LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

UNIVERSIDAD DE MÁLAGA

Service-Oriented Security Architecture for CII based on Sensor Networks

Javier Lopez, Jose Antonio Montenegro, *Rodrigo Roman*

29 June 2006

Summary

- Critical Information Infrastructures and Sensor Networks
- Research Problems
- *CRISIS* – SoA for CIIP
- Conclusions

Critical Information Infrastructures and Sensor Networks

Critical Information Infrastructures (CII)

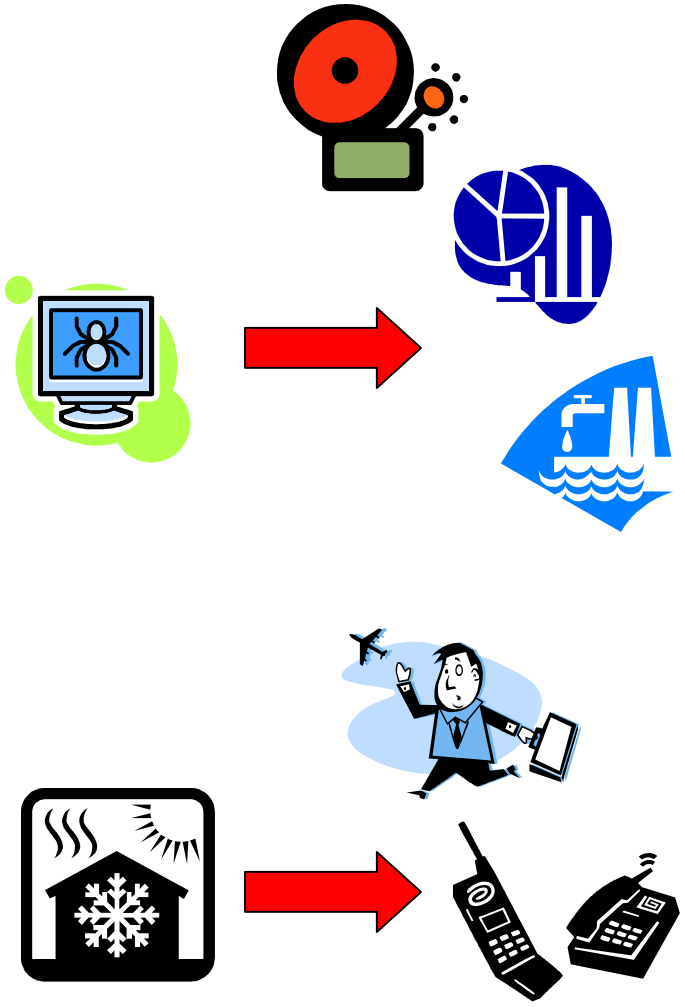
Critical Infrastructures

- Physical and information technology facilities, networks, services and assets.
- *Banking, Finance, Transport, Energy, Utilities, Health, Food supply, Communications...*
- If Disrupted/Destroyed => **Serious Impact on Health, Safety, Security and Economic well-being!**

Critical Information Infrastructures (CII)

Examples of problems

- *2003, World*. Slammer attacks. Finance affected (ATMs down). Emergency affected (911 stops in Seattle). Electricity affected (some SCADA stops).
- *2004, Italy*. An air conditioner breaks. Communication Blackout for about 6h in Rome. 70% check-in desks at Fiumicino off-line.



Critical Information Infrastructures (CII)

Critical Information Infrastructures

- How to support/control those Critical Infrastructures? **CII**
- Highly Interconnected (national or international), Software-based control systems
- **Advanced Security technologies are needed!** Complex and Dynamic Infrastructures with many layers

Critical Information Infrastructures (CII)

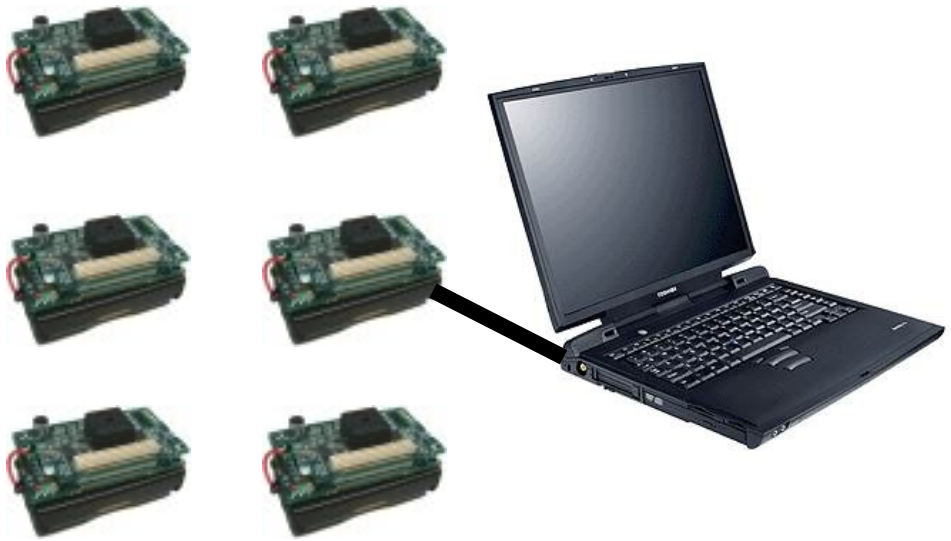
- *Who* – Unknown, multiple, concurrency
- *When* – Many events can happen anytime (concurrently), sequence unpredictable
- *Whom* – Accidental, Malicious, can affect anything!
- *What* – Cascade of (unpredictable?) consequences!

- What we need: Supply Services **at any cost!** (or at least, recover from problems ASAP ☺)
- Intelligent Distributed Control: *Wireless Sensor Networks*.

Wireless Sensor Networks (WSN)

What?

- Nodes: Constrained, Sensors, Wireless.
- Dense Network (100 - more...)
- ∑Nodes = WSN



Applications

- Healthcare
- Environment
- AmI (Smart Homes)
- Military
- ...

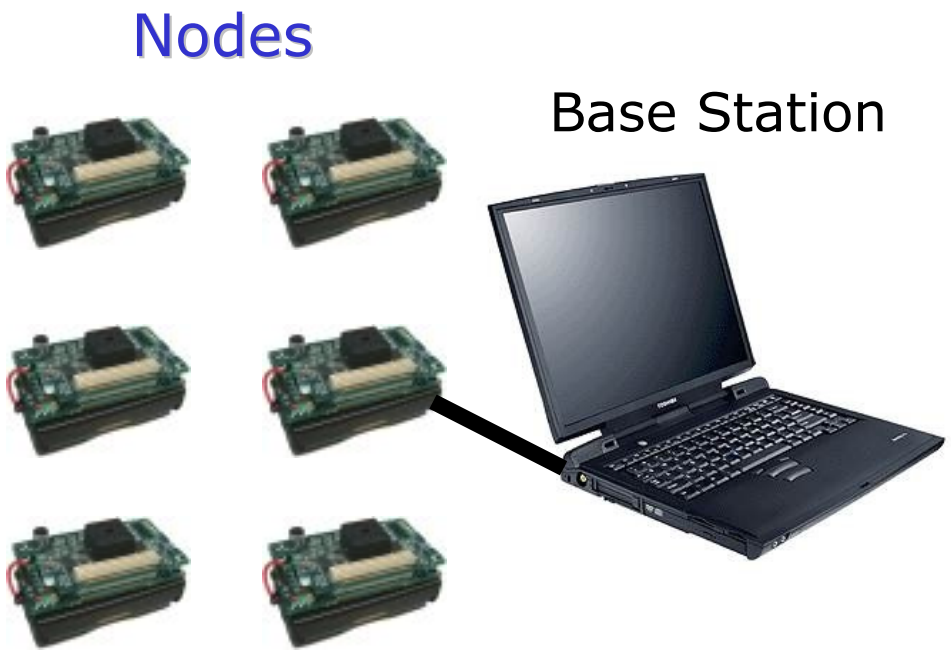
WSN – Nodes

Nodes Features:

- 8 Mhz, 128Kb I's
- Battery: 1 year ("stand-by")
- Radio (19.2 – 250 Kbps)

Roles:

- (Phy/Log) Harvesters
- Routers
- Distributed Platform

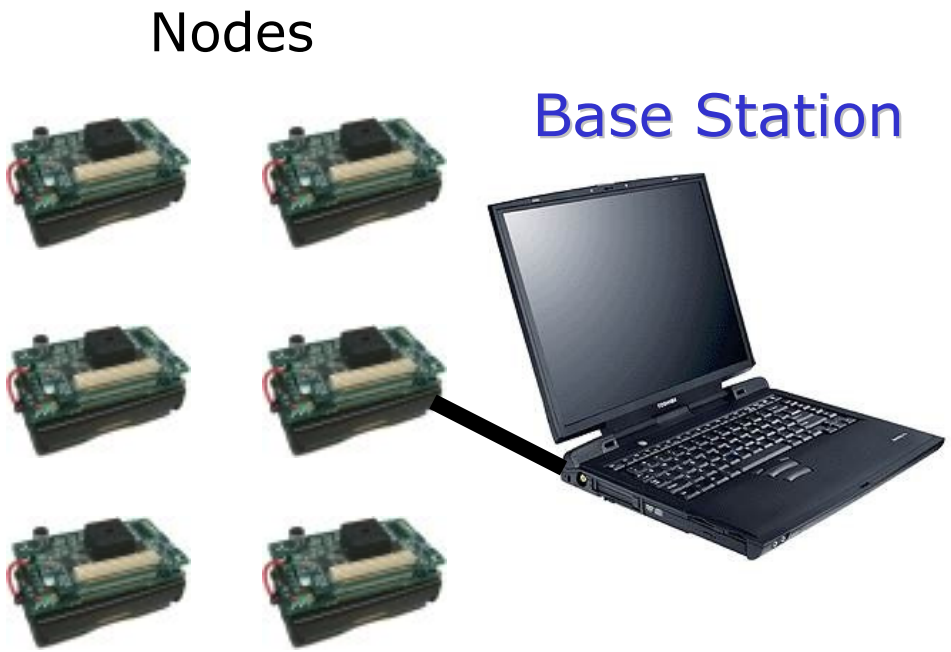


WSN – Base Station

B.S.: Less Constrained

Roles:

- Manager
- Interface (Data Dissemination Network)



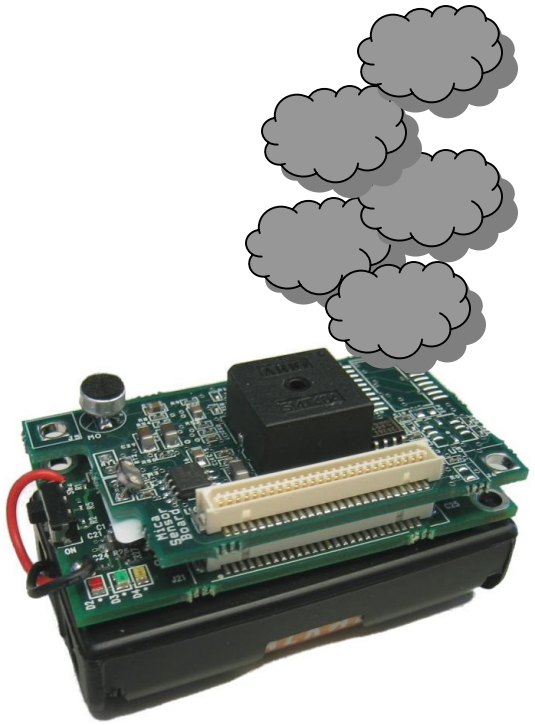
Research Problems

CII - Problems

Main challenge: Interdisciplinary nature. Physical, Logical, Assets, People…

- *Policies*
  - High-level policies (relationships between CII organizations)
  - Security policies of a CII (internal sections, delegation…)?
- *Resilience & Robustness*
  - Alert & Help Systems. Redundant/Extra systems?
- *(Early) Warning Systems*
  - *Before* and *After*
- *Models and Simulations*
  - Analyse behaviour, discover problems, trials
- *Risk Management and Quantification*

WSN - Problems



Every Node!

- Primitives
  - Security Primitives
  - Key Management
- Protocols
  - Routing
  - Data Management
  - Time Synchronization
- Services
  - Auditing / IDS-IRS
  - Location
  - QoS

CRISIS – SoA for CIIP

CRISIS

- *CRISIS?*
  - **CR**itical **I**nformation infrastructures **S**ecurity based on **I**nternetworking **S**ensors
  - Not completely solve all problems, but improve / provide a ground for future (research & commercial) solutions
- Goals
  - Security Services for Critical Information Infrastructures
    - Protect, Control, Evaluation
  - Architecture: Service-oriented Architecture – SoA
  - Technological platform: Wireless Sensor Networks – WSN
- *Ongoing Project*

CRISIS – Supporting Services

- *Low Level*
  - Architecture: MICA-like nodes
  - Goals: Create SW components for:
    - Secure Access, Control, and Analysis
- *High-Level*
  - Architecture: Interoperation of elemental mechanisms
  - Goals:
    - Security Policies (management of user/device attributes)
    - Specification of the middleware
    - Functional interdependences / Interfaces
- *Interoperability of Services*

CRISIS – Trust Management Model

- *Advanced Authentication Services*
  - Confidentiality and Integrity of Communications
  - Services for advanced authentication
  - Off-line / On-line mechanisms
- *Authorization Services*
  - Intelligent Authorization Gateway
  - Distributed Authorization System
- *Delegation Service*
  - Delegation Description Language
- Services: Information Sharing, Aggregation, Privacy

CRISIS – Secure Control System

- *Early Warning Systems (EWS)*
  - Information analyser ⇨
  - ⇨ Information provider, Automatic reaction, Seamless business continuity
- *Dynamic Reconfiguration System (DRS)*
  - EWS ⇨
  - ⇨ Automatic Reconfiguration
- Monitoring Services
  - || Auditing Procedures
- Forensic Techniques and Procedures
  - ⇨ Detailed guidelines for Accessing / Detecting / Locating

CRISIS – CII Testing and Evaluation

- *Low-Level: Security Verification Tool*
  - Analyse the security of the interconnections between systems
- *High-Level: Decision Support System*
  - Aids Human / Machine to make decisions
  - How? Simulation Model
    - …based on the properties of individual nodes, overall system and its context, interconnections.
    - …also based on faults and intrusions (failures, faults, events, human-related problems)
    - …will provide probabilities and real-time data
    - Properties represented in a formal notation

Conclusions

Conclusions

- Discussion of Technologies
- Combination of Critical Information Infrastructures and Wireless Sensor Networks
- CRISIS – ongoing project
  - A Result: Model for using a Key Management Model

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

UNIVERSIDAD DE MÁLAGA

Service-Oriented Security Architecture for CII based on Sensor Networks

Javier Lopez, Jose Antonio Montenegro, *Rodrigo Roman*

29 June 2006