UNIVERSIDAD DE MÁLAGA

A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks

M. Carmen Fernández-Gago, Rodrigo Roman, Javier López

University of Malaga

Outline

- Trust management systems
  - ✓ Trust management for Ad-Hoc networks
  - ✓ Trust management for P2P networks
- Wireless Sensor Networks
  - ✓ The problem of *trust* for WSN
  - ✓ Analysis of trust management systems for WSN
- Research Lines
- Conclusions

Trust Management Systems

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

Trust Management

Term used to define a coherent framework for security policies, credentials and trust relationships. PolicyMaker, KeyNote,…

They can be classified into:

- ✓ Credential-based Trust Management Systems
- ✓ Behaviour-based Trust Management Systems

Trust Management for Ad-Hoc Networks

- Behavioural-Based Systems (mainly).
  - ✓Applied to the Routing process
    - ❖ Initial Trust = Identity, Evaluation of other nodes
  - ✓Reputation-based. Use of entities such as the trust manager and reputation handling module
  - ✓All = Simple calculations used

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

Trust Management for P2P Networks

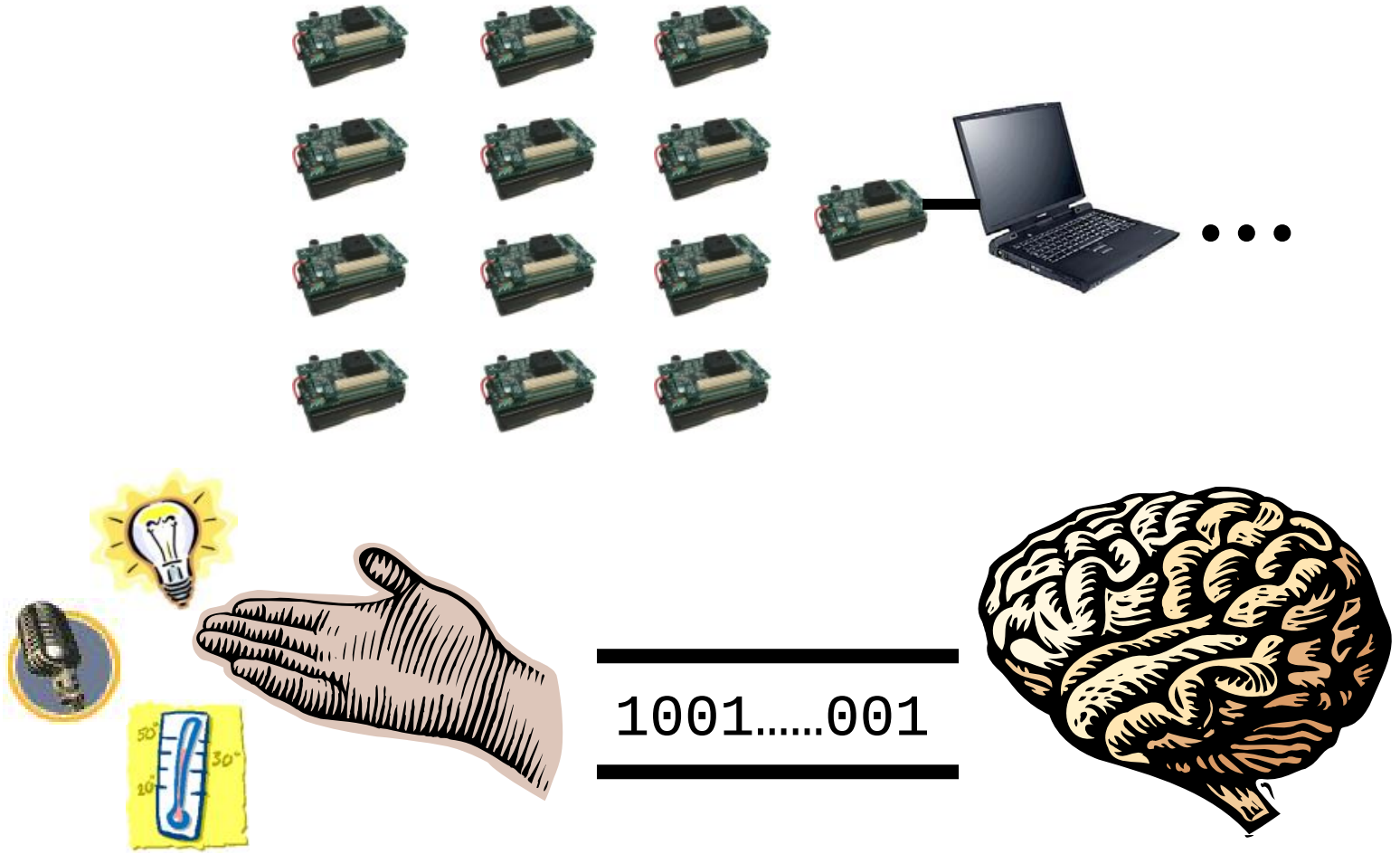
- Mainly behaviour-based systems.
  - ✓ Based on reputation (most of them).
    - ❖ Bayesian Networks
    - ❖ Statistics

  Examples: PET
- Few of them use public-key cryptography.

  Examples: TrustMe

Wireless Sensor Networks and Trust

Wireless Sensor Networks



Applicability of Wireless Sensor Networks

- Emerging use of this type of networks in real-life scenarios
- However, security issues arise
- WSN are very vulnerable
  - ✓Computational or energy constrainsts
  - ✓Accessible from the physical world

Trust in Wireless Sensor Networks

- Key aspect for WSN. Very useful for
  - ✓Detecting faulty or malicious behaviour
  - ✓Decision-making process
  - ✓*…Self-Configurability!!!*
- Very little has been done so far
  - A) Ganeriwal et al. Reputation framework for high integrity sensor networks based on bayesian formulation.

Trust in Wireless Sensor Networks II

B) Location-centric architecture for isolating misbehaviour and for establishing trust routing. (Tanachaiwiwat, 2005)

- ✓ Trust is calculated as a function of cryptography, availability and packet forwarding.

C) Yao et al (2005). Similar to approaches for Ad-hoc networks.

- ✓ Using *personal reference* and *reference* (sent by *juries*).

$$T_i = T_{pr(i)} \times W_{pr} + T_{r(i)} \times W_r$$

Analysis of Trust Management Systems for Wireless Sensor Networks

Applicability of Trust Management Systems to WSN

Very Important aspects for the analysis:

- Data Collection (for behavioural-based systems)
  - ✓Data collected from the node´s behaviour
- System Features of a Trust Management System
  - ✓Initialization procedures, hierarchy, trust evolution

Data Collection for WSN

- Hardware-related situations
  - ✓ Nodes not detected alive or appear and dissapear
- Communication layer
  - ✓ Node creating false alarms
  - ✓ Reporting non-requested answers to the base station
  - ✓ Node create packets outside “burst time”
  - ✓ Packet forwarding, packet delaying…
- Sensor Readings
  - ✓ Unusual values within a neighbourhood
- Misbehaviour in the core protocols or applications
  - ✓ Lying in the negotiation process or exchanging false information

Data Collection in the Existing Trust Management Systems for WSN

- Existing methods do not cover all the aspects mentioned above
- They look at
  - ✓Data consistency, forwarding issues (Ganeriwal et. al)
  - ✓Availability of a node (Tanachaiwiwat et. al)
  - ✓Existence of malicious behaviour (Yao et. al)

Applicability of Existing Trust Management Systems for P2P and Ad-Hoc Networks to WSN

- Aspects that can affect trust:
  - ✓ Power Constraint
  - ✓ Scalability and lifetime.
    - ❖ Number of members in WSN can be higher than in Ad-Hoc networks
    - ❖ Lifetime of WSN is usually longer than Ad-Hoc and P2P networks
  - ✓ Functionality: Behaviour of nodes
    - ❖ Any deviation in the functionality of a node can be considered a possible source of mistrust

Some Disadvantages of Existing Trust Management Systems for P2P and Ad-Hoc Networks to WSN II

- Using a *reputation manager*
  - ✓Very high-energy consuming for WSN
- Assigning *initial values*
  - ✓Contradictory with the nature of WSN
  - ✓Initially information about nodes is preloaded by the the user

Analysis of Existing WSN Approaches

- …It is mainly about what they *do not* have
- Data collected
  - ✓ …Not all events should be given the same importance (Ganeriwal)… but there should be different trust levels for different actions
- Storage of values
  - ✓ Either the base station or the nodes themselves
- Self-Confidence as input (?)

Research Lines
(some points to raise…)

Aspects to be considered in a Trust Management System for WSN I (Research lines)

- Initialization of the trust model
  - ✓ Initial trust values are not very important
  - ✓ More important are events occuring during the lifetime of the WSN
- Importance of events
  - ✓ Different trust values for different events
- Importance of the *Base Station*
  - ✓ Not all the information have to be gathered by the base station
  - ✓ However, a trust model for the base station is possible

Aspects to be considered in a Trust Management System for WSN II (Research lines)

- Awareness of trust history on the node's neighbourhood
  - ✓ Uncooperative nodes should be untrusted
  - ✓ Contradictory reports can be an evidence of malicious activity
- Possible restrictions of the trust management system over the sensor networks
  - ✓ The trust management system should be as lighweight as possible

Conclusions

Conclusions

- …Trust is important for WSN…
- …Trust Management for Ad-Hoc and P2P networks are not suited…
- …and there are Important factors to be considered in a WSN
  - ✓Data collection, relevance of data, history-aware, the role of the base station, etc.

?


Gracias