

# Wireless Sensor Network Agent Platform With Support For Cryptographic Protocols

Peter Pecho, František Zbořil

# Overview

- Wireless sensor networks (WSN)
- Artificial agents, agent platforms
  
- Threats and security in WSN
  - Conventional solutions
  - Non-conventional solutions
  
- Hardware cryptography platform for WSN
- Some results
- Summary

# Wireless Sensor Networks (WSN)

- Data-centric network – data collection, transport & evaluation
- Communication only via radio – ZigBee, etc.
- Most widely used platform: TinyOS(2)/NesC
- *Program = handlers + task raised from sensors, transceivers and other hardware elements*
- **Application range:**
  - Petrochemical & biochemical industry
  - Military
  - Medicine
  - Environmental monitoring



MICAz sensor node

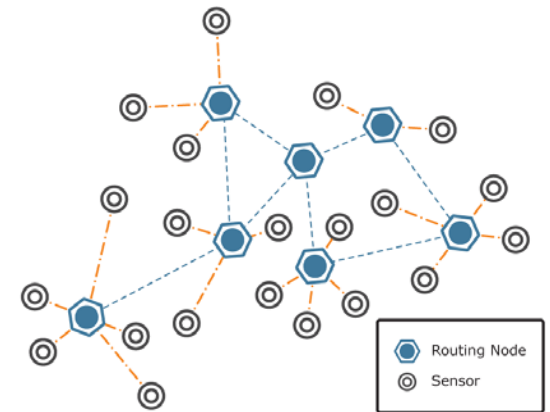
# Wireless Sensor Networks (WSN)

- **Hardware/Software requirements:**

- Application requirements – reliability, accuracy, scalability, long battery life
- **Security requirements** – confidentiality, data integrity, tamper resistance, etc.

- **Resource limitations:**

- Limited computational performance
- Limited RAM & Flash memory
- Limited battery capacity
- Limited radio range
- Usually ad hoc network topology



Example of a wireless sensor network

# Artificial Agents

- Autonomous intelligent entity
- Able to work toward some objectives
- Should be robust, reactive and mobile
- Controlled by an agent language (post declarative BDI languages like AgentSpeak(L))

## Limitations:

- Recent BDI languages are based on Java – **limitations of WSN**
- Interpretation works in an active cycle – **energy demands**
- Mobility on the Java level
- ...

# Artificial Agents and Agent Platforms

- **Developing of agent system suitable for WSN that contains:**
  - Agent platform, interface between HW (sensors) and agent
  - BDI like agent language (Agent Low Level Language)
  - Agent language interpreter
  
- **The agents and the agent platforms usually work in a hostile environment – we have to secure:**
  - Agent communication
  - Mobility of an agent code
  - Access control to particular agent platforms and agents
  - ...

# Wireless Sensor Networks Threats

- **Typical attacks:**

- Eavesdropping of communication
- Replay attack
- Jamming the communication
- Denial of service
- Node masquerade
- ...

- **Security countermeasures:**

- Radio channel protection – jumping over channels
- **Message protection – cryptography**
- Sensor hardware protection – only hardware solutions

# Wireless Sensor Networks Protection

## Conventional solutions

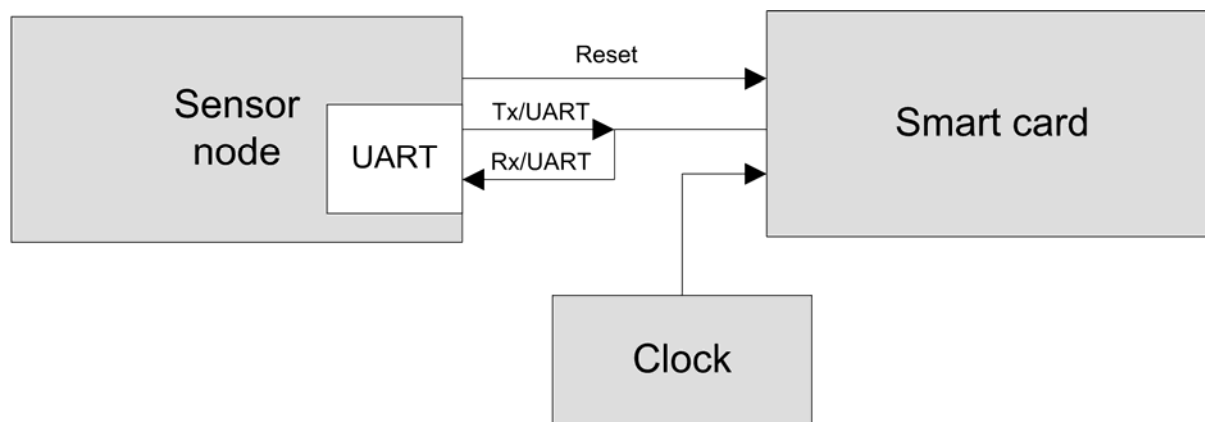
- Libraries or SW comp.
- Inf. security vs. limited resources
- Symmetric & stream ciphers
- TinySec, MiniSec
  
- **Pros:**
  - Easy to use
  - Least expensive solution
- **Cons:**
  - Secret key cryptography at low speed
  - No hardware protection

## Non-conventional solutions

- Various HW extensions of motes:
  - Add-on aux. microprocessor
  - Secure microcontroller
  - FPGA module
  - **Smartcard**
  
- **Pros:**
  - Acceleration of crypto oper.
  - Sensor HW protection
- **Cons:**
  - Higher price
  - Higher power consumption
  - More complex sensor node

# Smartcard Based Hardware Cryptography Platform

- Proposed platform uses smartcard as a crypto accelerator



- Smartcard-sensor node communication:
  - UART – I/O signal
  - Auxiliary pin on bus – reset signal
  - External clock (could be also used WSN internal clock)

# Smartcard



- Specialized computer with no human interface
- Offers acceleration of cryptographic operations
- Contains secure data storage
- Hardware resistant against physical attacks
  
- However: Smartcard  $\neq$  microprocessor + secured memory
- Rather: Smartcard = very cheap implementation of security concept called “Tamper Resistance Device”
  
- Smartcard can't be cloned or emulated.
- Stored data could be manipulated only by build-in microprocessor.

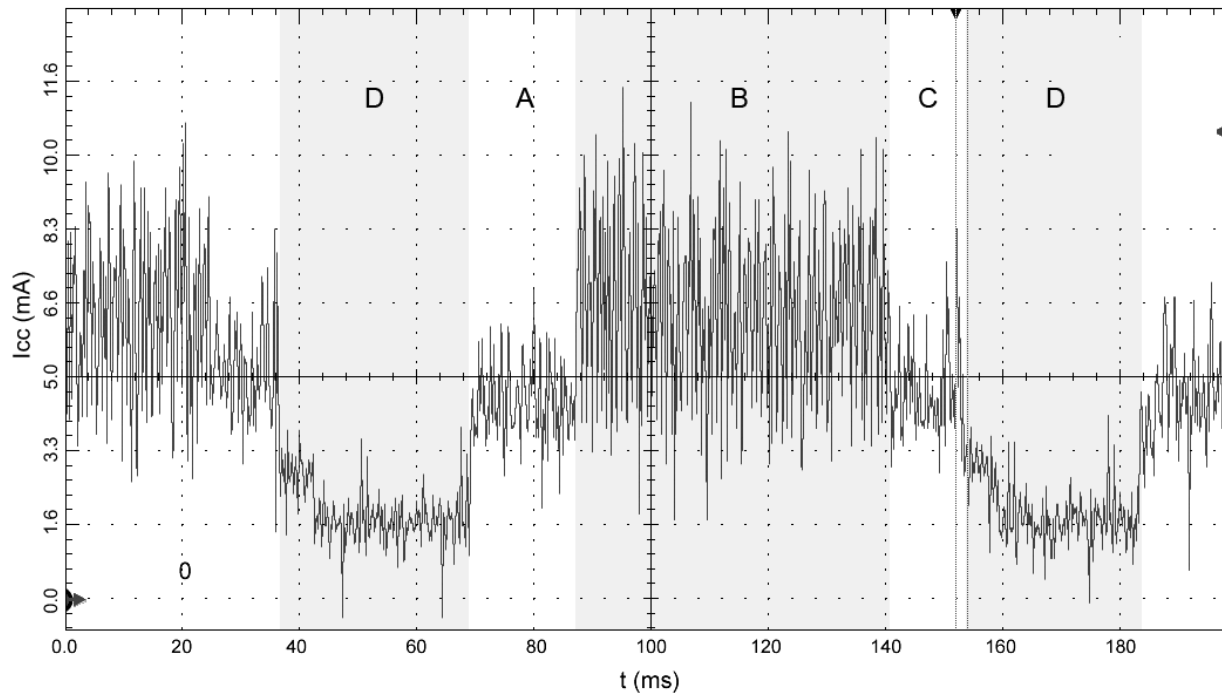
# Testing of Hardware Cryptography Platform

- Sensor node – MICAz (4MHz,  $V_{cc} = 3V$ )
- Smartcard – GemXpresso R4
  - Supported alg.: RSA, DES, AES, MD5, SHA, etc.
  - RSA keys supported up to 2048 bits
- **Our aim – compare SW and HW solution of RSA** encryption and signature using various key length **according to time and energy demands.**
- Results were compared with a paper evaluating energy consumption of software RSA [1].

[1] Amin, F., Jahangir, A., H., Rasifard, H.: Analysis of Public-Key Cryptography for Wireless Sensor Networks Security. In PROCEEDINGS OFWORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY VOLUME 31 JULY 2008 ISSN 1307-6884

# Power Demands of Smartcard

- MICAz (4MHz,  $V_{cc} = 3V$ ) active power supply  $I_{cc} = 5mA$



GemXpresso R4 power trace of RSA-512 signature

- **Power consumption of smartcard is equal to the MICAz sensor!**

# Time & Energy Demands of the Smartcard

## Time demands

			<b>T</b>
SW platform <sup>[1]</sup>	Signature	RSA-1024	22.03 sec.
SW platform <sup>[1]</sup>	Signature	RSA-2048	166.85 sec.
HW platform	Signature	RSA-1024	0.75 sec.
HW platform	Signature	RSA-2048	1.89 sec.

## Energy demands

			<b>W</b>
SW platform <sup>[1]</sup>	Signature	RSA-1024	726.99 mWs
SW platform <sup>[1]</sup>	Signature	RSA-2048	5506.05 mWs
HW platform	Signature	RSA-1024	15.23 mWs
HW platform	Signature	RSA-2048	46.41 mWs

[1] Amin, F., Jahangir, A., H., Rasifard, H.: Analysis of Public-Key Cryptography for Wireless Sensor Networks Security. In PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY VOLUME 31 JULY 2008 ISSN 1307-6884

# Summary

- Proposal of smartcard based hardware cryptography platform suitable for wireless sensor network agents.
- Smartcards are suitable crypto accelerators.
- Smartcards has **lower time demands** (up to 88 times) and also **lower energy demands** (up to 118 times) than SW solutions!
- These improvement allows accelerate cryptographic and also **improve of sensor node battery life**.
- Moreover, smartcards as a tamper resistant device offer **secure storage for public keys, secret keys and other sensitive data**.
- Price of the most smartcards is even lower that price of FPGAs, secure microcontrollers or secure memories (up to \$30).

Thank you for your attention.