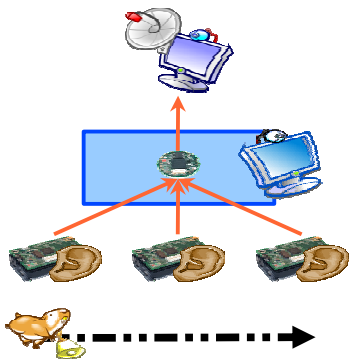


Visions and objectives

Wireless Sensor Networks (WSN) are a particular class of ad-hoc networks that have received considerable attention both in academia and industry. The sensor nodes are preferably tiny and low cost and consist of a simple processor, an energy unit, a wireless transceiver and application specific sensors. Typical applications envisioned for such networks – beside military ones – vary from wildlife tracking to biomedical and environmental surveillance.

Contrary to conventional networks, WSNs deal with limited energy and limited computation resources. Being spread out over a possibly hostile area, the sensor nodes face an adversary model which varies depending on the attackers capability and the hardware configuration. The attacker may be able to eavesdrop on communications, interfere with message transmissions, insert its own messages or even have physical access to the device and access to its stored data. Data encryption, authentication and integrity are of special interest especially when tamper resistance is not an option. However, since most of the well-known cryptographic solutions are computationally expensive, and thus not applicable for sensor nodes, achieving reasonable security becomes a substantial challenge.



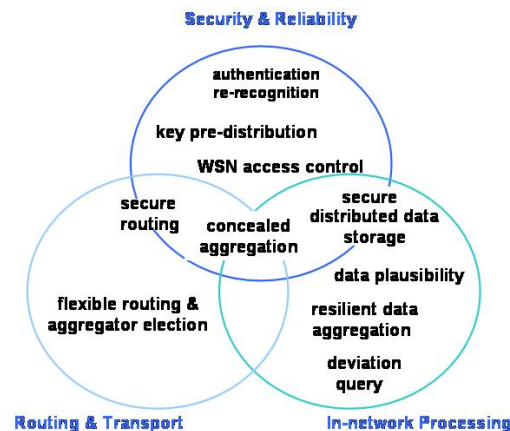
A typical application scenario for a large scale WSN consists of transporting the monitored data in a reverse multi-cast fashion from the sensors, which are spread over a

geographical area, to a central point called sink. At the sink, the retrieved information is analyzed and decisions are taken. In order to reduce the amount of traffic transmitted over the radio the sensed data are usually summarized at intermediate nodes on their way to the sink.

UbiSec&Sens technical approach

Wireless Sensor Networks (WSN)s are an exciting development with very large potential to have a significant beneficial impact on every aspect of our lives while generating huge opportunities for the European industry. What is needed to kick off the development and exploitation of WSNs is an architecture integrating comprehensive security capabilities right from the concept stage. UbiSec&Sens intends to solve this by providing a comprehensive architecture for medium and large scale wireless sensor networks. The overall project goals are to

- » focus the work on the intersection of security, routing and in-network processing
- » provide a complete toolbox of security aware components for sensor network application development
- » prototype and validate the UbiSec&Sens solutions in the representative wireless sensor network application scenarios agriculture, road services and homeland security.



Key research areas

Major research topics from the areas illustrated in are:

- » **Secure flexible routing and aggregator election** - The WSN must be flexible enough to cope with disappearing nodes. The overall scheme must support secure routing and reliable transport via multiple levels of in-network processing. In large WSNs multiple aggregator nodes and multiple levels of aggregation are used.
- » **Concealed data aggregation** - Enhanced mechanisms for end-to-end encryption from the sensors to the sink, also termed convergecast traffic, address the concern of reducing both the energy consumption at the sensor nodes and the effect of physical attacks on the nodes. Concealed Data Aggregation provides a good balance between energy-efficiency and security while still allowing data to be processed at the nodes.
- » **Secure distributed data storage** - In some applications, monitored data must be stored in a distributed way. Whenever it is undesirable or impossible to transmit volatile information to an authorised querying party in real-time, the WSN itself needs to store the monitored data. Since the WSN environment is volatile with nodes that disappear over time, security must be combined with replication.
- » **Enhanced key pre-distribution** - It is not possible for the manufacturer to configure all the sensitive information, such as keys, before the WSN is rolled out. Some sensitive information can only be determined and stored with knowledge of the final position of the nodes. Key pre-distribution schemes for different keying models, e.g. pairwise, group-wise, and even region-wise need to be in place.
- » **Pairwise / groupwise authentication** - In general, nodes need to build up security association without any pre-established secret or common security infrastructure. In

this case, pairs of entities will establish pair-wise relationships. It is also conceivable that groups of entities are able to establish new relationships.

» **WSN access control** - It is essential to provide an access control for end-users of WSN applications, which ensures access to the monitored data for authorized parties only, supports user-friendly data queries and is DoS resilient to save the sensors' battery capacity.

Expected impact

The results of UbiSec&Sens are a necessary step to progress the field of security and communication research in Europe as well as the competitiveness of the European industry. We believe they will also assist the European Commission to develop more comprehensive programs for innovative socially and economically beneficial sensor applications as parts of future research programs.

UbiSec&Sens partners

- » EURESCOM, Germany
- » RWTH Aachen, Germany
- » INRIA, France
- » IHP Microelectronics, Germany
- » INESC – Instituto De Novas Tecnologias, Portugal
- » Budapest University of Technology, Hungary
- » Ruhr University of Bochum, Germany
- » NEC Europe Ltd., U.K.

UbiSec&Sens at a glance

UbiSec&Sens is a Specific Target Research Project (STReP) in the thematic priority "Towards a global dependability and security framework" of the EU Framework Programme 6 for Research and Development.

Contacts

Uwe Herzog, Project Manager

Email: herzog@eurescom.eu

Phone: +49 6221 989 132

Dirk Westhoff, Technical Manager

Email: dirk.westhoff@netlab.nec.de

Phone: +49 6221 4342 149

Partners

EURESCOM

RWTH
MobNets

INRIA
RHÔNE-ALPES

iHP

inovov
INESC • INOVAÇÃO



NEC

The project started in January 2006 and will run for three years.

Ubi
Sec&
Sens

Ubiquitous Sensing and Security in the European Homeland



Information Society
Technologies