

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/225215711>

AES Data Encryption in a ZigBee Network: Software or Hardware?

Chapter · December 2009

DOI: 10.1007/978-3-642-17502-2_14 · Source: DBLP

CITATIONS

2

READS

178

5 authors, including:



Geoffrey Ottoy

University of Leuven

13 PUBLICATIONS 37 CITATIONS

SEE PROFILE



Lieven De Strycker

University of Leuven

47 PUBLICATIONS 182 CITATIONS

SEE PROFILE

AES Data Encryption in a ZigBee network: Software or Hardware?

Geoffrey Ottoy

Tom Hamelinckx, Bart Preneel, Lieven De Strycker and Jean-Pierre Goemaere

KaHo Sint-Lieven association K.U.Leuven Belgium
research groups: DraMCo / COSIC

Outline

- About the research groups
- Background information
 - ZigBee
 - Types of WSN
- Motivation
- Test setup
- Results
- Conclusions/future work



About the research groups

- DraMCo research group
KaHo Sint-Lieven (+ 5000 students)
Wireless and Mobile Communication

www.dramco.be

www.kahosl.be

- COSIC research group
K.U. Leuven (35.000 students)
Computer Security and
Industrial Cryptography

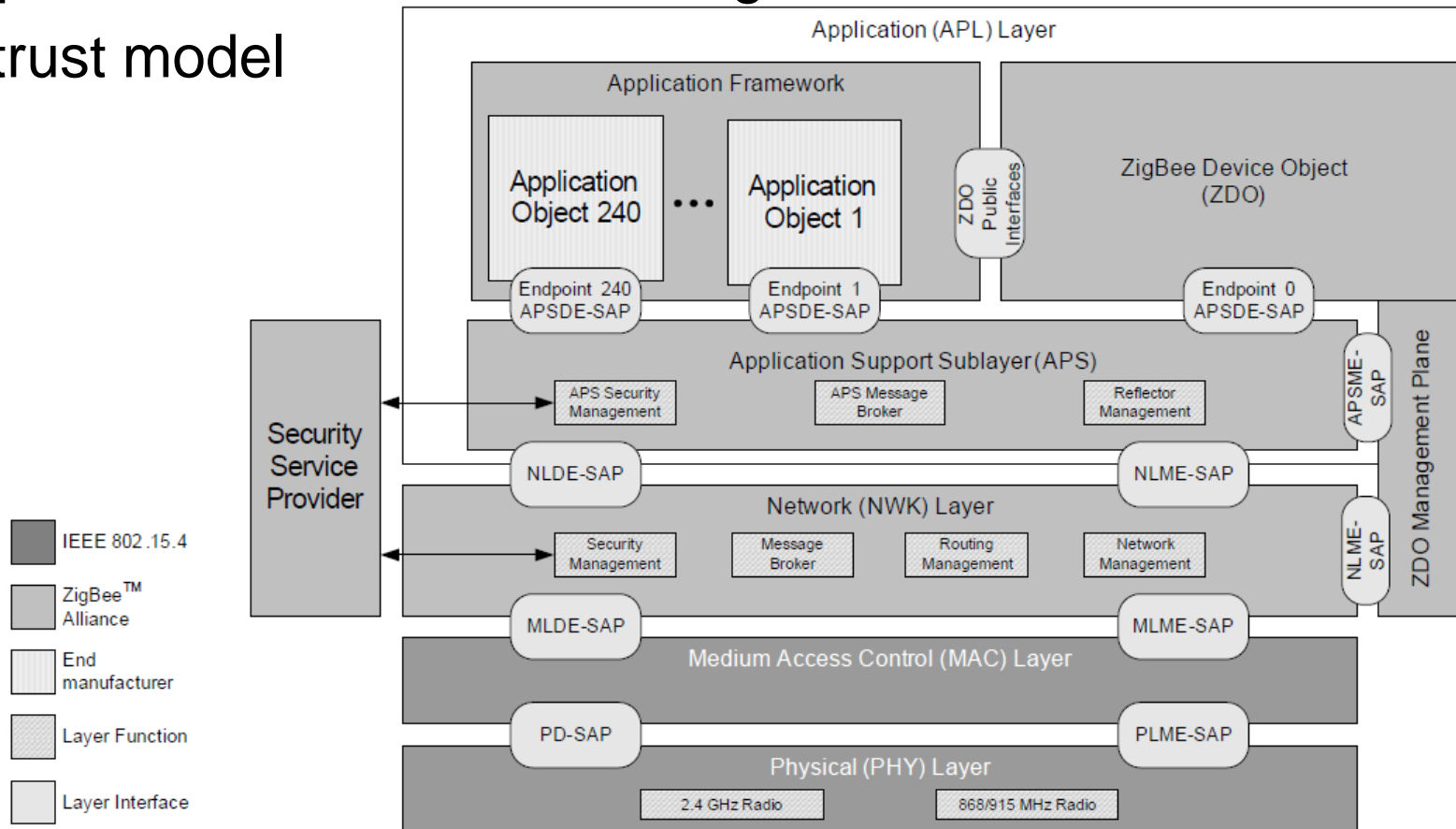
www.esat.kuleuven.be/cosic

www.kuleuven.be



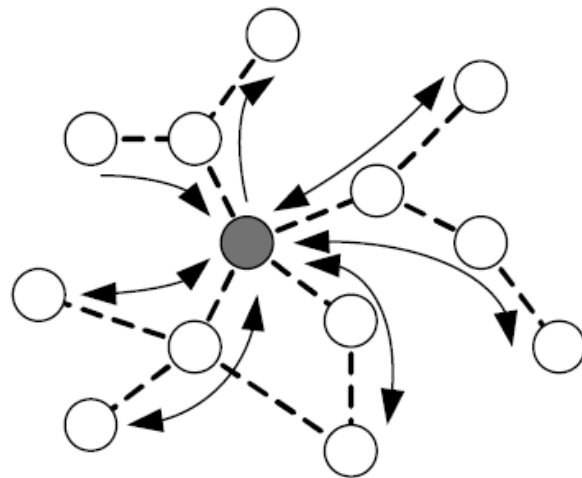
ZigBee

- ZigBee security = key establishment, key transport, frame protection and device management
- Open trust model

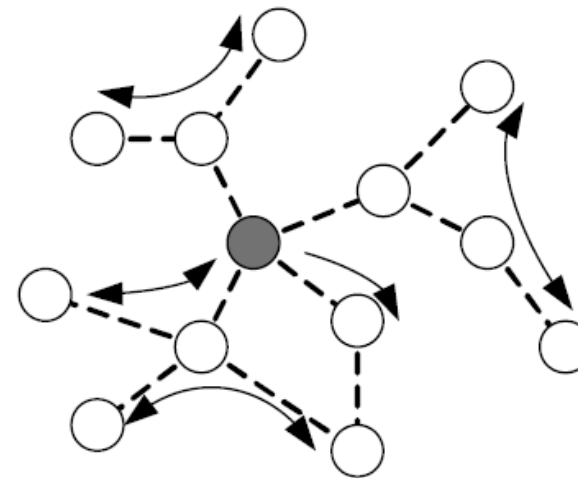


Types of WSN (applications)

- Centralized (e.g. fire detection) versus distributed (e.g. lighting)



— data flow
--- connection

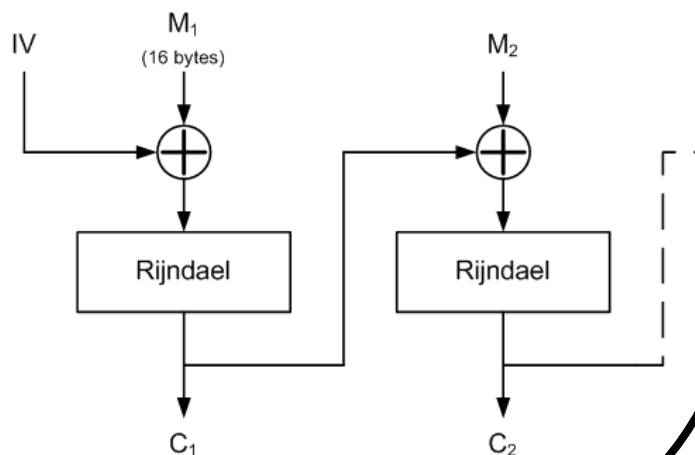


● sink node / network coordinator
○ node

- Combination is possible

What did we investigate and why?

- Properties of WSN (like ZigBee): low-data rate, robust, low-power, unattended operation, low processing power, etc.
- ZigBee: AES 128 (CBC) for data encryption (confidentiality)

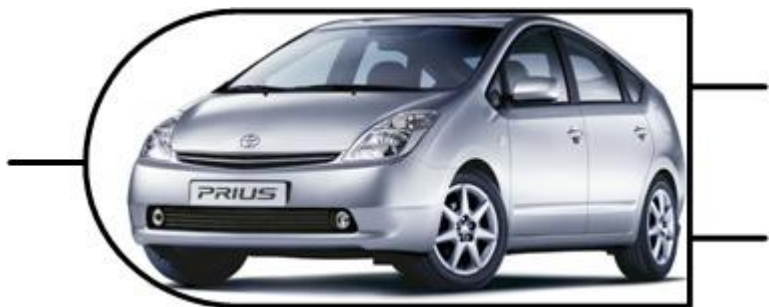


- Algorithm in hardware or software?

Keeping this in mind

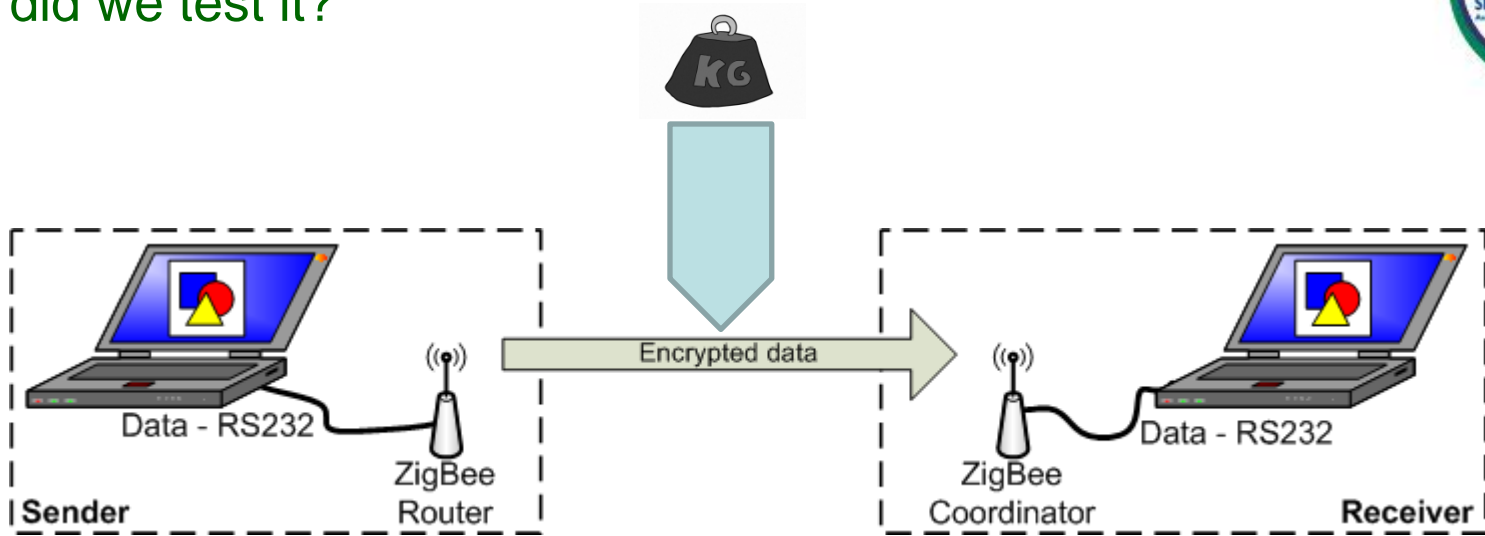
What did we investigate and why?

- Statement: *“Hardware is faster and (thus) more energy-efficient than software.”*

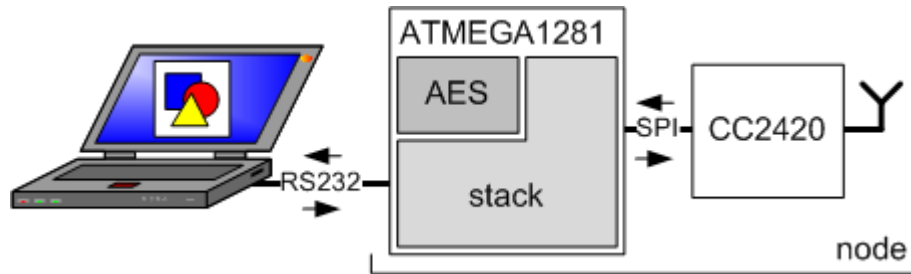
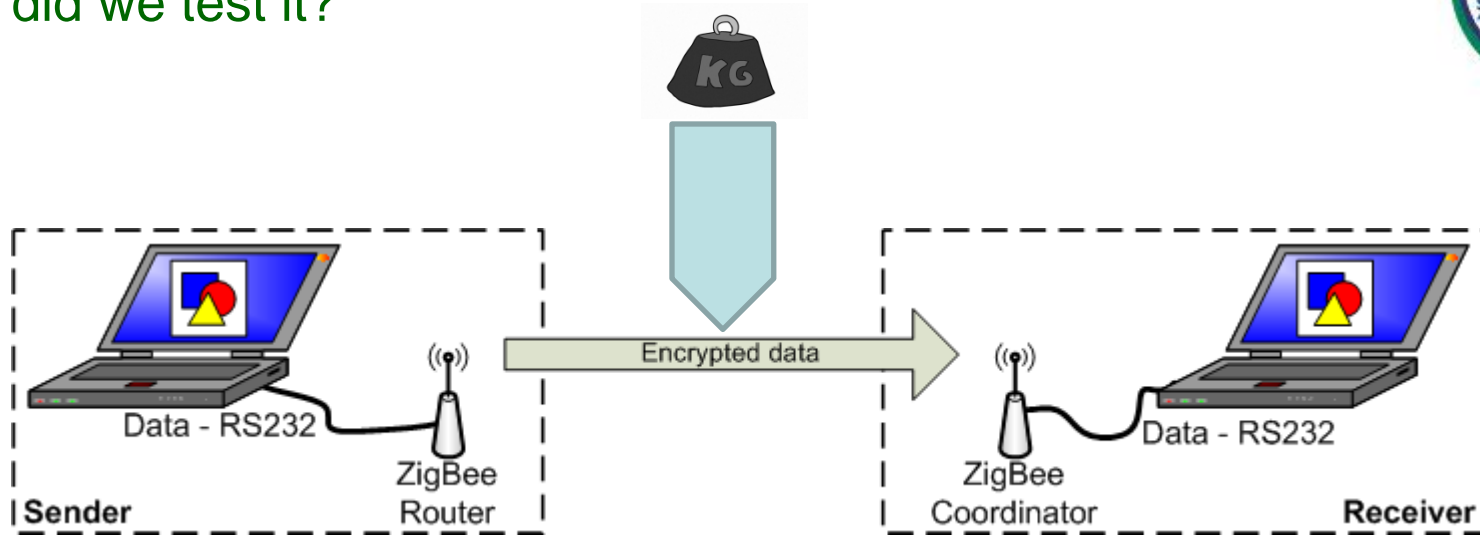


- But will the use of hardware pay off in sensor networks?
⇒ Test both approaches in a worst-case scenario.

How did we test it?

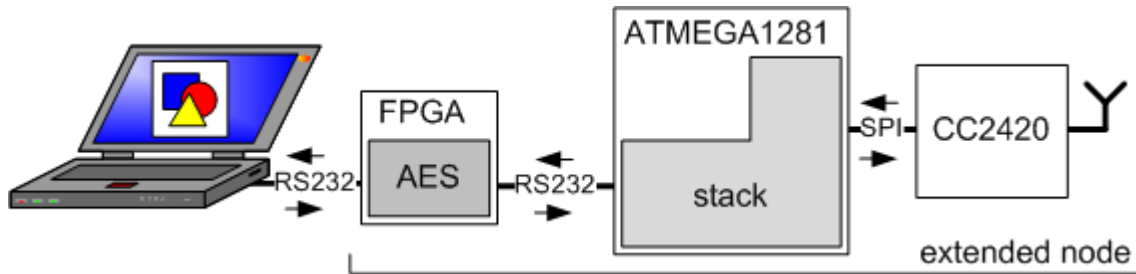
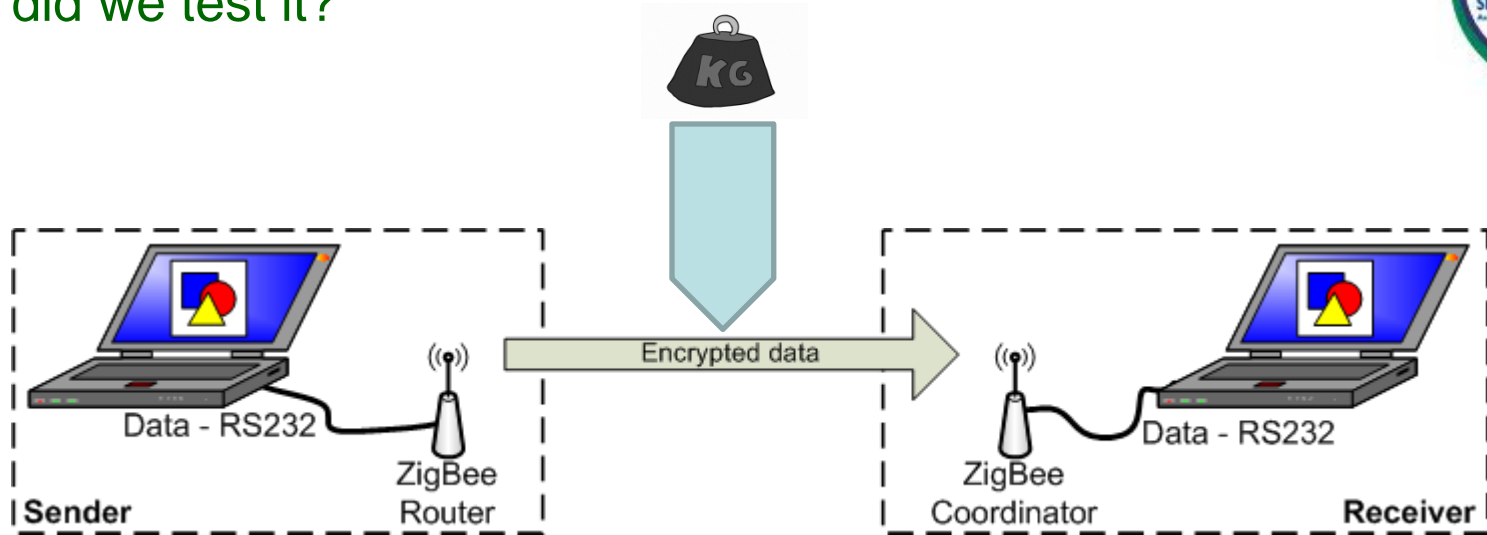


How did we test it?



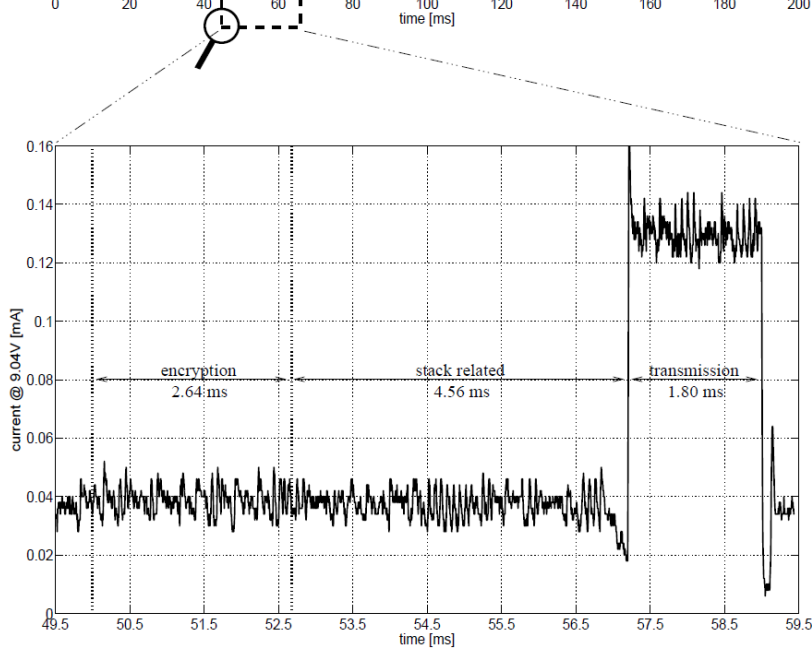
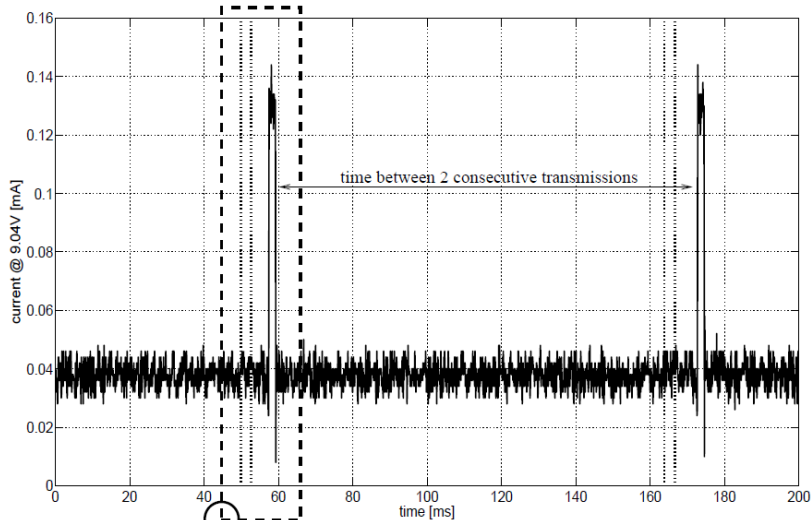
- written in C
- optimized for 8-bit Atmel MCU
- 8 MHz f_{MCU}

How did we test it?



- VHDL
- Optimized for speed
- 1 round/clock cycle

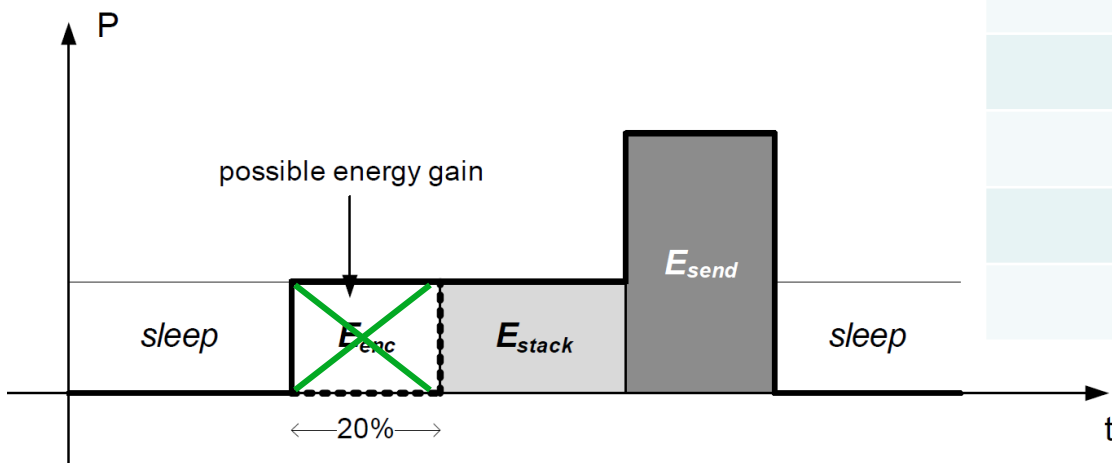
What have we found?



Measurement	Software	Hardware
E_{send}	2.01 mJ	2.01 mJ
E_{recieve}	343 μJ	343 μJ
E_{enc}	782 μJ	0.1 μJ
E_{dec}	949 μJ	< 0.2 μJ
data rate	2.0 kbps	2.1 kbps
E_{tot}	4.0 mJ	3.2 mJ

What can we conclude?

- Energy to send represents a large share of the total energy (TX power !)
- Hardware encryption = 20 % energy gain



Measurement	Software	Hardware
E_{send}	2.01 mJ	2.01 mJ
$E_{recieve}$	343 μ J	343 μ J
E_{enc}	782 μ J	0.1 μ J
E_{dec}	949 μ J	< 0.2 μ J
data rate	2.0 kbps	2.1 kbps
E_{tot}	4.0 mJ	3.2 mJ

Hardware or software?

- Depends on the application and network
- Transmission power \uparrow relative share of encryption energy \downarrow
- No influence on the data rate
- Implementing AES in software is feasible, but ...

What about the future?

- Dedicated co-processor (ZC, storage and management)
- Large network with different types of nodes

Questions?

Thank you for your attention

References

1. ZigBee Alliance: ZigBee Specification – Document 053474r17. (2007)
2. A. Menezes, P. van Oorschot, S. Vanstone: Handbook of Applied Cryptography. CRC Press, ISBN: 0-8493-8523-7, p.230 (1996)
3. T. Zia, A. Zomaya: An Analysis of Programming and Simulations in Sensor Networks. School of Information Technologies, University of Sydney (2006)
4. M. Mathews, M. Song, S. Shetty, R. McKenzie: Detecting Compromised Nodes in Wireless Sensor Networks. Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (2007)
5. J.P. Kaps: Cryptography for Ultra-Low Power Devices. A Dissertation Submitted to the Faculty of the Worcester Polytechnic Institute (2006)
6. J. Daemen, V. Rijmen: The Design of Rijndael: AES - The Advanced Encryption Standard, Springer, 2002.
7. Federal Information Processing Standards Publication 197: Specification for the Advanced Encryption Standard (AES). (November 2001).
8. E. Shi, A. Perrig: Designing Secure Sensor Networks. In: IEEE Wireless Communications, pp 38–43 (December 2004)
9. G. Gaubatz, J.P. Kaps, E. Öztürk, B. Sunar: State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks. Cryptography Information Security Lab, Worcester Polytechnic, Institute (2005)
10. A. Hodjat, I. Verbauwhede: Area-Throughput Trade-Offs for Fully Pipelined 30 to 70 Gbits/s AES Processors. IEEE Trans. Computers 55(4) pp 366–372 (2006)
11. S.J. Park: Analysis of AES Hardware Implementations. Department of Electrical and Computer Engineering, Oregon State University (2003)
12. S. Mangard, M. Aigner, S. Dominikus: A highly regular and scalable AES hardware architecture. In: IEEE Transactions on Computers, vol. 52–4, pp. 483–491 (April 2003)
13. A. Gielata, P. Russek, K. Wiatr: AES hardware implementation in FPGA for algorithm acceleration purpose. Proceedings of the International Conference on Signals and Electronic Systems, ICSES'08, pp. 137–140 (2008)
14. ZigBee Alliance, <http://www.zigbee.org>
15. IEEE Computer Society, IEEE Std 802.15.4-2006 (2006)
16. J. Sun, X. Zhang: Study of ZigBee Wireless Mesh Networks. Hybrid Intelligent Systems, International Conference on, IEEE Computer Society, pp 264–267 (2009)
17. V. Rijmen, N. Pramstaller: Cryptographic Algorithms in Constrained Environments (Chapter 6). In: Wireless Security and Cryptography, Edited by N. Skalvos, X. Zhang, CRC Press, ISBN: 978-0-8493-8771-5, pp. 186–195 (2007)
18. AES Lounge, <http://www.iaik.tugraz.at/content/research/krypto/AES/IAIK> - TU Graz.
19. Atmel: ATmega640/1280/1281/2560/2561 [Datasheet] (2005)
20. Chipcon: CC2420 ZigBee-Ready Transceiver [Datasheet] (2003)