# DESIGN OF A SENSOR NODE CRYPTO PROCESSOR FOR IEEE 802.15.4 APPLICATIONS

Goran Panić, Thomas Basmer, Schomann Henry, Steffen Peter,
Frank Vater and Klaus Tittelbach-Helmrich

IHP
Frankfurt Oder, Germany

**ABSTRACT**

The security emerges as a very important constraint for many wireless sensor network applications. This paper presents the design of a sensor node processor supported by a variety of security mechanisms including complex data cryptography and hash generation. Additionally, the processor core is enhanced with the hardware acceleration for IEEE 802.15.4 medium access layer operations. The paper describes the chip architecture and its components and gives the chip implementation details. Finally, the power and performance of the chip have been discussed and analyzed.

## I. INTRODUCTION

Wireless sensor networks (WSN) consist of a number of randomly distributed sensor nodes used for detection and monitoring of physical or environmental conditions such as temperature, pressure, sound, vibration, etc. Many applications such as military surveillance, industry automation or medical monitoring require a very high level of confidentiality of transferred data. The most common approach to increase the data security in a network is to use cryptography. However, using cryptography in a sensor network faces many challenges due to very limited performance and power resources of sensor nodes.

Traditional sensor nodes usually rely on commodity-of-the-shelf (COTS) components chosen to support some of the well-developed industrial or IEEE standards. The majority of the available solutions support some of the IEEE 802.15 set of standards. For low-rate applications typical for WSN, IEEE 802.15.4 emerged as the preferred standard [1]. IEEE 802.15.4 specifies the physical layer and media access control (MAC) for low-rate wireless personal area networks (LR-WPANs). It is the basis for the ZigBee, ISA100.11a, WirelessHART, and MiWi specifications, each of which further extends the standard by developing the upper layers which are not defined by 802.15.4.

The power limitation of sensor nodes implies the usage of 8- or 16-bit microcontrollers that consume low power but have limited memory resources and processing capabilities. The traditional nodes are usually incapable of efficiently processing complex security algorithms and protocol software for demanding applications. Our solution presented in this work, relies on the hardware acceleration for security algorithms and MAC protocol tasks. Although the additional hardware increases design complexity and total costs, it significantly improves the performance and power of the system.

The rest of the paper is organized as follows: Section II discusses some security aspects of sensor networks. Section III gives details on IEEE 802.15.4 MAC protocol. Section IV describes the system architecture. The implementation results are given in Section V. Finally, Section VI presents the results related to power and performance of the designed system and Section VII concludes the paper.

## II. SECURITY ASPECTS OF WSN

The problem of data security in WSN has been addressed at two abstraction levels, software and hardware. While the software solutions try to incorporate security mechanisms to the existing, traditionally designed, sensor network infrastructure, the hardware solutions at the other hand, concentrate to optimize the underlying sensor node hardware. The common approach to increase the data security in sensor networks is by applying secret key cryptography. There are two

978-1-4673-1295-0/12/$31.00 ©2012 IEEE 

well-established families of crypto algorithms: symmetric (shared-key cryptography) and asymmetric (public-key cryptography). The algorithms based on public-key cryptography usually offer high level of security but are also very computationally intensive. Therefore, the software implementation of public-key cryptography is often considered as inapplicable in traditional WSN [2]. The shared-key cryptography is generally faster and has better power efficiency than public-key. Potentially, it's a suitable solution for WSN, but the problem of setting secure communication between nodes, e.g. setting up the secret keys between communicating nodes, has to be addressed. This problem is also referred as the key agreement problem or the key distribution problem and is widely studied in general network environments [3]. There are three types of general key agreement schemes: trusted-server scheme, self-enforcing scheme, and key pre-distribution scheme. The commonly used trusted-node key distribution scheme is not feasible for WSN due to the lack of trusted infrastructure in the network. In the case of key pre-distribution scheme, where the key information is distributed among the nodes before deployment, the achieved network resilience remains limited and the additional computational overhead is affecting the performance [4]. Our approach relies on self-enforcing scheme that uses public-key certificates for key agreement. For that purpose, we designed a processor-based system that includes hardware acceleration for both public- and shared-key cryptography. The designed hardware solution enables high level of security at the cost of additional complexity and chip size.

## III. IEEE 802.15.4 MAC LAYER

IEEE 802.15.4 standard was designed to answer the requirements of low-rate wireless personal area networks. It describes fundamental lower network layers (physical and MAC) of a network focusing on low-cost, low-speed ubiquitous communication between devices. IEEE 802.15.4 supports low data rates (<250kb/s) and different network topologies (star and peer-to-peer). The network model differentiates between full-function device (FFD) and reduced-function device (RFD). FFD can work as a network coordinator or as a simple node. At the other hand, RFD is a simple node having limited resources and can only communicate with FFD.

The medium access control (MAC) enables the transmission of MAC frames through the use of the physical channel. Besides the data service, it offers a management interface and itself manages access to the physical channel and network beaconing. It also controls frame validation, guarantees time slots and handles node associations. Finally, it offers hook points for secure services.

A standard MAC implementation flow starts with a formal description of the protocol. The formal description results in a software implementation targeting a specific system. Depending on the target hardware, not all implementations include all of the MAC functionality described in the standard. However, there are also MAC implementations that claim to be system independent, but those are considered to be inefficient compared to dedicated solutions. A comparison between different MAC implementations is given in [5].

Our implementation of MAC evolved from a formal UML (Unified Modelling Language) description. The UML model was developed as a platform independent model. Our intention was to integrate complete MAC functionality in the hardware. Therefore, we didn't perform any profiling that would lead to hardware/software co-partitioning. The first step in the MAC design flow was to perform the decomposition of MAC tasks using Lollipop-notation of UML2 standard. During this step, the components describing specific MAC tasks were developed and the common interface to access data has been defined. The second step was to estimate required memory space to store control and status data and to buffer data packets. The execution was limited to a single task at the time. Upon completion of a single task the next task takes the control of data packet processing (round-robin scheme). When a single packet is processed, the core generates an interrupt to the microcontroller and updates its status register. More details on MAC implementation is given in [6].

## IV. SYSTEM ARCHITECTURE

The core of the designed system is an asynchronous 16-bit microcontroller developed by

Fraunhofer IPMS. The system includes a number of peripherals: IO ports, timer, crypto accelerators (ECC, SHA-1, AES and RSA), MAC and a baseband unit and serial ports (SPI and UARTs). The architecture of the system is shown in Figure 2.

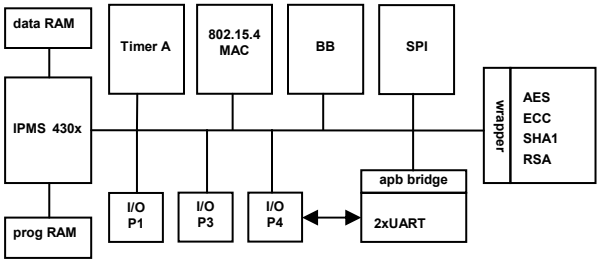


Figure 1. System Architecture

### A. Microcontroller

IPMS430x is an asynchronous 16-bit processor core fully compatible to Texas Instruments MSP430x architecture. The core is a latch-based design that applies poly-phase clocking in its control unit. In our implementation it is provided with 16kB of RAM and 2kB of program memory that is mainly used for debugging purposes. Main program memory is accessed externally vie external memory bus interface.

### B. IO Ports

The implemented IO ports (P1, P3 and P4) are fully compatible with TI digital IO specification. In our system port P2 is not integrated. The IO ports are 8-bit wide and can be individually programmed to connect external ports or internal signals. Port P1 is provided with interrupt capability.

### C. Serial Interface

To support serial communication with external devices (sensors, radio control interface, etc.), we implemented two asynchronous UARTs (TI 16550 compatible) and a single SPI master core. The UARTs were the part of an AMBA IP library having APB interface, so we provided a bridge for connection to the IPMS430x multiplexed bus. To reduce the total number of pads, we connected the external signals of one UART through P4 port. The integrated SPI core provides active edge selection and burst mode operation and can be used to connect multiple SPI slaves to the system.

### D. Timer

The timer is implemented according to 'Timer A' specification of TI MSP430X architecture. It provides three capture/compare units and supports pulse width modulated outputs connected through the IO ports. Additionally, the timer supports both synchronous and asynchronous capture modes, overflow detection and selection between multiple clock sources.

### E. MAC

Some of the features of the implemented MAC core have been already described in the previous section. The MAC core implements a memory block with the size of 512 bytes that is used for MAC data storage. The core doesn't implement a dedicated transceiver interface, since the communication with an analog front-end is to be maintained by some of the processor peripheral interfaces.

### F. Baseband

The implemented baseband controller complies with the DIN EN 13757-4 standard. EN 13757-4 is a communication standard for meters and remote reading of meters specified for short range devices running at frequencies 868-870MHz with data rates ranging from 2.4 to 66.6 kb/s. The baseband is extended with DSSS (direct sequence spread spectrum) functionality in order to improve communication in a highly jammed environment.

### G. Crypto Cores

The system implements hardware accelerators for both public- (ECC, RSA) and shared-key cryptography (AES) as well as for hash-generation (SHA-1). The cores are wrapped into a single crypto block that communicates with MCU over a 32-to-16-bit interface. Having both RSA and ECC in a single chip is not economically justified but it certainly widens the node application field. Nevertheless, our chip is only a prototype intended for use in different research areas and not a highly-optimized end product.

**AES.** The AES (Advanced Encryption Standard) is a symmetric cipher algorithm, which uses the same key for encryption and decryption. In our implementation, AES has key length of 256 bits with 4-bit address and 32-bit data memory-like interface to the processor. The advantage of AES

hardware implementation over the software is given in [7].

**ECC.** ECC stands for Elliptic Curve Cryptography and it is an asymmetric cipher algorithm that uses algebraic operations on elliptic curves over finite fields. The algorithm is able to provide a very high level of security with a relatively short key size. In our implementation, the algorithm supports the key size of 233 bits. The details related to the implementation of the ECC core are given in [8].

**RSA.** RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA needs longer keys and more computations for a similar cryptographic strength as ECC. However, RSA is part of several international standards so we still wanted to support it with the node. The implemented RSA component contains a 64-bit multiplication unit, a 128-bit addition unit, dedicated memory and a small logic that assist the processor performing the modular exponentiations of very long integers.

**SHA-1.** SHA-1 (Secure Hash Algorithm) is the most widely used cryptographic hash function of the existing SHA hash functions, and is employed in several widely-used security applications and protocols. SHA-1 produces a 160-bit message digest based on principles similar to those used in MD4 and MD5 message digest algorithms, but has a more conservative design.

## V. IMPLEMENTATION

The chip has been designed for IHP 0.13um CMOS technology. It has the size of 8.9mm$^2$ and contains 112 pads (80 signal- and 32 power/ground pads). The total cell area is less than 2mm$^2$ indicating that the chip is to a great extent pad limited. After production, the chip has been packaged and tested for correct functionality. Compared to the similar implementation presented in [9], the designed chip takes full advantage of lower scale process. It takes only half of the size of the other chip and includes additional logic and memory blocks for MAC and RSA. The layout of the chip is shown in Figure 2.

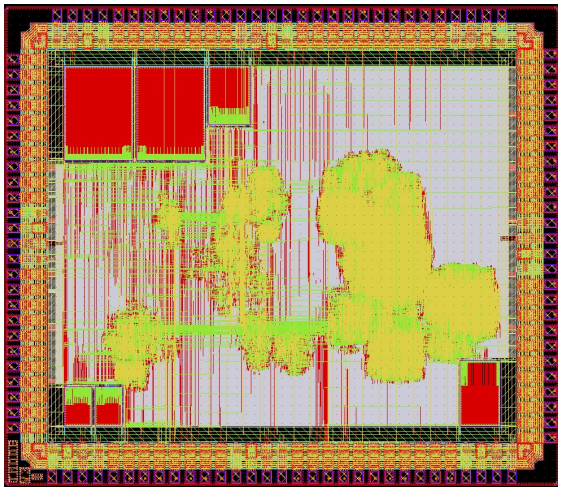

Figure 2. Layout of the chip

## VI. POWER AND PERFORMANCE

To accurately estimate the power of the chip, we performed the vector-based power estimation of the post-layout design using Cadence EPS (Encounter Power System) tool. The estimation is done for typical conditions ($V_{core}$=1.2V, $V_{pad}$ = 3.3V, T=25C) and target frequency of 12.5MHz. The acquired data are presented in Table I. The results do not include power consumption in IO, since the power information for the pads was not included in the available libraries for the target technology. However, the power measurements on the produced chip showed good matching with the power estimation for the core. Furthermore, the chip measurements have shown that the power consumed by the pads dominates the total power of the chip and is around 6mW.

Table 1: Post-Layout power estimation

| Chip Function | Total Power (mW) |
|---|---|
| SHA-1 | 1.4 |
| ECC Point Multiplication | 4.06 |
| ECC First Point Inversion | 2.57 |
| ECC Second Point Inversion | 2.55 |
| AES encoding | 1.28 |
| AES decoding | 1.26 |
| RSA | 1.28 |
| MAC | 0.44 |
| Baseband Transmit Data | 1 |
| Baseband Receive Data | 1.01 |

Along with the functional validation of the chip, we also measured the execution time and average

power consumption for different processing tasks. It was of special interest to determine what performance/power gain is achievable when specific encryption or protocol operations are executed in hardware. The ECC was the most computationally intensive task. Our system implementation shows 15 times improvement in power over the system described in [9] and accordingly 90000 times improvement in ECC computation over the software implementation on TI MSP430F1611 [10]. The significant performance improvements are achieved also with RSA and AES operations. AES crypto operation executes in 66 clock cycles compared to Texas Instrument software implementation that takes 6600 cycles for encryption and 8400 for decryption [11]. This implies the performance improvement of 100 times. The implemented RSA accelerator improves the RSA calculation by up to two orders of magnitude. In the case of MAC, we achieved 31 times improvement in CRC computational speed and around 10 times improvement in overall packet assembly time [6].

## VII. CONCLUSION

In this paper we presented the design of a low-power sensor node aimed for security-critical applications. The chip implements hardware support for different symmetric and asymmetric crypto algorithms and for hash generation. It targets the sensor networks based on IEEE 802.15.4 standard by implementing dedicated hardware for an efficient MAC processing. The chip is produced in 0.13um technology process and is successfully tested. The measurements showed the significant improvement in power and performance of specific security and protocol operations when compared to pure software implementation. However, the implemented dedicated hardware added an additional overhead to the chip size increasing the total cost of the system. Nevertheless, for a number of high-demanding applications, the achieved gain justified the trade-off. In the future, we plan further optimization of the system by embedding a Flash on the chip. That would further reduce the number of pads that turned out to be the major power consumer in the chip.

## REFERENCES


1. IEEE 802.15.4-2006 Standard for Information technology-Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). IEEE Computer Society. Revision of IEEE Std 802.15.4-2003. ISBN 0-7381-4996-9, 8 September 2006.

2. R. R. Brooks, B. Pillai, M. Pirretti, and M. C. Weigle, “Multicast encryption infrastructure for security in sensor networks,” International Journal of Distributed Sensor Networks, vol. 5, no.2, pp. 139–157, 2009.

3. C.Y. Chen, H.C. Chao, “A survey of key distribution in wireless sensor networks,” Security Comm. Networks, doi: 10.1002/sec.354, 2011.

4. H. Chan, A. Perrig, D. Song, „Random key predistribution schemes for sensor networks,” IEEE Symposium on Security and Privacy, pages 197–213, Berkeley, California, May 11-14, 2003.

5. T. Basmer, H. Schomann, S Peter, "Implementation analysis of the IEEE 802.15.4 MAC for wireless sensor networks," International Conference on Selected Topics in Mobile and Wireless Networking iCOST2011, pp.7-12, 10-12 Oct. 2011.

6. H. Schomann, "Untersuchung und Entwurf einer modularen Hardware-Architektur für das MAC-Protokoll des Standards IEEE 802.15.4 anhand vorhandener Software-Implementierungen," Diplomarbeit, BTU Cottbus, November 2011.

7. F. Vater, P. Langendörfer, “An Area Efficient Realisation of AES for Wireless Devices,” IT - Information Technology 2007, 188-193.

8. S. Peter, “Evaluation of Design Alternatives for Flexible Elliptic Curve Hardware Accelerators, Diploma Thesis,” BTU Cottbus, 2006.

9. G. Panić, T. Basmer, O. Schrape, S. Peter, F. Vater, K. Tittelbach-Helmrich, “Sensor Node Processor for Security Applications,“ 17th IEEE International Conference on Electronics, Circuits, and Systems (ICECS), 2012, 81-84.

10. J. Portilla, J. Andrés Otero, E. de la Torre, T. Riesgo, O. Stecklina, S. Peter, P. Langendörfer, “Adaptable Security in Wireless Sensor Networks by Using Reconfigurable ECC Hardware Coprocessors,” International Journal of Distributed Sensor Networks, Vol. 2010

11. Uli Kretzschmar, “AES128 – A C Implementation for Encryption and Decryption”, TI - White Paper, 2009