Análisis y Desarrollo de un canal encubierto en una red de sensores

Jose A. Onieva, Ruben Rios, Bernardo Palenciano*

NICS Lab – University of Málaga

http://www.nics.uma.es

**Dpto. de Infraestructura de TTI*

RECSI 2014, Alicante, 2-5 septiembre 2014

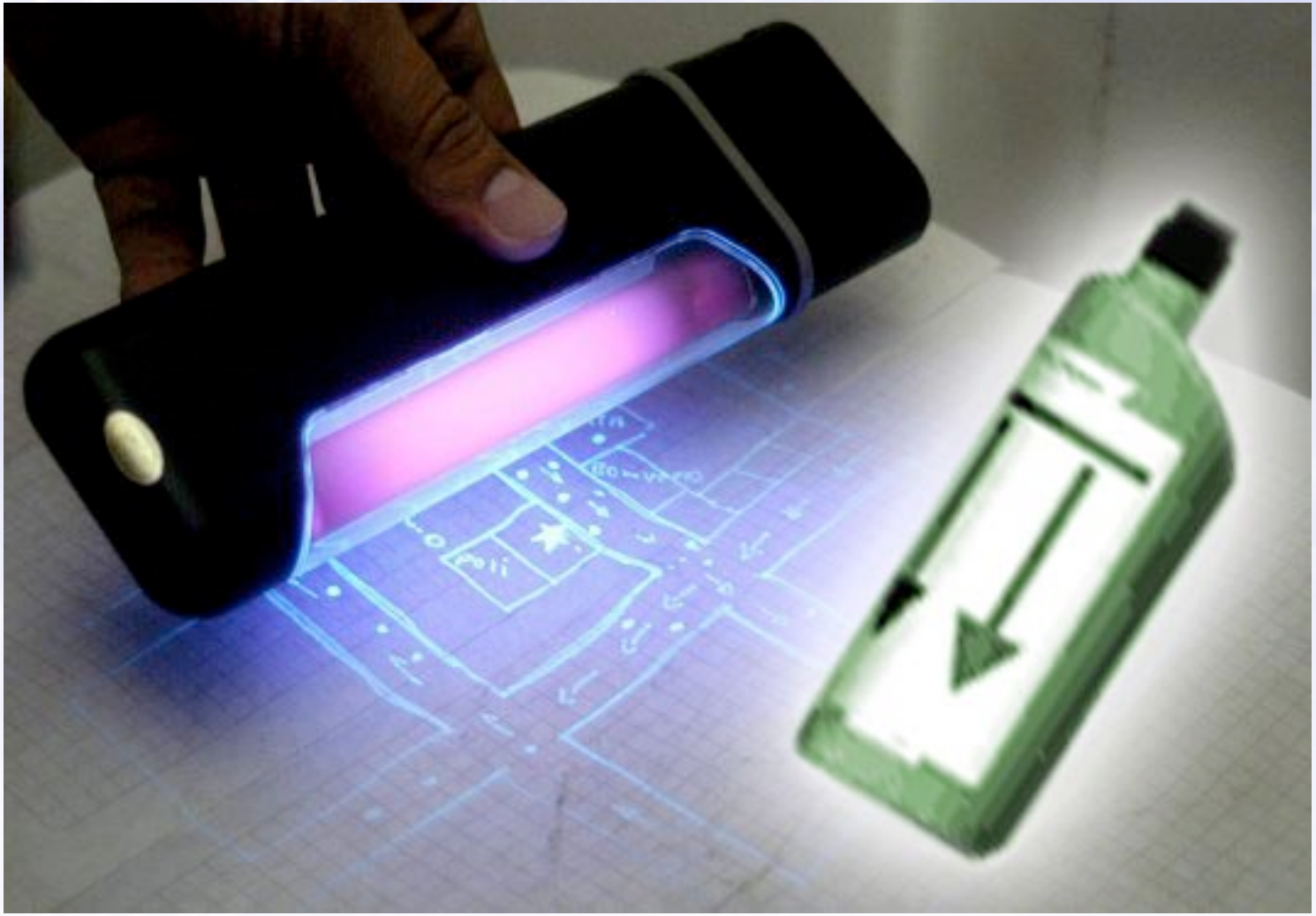
Agenda

- A Fictitious Scenario
- Covert Channels and WSNs
- Requirements needed for operation
- Protocol Design & Implementation
- Detectability
- Current and Future Work

A Fictitious Scenario

- Alice works in a company that uses a WSN to monitor the levels of water conditions in the Strait of Gibraltar for mussel farming.
  - At the same time, this company benefits from its strategic business location to carry out an illicit transport of substances in containers.
- Alice and Bob want to uncover the smuggling
  - Alice needs to tell Bob the container that carries the stash
  - No suspicion (at all) should be raise in the company

Covert Channels



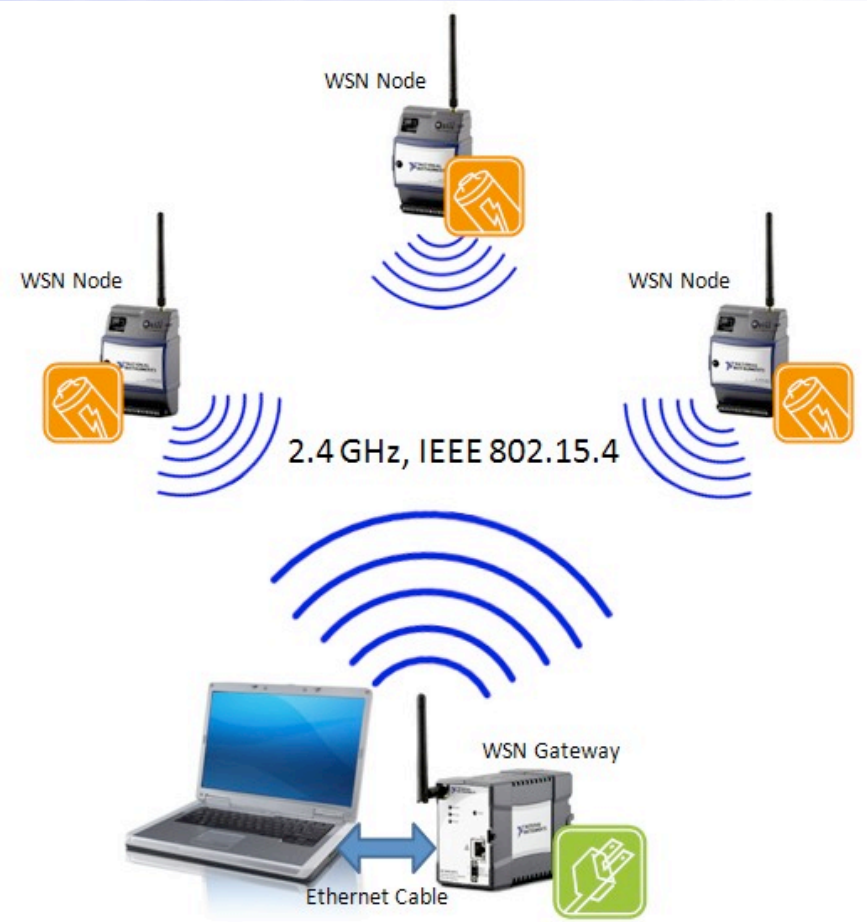
From serranoprada.com

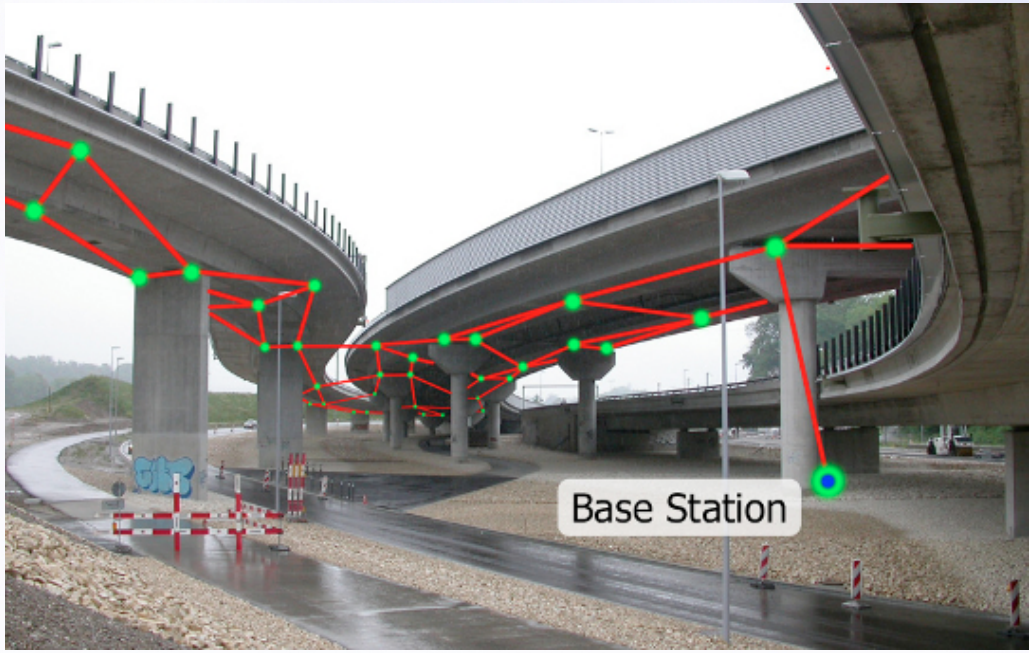
Covert Channels

- A covert channel is a form of hidden communication between processes
  - Encryption hides the communication content only

- Two main categories of covert channels:
  - Storage channels exploit ambiguous protocol specs. Some well-known network-based covert channels:
    - Covert_TCP (TCP/IP), Ozyman (DNS), HIDE_DHCP (DHCP), LOKI2, PingTunnel (ICMP), FirePass (HTTP).
  - Timing channels exploit the modulation of behaviour (e.g. sending times of network messages)
    - [Girling CG., 1987], [Luo et al., 2007], etc.

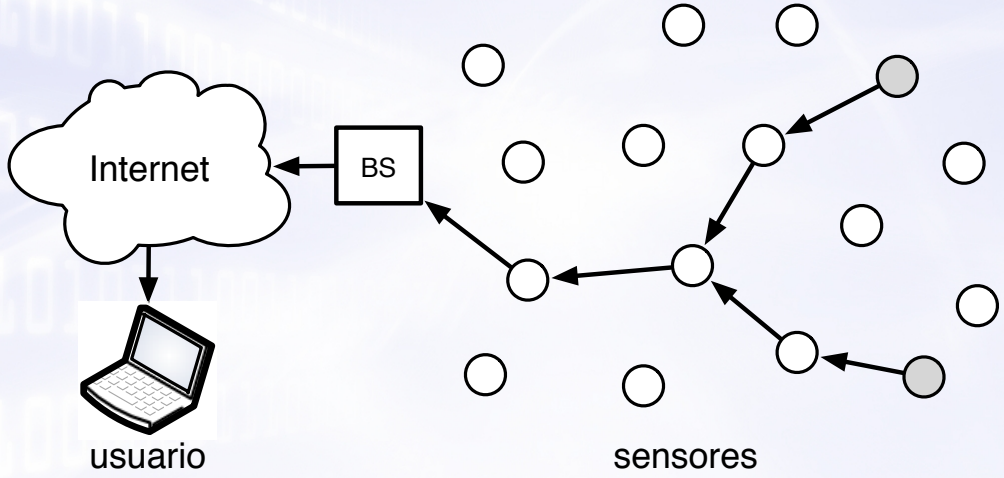
Wireless Sensor Networks





WSNs

- A wireless sensor network (WSN) is a distributed system with resource-constrained devices (nodes) whose main objective is to monitor a physical phenomenon.



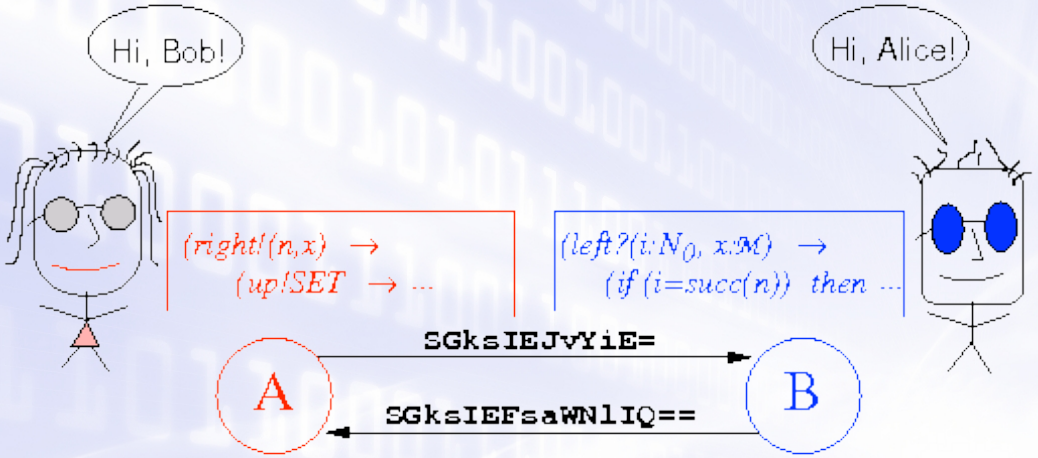
- One-hop vs. multi-hop
- Event-driven vs. query-based vs. continuous event notification
- Networks already deployed

Requirements

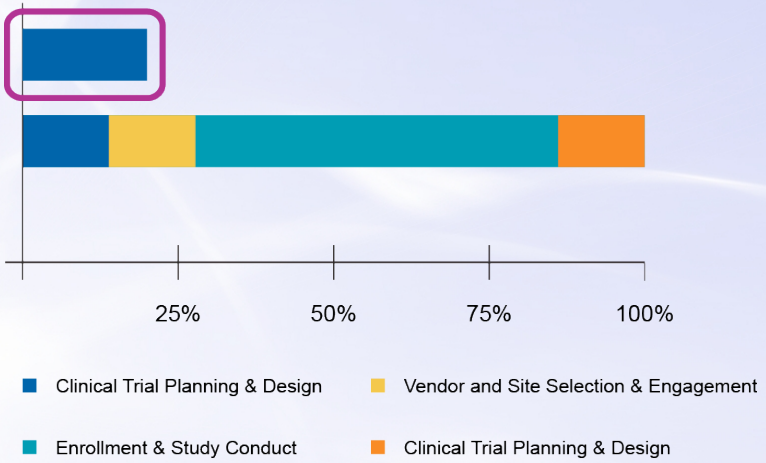
Requirements

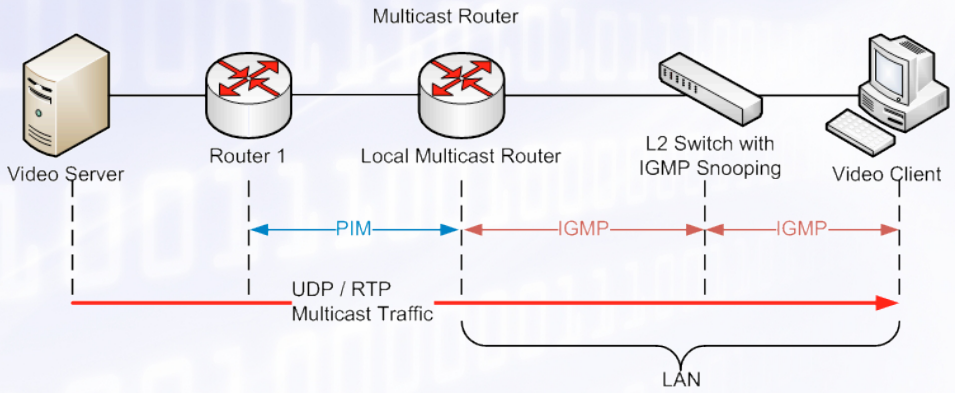
- Detectability 
- Integrity 
- Communication 
- Bandwidth 
- Energy consumption 

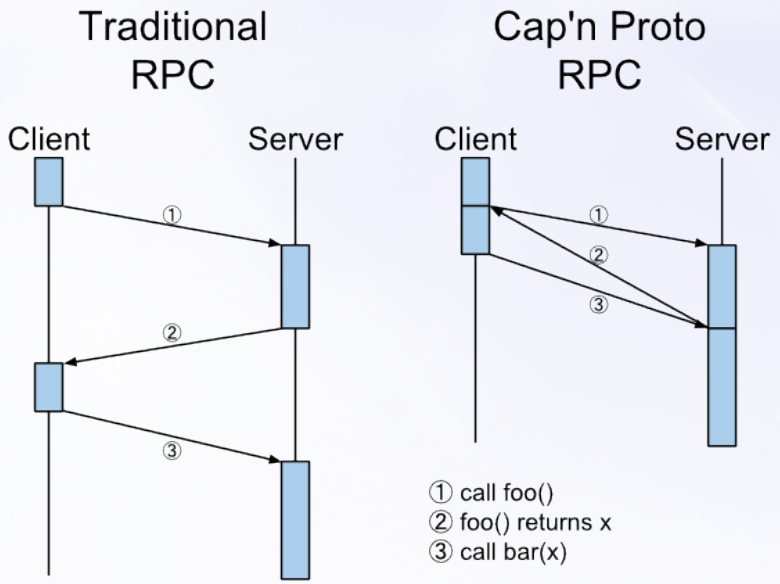
Design



Quality by Design: Spend more time up front for better quality trials



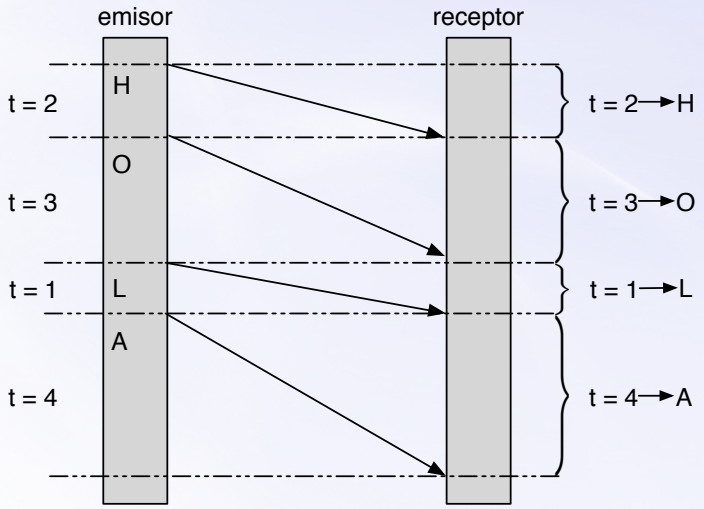




Design Decisions

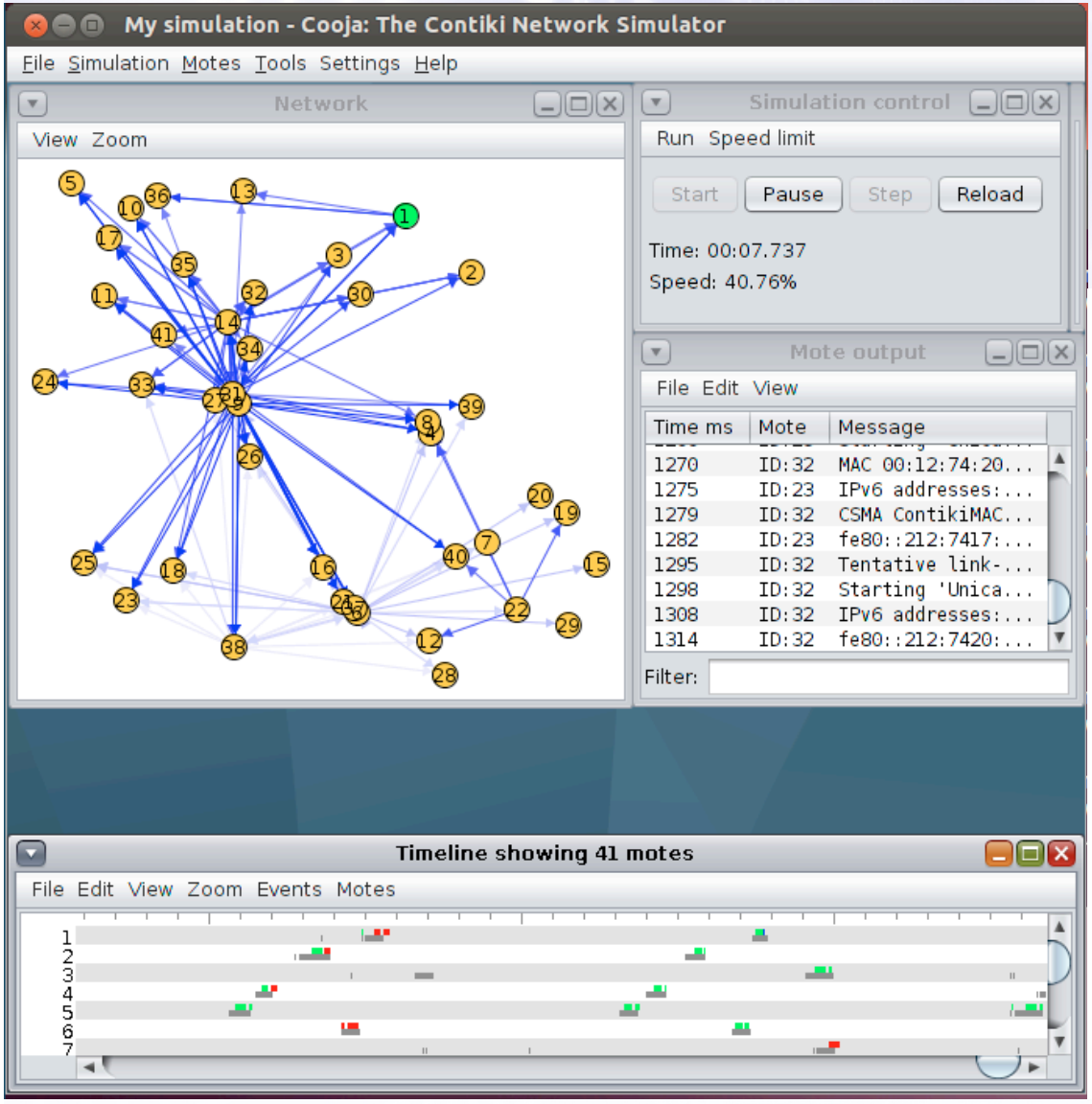
- We choose to design a covert timing channel based on the modulation of the data transmission intervals
  - Changing the collection times is not unusual
  - Requires no software modifications

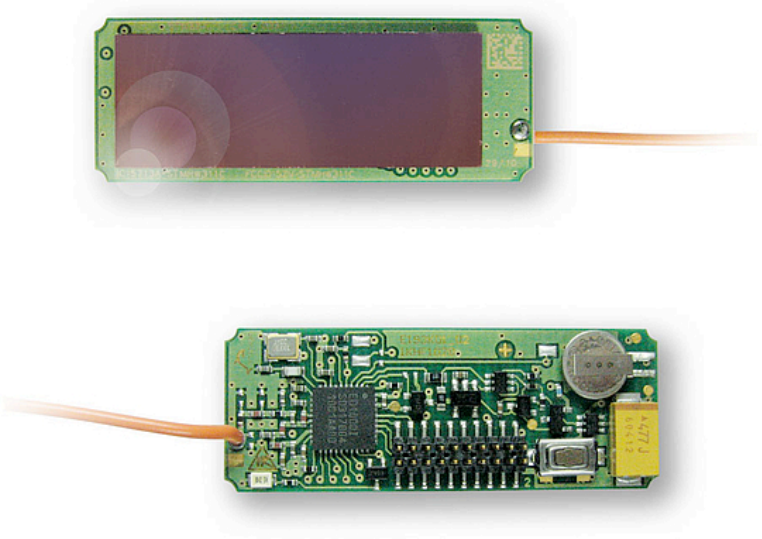
- Sender and recipient agree upon a suitable character-time coding
  - E.g. Huffman coding of Spanish language
  - Default interval *t* if no transmission



- The sender is at the base station and the recipient is an external observer

Implementation



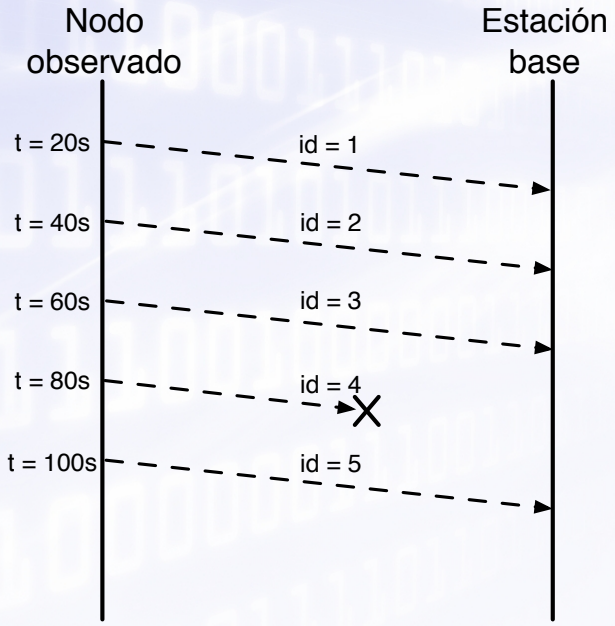


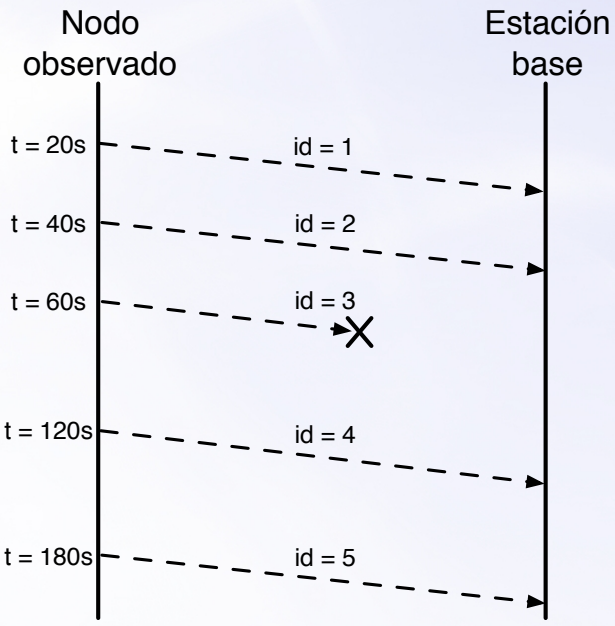
Implementation Elements

- Contiki OS for sensors
  - Use COOJA simulator for testing
- Sniffer
  - "Simulated" with packet broadacast in COOJA simulator
  - Existing solutions for WSN sniffers (e.g. Jackdaw).
- Physical sensors for tests
  - Tmote sky de Motiev
- Default transmission interval established in 15 secs

Implementation

- From experiments we observed some problems
  - The sniffer has a precision error around 1 ~ 2 seconds
  - Packet collisions limit the integrity and bandwidth of the channel





Implementation

- We (partially) solved these limitations at the expense of reduced bandwidth
  - Time distance between characters is of 5 seconds
  - Each character is transmitted 3 times
  - Use a CHANGE character for resynchronization in case of double symbols.
- Current bandwidth = 10 bytes / 38 minutes

Detectability

Detectability

- Intrusion Detection Systems in WSNs analyse
  - Modifications to the data collected by sensors
  - Code integrity verification
  - Data exchanged between sensors
- The only suspicious activity is the modification of the transmission interval for a time period
  - But the base station is assumed to be trustworthy
  - **The suspicion level can be lessened by reducing the bandwidth**
- Search of timing patterns are not straightforward in continuous-event monitoring

Current and Future Work

- Improving the bandwidth of the solution
  - Different (clusters of) motes having different transmission intervals
    - Synchronization becomes complex
    - How does this affect detectability?

- We are studying new ways of hiding information
  - Packet header fields
  - Routing paths
  - Packet order of arrival

The End

Thank You!