

MOBISEC 

June 3-5, 2009 - Turin, Italy

Safe, fault tolerant and
capture-resilient environmental
parameters survey using WSNs

Gianni Fenu and Gary Steri

University of Cagliari
Computer Science Department

Outline

- Introduction
- Model architecture and network functioning
- Data integrity and authenticity
- Capture-resilience
- Conclusions

Introduction

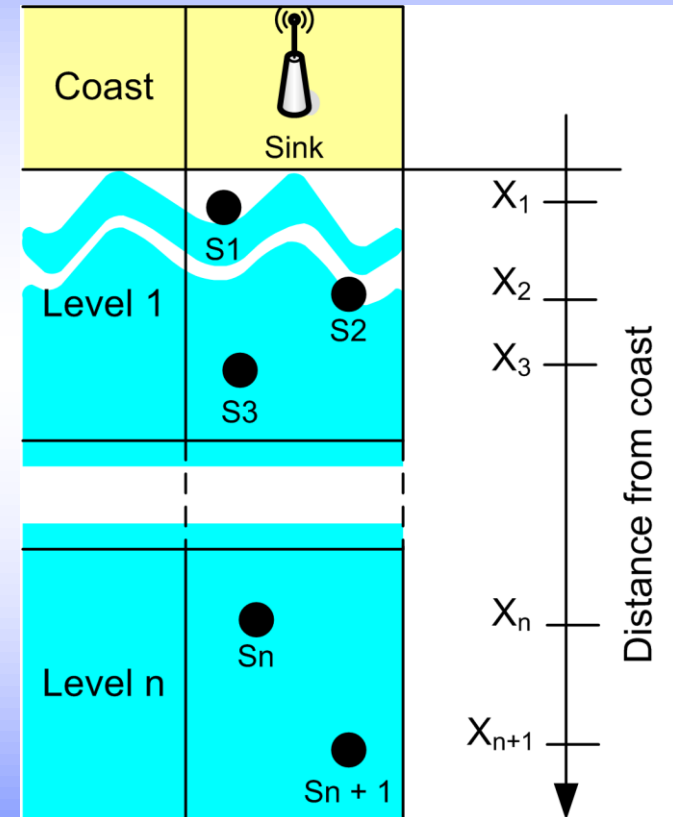
- SensorTree: network of wireless sensors installed on the sea surface to measure weather parameters
 - temperature
 - wind speed
 - luminosity

Outline

- Introduction
- **Model architecture and network functioning**
- Data integrity and authenticity
- Capture-resilience
- Conclusions

Model architecture and network functioning (1/4)

- Each node lies within a rigorous level architecture
- Indefinite number of levels
- Level's dimension determined by transmission range (height/width = 5/4)
- No overlapping areas

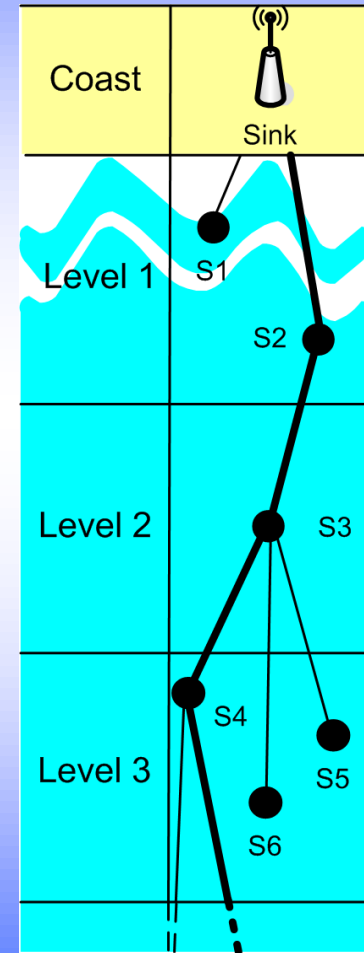


Model architecture and network functioning (2/4)

- Tree construction:
 - downward network growth starting from the Sink node
 - a node s1 sends a PowerOn request containing a list of parameters
 - Sink sends a PowerOn reply, adds s1 in its children list and mark it as “preferred” child. Sink is the “preferred” root of s1
 - in addition for subsequent nodes:
 - s1 does not reply to the PowerOn request sent by s2
 - Sink checks battery levels for preferred child choice

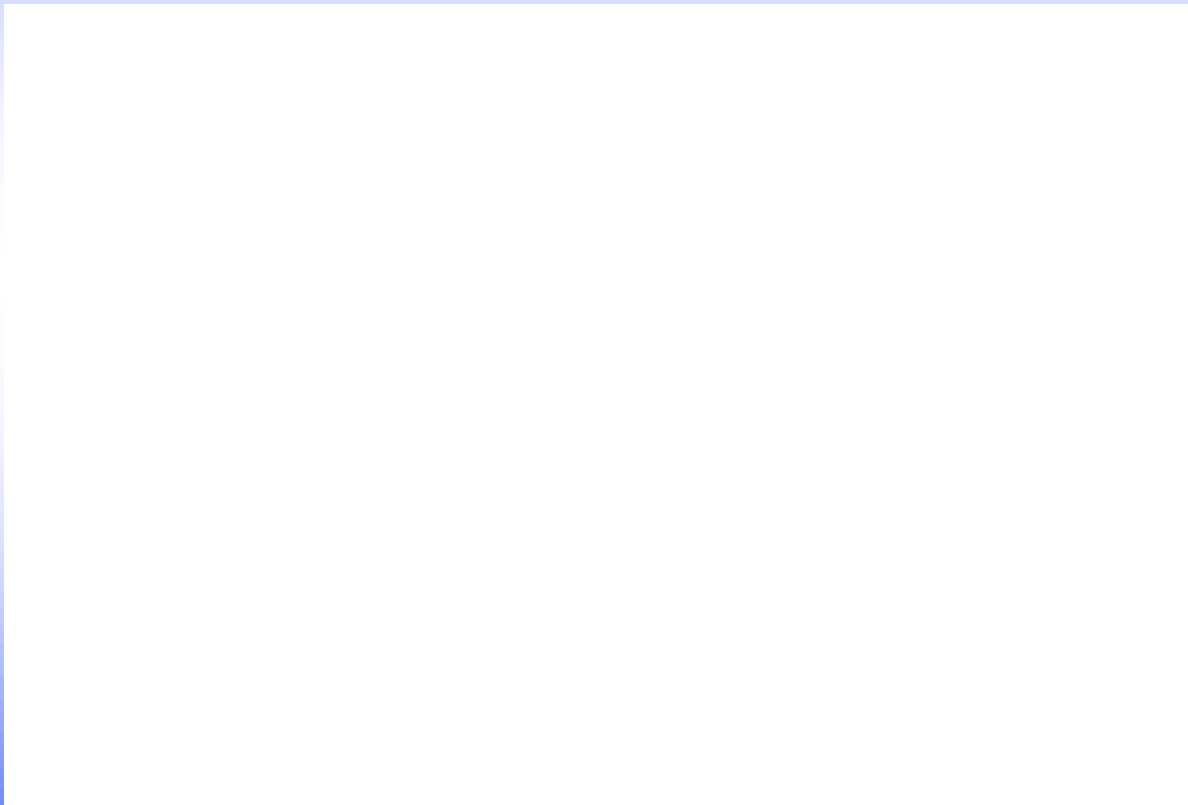
Model architecture and network functioning (3/4)

- Network convergence :
 - Every T seconds each node sends a StatusRefresh notification
 - Tree tracking: refresh procedure propagated recursively until the lower level
 - 4 recursive query modes:
 - all nodes
 - one node
 - one level
 - a point



Model architecture and network functioning (4/4)

- Automatic rejoining:



Outline

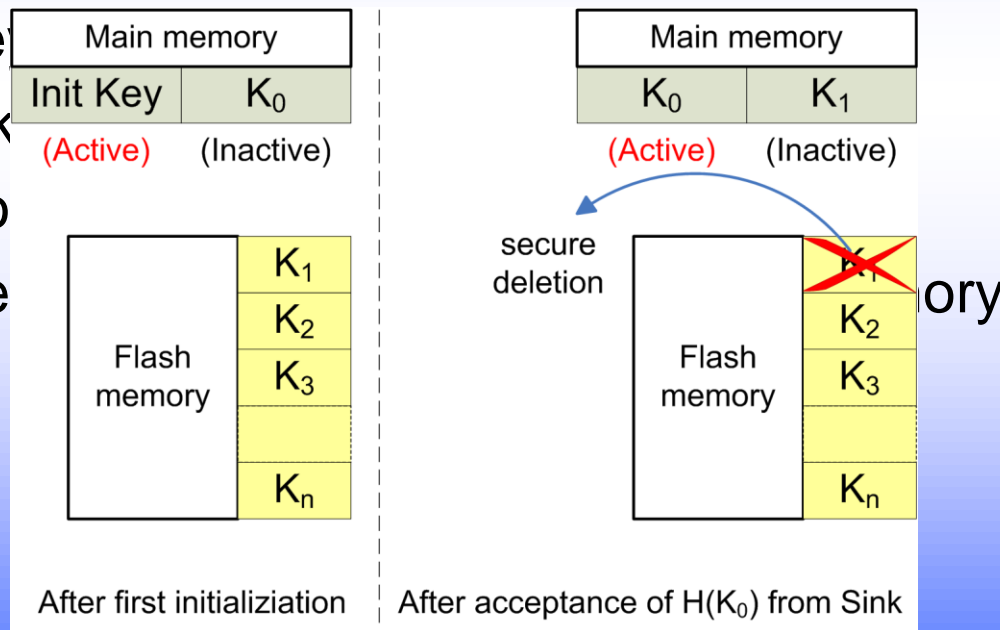
- Introduction
- Model architecture and network functioning
- **Data integrity and authenticity**
- Capture-resilience
- Conclusions

Data integrity and authenticity (1/2)

■ Nodes initialization:

- each node needs a unique key (HMAC standard for messages authentication)

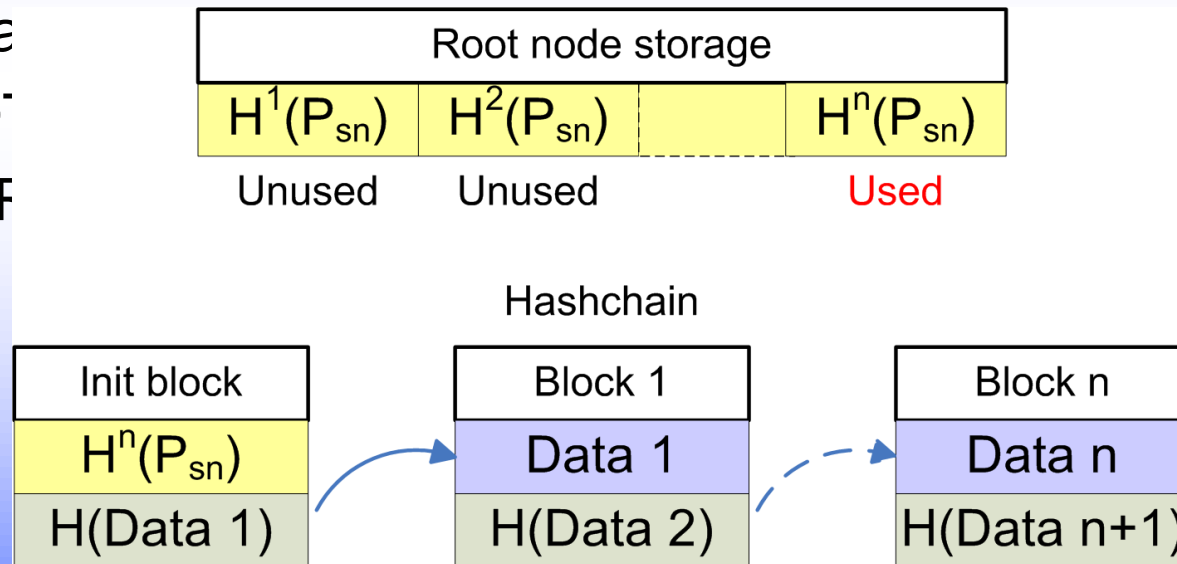
- first key
- list of keys
- hash of
- secure



Data integrity and authenticity (2/2)

- Data collection and hashchains:
 - each preferred root collects data from its children
 - haschains initializations for communicate with Sink

- h_n
- O
- TF



Outline

- Introduction
- Model architecture and network functioning
- Data integrity and authenticity
- **Capture-resilience**
- Conclusions

Capture resilience (1/2)

■ Problems:

- Physical protection of the nodes
- Main memories
 - electromigration stress due to long-term retention
 - traces for restoring information
- Secondary memories
 - transistors do not return fully to their initial state
 - it is possible to distinguish between previously programmed and not programmed transistors

Capture resilience (2/2)

■ Solutions:

- Active key and first key of the activation pool stored in the main memory only
 - keys are not used for a too long period of time
 - bit flipping
 - reverse current to reverse the electromigration stress in case of tamper detection
- Secure deletion from flash memory of the loaded keys
 - Gutmann, Schneier, DoD-3

Outline

- Introduction
- Model architecture and network functioning
- Data integrity and authenticity
- Capture-resilience
- **Conclusions**

Conclusions

- Simulator which fulfils all requirements of SensorTree network
- Ongoing development project for creating the network
- Tree structure
 - efficient communication between the nodes
 - minimizing the paths to Sink
- Level subdivision
 - critical areas detection
 - independent trees

Conclusions

- Improvements:
 - intra-level communications
 - some groups of nodes as landmarks
 - differentiation of data collection modes
 - control protocol to quickly solve tree interruptions
 - Sink mobility or multi-Sink configurations
 - cryptography