Energy-Efficient Security in Smart Metering Scenarios

Anton Hergenröder, Christian Haas Institute of Telematics
Karlsruhe Institute of Technology, Karlsruhe, Germany
Email: anton.hergenroeder@kit.edu, christian.haas@kit.edu

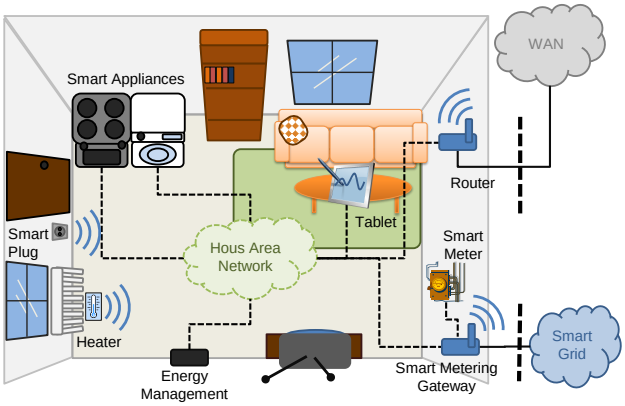

Fig. 1. Smart Metering in Smart Home scenario

I. Introduction

Responsible usage of electrical energy is becoming increasingly important. Electrical energy supply and utilization have to be optimized for efficiency and comfort. Modernization of the public power supply comes into existence as so called *Smart Grid*. However the energy consumption has to be optimized as well. In the future, homes will be equipped with an energy management infrastructure, which monitors the energy consumption of household appliances and controls their operation. Doing so, it is possible to optimize the energy consumption and also reduce the costs, by running some appliances at nighttime where the electricity costs are low. This is convenient for appliances like a washing machine or a dryer. Such homes with intelligent energy management infrastructures are called *Smart Homes*. They are an important part of the smart grid. The integration of smart homes in the smart grid is done by so called *Smart Metering* systems. Smart meters for electrical energy, heating and water supply are capable of communicate the collected data to the providers and metering service providers. In Fig. 1 the described smart home scenario is presented.

The development of energy management systems for smart homes emerges some significant challenges. At first, there are a lot of sensors needed to monitor the appliances and all relevant environmental information. Temperature, humidity, lighting conditions of each room in a house must be collected as well as energy consumption of all relevant appliances. Since it is very costly and complicated to connect all the sensors by wire, it is convenient to use wireless sensor networks (WSNs). Second, there is demand to information security. Collecting all the sensor data in a smart home, an attacker could learn personal information of the inhabitant. Manipulation of the sensor data or control messages can also lead to safety risks, e.g. when driving a heater too hot or remotely control the stove. Therefore, the Federal Office of Information Security (BSI) in Germany has published a protection profile and technical guidelines for the gateway of a smart metering system [7]. Consequently, the security requirements defined in this document should also be met by the whole smart home.

In the scope of the project *KASTEL* [8], we develop a prototype of a real smart home. Our goal is to extend an existing living lab with a secure smart metering solution based on wireless sensor networks. In our work, we address the challenges of secure communication in WSNs. Sensor nodes have to be small and cheap, which results in resource restrictions typical for WSNs, namely little energy and low computational power. Therefore communication and security mechanisms have to be energy-efficient. For energy efficient-security we use a hardware-based security modules attached to standard sensor nodes to compute cryptographic functions efficiently and fast.

II. Demo scope

In our demo, we will evaluate the energy consumption and overhead of secure communication in a basic smart metering scenario as shown in Fig. 2. For demonstration we use a part of our work in progress smart home prototype. We will use two custom built smart plugs that are attached to two wireless sensor nodes (IRIS). We will provide a live measurement of the energy consumption of a house appliance (3 lamps). The energy values will then be transmitted and displayed at a base station. For the communication, we will use a 6LoWPAN network, based on TinyOS blip. One of the two sensor nodes will use a hardware based security module (VaultIC420) to secure the communication to the base station. As we are primarily interested in the energy overhead for the security mechanisms, we will measure and compare the energy consumption of both sensor nodes using two SNMDs. We will show, that a secure smart metering scenario can be built efficiently and without a big overhead in terms of energy.

We will now shortly describe the different parts of our demo.

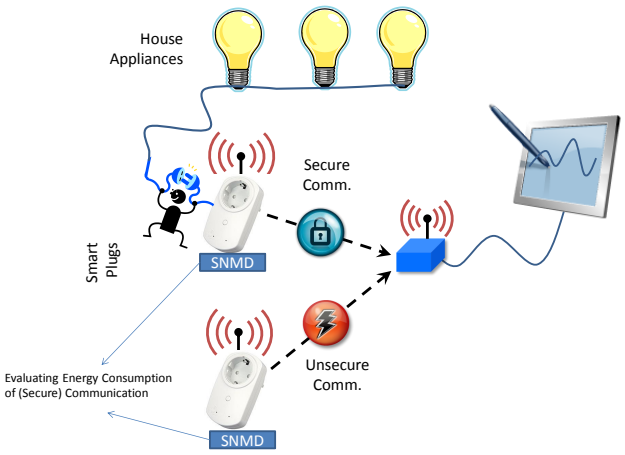

Fig. 2. Demo Setup with Secure Communication in Smart Metering Scenarios

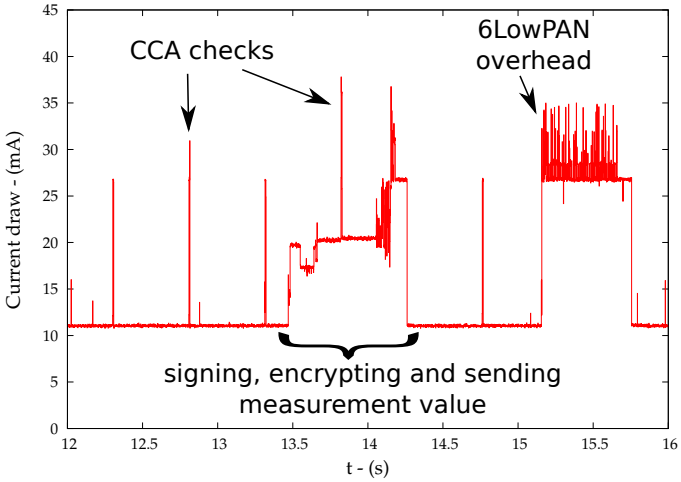

Fig. 3. Live measurement of the sensor nodes' current draw as shown in the demo.

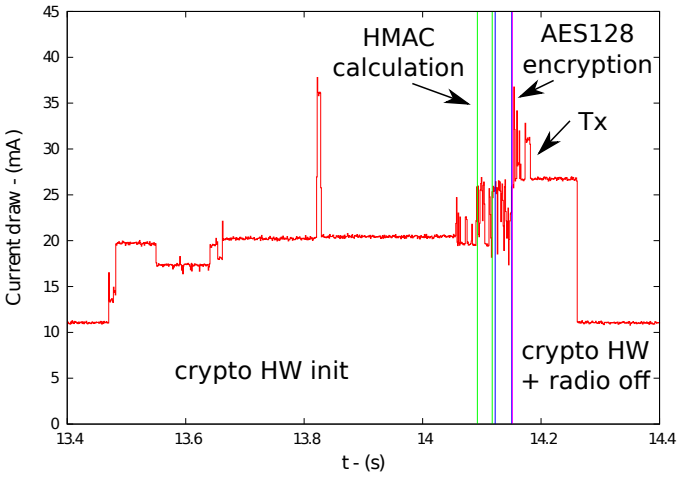

Fig. 4. Detailled view on the current draw of the hardware based security module while performing cryptographic operations.

A. Security Mechanisms

The VaultIC420 [2] has the capability to compute a wide range of symmetric and asymmetric cryptographic algorithms, as well as different hash functions. In our demo we will use the most popular algorithms that have been proposed for WSNs, AES-CBC for encryption/decryption and message digests with HMAC-SHA1.

B. Evaluation of Energy consumption

We evaluate the energy consumption of the proposed security mechanisms by measuring the energy consumption of the IRIS sensor nodes. For a distributed measurement of energy we use Sensor Node Management Devices (SNMD) [1] which are also deployed at the SANDbed testbed at the Karlsruhe Institute of Technology. Attached to each SNMD is a standard IRIS sensor node and a sensor board with the VaultIC420. SNMDs are capable of high resolutive voltage and current measurements. The SNMD provides sampling frequencies of up to $500kHz$ with an average measurement error below 1% [4]. We will show, that a secure smart metering system can be built with little overhead for the security mechanisms.

C. Network architecture

6LoWPAN has been proposed to build future smart home appliances. In this demo we will use TinyOS blip [6] for the wireless communication of the sensor nodes. Therefore, our demo setup can be integrated and used in most smart home environments.

III. Demo Results

In our demo, we evaluate the energy consumption of the proposed security mechanisms by measuring the energy consumption of the IRIS sensor nodes.

Figure 3 shows a live energy consumption measurement of our smart metering sensor node applied to a house appliance (3 lamps). In this figure, the current draw of the IRIS node that is equipped with the hardware based security module is shown. Despite the energy costs for signing and encrypting the measurement value, we are able to highlight the energy consumption for the communication. For example, the periodic CCA checks as used in TinyOS-LPL or the additional overheard for the 6LowPAN communication are shown.

Figure 4 shows a detailed measurement of the simple duty-cycling mechanism for the hardware based security module we are using in our demo. Whenever not used, the crypto chip is powered down due to the relatively high current draw of approx. $20mA$. Therefore, we need to perform a crypto chip initialization before we can use the hardware module. After the initialization, the current draw of the HMAC calculation and the AES calculation is shown. When the encrypted value is successfully transmitted, the hardware module is powered down to save energy.

REFERENCES

[1] A. Hergenröder and J. Wilke and D. Meier, *Distributed Energy Measurements in WSN Testbeds with a Sensor Node Management Device (SNMD)*, Workshop Proc. of the 23th International Conference on Architecture of Computing Systems, 2010.

[2] ATVaultIC420 security module, http://www.insidesecure.com/.

[3] C. Haas, A. Hergenröder, J. Wilke, T. Wiskot and M. Niedermann, *Demo: Evaluating Energy-Efficiency of Hardware-based Security Mechanisms*, 9th European Conference on Wireless Sensor Networks, 2012

[4] A. Hergenröder and J. Horneber, *Facing Challenges in Evaluation of WSN Energy Efficiency with Distributed Energy Measurements*, Multihop Wireless Network Testbeds and Experiments Workshop, IEEE Computer Society, 2011

[5] Shelby, Z. & Bormann, C. 6LoWPAN : The Wireless Embedded Internet John Wiley & Sons, Inc., 2009

[6] Hui, J. W. & Culler, D. E. IP is Dead, Long Live IP for Wireless Sensor Networks, 2008

[7] Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)," Federal Office for Information Security Germany, Protection Profile 1.2, 2013.

[8] Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL), www.kastel.kit.edu.