Technische Universität München
Network Architectures and Services
Prof. Dr. Georg Carle

19.01.2012

**Master Thesis / SEP / IDP**

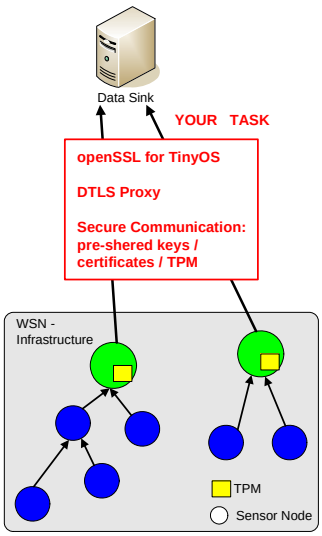
# DTLS implementation for constraint sensor hardware

## Motivation

At our department we have established a Wireless Sensor Network (WSN) consisting of sensor nodes which use TinyOS as an operating system. TinyOS it self is a modular constructed. Those modules are programmed with nesC a derivate of C/C++. Our existing infrastructure uses TinyIPFIX for data transmission over BLIP.
Depending on the WSN application security during data transmission rises in the priority as well as the usage of well proofed and evaluated standards. For this task in common P2P-networks different protocols are used (e.g. for authentication tasks between WSN components and data sink). In general the protocols are too powerful for our used constraint hardware (e.g. power, memory and computational capacities). Thus, the protocols must be flattened. In order to optimize the security between the WSN components itself pre-shared key mechanisms can be integrated and combined with certificate strategies.

## Your task …

… is to evaluate the existing security protocols for wireless sensor nodes in order to find a subset which might geht along with our hardware. The existing solution works with DTLS and openSSL using a sensor node with an onboard TPM chip. Thus, we are focusing on a security solution which offers the opportunity to use DTLS for that more constraint hardware. In order to face the security task the development of a key management mechanism including key deployment is requested.
Finally the developed solution must be integrated into the established network at the department and be evaluated on different network sizes and structure.




Regulated by thesis type the complexity will be attached !

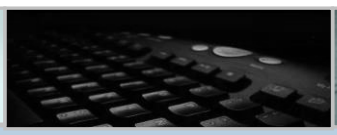
## Requirements

- Basic familiarity with security concepts (DTLS, TPM, pre-shared key, certificates) and data management systems
- Knowledge of C and/or Java required, nesC and TinyOS a plus
- Integration with an existing WSN architecture

## Keywords

Wireless Sensor Networks, Security, Standardization, Data Management Systems





More information provided by Corinna Schmitt
Contact: schmitt@net.in.tum.de, Room 03.05.059