Featuring Trust and Reputation Management Systems for Constrained Hardware Devices*

Rodrigo Román, M. Carmen Fernández-Gago, Javier López
University of Málaga, Spain

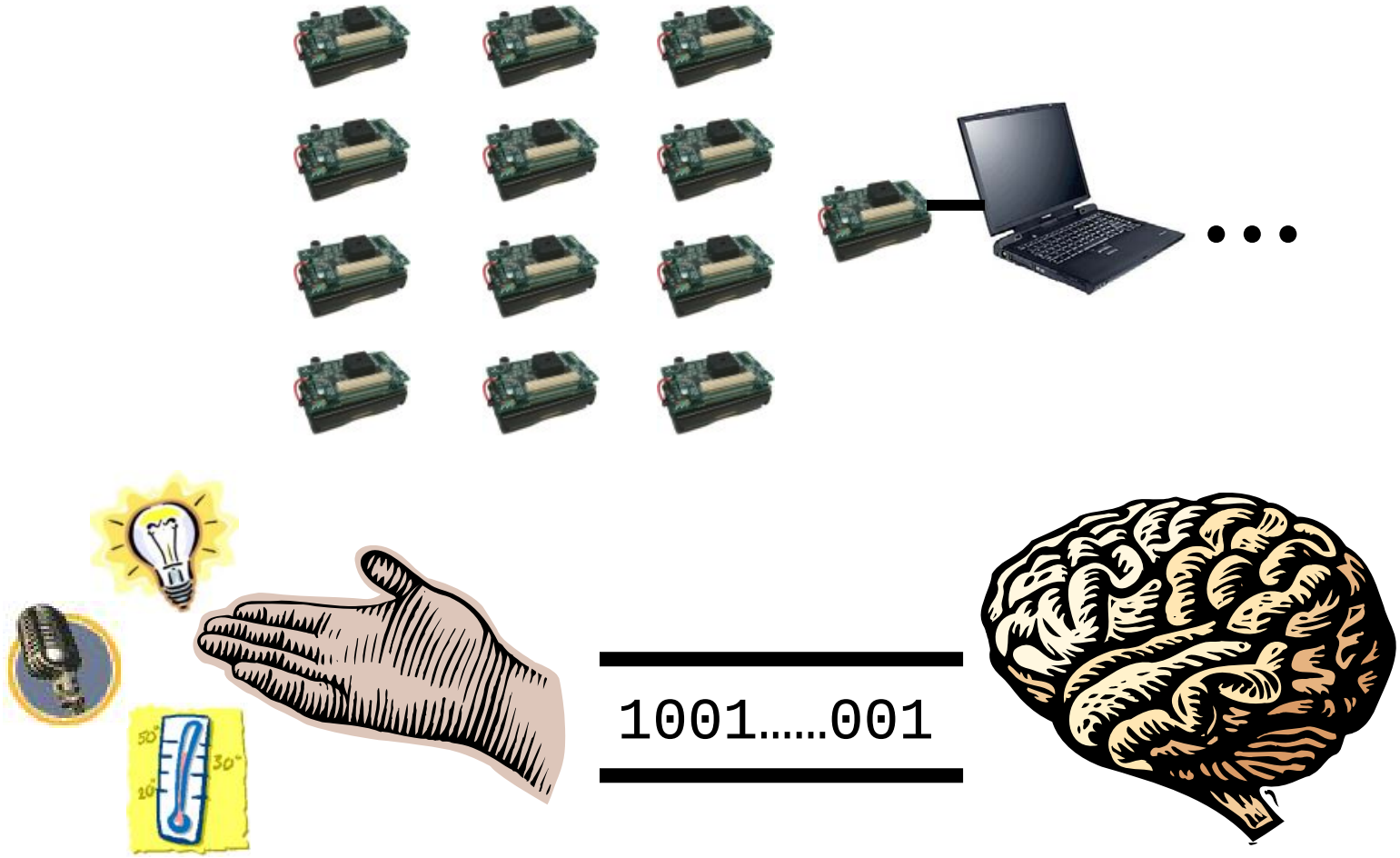
***(Wireless Sensor Networks)**

Contents

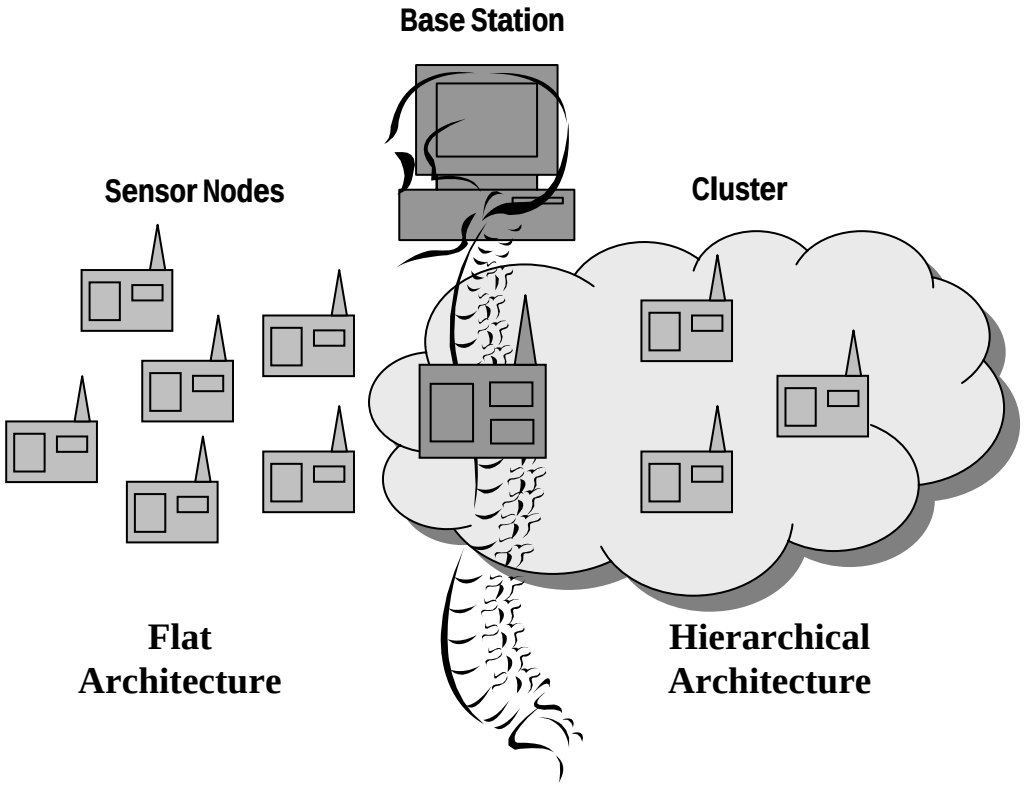
- **Wireless Sensor Networks (WSN)**
- **WSN and Trust**
- **Features for Trust Management Systems in WSN**
- **Conclusions**

Wireless Sensor Networks (WSN)

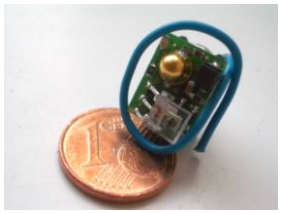
WSN – A “Living being”…



WSN – A “Living being”…



WSN – Node Capabilities



WEAK (Class I)

- 4 Mhz
- 8 bit
- 64B RAM
- 1.4kB ROM
- 1.5mA Energy

NORMAL (Class II)

- 4~8 Mhz
- 8~16 bit
- 4~10 kB RAM
- 48~128 kB ROM
- ~2mA Energy

HEAVY-DUTY (Class III)

- 13~180 Mhz
- 32 bit
- 256~512 kB RAM
- 4~32 MB ROM
- ~40mA Energy

WSN – Security

- Wireless Sensor Networks need security!
  - …at least, a minimal set of security primitives and protocols to assure its functionality (*Usability*)
- Security Primitives (SKC, PKC), Key Management, Situation Awareness…
  - …Trust.

Security Primitives	*Key Management & PKI*	*Situation Awareness* -------- ***Trust*** *& IDS*	*Core Protocols*

WSN and Trust

Trust: "*The firm belief in the reliability or truth or strength of an entity.*"

Trust Management Systems

- Trust Management
  - Term used to define a coherent framework for security policies, credentials and trust relationships
- They can be classified into:
  - Credential-based Trust Management Systems
    - Enable Access Control. Not interesting (here)…
  - Behaviour-based Trust Management Systems
    - Based on the concept of *Reputation*.
    - … applicable to distributed systems, like WSN

Reputation: *"What is generally said or believed about a person or the character or standing of a thing"*

Trust and WSN?

- Why Trust? *Uncertainty = (Opportunism + Information Asymmetry)*
  - Opportunism: "Transacting partners have different goals"
    - … not true in WSN ("living being" simile)
  - Inf. Asymmetry: "a partner does not have all the information it needs about others"
    - … not true in WSN? (honest, collaborative nodes)
    - *Attacks + faulty nodes:* generates Asymmetry… Uncertainty
- Why Trust "on" WSN?
  - *Self-configurable networks*: react and take autonomous decisions
  - … need to have mechanisms that help making choices

Uncertainty: *"When the outcome of a certain situation cannot be clearly established or assured"*

State of the Art

- Existing approaches in Ad-Hoc/P2P Networks…
  - …not suitable for distributed networks such as sensor networks.
  - Device capabilities, scalability, lifetime, network behaviour.
- WSN-specific State of the Art:
  - Trust Management through grouping (Zhang et. al., Crosby et. al.)
  - Ad Hoc-like Trust Management, Trust per node (Yao et. al.)
  - Certainty [self-assessment] (Chen et. al.)
  - Calculation using bayesian formulation, BS role (Ganeriwal et. al.)
  - Application-specific trust, Routing (Tanachaiwiwat et. al.)

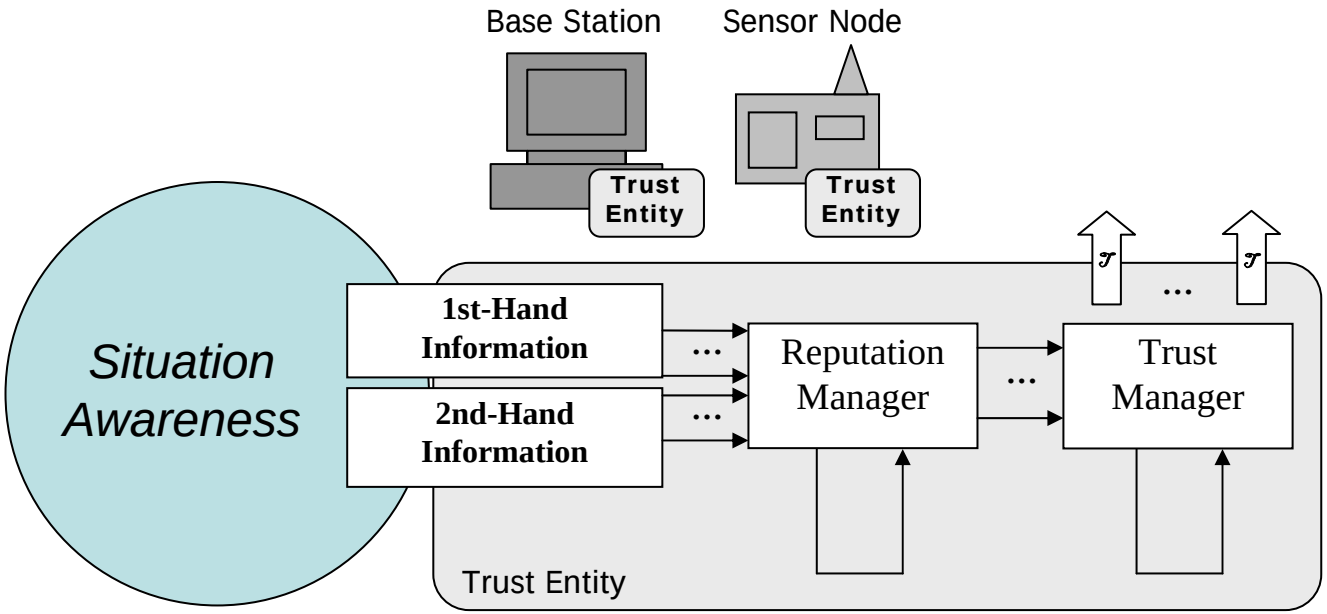
Features for Trust Management Systems in WSN

"State of the Art is not wrong, but is not complete"

Why “Features of TMS”?

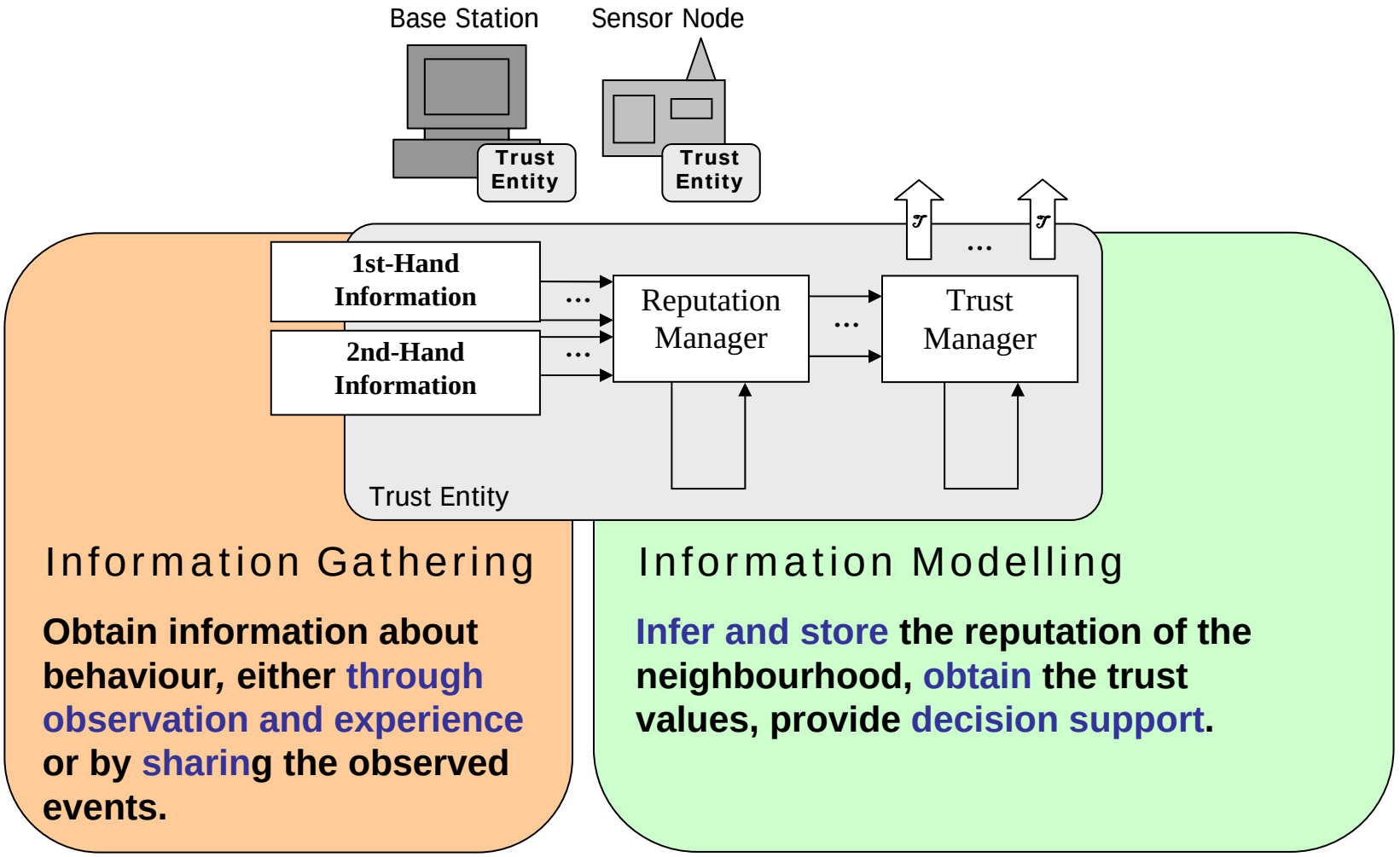
- State of the Art is not bad…
  - …however, it is incomplete
- Main purpose of this “Features”?
  - Consider what have been neglected
    - Initialization, Granularity…
  - Deliver a common architecture
    - All the SotA can be mapped to it
  - Review specific aspects of WSN
    - Location, Behavioural patters…
- Not mathematical results, just a foundation *(Not going to provide the panacea… but painkillers should be a good starting point)*

Architecture and Components



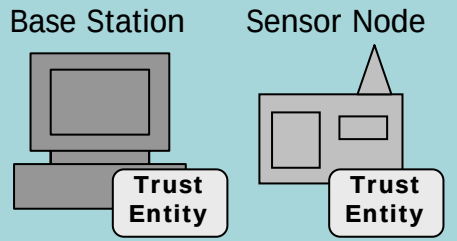
Know the Situation, Model the information, Provide a metric

Architecture and Components



Architecture and Components

Location of the Trust Entities

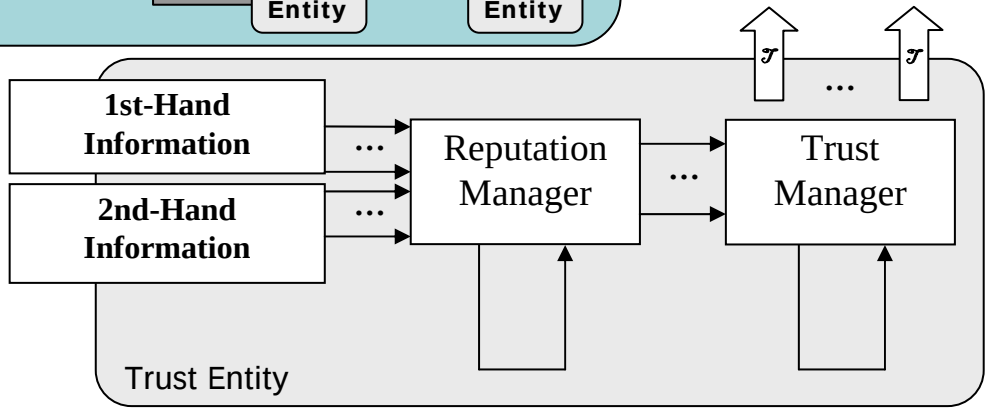


Sensor Nodes

Nodes are autonomous, need to measure their neighbours in order to achieve good coverage

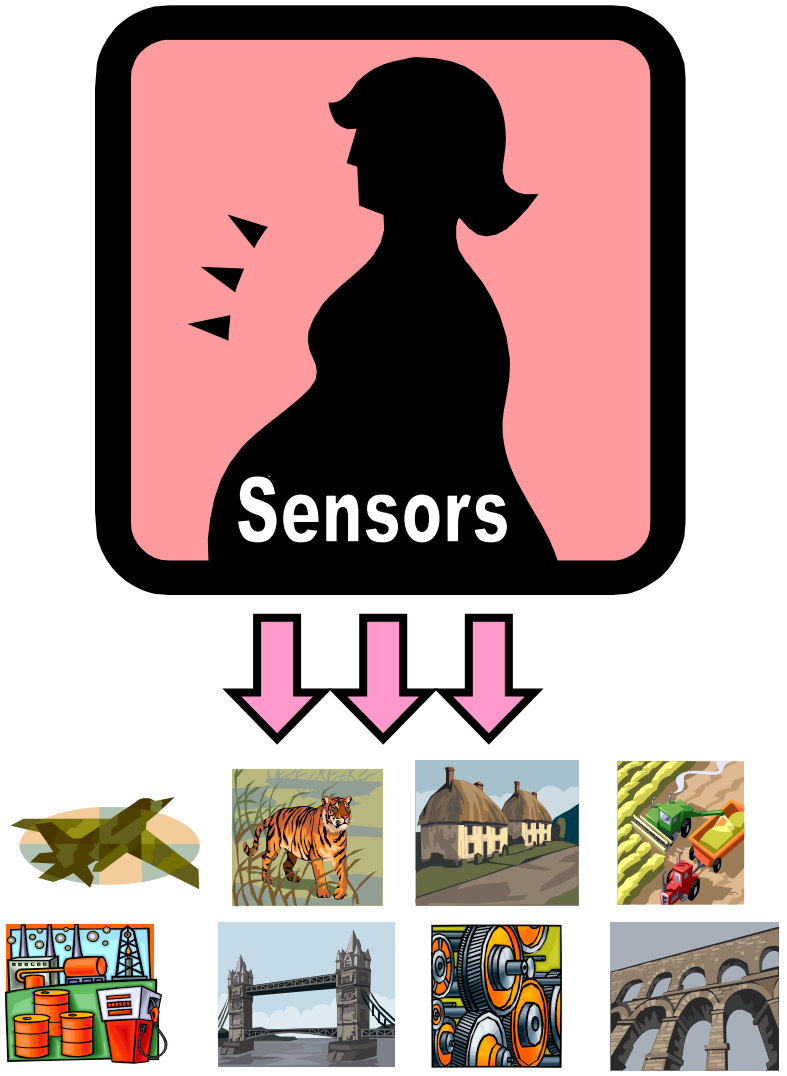
Base Station

"Bridge" to all control and data packets. Take advantage of this wealth of information (powerful!)



Initialization & Information Gathering

- Initialization
  - … what are the initial trust and reputation values?
- Sensor nodes are “born” from the same “cell”
  - … they are programmed in a controlled environment
  - Nothing malicious, HW tested
- Initial reputation should not affect negatively on the beginning
- No credentials? No admittance



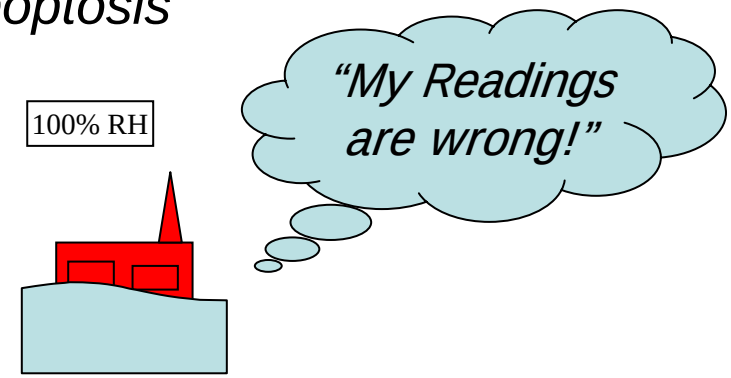
Initialization & Information Gathering

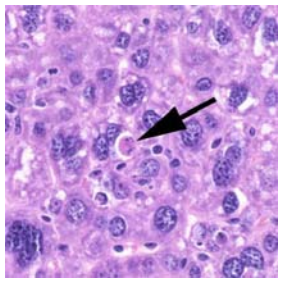
- Information Gathering – "First-hand"
  - Monitoring the environment
    - Packets…
    - Sensor Readings…
  - …work to do (but already with a foundation stone)

Abnormal event (disease)	Collateral effect (symptom)
Jamming	Wide data unavailability
Hw. failure ("unavailable" node)	Data unavailability
Node subversion	Node temporarily unavailable
Tampered, Malfunctioning sensor	Deviations, Inconsistences
Packet Replaying	Packet too old
Message creation	Changes in packet density, Inconsistent alerts
Packet alteration	Changes in packet (only for broadcasted)
Feature advertising	Inconsistent feature with neighborhood
Time-Related attacks	Long delays, Traffic imbalance

Initialization & Information Gathering

- Information Gathering – “Second-hand”
  - Distribute reputation over nodes!
    - Security problems, integration of honest reports…
    - Tools: Redundancy, Cryptographic techniques
- WSN-specific details
  - *Incoherencies* = Existence of malicious entity
  - *Apoptosis*

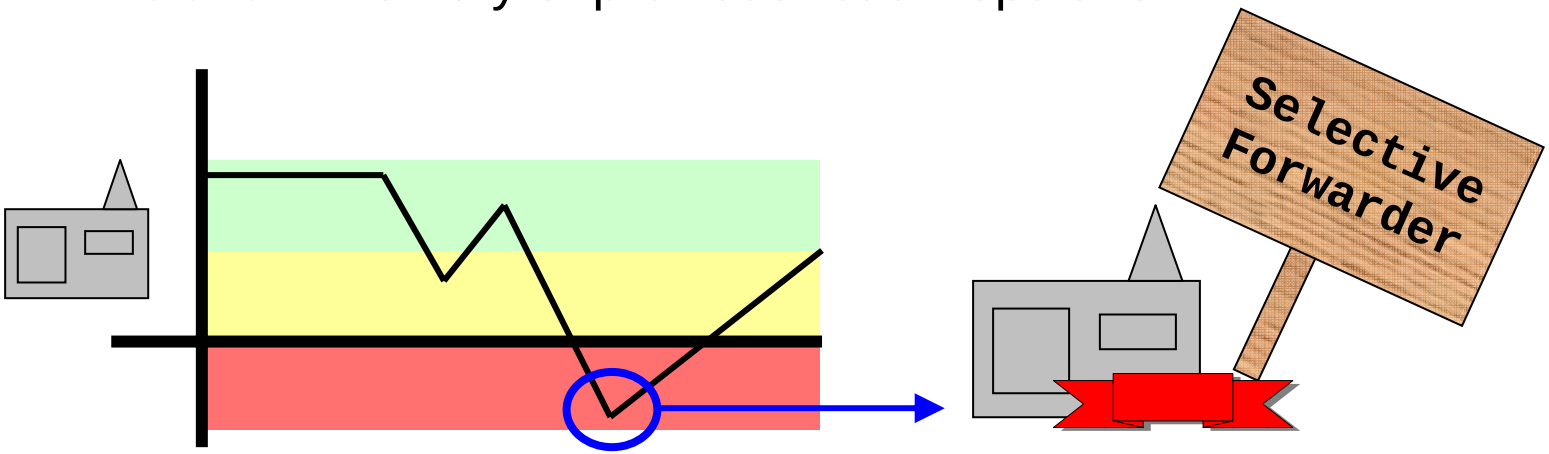




Description: Section of mouse liver showing an apoptotic cell indicated by arrow

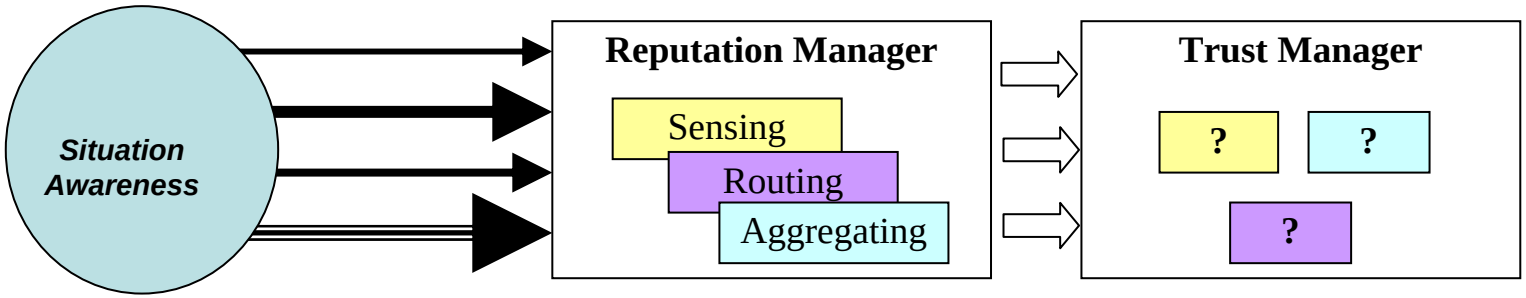
Information Modelling

- WSN specific behaviour
  - “There should be little deviation”
    - Updating the reputation values
  - “Nodes are not malicious by nature”
    - Aging: really “bad” reputation should not be forgotten
    - Evolution: Memory of previous “bad” reputation



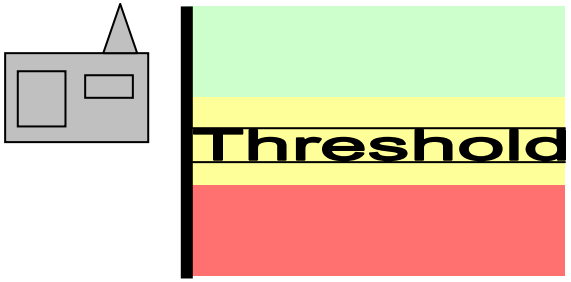
Information Modelling

- Input
  - Events have different Influence (Unavailability Vs Selective Forwarding)
- Granularity
  - Reputation = set of values
    - Separate opinions about actions of peers
  - Trust = set of values
    - Decide outcome of specific interaction

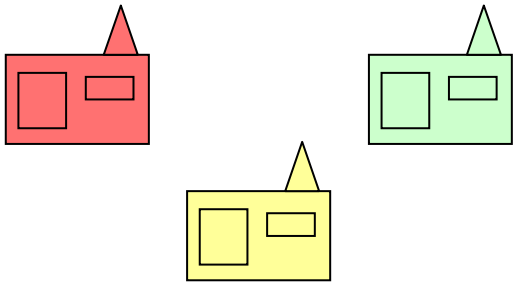


Information Modelling

- Calculating the Trust/Reputation values
  - Weight and Combine according to…
    - Importance
    - Risk
- Threshold (“trusted” v “not trusted)
  - Also dependent of Importance / Risk
  - Other ways: choosing the best partner (groups)



“To trust or not to trust…”

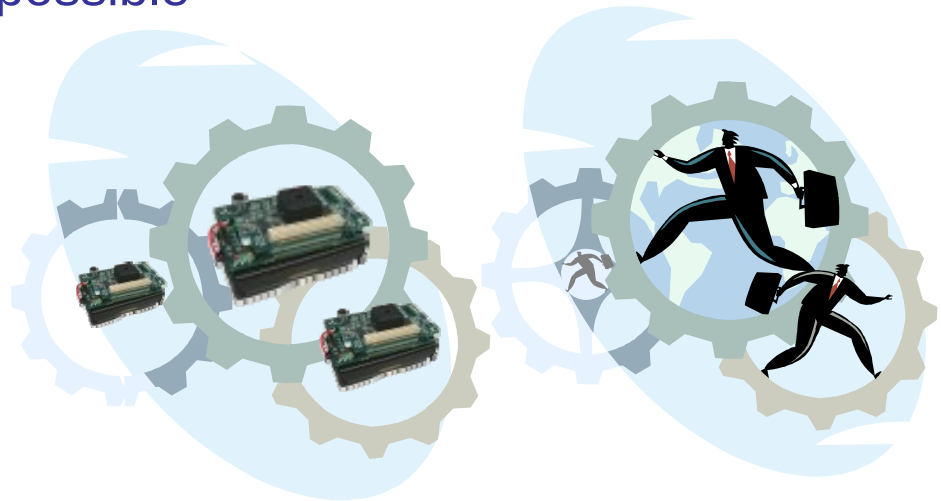


“To choose or not to choose…”

Conclusions

Conclusions

- Trust Management is needed by Wireless Sensor Networks
  - Self-Configurability, Survivability, …
- State of the Art is not wrong, but is not complete
  - Take into account different factors, WSN-specific details
- The ultimate goal: Achieve a lightweight and useful Trust system
  - …it can be possible



LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

UNIVERSIDAD DE MÁLAGA

Featuring Trust and Reputation Management Systems for Constrained Hardware Devices