Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

by

Chris Karlof, David Wagner

Presented by Guillaume Marceau

Using slides from Ivor Rodrigues

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

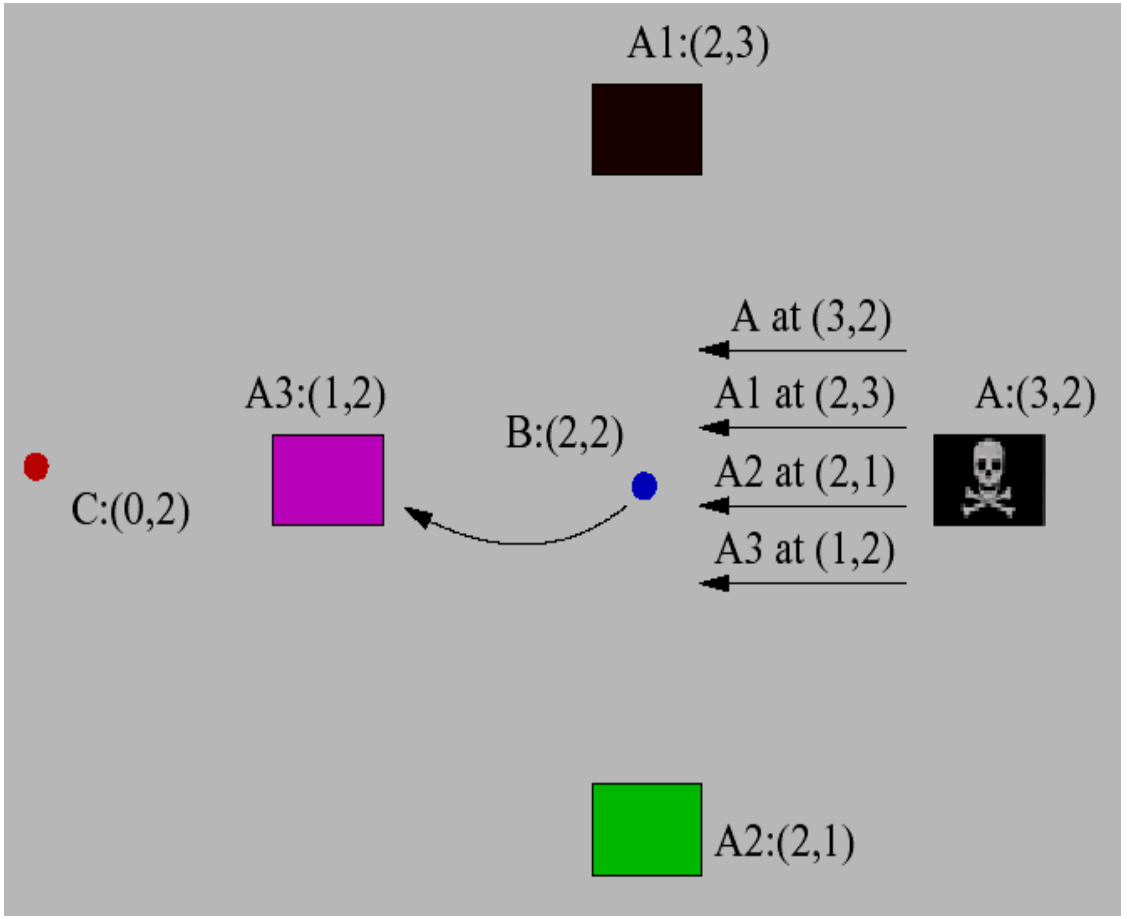
Selective Forwarding

- 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

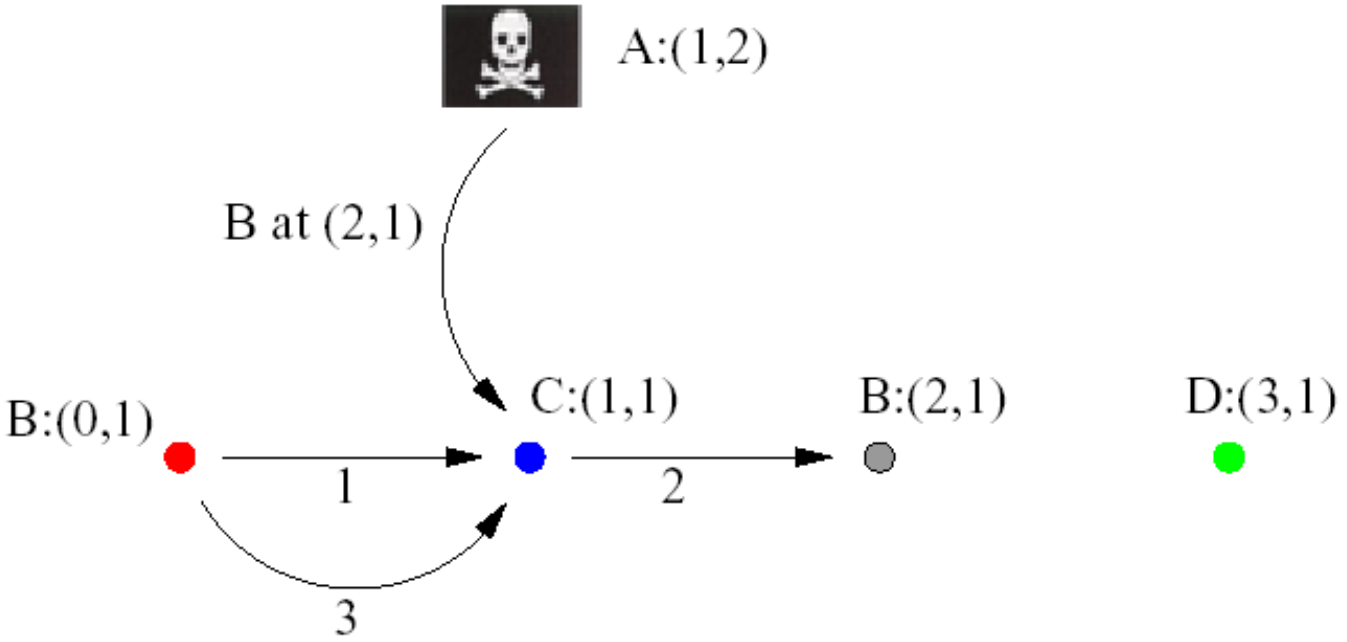
Geographical Attacks and Attackers



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

Geographical Attacks and Attackers

– GPSR.



Minimum cost forwarding

- Compute a distributed shortest-path
- Attacks
  - Very susceptible to sinkholes attacks
  - Very easy to stage a HELLO flood

LEACH: low-energy adaptive clustering hierarchy

- Assumes that transmission to the base station is always possible, but costly
- Aggregate motes into cluster. Rotate the cluster-head
- Attacks
  - HELLO flood
  - Sybil attack to impersonate all the cluster heads

Rumor routing

- Similar to the vehicular routing paper
- Remembers the route taken
- To return packets reverse the recorded route

- Attacks:
  - Sink messages passing by
  - Jellyfish attack: Forward multiple copies of the agent
  - Reset TTL, keep previously seen nodes

GAF, geography-informed energy conservation

- Only one mote awake per square
- Attacks:
  - Spoof messages, disable the entire network

SPAN

- Coordinators always stay awake
- Negotiated step up and step down

- Attacks:
  - Fake a message, wins the coordinator election

Countermeasures

Sybil attack:

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

Countermeasures

Hello Flooding:

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

Countermeasures

Wormhole and sinkhole attacks:

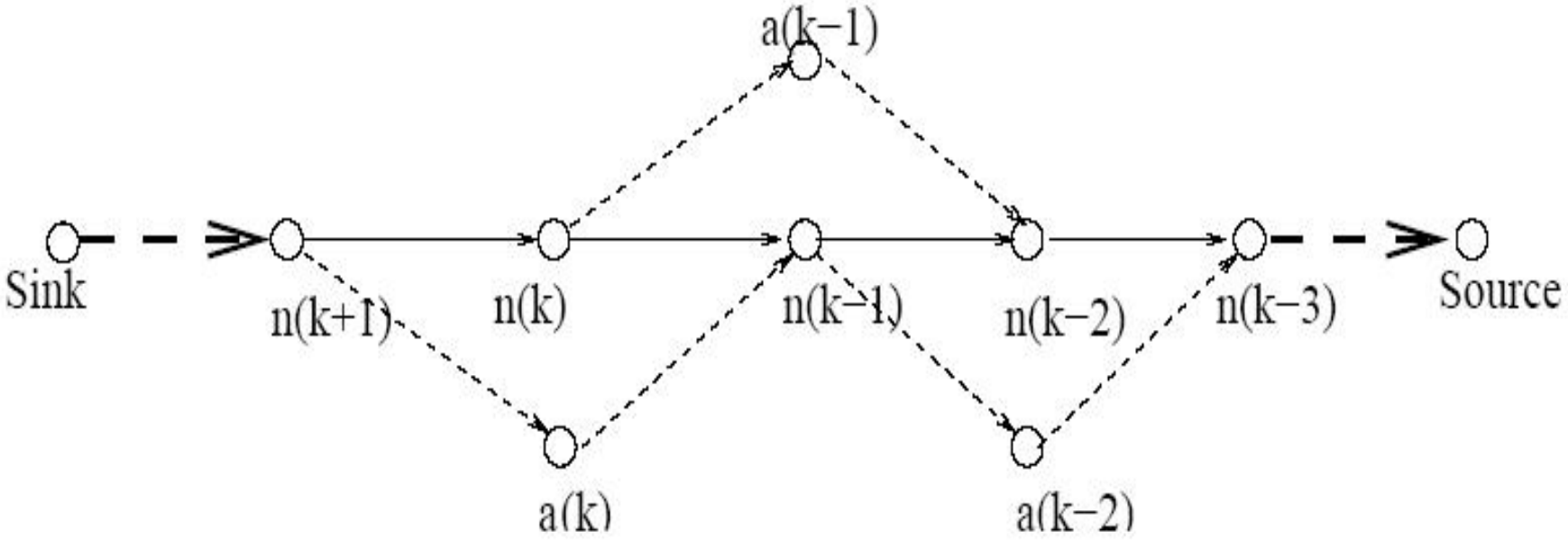
- Use time and distance
- Geographic routing resists such attacks well
- Traffic directed towards Base station and not elsewhere like sinkholes

Leveraging Global knowledge

- Fixed number of nodes
- Fixed topology.

Selective Forwarding

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



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?

Few Observations

- What happens if someone spoofs a legitimate node identity and paralyze it. What are the countermeasures? Is it 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)