

# Security for distributed wireless sensor nodes

**Ingrid Verbauwhede**

Department of Electrical Engineering  
University of California Los Angeles

ingrid@ee.ucla.edu

1



## Outline

- Motivation
- Security attacks
- What is different, special to sensor networks
- Links to other security problems
- Topics of research

2



## Motivation

- security problems & cryptographic techniques to protect them.
- **Privacy** for individual sensors: *depends*
  - tank passes in a battlefield: not really needed
  - individual heart beats of patients: not much information
  - at home: sensor tells me that the jacuzzi is ready: not much information
- **Authentication** for individual sensors: *for sure*
  - don't want the enemy to inject false alarms on tank locations
  - don't want to adjust the insulin level of the wrong patient
  - don't need to know that my neighbor's jacuzzi is ready

3



## Sensor specific attacks ?

<b>Attack</b>	<b>solution</b>	<b>Sensor specific</b>
False messages Replay messages	authentication	no
Distributed Denial of service	Security checks in nodes (challenge response)	no
Jamming/interference Signal hiding	Spread Spectrum Radio (with non-linear codes)	no
Pattern or traffic analysis	Random activity, noise sources	no

Almost every attack to a sensor node has an equivalent in a regular network, or in radio communication.  
Main difference = energy drainage instead of performance drop

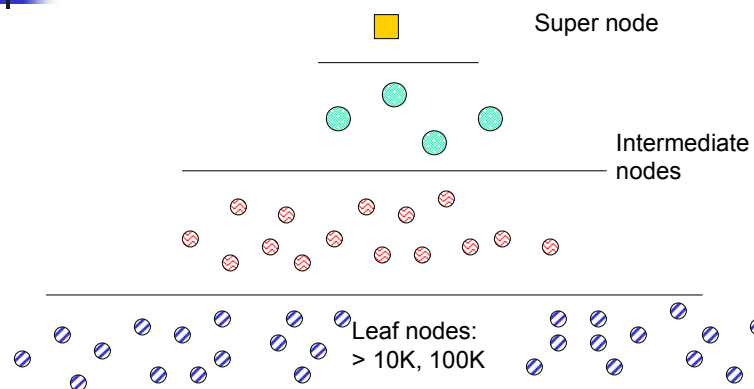
4

## Research approach

- Adapt security level to information content!
- Combine with distributed computing
- Assume a hierarchical structure

5

## Hierarchy of nodes



Hierarchy established dynamically, depending application or circumstances

6










## Assumptions

- Distributed network of heterogeneous nodes  
(different types of sensors, different levels of processing capabilities)
- nodes establish at hoc connections
- Assume the existence of a hierarchy of nodes, with
  - *hierarchy is dynamically established*
  - *hierarchy might change depending on application, power budget*
- the higher up in the hierarchy, the more energy is available and the higher the security level
- if an intermediate node is compromised, the tree below it will be.

7



## Hierarchy of security

	<b>Information content:</b>	<b>Energy availability</b>	<b>Security requirement</b>	<b>Trust Level:</b>
	highest	unlimited	highest	Top
	Distributed optimization	Medium	Medium	Medium
 	Low processing: •feature extraction •motion detection	Low	Low	Low
  	Extremely low •Short messages •Small set of possibilities •Yes/no or Red/green/blue	Extremely low	None to low	Assume zero, Build up

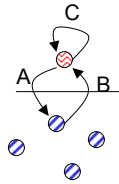
8



## Cryptographic techniques

Between Levels:

- Challenge response system (i.e. communication initiated by the higher level)
  - to avoid denial-of-service (energy drainage)
- Communication versus computation!



A: challenge (includes time factor, randomness)

B: response

C: verify response

- Response could contain requested information since possible answers are from limited set.
- Requires one-way hash function or encryption in leaf nodes.
- Requires two radio transmissions per leaf node!

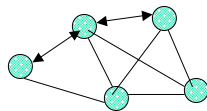
9



## Cryptographic techniques (cont.)

At intermediate levels:

- Set up "conference key",
- Combine with distributed computations & optimizations



$$\min( E_C + E_R + E_S )$$

Energy Computations, Energy Radio, Energy Security

Example: Burmester-Desmedt conference key protocol:

- exponentiation  $z_i$
- broadcast  $z_i$
- exponentiation,  $X_i = f(z_{i-1}, z_{i+1})$
- broadcast  $X_i$
- exponentiation, compute  $K = f(z_i, X_i)$

10



## Inference Control in database

---



Sensor data (similar to a “mystery box”)

- It is yellow
- It does not make noise
- It turns its head towards the sun



- Individual sensors: not much information content
- Data fusion: information extraction
- If the good guys can , so can the “bad” guys.

Inference control in data bases (1980's):

- allow statistical data extraction
- protect privacy of individuals
  - e.g. medical or employee data bases
- add noise or restrict access

11



## Conclusions:

---

- Individual tasks similar/related to existing problems
- Combination of these tasks unique to sensor networks
- Current activities:
  - Power security trade-off
  - Measure of security for energy budget
  - co-processors for low power encryption
- Cryptographic techniques with minimal *communication* overhead

12