



Detecting Wormhole Attacks in Wireless Networks Using Local Neighborhood Information

W. Znaidi, M. Minier and JP. Babau

Centre d'Innovations en Télécommunication & Intégration
de services

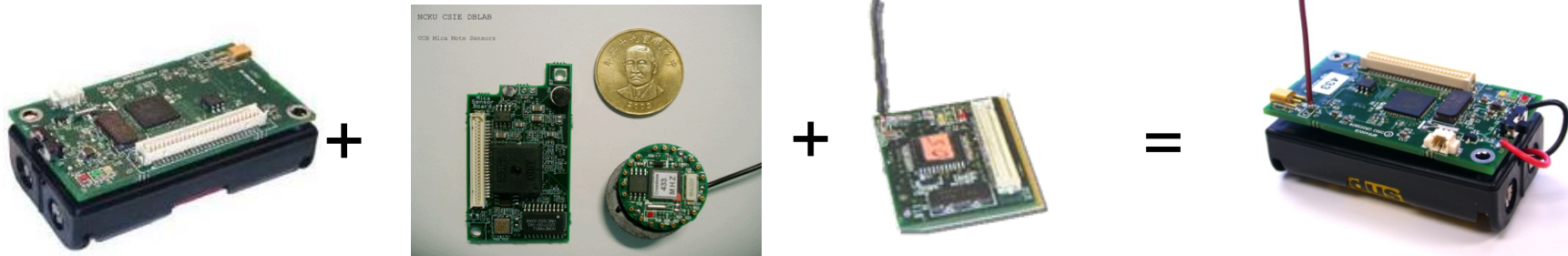
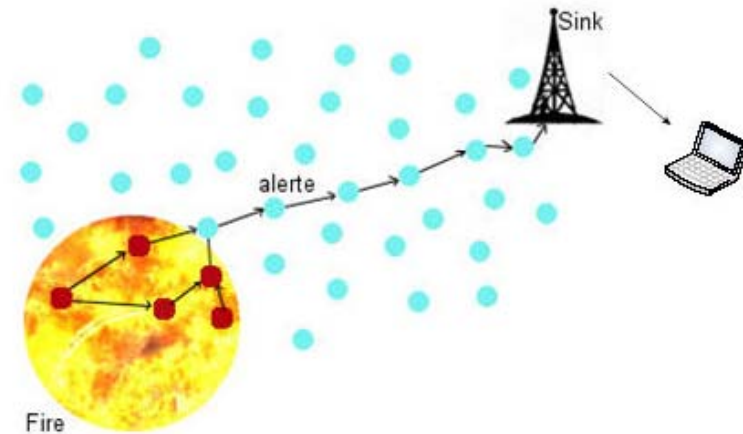
wassim.znaidi@insa-lyon.fr

Outline

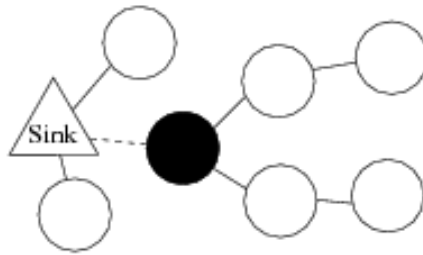
- Introduction and related work
- Our proposition
- Simulations and some results
- Conclusion

a Wireless Sensors Network

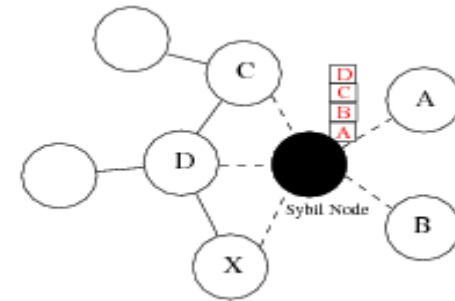
- No infrastructure
- Hundreds/Thousands of tiny devices
- Difficult/impossible access to nodes
- A typical application: the fire detection
- Sensor Devices :
 - Have limited energy, memory and computation resources
 - No tamper-resistant devices (physical compromising)



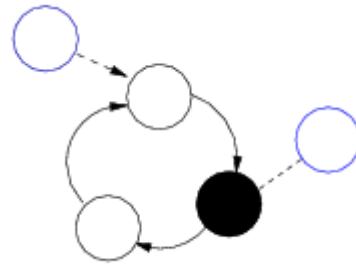
Attacks



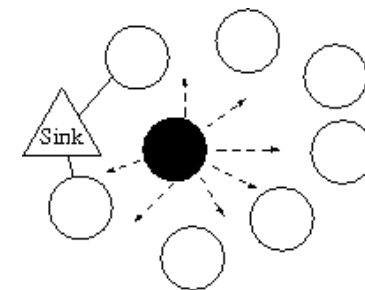
Sinkhole attack



Sybil attack



Routing cycle attack

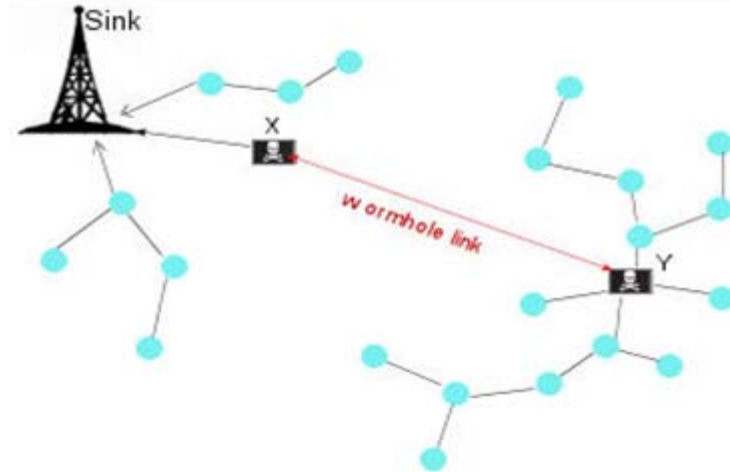


Hello flooding attack

Others attacks: Tampering, jamming, blackholes, **wormhole**, collision, desynchronisation, traffic analysis, eavesdropping, ...

What is a wormhole?

- **Wormhole Attack:** Two wireless devices (X and Y) connected with an out-of-band connection (by cable or high-power Wireless radios).



- Y captures wireless transmissions in its neighborhood, transfers them through Wormhole Link to X, and X re-injects all the packets there into the network (and vice versa).
- Characteristics:
 - Dangerous : all the traffic attracted to X-Y
 - Easy to mount and to launch
 - Hard to detect

What is a wormhole?

- Network effect:
 - Routing protocol may choose routes that contains the wormhole link
 - Monitor traffic or drop packets, etc.
 - distorts the network topology

Our goal: Detection and prevention of the wormhole attack
in WSNs

Overview of some detection algorithms of wormhole attack

Protocol	Description	Drawbacks
Hu and al. 2003	Use of packet leaches with geographical and temporal information	requires synchronized clocks and GPS equipped devices
L. Hu and al. 2004	Use the direction of the antenna Of the neighbors	use of directional antenna
R. Maheshwari and al. 2007	Search for forbidden structure caused by the wormhole	Difficulty to compute a parameter to determine forbidden structure

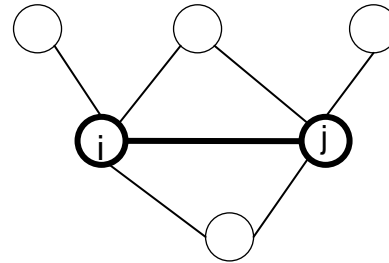
Our detection algorithm

- Main idea:
 - Every sensor node computes the connectivity degree of its neighbors
 - Using this parameter, each node declares if it detected the presence of the wormhole
- Assumption:
 - Bidirectional link
 - Static and dense network

Background used

- Edge-clustering coefficient:

$$C_{i,j}^g = \frac{z_{i,j}^g}{s_{i,j}^g}$$

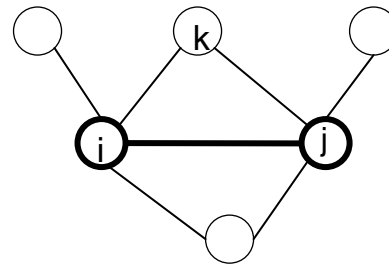


Ex. $g=3$

$$C_{i,j}^3 = \frac{2}{4}$$

- Modified edge-clustering coefficient:

$$C_{i,j \setminus X}^g = \frac{z_{i,j \setminus X}^g}{s_{i,j \setminus X}^g}$$

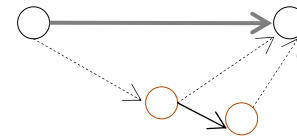


Ex. $g=3$

$$C_{i,j \setminus k}^3 = \frac{1}{3}$$

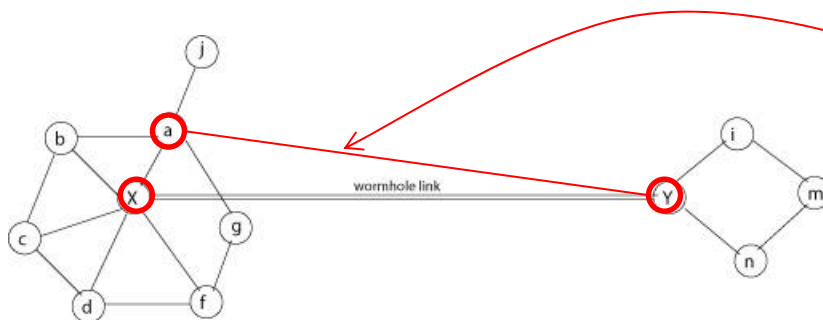
Def. of the wormhole using the edge-clustering coefficient

- Assumption: in a dense network such a WSN, we suppose that every couple of sensor nodes has at least one common 1-2 hop neighbor



- Let a and b two nodes in the WSN:
a declares b as a wormhole if $\exists X \in V_1(b)$ such $C_{a, X \setminus b}^{g=3,4} = 0$

- Example:



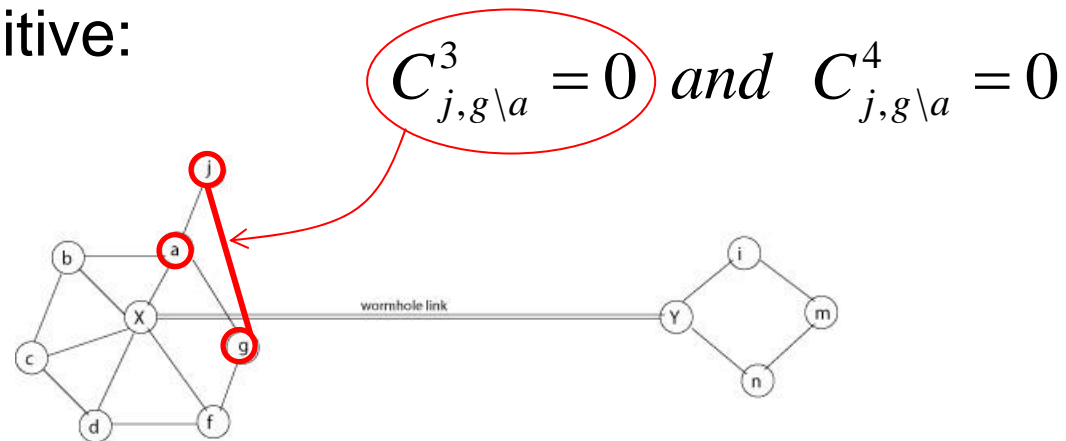
$$C_{a, y \setminus X}^3 = 0 \text{ and } C_{a, y \setminus X}^4 = 0$$

Node a declares X as a wormhole node

Limitation and Solutions

- Generalization: X is away l -hop from node a
a declares X as a wormhole if $\exists k \in V_1(X)$ such $C_{a,k \setminus X}^{l+2} = 0$

- But: False positive:



- Solution: use the voting technique: every node declares a wormhole only if it received a sufficient number of alerts.

Proposed algorithm

1. **Neighborhood discovery**: each node maintains the list of its 1-hop and 2-hop neighbors.
2. **Computing**: each node computes first C_{\dots}^3 , if it's = 0 then it computes C_{\dots}^4 .
3. **Isolation**: if a node is declared as a wormhole, it uses the voting technique

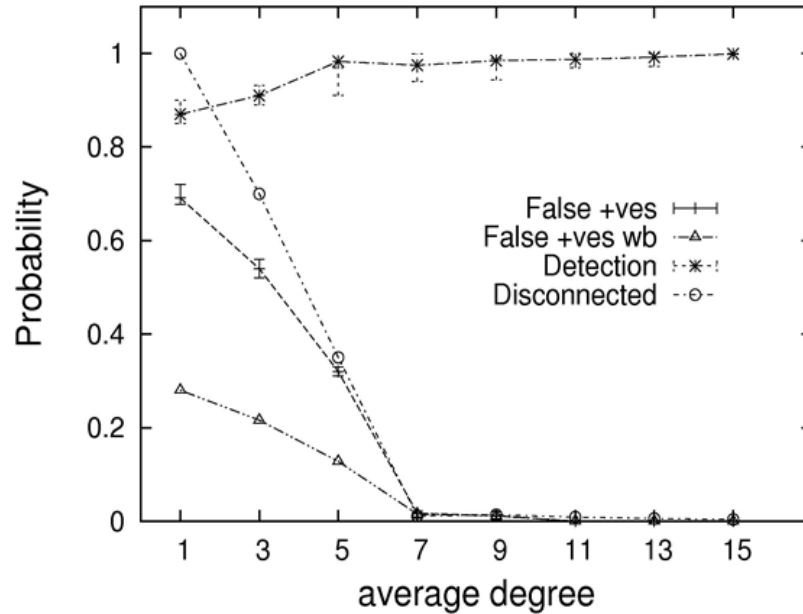
Our algorithm is distributed, uses local neighborhood information and no extra hardware.

Simulations

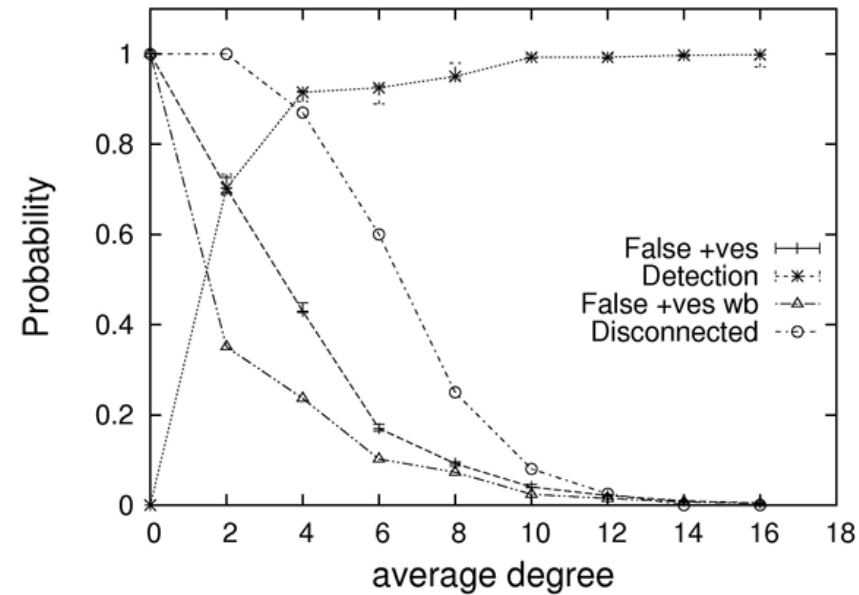
- Scenario:
 - Single wormhole
 - 2 different topologies: random and grid distribution
 - 125 nodes over 400mx400m
 - Disk graph connectivity model
 - IEEE 802.11 MAC layer
- WSNNet Simulator (developed in CITI Lab)
<http://wsnet.gforge.inria.fr/>

Some results

Grid topology

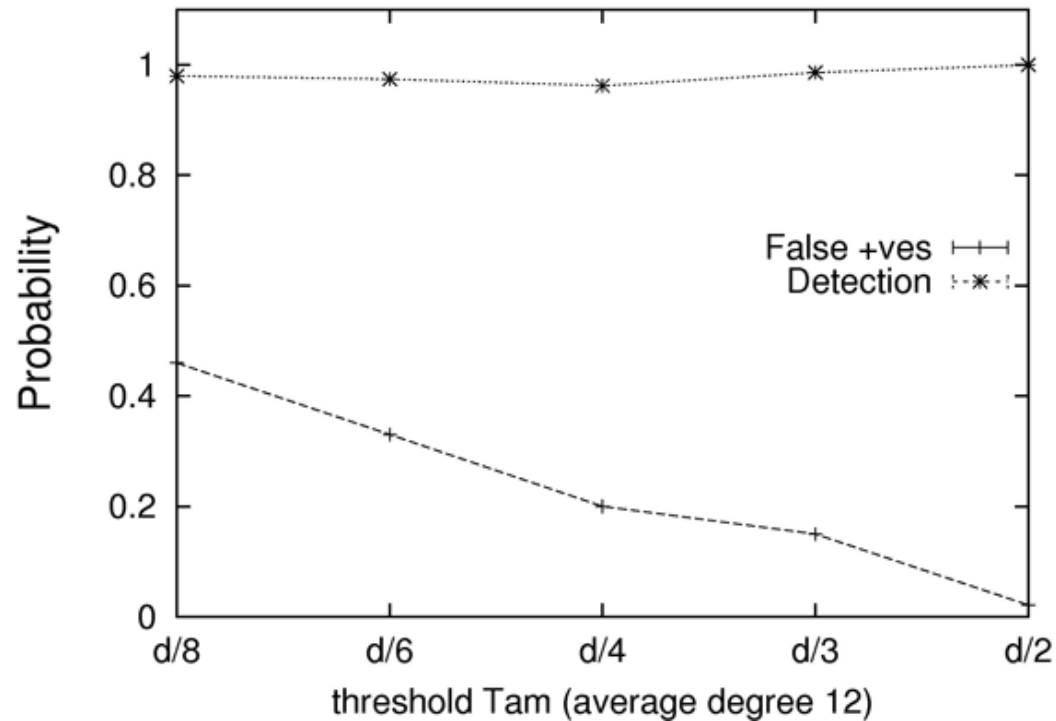


Random topology



Probability of wormhole detection, graph disconnection, false positive and false positive without boundary nodes

Some results



Impact of the threshold T_{am} on the false positive probability

Conclusion

- Our algorithm is resilient to wormhole attack:
 - Without relying on any location inform (GPS)
 - Without introducing any special hardware
 - No packet added
- Our algorithm is simple, practical, local and provides a 100% detection of the wormhole detection.
- The mechanism used in our protocol such the edge-clustering coefficient, can be used for other proposals such auto-organization in WSNs

Perspectives

- Secured WSN: key management and access control, aggregation of MAC, Trust management
- Risk management and security polities



Thank you !

Questions ?



Detecting Wormhole Attacks in Wireless Networks Using Local Neighborhood Information

W. Znaidi, M. Minier and JP. Babau

Centre d'Innovations en Télécommunication & Intégration
de services

wassim.znaidi@insa-lyon.fr

PIMRC 2008