TLS-Level Security for Low Power Industrial IoT Network Infrastructures

Jochen Mades, Gerd Ebelt, Boris Janjic
KSB SE & Co. KGaA
Frankenthal, Germany
{jochen.mades, gerd.ebelt, boris.janjic}@ksb.com

Frederik Lauer, Carl C. Rheinländer, Norbert Wehn
University of Kaiserslautern
Kaiserslautern, Germany
{flauer, rheinlaender, wehn}@eit.uni-kl.de

***Abstract*—The *Industrial Internet of Things* (IIoT) enables communication services between machinery and cloud to enhance industrial processes e.g. by collecting relevant process parameters or providing predictable maintenance. Since the data is often origin from critical infrastructures, the security of the data channel is the main challenge, and is often weakened due to limited compute power and energy availability of battery-powered sensor nodes. Lightweight alternatives to standard security protocols avoid computationally intensive algorithms, however, they do not provide the same level of trust as established standards such as *Transport Layer Security* (TLS).**

In this paper, we propose an IIoT network system that enables a secure end-to-end IP communication between ultra-low-power sensor nodes and cloud servers. It provides full TLS support to ensure perfect forward secrecy by using hardware accelerators to reduce the energy demand of the security algorithms. Our results show that the energy overhead of the TLS handshake can be significantly reduced to enable a secure IIoT infrastructure with a reasonable battery lifetime of the edge devices.

I. Introduction & Related Work

As one of the largest manufacturer of pumps and industrial valves in the world, KSB aims at providing high quality, reliability, and best services to their customers. Pump systems often represent key components in safety-relevant plants and infrastructure systems, such as fire-fighting systems or cooling systems in power plants. Therefore, dysfunctions can lead to human damage and incalculable economic risks. To prevent the hazards, pump systems are usually maintained manually in regular intervals, which however, causes high costs and does not prevent sudden malfunctions. Hence predictive maintenance concepts were introduced in which industrial machines are equipped with sensors to monitor quantities that provide information about internal physical conditions. This sensor data is transferred to central cloud servers that analyze and extract relevant information. To be a viable solution, it is important that the sensor devices can be attached post-hoc on existing machines. Therefore, these devices often must be battery-powered and communicate wirelessly with data collection units or cloud systems. As a result, low power system design becomes essential in order to reduce costly battery replacement cycles. Furthermore, as wireless communication is always exposed to attackers, the security aspect of the communication becomes a primary requirement for such IIoT systems [1]. The most widespread protocol for state-of-the-art network communication security is the TLS protocol. However, the underlying algorithms have been valued as too computationally-intensive to be performed on resource-constrained embedded platforms [2]. Therefore, lightweight alternatives like *energy-efficient Datagram TLS* (eeDTLS) [3], E-Lithe [4] and *Compact TLS* (CTLS) [5] have been proposed. However these alternatives are not supported by important cloud platforms like AWS IoT [6] or Google IoT Core [7], because the clear majority of existing IoT devices that use these platforms like home appliances or lamps is not as energy constrained as the aforementioned applications. Most commercial solutions like ABB's Ability Smart Sensor [8] use wall-powered gateways which handle the TLS connections to the cloud and at the same time communicate over non-*Internet Protocol* (IP)-based protocols with battery-powered sensor edge devices. This approach avoids bulky IP handling on the low-power devices but in turn lacks on end-to-end encryption.

To provide the same trust to the IIoT infrastructure as in modern internet communication, a true end-to-end communication between edge device and cloud server is required. Thus both parties must support TLS on top of the standard IP to be compatible with the leading IoT cloud suppliers.

In this paper, we present a secure industry-capable IIoT network system that provides a high level of trust as it only sticks to well-established standards and overcomes the energy concerns by optimizing the computationally-intensive cryptographic algorithms using dedicated hardware accelerators.

This IIoT network is part of KSB's digitization strategy by adding an innovative, secure and reliable data-to-cloud communication system. Furthermore, it is a mayor milestone towards cloud controlled pump systems and strengthens the place of KSB as one of the leading pump manufacturers.

II. Secure Ultra Low-Power IIoT Network

Our system is based on wireless *Personal Area Networks* (PAN) which are connected to the internet via gateways, utilizing the given infrastructure such as power supply and standard internet connection like Ethernet. This way, no cellular network service like Narrowband(NB)-IoT is required, which is often not available for pump systems as they are usually located in underground installations. To avoid intermediate security-critical protocol-converting units, the low power PAN between gateway and edge device must be capable of

978-3-9819263-4-7/DATE20/©2020 EDAA

handling IP-based data transfers. Therefore, the 6LoWPAN (IPv6 over Low power Wireless PAN) standard has been employed, which reduces the amount of data for bandwidth-constrained communication channels. Although 6LoWPAN is mostly found in IEEE802.15.4-based protocols, *Bluetooth Low Energy* (BLE) has been shown to outperform IEEE802.15.4 for 6LoWPAN in terms of energy efficiency [9]. As BLE is furthermore more robust to obstacles [10], the PAN of the proposed system is realized using BLE. Regarding the IoT application layer, the *Message Queuing Telemetry Transport* (MQTT) protocol is applied to maintain compatibility with common cloud vendors [6] [7]. As shown in Figure 1, the gateway only acts as transposer in the physical and link layer, thus no security-related requirements apply to it.

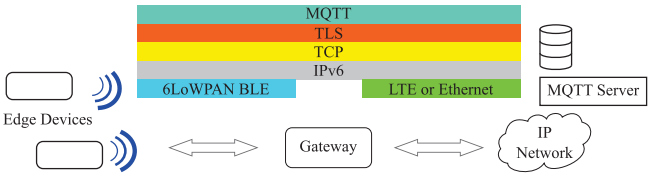

Fig. 1. Proposed IP Layer Structure Throughout the Network Topology

Besides the complex IP handling, the edge device needs to handle the computationally-intensive TLS protocol despite its strict energy consumption limitations. In order to reduce the computational effort, only cipher suites based on *Elliptic Curve Cryptography* (ECC) have been considered. To provide the highest security level, the concept of perfect forward secrecy was applied with ephemeral encryption keys by employing the cipher suite `TLS_ECDHE_ECDSA_AES_128_GCM_SHA256`. The ECC computations have been optimized by utilizing dedicated hardware accelerators. The main computational unit of the sensor node device is the nRF52840 *System on Chip* (SoC) by Nordic Semiconductor, which has an integrated ECC accelerator (ARM CryptoCell-310). In order to additionally evaluate the potential of an external ECC hardware accelerator, the ATECC508, a low-cost cryptographic coprocessor from Microchip, was applied. MbedTLS is used as TLS library. The gateway is based on a Raspberry Pi 3, and the Mosquitto software provides the MQTT broker on an IPv6 capable server.

III. Evaluation & Results

In our results we focus on the energy overhead of the TLS handshake process, covering the certificate-based mutual authentication and the exchange of the encryption key. Thus, the overheads represent the price that has to be paid for trust and security. The results are segmented into three groups of ECC implementation: plain software solution (SW), external hardware acceleration with the ATECC508 (HW_{AT}) and internal hardware acceleration using the CryptoCell (HW_{CC}). Figure 2 (top) shows the time and energy overhead caused by the TLS handshake process for each MQTT connection.

Figure 2 (bottom) shows different battery lifetime estimations of the sensor edge device, depending on the ECC

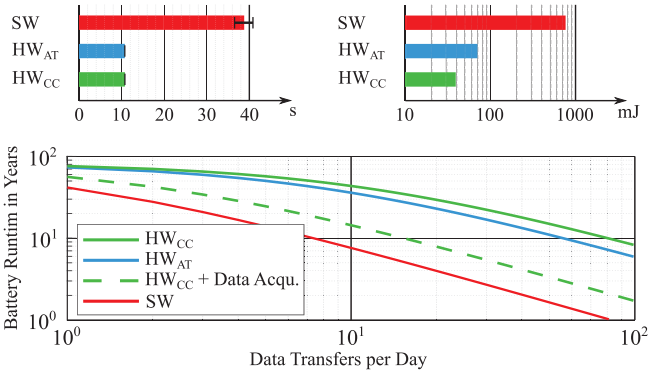

Fig. 2. Handshake overhead (top) and battery runtime estimation (bottom)

implementation type and the number of MQTT connections per day. Besides the handshake process, each connection includes a data transfer of 128 bytes. The sleep current is 2.5µA. An AA Lithium cell (thionyl chloride, 3.6V, 2.6Ah) is employed as battery, 70% of its capacity considered as usable. The dashed line represents the use case of a real predictive maintenance application. It includes 20s and 300mJ for recording vibration sensor data with a KSB sensor unit.

IV. Conclusion

This work contributes to the area of IoT security, that has been valued as one of the most critical challenges in the IoT field [1]. To the best of our knowledge, this is the first system which closes the gap between using well-established security standards and ultra low power devices in the area of IIoT networks. With the presented strategy, battery lifetimes can be enhanced up to one order of magnitude compared to state-of-the-art software implementations. Our results show, that cryptographic hardware accelerators make TLS-based security feasible for battery-powered IoT edge devices.

References

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[2] M. Frustaci, P. Pace, and G. Aloi, "Securing the IoT world: Issues and perspectives," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, Sep. 2017, pp. 246–251.

[3] U. Banerjee, C. Juvekar, S. H. Fuller, and A. P. Chandrakasan, "eeDTLS: Energy-efficient datagram transport layer security for the internet of things," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Dec 2017, pp. 1–6.

[4] A. Haroon, S. Akram, M. A. Shah, and A. Wahid, "E-lithe: A lightweight secure dtls for IoT," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Sep. 2017, pp. 1–5.

[5] TLS Working Group, "Compact TLS 1.3 - Draft," 2019, viewed on 27.08.2019. [Online]. Available: https://tools.ietf.org/html/draft-rescorla-tls-ctls-02

[6] AWS IoT Developer Guide, "Security and Identity for AWS IoT," 2019, viewed on 27.08.2019. [Online]. Available: https://docs.aws.amazon.com/iot/latest/developerguide/iot-security-identity.html

[7] Cloud IoT Core, "Requirements," 2019, viewed on 27.08.2019. [Online]. Available: https://cloud.google.com/iot/docs/requirements

[8] ABB, "Ability Smart Sensor - FAQ," viewed on 27.08.2019. [Online]. Available: https://new.abb.com/motors-generators/de/motoren-generatorenservice/erweitertes-service-angebot/smart-sensor/

[9] P. Trelsmo, P. Di Marco, P. Skillermark, R. Chirikov, and J. Ostman, "Evaluating IPv6 connectivity for IEEE 802.15.4 and Bluetooth Low Energy," in *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, March 2017, pp. 1–6.

[10] Rohan Tabish, Adel Ben Mnaouer, Farid Touati, and Abdulaziz M. Ghaleb, "A comparative analysis of BLE and IEEE802.15.4 (6LoWPAN) for U-HealthCare applications," 11 2013.