A Security and NFC Enhanced Wireless Sensor Network Node

Antonio Jonjic†, Jasmin Grosinger*, Wolfgang Bösch*, Thomas Herndl†, Rainer Matischek† and Gerald Holweg†
* Institute of Microwave and Photonic Engineering, Graz University of Technology, Graz, Austria
† Development Center Graz, Infineon Technologies Austria AG, Graz, Austria

***Abstract*—We propose to use asymmetric public-key based encryption in large scale and widespread wireless sensor networks. In this work, we show that asymmetric public-key encryption can be implemented time and power efficiently on hardware constrained wireless sensor nodes. To achieve efficient public-key encryption, we combine a sensor node processor unit with a sophisticated near field communication (NFC) cryptographic coprocessor. This type of cryptographic coprocessor has a low-power hardware accelerated cryptographic unit that is typically used in contactless cryptographic smart cards. The NFC interface also provides a secured wireless link. We beneficially exploit this characteristic to implement a device authorization scheme for out-of-band network configuration like pairing and device identification number assignment.**

I. Introduction

Some fields of wireless sensor network (WSN) applications like environmental monitoring or infrastructure protection require a large network size and an inaccessible wide deployment area. For such application scenarios asymmetric public-key encryption is favorable in comparison to a pre-distribution of private-keys to all pairs of nodes [1], [2].

So far, public-key deployment in large WSNs is based on software implementations [3], [4], [5], [6], [7], [8]. The results of previous publications report that public-key cryptography is not suited for WSNs, because software implemented public-key cryptography is inefficient in time from a practical point of view. But unlike previous work, we do not use a software implementation of the cryptographic algorithms. We propose to use a sophisticated cryptographic hardware that enables time efficient elliptic curve cryptography and other public-key algorithms and primitives. In comparison to previous hardware implementations [9], [10], [11], we do not design special processor cores to implement public-key cryptography, we use a dedicated secure cryptographic controller that provides a beneficial separation of the protocol and cryptographic processes.

This paper is structured as follows. Section II presents a WSN node that is enhanced with a near field communication (NFC) secure cryptographic controller for public-key cryptography. Section III describes technical details of the cryptographic controller and details of security improvements. Finally, future work is discussed in the conclusions.

This work was performed as part of the K-project "Secure Contactless Sphere — Smart RFID Technologies for a Connected World" that is funded by the Austrian Research Promotion Agency (FFG) and the ARTEMIS JU Project "Internet of Energy", Project No. 269374.

II. NFC Enhanced WSN Node

For the realization of a public-key based encryption in a large WSN, we combine a processor unit of a WSN node with an NFC cryptographic coprocessor that is used in contactless cryptographic smart cards. Figure 1 and Figure 2 show the implemented WSN node. The upper block diagram of Fig. 1 depicts a conventional WSN node with a security featured microcontroller for comparison reasons. The lower block diagram of Fig. 1 and Fig. 2 show the NFC enhanced wireless sensor node that consists of a microcontroller unit (XMC1100 [12]), and a multichannel-multi-protocol transceiver (TDA5340 [13]) that is connected to an ultra high frequency (UHF) antenna. The sensor is a Hall effect-based current sensor for power metering (TLI4970 [14]). The cryptographic coprocessor is a highly evolved cryptographic hardware product typically used in passive powered security smart cards (SLE78xx [15]). The NFC coprocessor is connected to a high frequency (HF) loop antenna.

The cryptographic coprocessor supports hardware accelerated public-key cryptographic algorithms and cryptographic hash-functions. These algorithms – Rivest, Shamir and Adleman (RSA) and elliptic curve cryptography (ECC) – have a performance in time that is two to three decades higher than the performance of algorithms implemented in software on conventional microcontrollers. While the software implemented cryptographic algorithm performance is measured in ms, the performance of smart card cryptographic controllers is measured in μs.

A. Process Separation

We use a general purpose microcontroller, with no special cryptographic hardware features (see Fig 1 and Fig 2). We see this as an advantage in relation to the process of firmware/software development. Programming of security featured firmware is a critical and complex task, with the risk of significant security gaps if no proper caution is taken. Therefore, special knowledge is required, especially when programing such smart card secure cryptographic controllers. The physical separation of the protocol, sense, and control processes and the security cryptographic processes has the

advantage that specialised vendors can offer secured and verified cryptographic firmware. This cryptographic firmware can be read only memory (ROM) masked programmed, or stay flexible and be updated securely by an authorized vendor. Without the need of doing encryption, the WSN node microcontroller can be chosen in a flexible manner. We decided to use a small, energy efficient microcontroller that has a small memory and therefore consumes significantly less power.

B. Security Aspects

The lower block diagram of Fig. 1 shows that the NFC secure cryptographic controller is connected over a serial peripheral interface (SPI) with the general purpose microcontroller. It could be assumed that this SPI interface exposes a weak link, allowing attackers to probe the SPI interface through electromagnetic emission or by microprobing. This can be avoided by numbers used once (NONCEs) in the encryption process. NONCEs are usually a message counter and number each message encrypted and send with a plaintext. NONCEs and cipher characteristics make it possible that identical messages sent at different times – like "light on" – will result in a completely different ciphertext. A known-plaintext attack has therefore no chances of success, as long as the attacker do not gain access to the shared secret.

III. Cryptographic Controller

The NFC secure cryptographic controller supports hardware acceleration for the most common public-key cryptographic algorithms. These are 1024/2048-Bit RSA and 160-Bit ECC over GF(p) and GF(2^n) (see Fig. 3 ACP hardware block). The cryptographic controller has a true random number generator (TRNG) periphery instead of only a pseudo random number generator (PRNG) as in conventional WSN nodes. Random number generators (RNG) with a high entropy are essential for the security of cryptographic algorithms. Therefore, hardware based TRNGs increase the security strength of cryptographic protocols. Also, the cryptographic controller offers hardware accelerated hash functions for an efficient public-key cryptography (see Fig. 3 HASH hardware block). The cryptographic controller supports main cryptographic hash functions like: secure hash algorithm (SHA)-1, SHA-256 and message-digest algorithm (MD)-5. Cryptographic hash functions are necessary to create digital signatures, message authentication codes, and certificate-based encryption.

A. Double Encryption

The greatest security advantage of the NFC secure cryptographic controller is double encryption. In case of double encryption, both running programs and data is protected. This is done by the memory encryption/decryption unit (see Fig. 3 MED hardware block) which decrypts and encrypts the data and the code before the memory storage.

B. Secured NFC Interface

A major part of the research in the field of WSNs is the issue of secure key distribution. For symmetric encryption algorithms, every wireless sensor node in a network has to have the same secret key. When we imagine that WSN nodes can be spatially distributed over a large area, and are therefore vulnerable to theft, then it is clear that the ability of updating the secret key is important. In the case of our proposed design, this can be performed securely and fast over the NFC interface (see Fig. 3 radio-frequency identification interface (RFI) hardware block). Also, for public-key encryption algorithms this can be an advantage, for example public/private keypairs could be generated externally and then they could be initiated over the secured NFC interface.

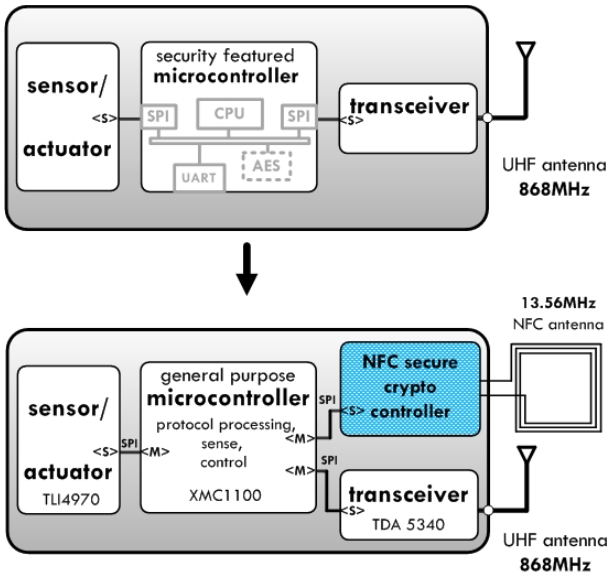

Fig. 1. The upper bock diagram depicts a conventional WSN node with a security featured microcontroller for comparison reasons. The lower block diagram shows the NFC enhanced wireless sensor node with the 32 Bit 12 MHz XMC1100 microcontroller unit, the 868 MHz multichannel-multi-protocol transceiver (12.5 mA at 10 dBm) that is connected to the UHF antenna, a planar inverted-F antenna designed for 868 MHz and provides a small form factor. The sensor actuator is the Hall effect-based TLI4970 current sensor (max. 25 A) for power metering. The SLE78xx cryptographic coprocessor is a highly evolved cryptographic hardware product and supports cryptographic algorithms like RSA-1024 Bit, RSA-2048 Bit, ECC GF(p)-160 Bit, ECC GF(2^n)-160 Bit and hash functions like SHA-1, SHA-256, and MD5. The coprocessor is connected to the HF antenna, an NFC coil antenna designed for 13.56 MHz.

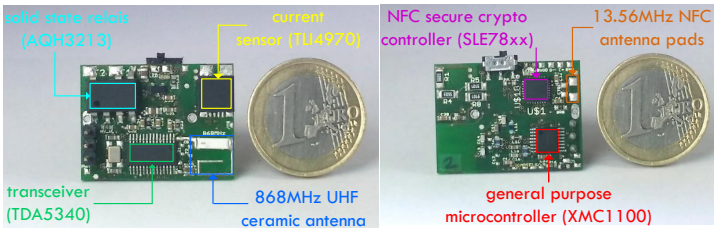

Fig. 2. This figure shows the printed circuit board (PCB) design of the NFC enhanced WSN node. The compact design of the WSN node PCB enables the installation into small devices and casings. The NFC antenna pads offer the ability to attache application-specific designed NFC antennas.

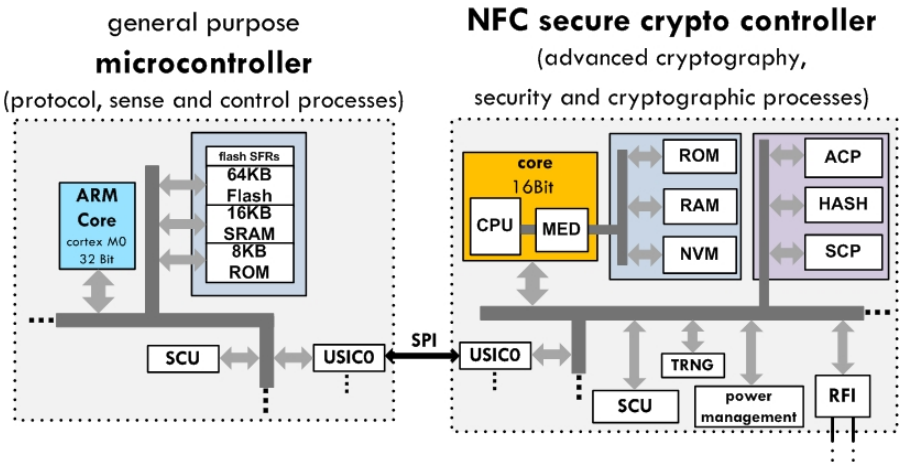

Fig. 3. This figure shows the system architectural approach for achieving a high-level of security and efficient encryption, especially public-key based encryption. Through this system architecture approach the protocol processing, sensing, and control processes are physically and logically separated from the security and cryptographic processes. The left side of the figure shows the general purpose microcontroller, the right side of the figure shows the temper resistant high-security smart card cryptographic controller. The key hardware components of the cryptographic controller are: the asymmetric cryptographic processor (ACP), the symmetric cryptographic processor (SCP), and the hash functions hardware block (HASH).

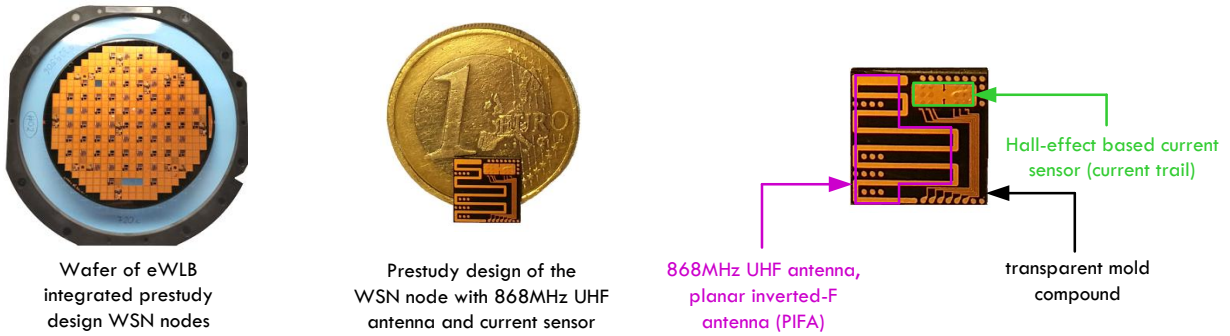

Fig. 4. The picture shows an eWLB packaged preliminary design of our wireless sensor node. This design contains the 868 MHz UHF antenna that is implemented as a planar inverted-F Antenna (PIFA) and the 25 A current sensor (TLI4970). The purpose of manufacturing this design was to investigate how the eWLB mold compound influences the 868 MHz UHF link and also to analyse the influence of the 50 Hz AC current on the 868 MHz UHF link. The eWLB package mould compound is transparent at the bottom, so the metal redistribution layer is visible. Therefore, the 868 MHz UHF antenna and the current sensor trail are visible. The current sensor digital interface is additionally connected to outside pins (balls). The eWLB packaging technology allows the integration of passive electronic components and even radio frequency components like antennas in one single chip package.

C. High Level Physical Security

There are significant differences in tamper and invasive attack resistance strength of available security featured micro-controllers. They vary from low-level to mid-level protection. In the best case, a sophisticated attacker would need days to weeks to crack a microcontroller with a mid-level protection at moderate costs. Smart card cryptographic controllers are high-level protected devices, because they are used in the security critical financial payment industry. The NFC secure cryptographic controller offers a high level of invasive attack protection (SLE78xx [15]).

IV. Conclusions

In this paper, we describe a system architecture for a WSN node that solves the problem of inefficient public-key cryptography in WSNs. An initial prototype of the WSN node has already been realized for pre-studies (see Fig. 2). For the purpose of antenna pre-studies we additionally integrated a UHF planar inverted-F antenna and the sensor current trail (TLI4970 [14]) in an embedded wafer level ball grid array (eWLB) package that offers a high miniaturization factor (see Fig. 4). In our future work, we will proof the effectiveness of our proposed system architecture by measuring and analysing the implementation of a proprietary public-key protocol (see Fig. 5). This public-key based communication protocol will enhance the time efficiency of the encrypted data transfer. The results of the performance measurements of the prototype will verify that public-key cryptography is suitable for direct use on resource constrained hardware platforms like WSN nodes.

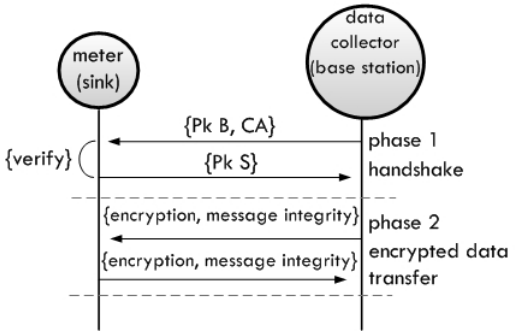

Fig. 5. This figure shows the high level view of the communication protocol that will be implemented (Pk B : base station public-key, CA : base station certificate, Pk S : sink (node) public-key): The protocol security function fulfills data confidentiality, message integrity, and base station authentication. A handshake phase is necessary to first exchange public-keys. No session key is generated (direct asymmetric encryption). The meter device in the figure will be a smart socket in a planned application demonstrator.

REFERENCES

[1] K. Piotrowski, P. Langendoerfer, and P. Steffen, "How Public Key Cryptography Influences Wireless Sensor Node Lifetime," in *Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks*, October 2006.

[2] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: Securing Sensor Networks with Public Key Technolog," in *Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks*, October 2004.

[3] K. P. AI-Sakib and S. H. Choong, "Feasibility of PKC in Resource-Constrained Wireless Sensor Networks," in *Proc. International Conference on Computer and Information Technology*, December 2008.

[4] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, *Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs*. Santa Clara, USA: Springer Science+Business Media, LLC, 2004.

[5] M. H. Mokammel, K. P. Al-Sakib, G. C. Byung, and S. H. Choong, "An Efficient PKC-Based Security Architecture for Wireless Sensor Networks," in *Proc. IEEE Military Communications Conference*, October 2007.

[6] C. Xu and Y. Ge, "The Public Key Encryption to Improve the Security on Wireless Sensor Networks," in *Proc. International Conference on Information and Computing Science*, May 2009.

[7] L. Ronghua, J. Han, X. Zeng, Q. Li, M. Lang, and J. Zhao, "A Low-Cost Cryptographic Processor for Security Embedded System," in *Proc. Asia and South Pacific Design Automation Conference*, March 2008.

[8] D. Yong-ping and H. Hong-li, "Tradeoff Design of Low-cost and Low-Energy Elliptic Curve Crypto-processor for Wireless Sensor Networks," in *Proc. Asia and South Pacific Design Automation Conference*, September 2012.

[9] M. H. Ahmed, S. W. Alam, N. Quereshi, and I. Baig, "Security for WSN Based on Elliptic Curve Cryptography," in *Proc. International Conference on Computer Networks and Information Technology*, July 2011.

[10] A. R. Mishra and M. Singh, "Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network," *International Journal of Engineering Research & Technology*, vol. 1, no. 3, May 2012.

[11] M. Salam, P. Kumar, and H. Lee, "Security for WSN Based on Elliptic Curve Cryptography," in *Proc. International Conference on Networked Computing and Advanced Information Management*, August 2010.

[12] I. T. AG. XMC1100 by INFINEON TECHNOLOGIES AG. online. http://www.infineon.com/cms/de/product/microcontroller, visited 2014-07-20.

[13] ——. TDA5340 by INFINEON TECHNOLOGIES AG. online. http://www.infineon.com/cms/de/product/rf-and-wireless-control/wireless-control/transceiver, visited 2014-07-20.

[14] ——. TLI4970 by INFINEON TECHNOLOGIES AG. online. http://www.infineon.com/cms/de/product/sensor-ics/current-sensor, visited 2014-07-20.

[15] ——. SLE78xx by INFINEON TECHNOLOGIES AG. online. http://www.infineon.com/cms/de/product/smart-card-ic, visited 2014-07-20.