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

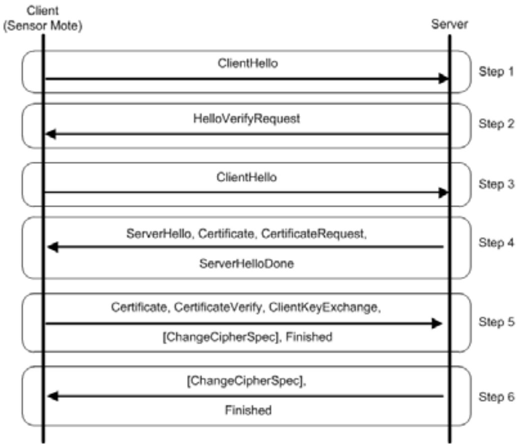
08.08.2011

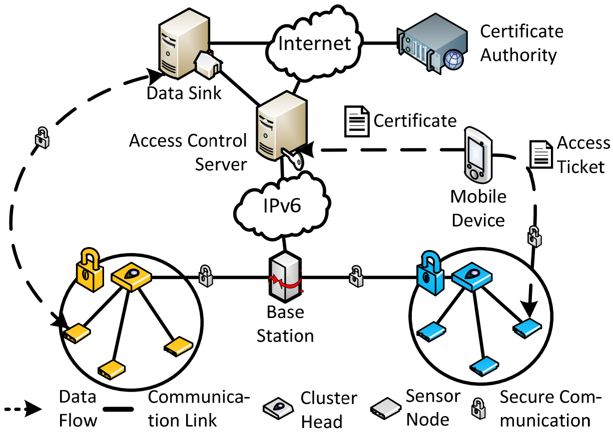
Bachelor / Master Thesis

Security for very constrained objects based on pre-shared keys

Motivation

Many usecases for Wireless Sensor Networks (WSNs) involve the collection and transmission of sensitive data. Yet, many deployments currently do not protect this data through suitable security schemes. We propose an end-to-end security scheme build upon existing internet standards, specifically the Datagram Transport Layer Security protocol (DTLS). By relying on an established standard existing implementations, engineering techniques and security infrastructure can be reused which enables easy security uptake from application developers.





Your task

You are tasked with bringing standard compliant security to very resource constrained sensor nodes in an end-to-end security architecture. Based on an existing implementation of a DTLS-handshake you will select and implement a key exchange that is based on DTLS and requires little Energy, RAM and ROM. This handshake will be executed both with a Data Sink (PC) and a more powerful node within the network, called a Cluster Head. Therefore you will implement the server side of your handshake both on a PC, based on OpenSSL, as well as another sensor node, based on our existing DTLS implementation.

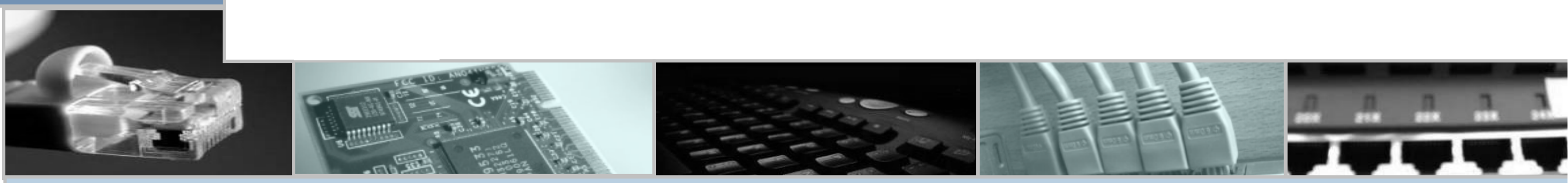
An evaluation of the performance, energy consumption and resource efficiency of your security scheme completes your thesis

Requirements

- Basic familiarity with security concepts
- Knowledge of C required, nesC and TinyOS a plus
- Integration with an existing WSN security framework

Keywords

Wireless Sensor Networks, Security, Standardization



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