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

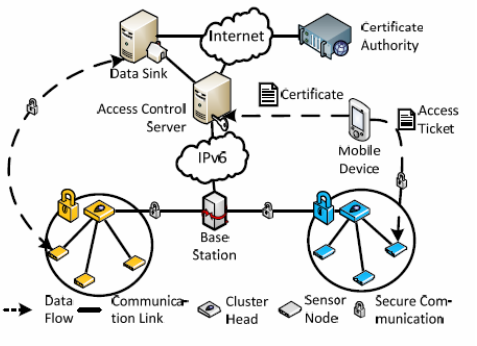
12.01.2012

SEP / Bachelor / Master Thesis

Optimize the Performance of DTLS in Internet of Things (IoT)

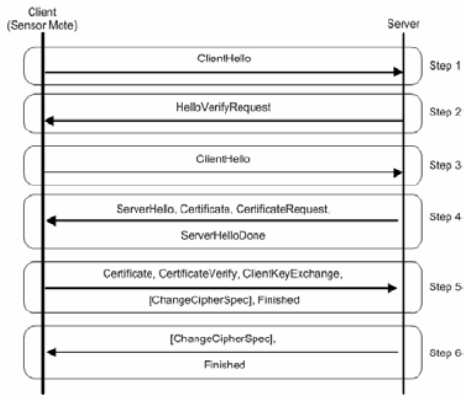
Motivation

Many use cases for Internet of Things (IoTs) involve the collection and transmission of sensitive data. Yet, many deployments currently do not protect this data through suitable security schemes. We have developed 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 design and implement an efficient communication protocol (on transport layer) to optimize the transmission performance of existing IoT DTLS framework.



DTLS was not designed for IoTs, which features low bandwidth and low energy supply originally. Consequently, the communication overhead of DTLS handshake is very high and the end-to-end key establishment latency of it is very long currently. You will investigate novel methods such selective acknowledgement, parallel transmission scheduling and header compression to reduce communication overhead and the end-to-end latency of DTLS handshake. An evaluation of the performance, energy consumption and resource efficiency of your security scheme completes your thesis.

This thesis is a cooperation with CSIRO Brisbane (AUS) and a visit at the company for research during thesis is offered and partly funded.

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, IoT

CSIRO





More information provided by Corinna Schmitt, Thomas Kothmayr and Wen Hu (CSIRO)
Contact: schmitt@net.in.tum.de, Room 03.05.059