UbiSec&Sens

IST PRIORITY
CALL 4
Instrument: STREP
SPECIFIC TARGETED RESEARCH PROJECT

Research topic: FP6-2004-IST-4
Towards a global dependability and security framework
IST-2004-2.4.3

Agenda

Project Overview

Technical Excursus

Potential Impact

Contract No: 26820
EU Contribution: 1.9 MEUR
Starting Date: 1/1/2006
Duration: 36 month

Co-ordinator

Uwe Herzog
EURESCOM
herzog@eurescom.de

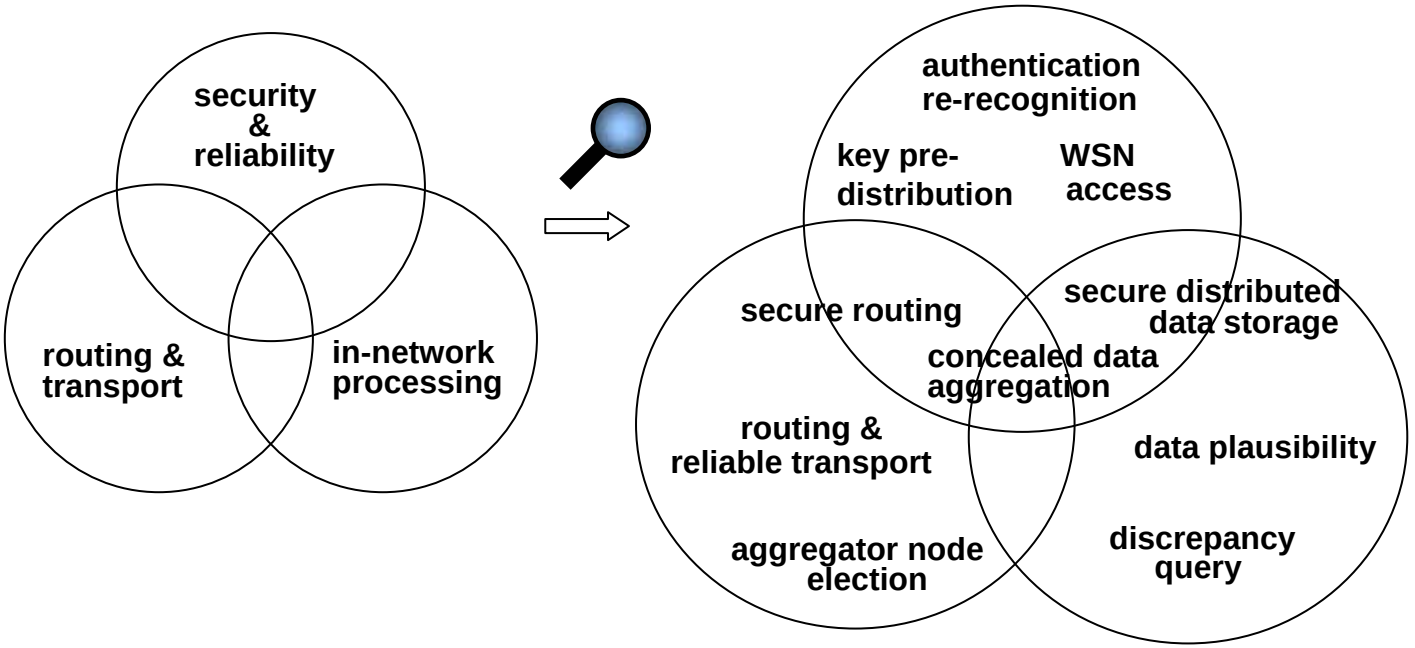
Partners

01	EURESCOM – Coordinator	Germany
02	RWTH Aachen	Germany
03	INRIA	France
04	IHP Microelectronics	Germany
05	INOV	Portugal
06	Budapest University of Technology and Economics	Hungary
07	Ruhr University Bochum	Germany
08	NEC Network Development Laboratories	U.K.

Project Goals

- to provide a security and reliability architecture for medium and large-scale wireless sensor networks acting in volatile environments,
- apply a radically new design cycle for secure sensor networks,
- to provide a complete toolbox of security and reliability aware components for sensor network application development,
- focus on the intersection of security, routing and in-network processing,
- solutions will be prototyped and validated in the representative wireless sensor application scenarios of agriculture, road services and homeland security

Centre of Gravity



Objectives

- flexible routing and in-network processing,
- concealed data aggregation,
- data aggregation with discrepancy query and multiple monitoring sensors,
- encrypted distributed data storage,
- enhanced key pre-distribution,
- provably secure routing,
- resilient data aggregation,
- pairwise/groupwise authentication or re-recognition,
- energy-efficient components

Strategy

design cycle is an iterative process to

- incorporate a balanced security level right from the beginning, and
- ensure the energy-efficient and storage-sensitive cross-layer integration and optimisation of the security features.

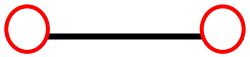
Assumptions

- device classes: both, tamper resistant and non-tamper resistant devices
- radio standard: IEEE 802.15.4 WPAN

Threat Models

Dolev-Yao: 

WSN adapted Dolev-Yao: 

Paradox state of the art: 

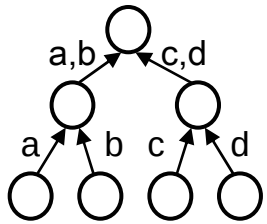
Threat-Model with up to 5 years delay [Gligor05]

Design Options

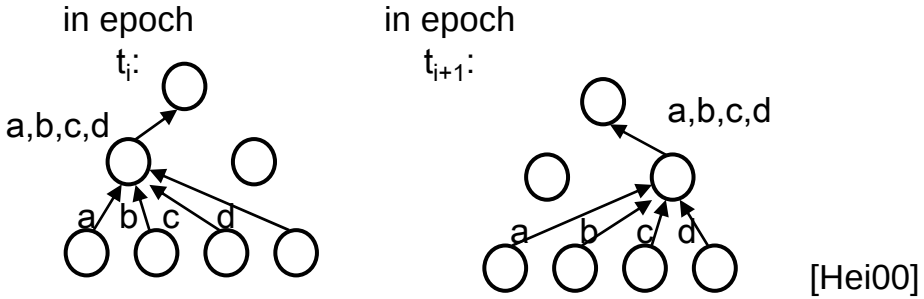
- Tamper-resistant unit (too expensive)
- "Probabilistic" security (attacker receives only limited gain)

Traffic Pattern…

- reverse multicast:

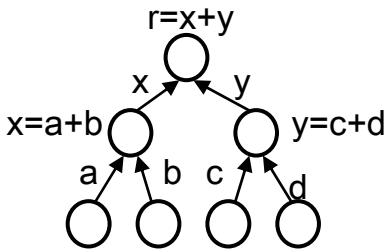


- changing roles:

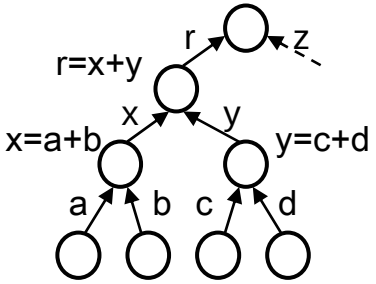


[Hei00]

- in-network processing:



- aggregator hierarchy:

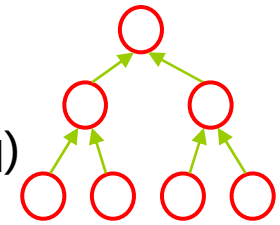


"How to conceal WSN traffic?"

Option 1: **Hop-by-Hop Encryption**

Pros:

- available (RC5 [TinySec], AES-CCS64 [IEEE 802.15.4])



Cons:

- trade-off between system security vs. aggregator node election flexibility

	system security	flexibility
systemwide key	no	high
groupwise keys	medium	medium
pairwise keys	high	no

- lack of security at aggregating backbone nodes
- additional energy for enc/dec operation in the backbone

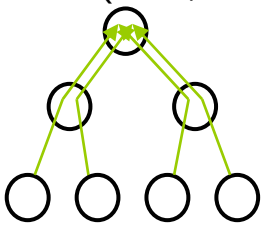
Option 2: **End-to-end Encryption**

Pros:

- saves energy consuming encryption operations in the backbone
- no lack of security at aggregating backbone nodes
- most flexible for aggregator node election process over different epochs

Option 2a: **E2E-E**

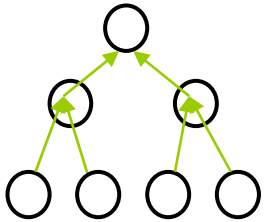
Pros:
available (RC5, AES..)



Cons:
high trans. overhead

Option 2b: **E2E-E**

Pros:
low trans. overhead



Cons:
How to achieve?

Concealed Data Aggregation (CDA):

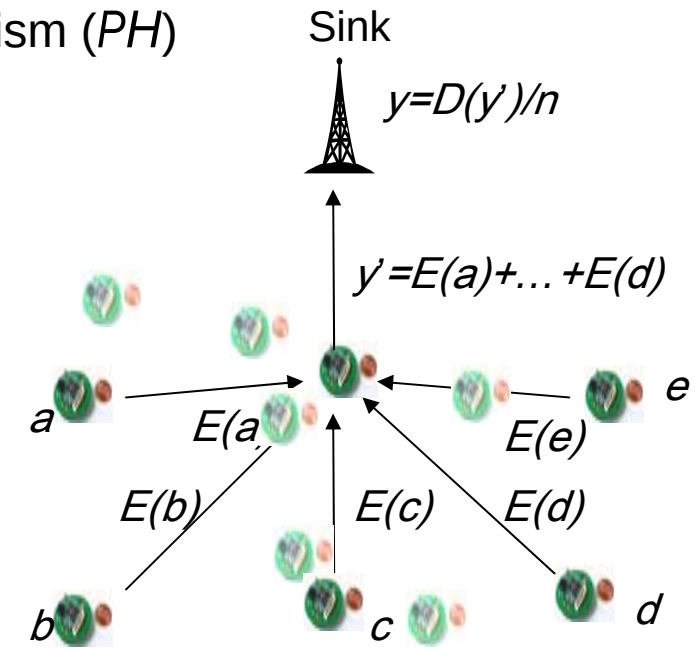
- additive/multiplicative privacy homomorphism (*PH*)

$$a+b=D_k(E_k(a)\oplus E_k(b))$$
$$a\cdot b=D_k(E_k(a)\otimes E_k(b))$$

with groups $(Q,+),(Q,\cdot)$, $(R,\oplus),(R,\otimes)$ and

$$E: K\times Q \rightarrow R$$
$$D: K\times R \rightarrow Q$$

with $a,b\in Q$, and $k\in K$



aggregation function "average" of n sensor nodes

- aggregation functions
  - average,
  - variance and
  - movement detection
  - **no** min/max

- suits also for aggregator hierarchies

Application I (Agriculture)

- protection of the cultivated plants from fungal diseases
- plant protection has a special meaning due to the high quality requirements
- sensors for the collection of the weather process can be the basis for prognosis models for pest control
- plausibility, in-network processing of the “average”, distributed and replicated storage of monitored data

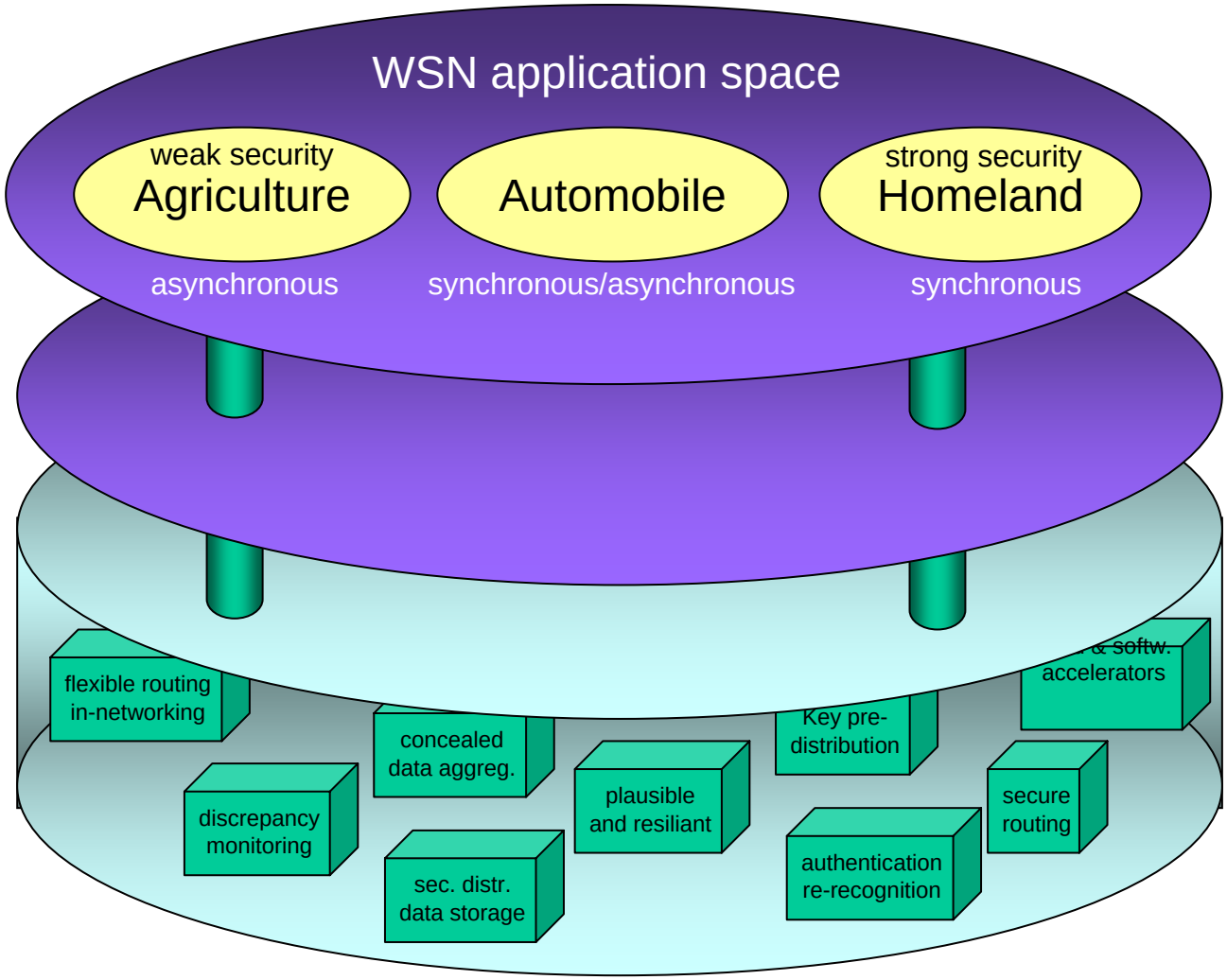
Application II (Road Service)

- driver receives information about the current road status at critical points on the road ahead (Daidalos II)
- WSN is connected to a fixed network (Daidalos II)
- fluctual information can then be incorporated into a digital route planner response and will be displayed on an on-board unit
- WSN requires a long lifetime, high reliability and robustness
- authentication, confidentiality, plausibility, real-time responsiveness

Application III (Homeland Security)

- detect/mitigate the effects of terrorist nuclear, chemical and bio-chemical attacks in public places (airports, bus stations, train stations, underground metro, stadiums)
- protection of special high risk events, like party conventions, political demonstrations, visits of controversial people
- WSN highly reliable and robust even if considerable parts of the WSN are dormant, already inactive or destroyed
- “maximum/minimum” aggregation functions , encrypted data storage
- strong link to ESDP, roll-out at EU-25 border

WSN Security Toolbox Concept



http://www.ist-ubisecsens.org

Project Summary

Wireless Sensor Networks (WSN)s are a exciting development with very large pote ntial to have a significant beneficial impact on every aspect of our lives while generating huge opportunities for European industry. What is needed to kick off the development and exploitation of WSNs is an architecture for medium and large scale wireless sensor networks integrating comprehensive security capabilities right form the concept stage. This would support the rapid development of sensor networks and would open up the application domain for commercial activities.
UbiSec&Sens intends to solve this by providing a comprehensive architecture for medium and large scale wireless sensor networks with the full level of security that will make them trusted and secure for all applications. In addition ***UbiSec&Sens*** will provide a complete tool box of security aware components which, together with the ***UbiSec&Sens*** radically new design cycle for secure sensor networks, will enable the rapid development of trusted sensor network applications.

The ***UbiSec&Sens*** approach is to use three representative WSN scenarios to ite ratively determine solutions for the key WSN issues of scalability, security, reliability, self-healing and robustness. This will also give a clearer understanding of the real-world WSN requirements and limitations as well as identifying how to achieve a successful rollout of WSNs.

News:

- Jan. 23-24th Kick-off meeting at EURESCOM, Heidelberg
- UbiSec&Sens presented at EU workshop “From “RFID to the Internet of things”, 6-7th March, Brussels
- Next meeting: 22/23 March at INRIA Gre-noble

The results of ***UbiSec&Sens*** are a necessary step to progress the field of security and communication research in Europe and, as well as advancing the competitiveness of the European industry, they assist the European Commission to develop more comprehensive programs for innovative socially and economically beneficial sensor applications to be part of future research programs after 2007.