



Data acquisition, processing and providing in a heterogeneous, hierarchical Wireless Sensor Network

Corinna Schmitt, Georg Carle

Technische Universität München, Chair for Network Architectures and Services, Germany

A Wireless Sensor Network (WSN) consists of small embedded devices – called motes or nodes – with limited space for the equipment. Corresponding to the applications the hardware is very specialized (e.g. different sensors, memory, energy supply). Those components are also limited factors of such a network. The main goals are to guarantee long life times and maximal data collection for a WSN. Thus, special software must be developed which fulfills different tasks corresponding the network, hardware and application requirements.

The first technology for WSN - the Berkeley Motes - were developed by David Culler and Jason Hill 2000 and are produced by the company Crossbow Technology (<http://www.xbow.com>). Today many different motes are available with special hardware corresponding to the different applications. Sensor boards for brightness, sound and vibration measurements are available for the typical motes. Especially for the requirements of the motes the operating system TinyOS was developed which main characteristic is a two-level schedule and a modular architecture. The software works with tasks, commands and events which have different priorities for their execution.

Applications:

- Health area: Monitoring patients and animals, assist disabled patients
- Military area: Command, control, communication, computing, intelligence, surveillance, reconnaissance, targeting systems
- Home area: Managing inventory, monitoring product quality (Condition Monitoring), monitoring disaster areas (Structural Health Monitoring)

International running research projects:

- Golden Gate Bridge Project, San Francisco, USA (<http://www.cs.berkeley.edu/~binetude/ggb/>)
- Great Duck Island Project, Maine, USA (<http://www.coa.edu/html/greatduckisland.htm/>)
- ZebraNet, Africa (<http://www.peizhang.com/research/research/research.htm>)

In our scenario we want to establish a secure and high-performance WSN which consist of several small sub-networks. Exclusive motes with more resources will act as Gateways to perform the collected data down to the sink of the whole WSN – the Base Station. This information transmission works over RF communication. The Base Station is fixed connected to a Server which is responsible for the data modification, analysis corresponding to the interested context and for the final data storage. The Server should offer a user interface. It should give external users the chance to request the collected data. The communication all over different network parts can be wired or wireless. Thus, a secure communication channel must be offered and should be realized by using certificates and keys which may be assisted through trusted computing mechanisms. Additional challenges are the guarantee of data confidentiality, data integrity, data freshness, availability, self-organization, time synchronization, secure localization and authentication of motes. We want to verify different approaches and implement the selective ones corresponding to our needs under attention to the hardware and security requirements. Currently this project is in working process.

Overview of research tasks:

- Use resources meaningful
- Ensure secure communication in wireless and wired sections
 - Symmetric key creation between
 - a) Embedded Sensor Nodes in small WSN
 - b) Embedded Sensor Nodes and Gateways
 - c) Gateway and Base Station
 - Certificate creation between Base Station and Server for global data storage, analysis and provisioning
 - Using of Trusted Platform Module (TPM) and its technology
- Use verification of special secure needs on different layers (Link-Layer, Network-Layer, Transport-Layer)
- Meaningful data analysis
 - Data pre-processing on special nodes
 - Data analysis corresponding special context on the Server
 - Modification of mote's programs if needed

Overview of verification and implementation tasks:

- Verification of security levels for different component types corresponding to their requirements ✓
- Analysis of existing approaches for secure communication ✓
- Creation of secure communication possibilities between network components (e.g. keys, certificates) – **under construction**
- Running calculation of crypto graphical functions on motes with more resources (e.g. energy, memory)
- Verification of the data analysis in special context – **exemplary data sets of an WSN without security views are available**
- Providing analyzed data to external users through special developed interface (Remote Attestation, Remote Authentication, TPM technology) – **partly implemented**

References:

- Hu et al, *secFleck: A Public Key Technology Platform for Wireless Sensor Networks*, EWSN 2009
- Walters et al, *Wireless Sensor Network Security: A Survey*, Security in Distributed, Grid, Mobile, and Pervasive Computing, 2007
- Shih et al, *A public key technology platform for wireless sensor networks*, SenSys 2008
- Culler, *Secure, low-power, IP-based connectivity with IEEE 802.15.4 wireless networks*, Industrial Embedded Systems, 2007 (<http://www.eecs.berkeley.edu/~culler>)
- Pakzad et al, *Design and Implementation of Scalable Wireless Sensor Network for Structural Monitoring*, In ASCE Journal of Infrastructure Engineering, 2008
- Akyildiz et al, *A Survey on Sensor Networks*, IEEE Communication Magazine, 2002
- UC Berkeley, TinyOS Project, <http://www.tinyos.net>
- Trusted Computing Group, <http://www.trustedcomputinggroup.org>

