

Efficient Hardware Implementation of Security Processing for IEEE 802.15.4 Wireless Networks

Panu Hämäläinen, Marko Hännikäinen, and Timo D. Hämäläinen

Tampere University of Technology

Institute of Digital and Computer Systems

P. O. Box 553, FI-33101 Tampere, Finland

Tel: +358 3 3115 2111, Fax: +358 3 3115 4561

Email: panu.hamalainen@tut.fi, marko.hannikainen@tut.fi, timo.d.hamalainen@tut.fi

Abstract—The IEEE 802.15.4 standard defines the medium access control and physical layer for low-rate, low-power Wireless Personal Area Networks (WPAN). As a number of WPAN applications require protected communications, the standard defines security procedures. Since the procedures typically consume most processing capacity in the limited 802.15.4 devices, efficient implementations are needed. As a solution, this paper presents a compact and energy-efficient hardware design, supporting all the security suites of the standard. Compared to typical WPAN processors, the presented FPGA prototype and the estimated ASIC implementation offer significantly higher performance and lower energy consumption. The FPGA throughput at the highest security level is 90 Mb/s and the energy consumption is 1/190 of an 8-bit microcontroller and 1/5 of an ARM9. The estimated energy consumption for the equivalent ASIC implementation is 1/10 of the FPGA prototype. In addition to 802.15.4, the hardware design supports all wireless technologies derived from the IEEE 802.11i security specification.

I. INTRODUCTION

Communications are steadily shifting from wired media to wireless networks. Along with high-speed technologies, a need for low-rate and low-power wireless networks for short-range monitoring and control has emerged. Automation, safety, healthcare, and entertainment at homes, public buildings, and industry are seen as the major application fields. Example applications include heating and alarms systems, remote controllers, and data transfers between personal portable devices.

IEEE 802.15.4 [1], ratified in the end of the year 2003, is one of the first standards defining the radio and the medium access control layer for a low-rate, low-power Wireless Personal Area Network (WPAN). The technology is also referred to as ZigBee, which is an industry alliance working on the 802.15.4 and upper protocol layers. The 802.15.4 standard supports three frequency bands (868 MHz, 915 MHz, and 2.45 GHz) and data rates up to 250 kb/s. The 802.15.4 devices either form a star topology network or communicate through peer-to-peer connections.

It is clear that, e.g., alarm systems must be protected from unauthorized exploits. Hence, the 802.15.4 standard specifies cryptographic procedures for protecting communications at the medium access control layer. Security procedures are generally among the tasks requiring most processing capacity in network devices. Thus, the overall processing limitations as well as energy consumption can be significantly alleviated

with efficient security processing implementations, which is especially desirable in battery-powered devices. This paper presents a compact and energy-efficient hardware design for the 802.15.4 security processing. Since the standard utilizes the work of the IEEE 802.11i security group [2], the design supports other new wireless IEEE technologies as well.

The paper is organized as follows. Section II presents an overview of the 802.15.4 security processing. Section III discusses the different alternatives for the hardware implementation of the processing. In Section IV the implementation of the alternative argued to be best suited for 802.15.4 is presented. The implementation results are reported in Section V. The section also compares the results to processors of the same application domain. Section VI concludes the paper.

II. OVERVIEW OF 802.15.4 SECURITY PROCESSING

The 802.15.4 standard [1] defines optional cryptographic security suites for providing either confidentiality, integrity, or both. Confidentiality is achieved through encryption using Advanced Encryption Algorithm (AES) [3] in Counter mode (CTR) and integrity through Message Integrity Codes (MIC) generated with AES in Cipher Block Chaining Message Authentication Code (CBC-MAC) mode. Hence, the integrity also includes authentication of origin. The combination is offered with AES in the CTR with CBC-MAC mode (CCM).

The 802.15.4 security suites and their services are summarized in Table I. The length of the 128-bit MIC can be truncated to 32 or 64 bits by choosing corresponding AES-MIC or AES-CCM suites. The AES-CTR and AES-CCM suites can optionally be configured to utilize freshness protection against replay attacks. Authentication and key exchange are not defined in the standard. They must be implemented on the higher protocol layers.

In the AES-CTR and AES-CCM suites the 802.15.4 payload data is en/decrypted by XORing a key stream produced from a secret key and a counter with the data. The counter is incremented for each data block. It consists of a nonce and a 16-bit block counter (in the standard there are also other fields but in this work they are all regarded as a part of the nonce). For integrity the AES-MIC and AES-CCM suites process each data block with AES after XORing the plaintext block with the previous ciphertext block. The last ciphertext

TABLE I
802.15.4 SECURITY SUITES AND THEIR SERVICES

Suite	Confidentiality	Integrity	Freshness
AES-CTR	✓	-	✓
AES-MIC-128	-	✓	-
AES-MIC-64	-	✓	-
AES-MIC-32	-	✓	-
AES-CCM-128	✓	✓	✓
AES-CCM-64	✓	✓	✓
AES-CCM-32	✓	✓	✓

block is truncated to the length defined by the selected suite and output as the MIC. The MIC protects selected portions of the 802.15.4 header and the payload. In the AES-CCM suites also the MIC is encrypted. The security suites only require the 128-bit-key forward functionality of AES itself.

III. HARDWARE DESIGN ALTERNATIVES

There are a number of alternatives for the hardware implementation of the 802.15.4 security processing. Since AES is the computational core, its design has a significant effect on the energy consumption and performance of the whole design.

Similarly to other block ciphers with rounds, the basic approaches for the AES implementation are the iterated, pipelined, and loop-unrolled architectures [4]. In the iterated architecture the processed block is circulated through a single-cycle round logic. The pipelined architecture consists of the AES rounds with registers in between. A loop-unrolled architecture performs two or more rounds at a clock cycle and the execution is either iterated or pipelined. More advanced methods include sub-pipelining and different combinations of the three basic approaches [4]. As the iterated architecture is the smallest, it is considered the most cost-effective choice for 802.15.4 in this work. Due to the low data rates of 802.15.4, high enough throughput is also achieved.

Each 32-bit piece of a data block can be processed independently during an AES round. Hence, the area of a round can be decreased with a 32-bit folded round [5], reducing the width of the data path by the factor of four. Even though the cycle count is increased with the same factor, in this work the area savings are regarded more significant and folding is utilized.

The AES substitution boxes (S-box) [3] are often implemented as memory-based look-up-tables (LUT). The LUT size can be decreased at the cost of latency when the S-box representation is transformed into another arithmetic domain [6]. On the other hand, the latency can be shortened by combining more operations into large LUTs, which require fewer accesses. Whereas memory-based S-boxes are the best choices for compact Field Programmable Gate Array (FPGA) designs, combinatorial logic is well-suited for Application Specific Integrated Circuits (ASIC). Also, in FPGAs combinatorial logic can be used for fine-grained pipelining in high-speed designs at the cost of resources [7]. In this paper the prototype implementation of the 802.15.4 security processing is targeted

to a FPGA, and thus, memory-based S-boxes are utilized for a compact design. However, they can be easily substituted with another technique due to the modularity of the design.

The AES roundkeys can be precomputed or generated on-the-fly [4]. Precomputing requires setup time and memory but it also implies power savings as the key logic has to operate only once per AES key [5]. Opposed to on-the-fly computation, precomputation can share resources with the AES data path, supporting compact designs. Thus, precomputation is chosen for the 802.15.4 implementation.

In addition to the speed, power, and area requirements, the utilized encryption mode defines the reasonable architectural choices for the AES core. The throughputs of the CTR mode and the CTR encryption in the CCM mode can be unlimitedly increased by utilizing pipelining and parallel cores. However, due to the feedback loop of the MIC mode and the CCM MIC generation, already a single, iterated core achieves the maximum throughput for the MIC computation. Therefore, in 802.15.4 the most cost-efficient choice is to utilize only one, iterated AES core. In order to reduce buffering, in this paper the CCM mode interleaves the MIC and CTR processing.

IV. 802.15.4 SECURITY PROCESSING DESIGN

The prototype hardware of the 802.15.4 security processing is implemented in register transfer level VHDL and synthesized to an Altera Cyclone FPGA. The design consists of a compact AES core with pre-computed key schedule and control logic for supporting all the 802.15.4 security suites.

A. Implementation Platform

The FPGA utilized in this work is Altera Cyclone EP1C4F324C6 [8]. It is comprised of a two-dimensional logic array, consisting of Logic Array Blocks (LAB), each containing 10 Logic Elements (LE) and interconnects. A LE constitutes of a 4-input LUT and a register. The FPGA contains also embedded M4K memory blocks, which can be used for implementing a variety of memory functions, including shift registers, FIFO buffers, and single- and dual-port RAMs and ROMs. An M4K can store up to 4,608 bits. EP1C4F324C6 contains 4,000 LEs and 17 M4K blocks. The design tools utilized in this work are ModelSim SE PLUS 5.8d 2004.06, Precision RTL Synthesis 2003b.41, and Quartus II v4.1.

B. AES Design

The design of the AES core is based on the folded round design of [5]. In this work the decryption functionality is removed and the intermediate results (*state*) are stored in four 8-byte dual-port RAMs (DPRAM) as the M4Ks do not support shift registers with suitable tap distances. The data path architecture is presented in Fig. 1. In the following, the names SubBytes, ShiftRows, MixColumns, Rcon, and *state* are consistent with the AES specification [3].

In the figure all the connections are 32 bits wide. The clocked entities are marked with '>'. The core consists of the encryption and roundkey generation sharing the *data in* port and the 32-bit SubBytes implemented as two 256-byte

TABLE III
SECURITY PROCESSING IMPLEMENTATION IN EP1C4F324C6

Measure	Value
Data path width, bits	32
Logic elements	1,434
Memory bits (M4Ks)	7,808 (11)
Max. clock, MHz	78
Internal power @50 MHz, mW	98.92
- Standby power, mW	60.00
- LE power, mW	14.91
- M4K power, mW	7.16
- Clock tree power, mW	16.85

TABLE IV
PERFORMANCE OF SECURITY PROCESSING IMPLEMENTATION

Measure	CTR	MIC	CCM
Key setup, cycles	48	48	48
Cycles per block	57	57	112
Throughput @78 MHz, Mb/s	176	176	90

In the CCM mode the processing starts with MIC computation for the 802.15.4 header and then constantly alternates between the CTR and MIC configurations for the payload. The order of CTR and MIC processing must be switched in decryption. As an opposite of the CTR mode, in CCM *ctr* is set to the value 1 for the first data block. When the MIC is computed or input, it is en/decrypted by setting *ctr* to zero [1]. In the decryption the decrypted MIC is output first, followed by the computed MIC.

V. RESULTS

The results for the 802.15.4 design in EP1C4F324C6 are presented in Table III. In addition to the AES core, memory bits are used by the masking logic (16×128 bits). The folded core consumes 36% of the reserved LEs and 74% of the reserved memory bits. The presented power figures are for the CCM mode with a static key. It was measured that the powers of the other modes are also very close to CCM. The performances for the 802.15.4 processing modes are presented in Table IV.

Table V compares the security processing design with implementations in typical processors of the 802.15.4 application domain. The throughputs (T_p) are for the CCM mode at the reported clock frequency. DS80C323 [9] is an 8-bit, 8051-compatible microcontroller and ARM966E-S [10] is a 32-bit processor aimed at embedded devices. The throughput for DS80C323 is derived from [11] and for ARM9 from [12]. CCM requires two AES passes for a data block. The processor powers do not include memories.

The table also presents the power and the throughput for an ASIC estimate of the 802.15.4 security processing design. Ref. [13] reports a $0.18 \mu\text{m}$ CMOS AES design comparable to the block-wide core of this paper. Equal throughputs are achieved with both the designs at the same clock frequency. The power of the 802.15.4 ASIC estimate is computed by assuming that the power differences in the ASIC technology are consistent

TABLE V
COMPARISON OF 802.15.4 SECURITY PROCESSING IMPLEMENTATIONS

Platform	Clock (MHz)	Power (mW)	T_p (Mb/s)
FPGA	50	99	57
ASIC (estimate)	125	28	140
DS80C323 [9] [11]	18	30	0.09
ARM966E-S [10] [12]	200	140	16

with the dynamic power (standby power excluded) differences between the FPGA designs of this paper.

Significant energy savings are achieved with the 802.15.4 design compared to the processor implementations. With pre-computed roundkeys the energy consumption of the CCM mode in the FPGA is $0.22 \mu\text{J}$ per data block, which is $1/190$ of DS80C323 and $1/5$ of ARM9. The energy consumption of the ASIC estimate is $1/10$ of the FPGA.

VI. CONCLUSION

This paper presented a compact and energy-efficient hardware design for the 802.15.4 security processing. The design was argued to offer the best architectural area/power/performance ratios for the low-power wireless devices. Compared to typical WPAN processors, the implemented FPGA prototype and the estimated ASIC implementation provide significantly lower energy consumption and higher performance. The same design can also be utilized in WLAN terminals employing the IEEE 802.11i standard.

REFERENCES

- [1] *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPAN)*, IEEE Std. 802.15.4, 2003.
- [2] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements*, IEEE Std. 802.11i, 2004.
- [3] *Advanced Encryption Standard (AES)*, FIPS Std. 197, 2001.
- [4] X. Zhang and K. K. Parhi, "Implementation approaches for the Advanced Encryption Standard algorithm," *IEEE Circuits and Systems Magazine*, vol. 2, no. 4, pp. 24–46, 2002.
- [5] P. Chodowiec and K. Gaj, "Very compact FPGA implementation of the AES algorithm," in *Proc. 5th Int. Workshop Cryptographic Hardware and Embedded Systems (CHES 2003), Cologne, Germany, Sept. 8–10, 2003*, ser. Lecture Notes in Computer Science, C. D. Walter, C. K. Koc, and C. Paar, Eds., vol. 2779. Springer-Verlag, 2003, pp. 319–333.
- [6] C.-P. Su, T.-F. Lin, C.-T. Huang, and C.-W. Wu, "A high-throughput low-cost AES processor," *IEEE Communications Magazine*, vol. 41, no. 12, pp. 86–91, 2003.
- [7] X. Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm," *IEEE Trans. VLSI Systems*, vol. 12, no. 9, pp. 957–967, 2004.
- [8] (2005) Altera website. [Online]. Available: <http://www.altera.com>
- [9] *DS80C320/DS80C323 High-Speed/Low-Power Microcontrollers*, Maxim/Dallas Semiconductors, 2004.
- [10] ARM website. [Online]. Available: <http://www.arm.com>
- [11] J. Daemen and V. Rijmen, "AES proposal: Rijndael," Mar. 1999. [Online]. Available: <http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael-ammended.pdf>
- [12] P. Hämäläinen, J. Heikkinen, M. Hännikäinen, and T. D. Hämäläinen, "Design of transport triggered architecture processors for wireless encryption," in *Proc. 8th Euromicro Conference on Digital System Design (DSD 2005)*, Porto, Portugal, Aug. 30–Sept. 3, 2005, (to appear).
- [13] I. Verbauwede, P. Schaumont, and H. Kuo, "Design and performance testing of a 2.29-GB/s Rijndael processor," *IEEE Journal of Solid-State Circuits*, vol. 38, no. 3, pp. 569–572, 2003.