforced Path

## Security Requirements

- **Authentication** Verifying that principals are who they claim to be can be achieved through appropriate proof of identity (i.e. encrypted signature)
- **Integrity** Ensure that information is not changed in transit, either due to malicious intent or by accident
- **Data Confidentiality** In most applications nodes communicate very sensitive data such as surveillance information and industrial secrets. Such applications need to rely on confidentiality. The standard approach for keeping confidentiality is through the use of encryption
- **Data Freshness** To ensure the freshness of each message such that the data is recent, and to ensure that no old messages can be replayed
- **Availability** We can lose the availability of a sensor due to the loss of energy because of computation and communication

- **Self-Organization** Distributed sensor networks must self-organize to support multihop routing. Such self organization is very hard to be done in a secure way
- **Secure Localization** The utility of a sensor network often relies on its ability to accurately and automatically locate each sensor in the network. However, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals, etc

## Security Threats

- **Spoofer, altered, or replayed routing information** Attacks targeted at the routing information exchanged between nodes so that adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, and increase end-to-end latency.
- **Selective forwarding** Malicious nodes in multi-hop networks may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further.
- **Sinkhole attacks** The adversary collects nearly all the traffic from a particular area through a compromised node, creating a sinkhole with the malicious node at the center.
- **Sybil attacks** A single adversary node presents multiple identities to other nodes in the network [2].

- **Wormholes** An adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part [6].
- **HELLO Flood attacks** Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker with large transmission power could convince every node in the network that the adversary is its neighbor.
- **Acknowledgment spoofing** Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgments for “overheard” packets addressed to neighboring nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive.

## Threat model - Characteristics - Security model

- Threat models:
  - ▶ sensor-class (mote-class) attackers vs laptop-class attacker
  - ▶ outsider attacks vs insider attacks
- Characteristics of sensor networks:
  - ▶ power is a scarce resource
  - ▶ very little computational power  $\leftrightarrow$  public-key cryptography is so expensive as to be unusable
  - ▶ communication bandwidth is extremely limited and multihop routing is used as a way of saving energy
- Security model:
  - ▶ insecure wireless communication
  - ▶ limited node capabilities
  - ▶ possible insider threats
  - ▶ the adversaries can use laptops with high energy and long range communication to attack the network



## Outsider attacks and link layer security

- Link layer encryption and authentication using a globally shared key.
- The Sybil attack is not relevant (nodes are unwilling to accept even a single identity of the adversary).
- The majority of selective forwarding and sinkhole attacks are not possible (the adversary is prevented from joining the topology).
- Attacks not countered are wormhole attacks and HELLO flood attacks:
  - ▶ nothing prevents adversary from using a wormhole to tunnel packets sent by legitimate nodes in one part of the network to legitimate nodes in another part to convince them they are neighbors
  - ▶ by amplifying an overheard broadcast packet with sufficient power to be received by every node in the network
- Ineffective in presence of insider attacks or compromised nodes.  
↔ Insiders can attack the network by spoofing or injecting bogus routing information, creating sinkholes, selectively forwarding packets, using the Sybil attack, and broadcasting HELLO floods.

## The Sybil attack

- Every node share a unique symmetric key with a trusted base station.
- Two nodes use a Needham-Schroeder like protocol to verify each other's identity and establish a shared key.
- A pair of neighboring nodes can use the resulting key to implement an authenticated, encrypted link between them.
- The base station limits the number of neighbors a node is allowed to have
  - ↔ to prevent an insider from wandering around a stationary network and establishing shared keys with every node in the network.

## HELLO flood attacks

- Verification of the bidirectionality of a link before taking meaningful action based on a message received over that link.
- Identity verification protocol as for the Sybil attack is sufficient for prevention.

## Wormhole and sinkhole attacks

- Wormholes are hard to detect because they use a private, out-of-band channel invisible to the underlying sensor network.
- A technique for detecting wormhole attacks is presented in [5], but it requires extremely tight time synchronization.
- Sinkholes are difficult to defend against 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.
- Protocols that construct a topology initiated by a base station are most susceptible to wormhole and sinkhole attacks.
- Solution: carefully design routing protocols in which wormholes and sinkholes are meaningless eg. class of geographic routing protocols.
  - ↔ Geographic protocols construct a topology on demand using only localized interactions and information and without initiation from the base station.

## Leveraging global knowledge

- Challenge in securing large sensor networks is their inherent self-organizing, decentralized nature.
- To account for topology changes due to radio interference or node failure, nodes would periodically update a base station with the appropriate information.
- Drastic or suspicious changes to the topology might indicate a node compromise.
- Restricting the structure of the topology can eliminate the requirement for nodes to advertise their locations if all nodes' locations are well known, eg. nodes can be arranged in a grid with square, triangular, or hex shaped cells.

## Selective forwarding

- Multipath routing: Messages routed over  $n$  paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most  $n$  compromised nodes and offer probabilistic protection when over  $n$  nodes are compromised.
- Completely disjoint paths are difficult to create.
- Braided paths [11]: nodes may be in common, but no links in common (i.e., no two consecutive nodes in common).
- Multiple braided paths may provide probabilistic protection against selective forwarding and use only localized information.
- Dynamic choice of a packet's next hop probabilistically from a set of possible candidates to reduce the chances of an adversary gaining complete control of a data flow.

## Authenticated broadcast

- Base stations are trustworthy, adversaries must not be able to spoof broadcast or flooded messages from any base station.
- $\mu$ TESLA [9] is a protocol for efficient, authenticated broadcast and flooding.
  - ▶ Symmetric key cryptography and minimal packet overhead.
  - ▶ Asymmetry for authenticated broadcast and flooding by using delayed key disclosure and one-way key chains
  - ▶ Preventing replay  $\leftrightarrow$  messages authenticated with previously disclosed keys are ignored.
  - ▶ Loose time synchronization.

# Attacked Directed Diffusion

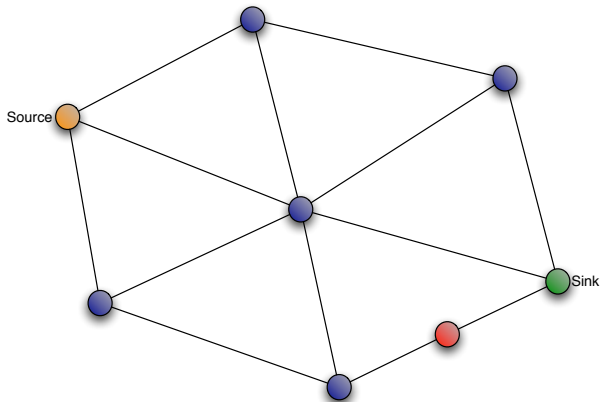


Figure: Simple Attack



# Directed Diffusion

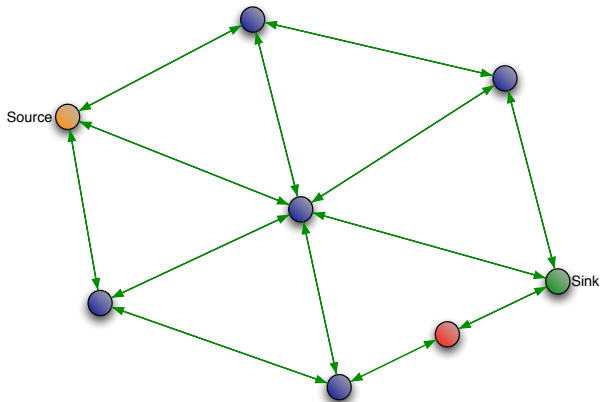


Figure: Interest Propagation is Normal

# Directed Diffusion

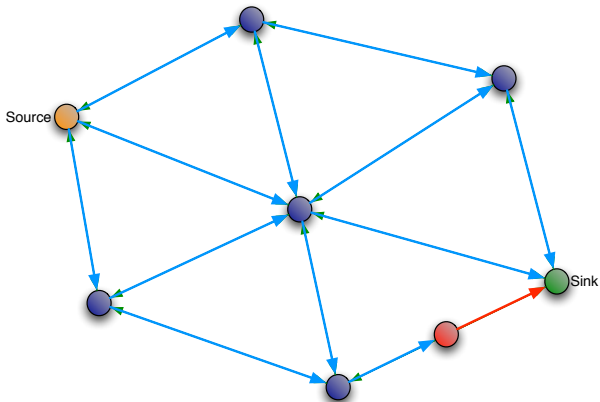


Figure: Attacker Alters the Informed Hop Count

# Directed Diffusion

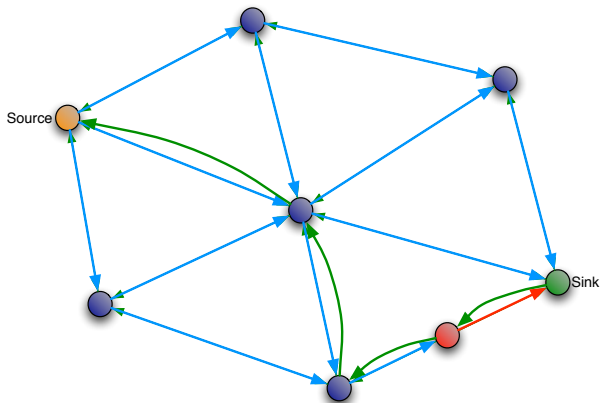


Figure: Attacker Selected for Reinforcement

# Directed Diffusion

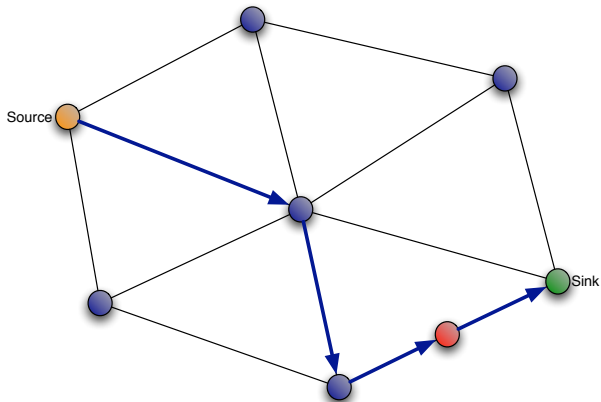


Figure: Attacker has Access to All Data

## Proposed Solution for Directed Diffusion

- We ensure data confidentiality (Data chunk) and data integrity (Requirement/Hopcount chunk)
- SNEP (Secure Network Encryption Protocol):
  - ▶ providing data confidentiality, two-party data authentication, and data freshness, with low overhead
  - ▶ do not deal completely with compromised sensors, merely ensure that compromising a single sensor does not reveal the keys of all the sensors in the network.

$E = \{D\}_{\langle \mathcal{K}_{encr}, C \rangle}$  {to achieve confidentiality, use encrypted data}

$M = \text{MAC}(\mathcal{K}_{mac}, C|\{E\})$  {to achieve data integrity, use a message authentication code (MAC)}

- ▶  $D$ : data
- ▶  $\mathcal{K}_{encr}$ : encryption key
- ▶  $C$ : counter
- ▶  $\mathcal{K}_{encr}$  and  $\mathcal{K}_{mac}$ : derived from the master secret key  $K$

## Summary

- Current routing protocols optimize for the limited capabilities of nodes and the application-specific nature of networks.
- Secure sensor network routing protocols requirements, threats and countermeasures.
- Routing security must be included as part of the overall sensor network design.

# For Further Reading I



J.N. Al-Karaki and A.E. Kamal.

Routing techniques in wireless sensor networks: a survey.

*IEEE Wireless Communications*, 11(6):6–28, 2004.



J.R. Douceur.

The sybil attack.

In *1st International Workshop on Peer-to-Peer Systems (IPTPS02)*,  
March 2003.



D. Ganesan, B. Krishnamachari, A. Woo, D. Culler, D. Estrin, and  
S. Wicker.

An empirical study of epidemic algorithms in large scale multihop  
wireless networks.

Technical report, 2002.



Z.J. Haas, J.Y. Halpern, and L. Li.

Gossip-based ad hoc routing.

*IEEE/ACM Trans. Netw.*, 14(3):479–491, 2006.

# For Further Reading II



Y. Hu, A. Perrig, and D. Johnson.

Wormhole detection in wireless ad hoc networks.  
Technical report, 2002.



Y.C. Hu, A. Perrig, and D.B. Johnson.

Wormhole detection in wireless ad hoc networks.  
Tech. Rep. TR01-384, Department of Computer Science, Rice  
University, June 2002.



C. Karlof and D. Wagner.

Secure routing in wireless sensor networks: Attacks and  
countermeasures.

*In First IEEE International Workshop on Sensor Network Protocols and  
Applications*, pages 113–127, May 2003.






J. Kulik, W. Heinzelman, and H. Balakrishnan.

Negotiation-based protocols for disseminating information in wireless  
sensor networks.

*Wirel. Netw.*, 8(2/3):169–185, 2002.



## For Further Reading III

-  A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler.  
Spins: security protocols for sensor networks.  
*Wirel. Netw.*, 8(5):521–534, 2002.
-  J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary.  
Wireless sensor network security: A survey, 2006.
-  Y. Yu, R. Govindan, and D. Estrin.  
Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks.  
Technical report, 2001.