Journée Systèmes Embarqués et Objets Communicants

Internet of Things security overview

From communication to sensor

Cédric Marchand

cedric.marchand@ec-lyon.fr

04/01/2019

Agenda

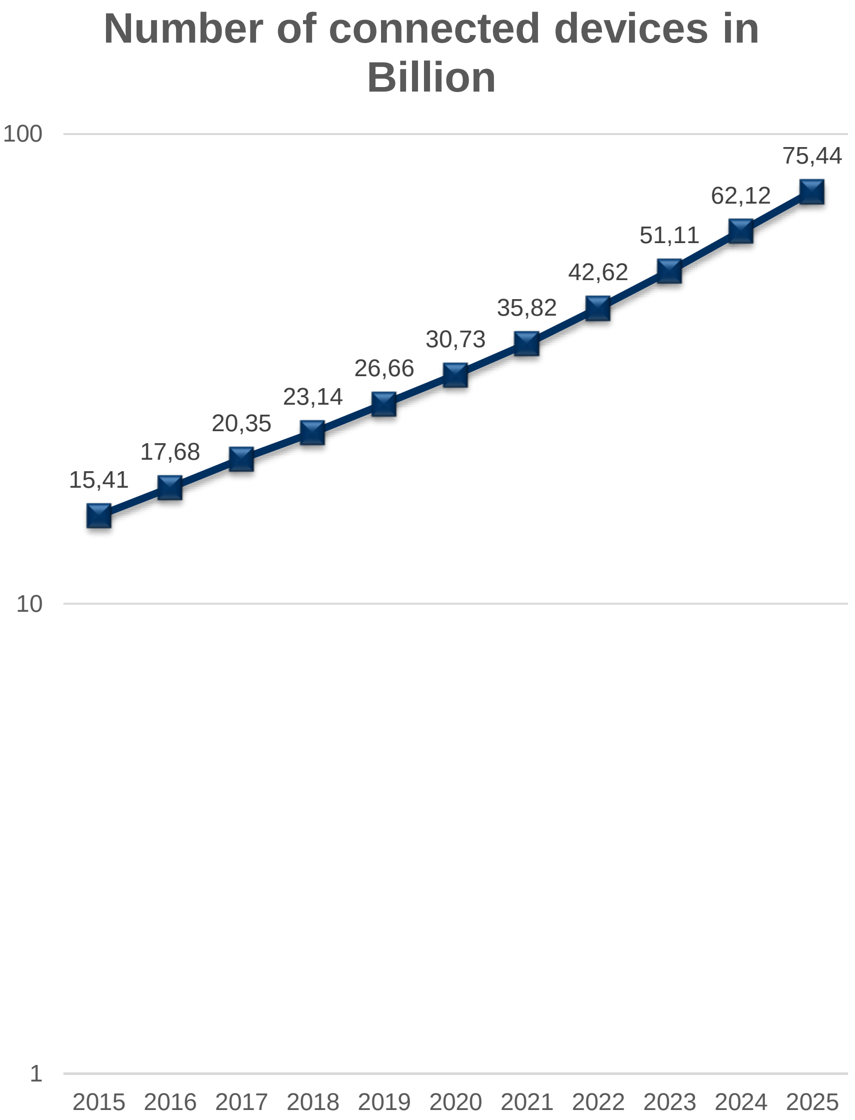
1. Introduction

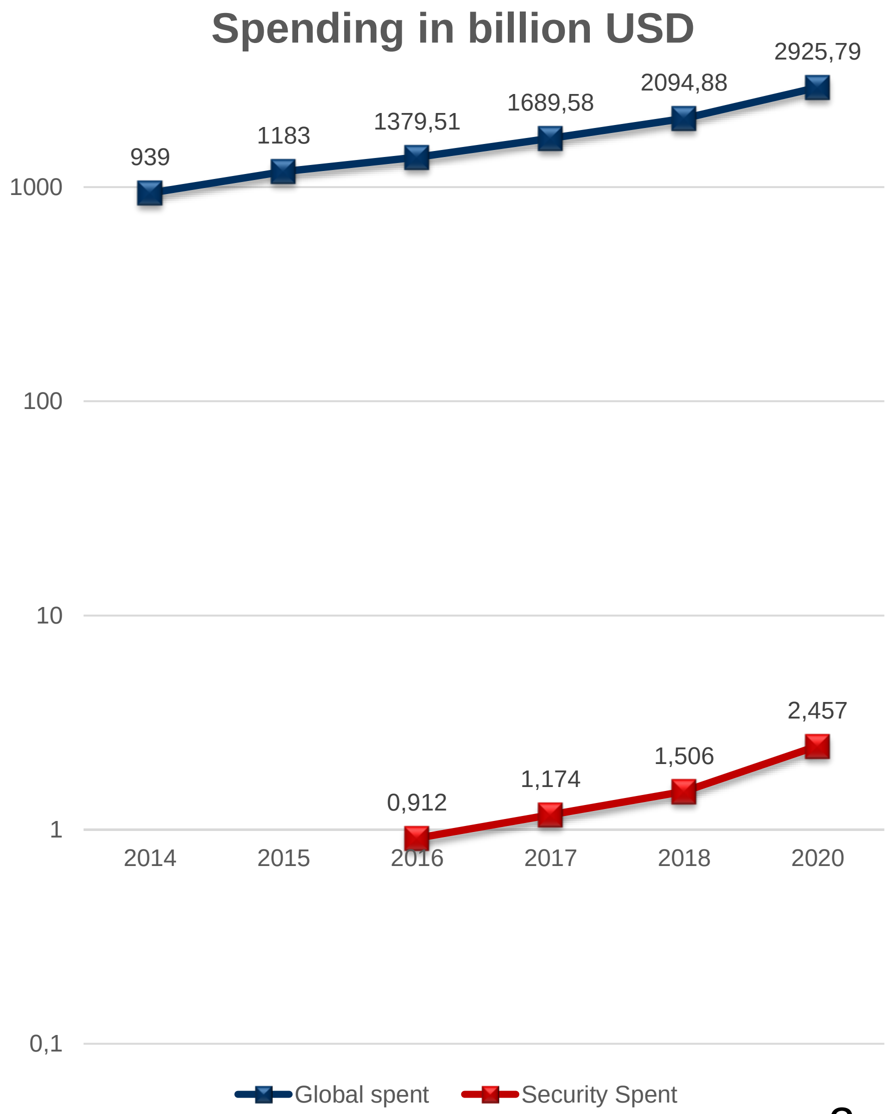
2. Communication network security

3. Sensor nodes security

4. Conclusion

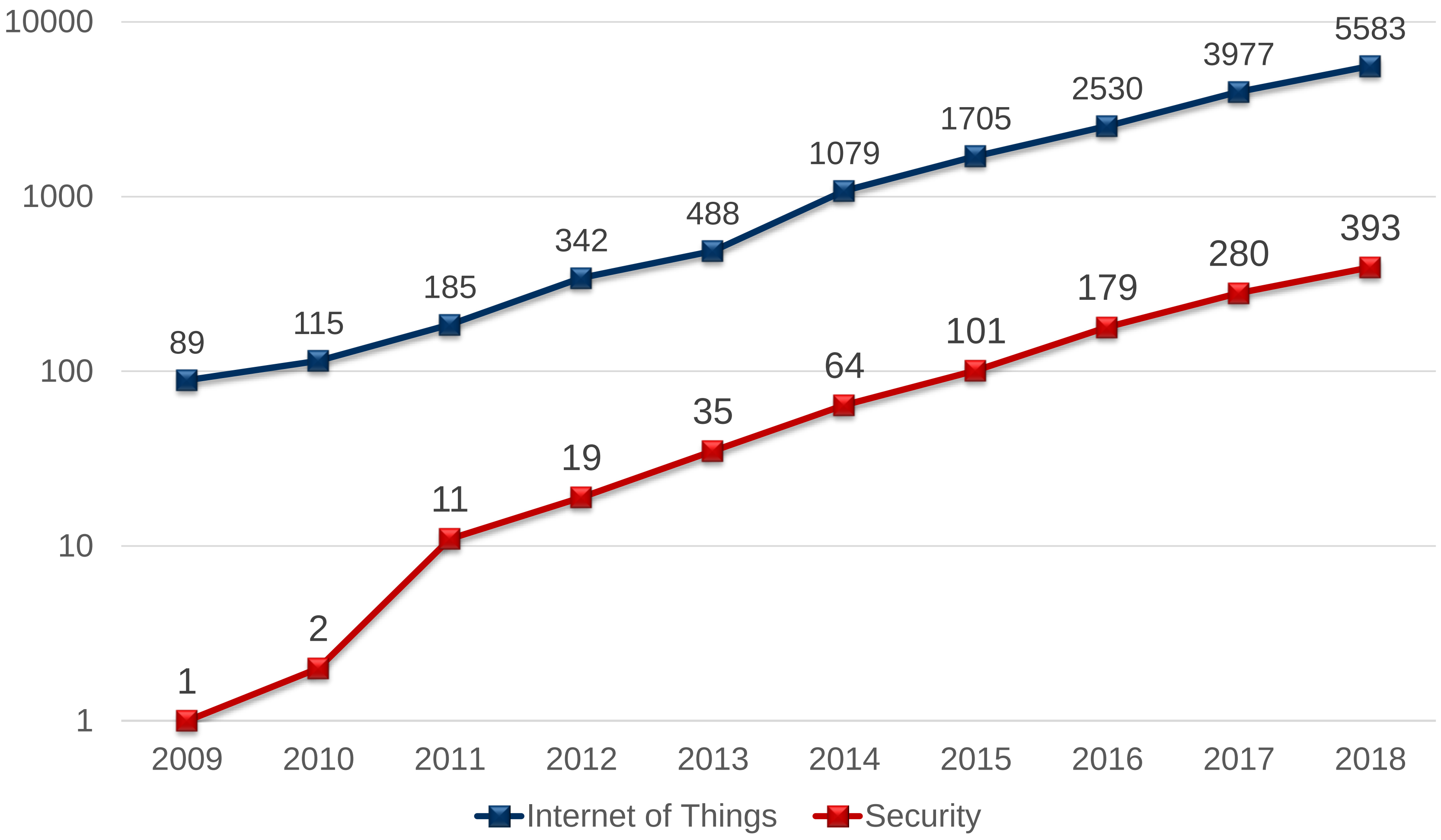
Introduction: Global market Statistics





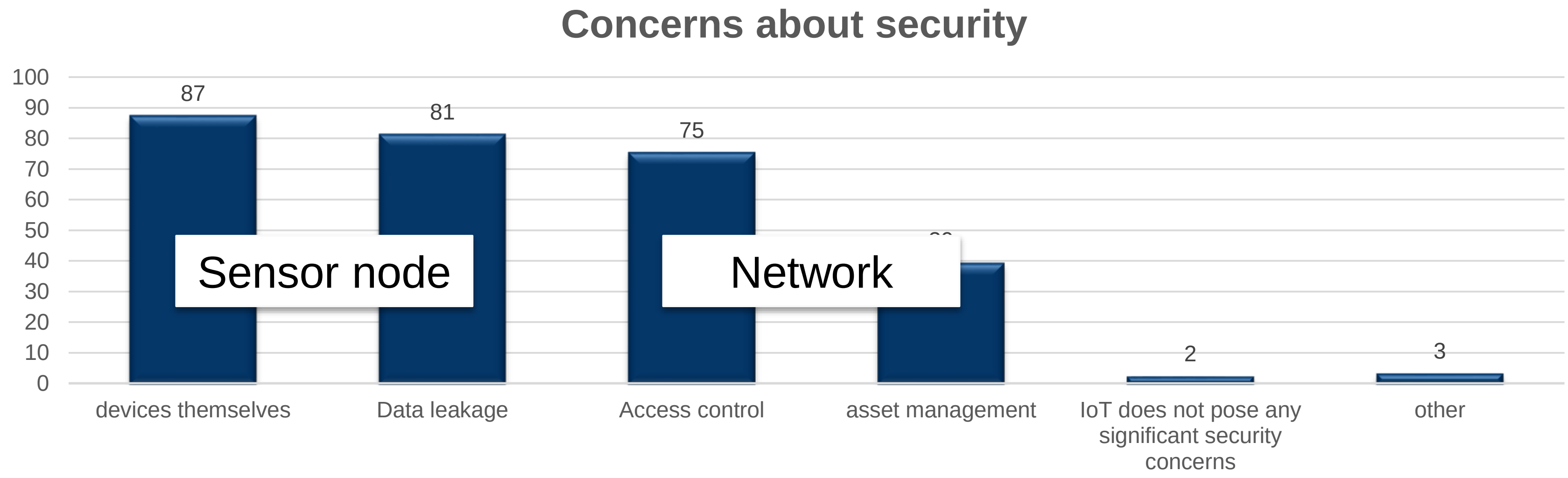
Source : Statista

Introduction: Scientific production since 2009



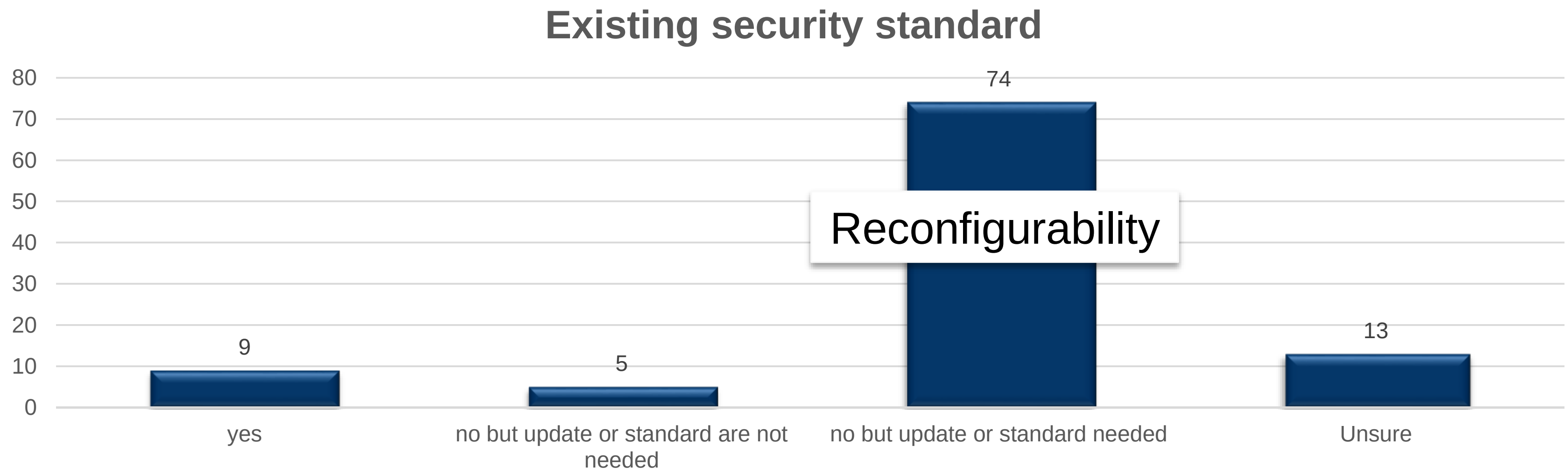
Source : DBLP

Introduction: Security concerns surveys


Concerns about security

Sensor node

Network


Existing security standard

Reconfigurability

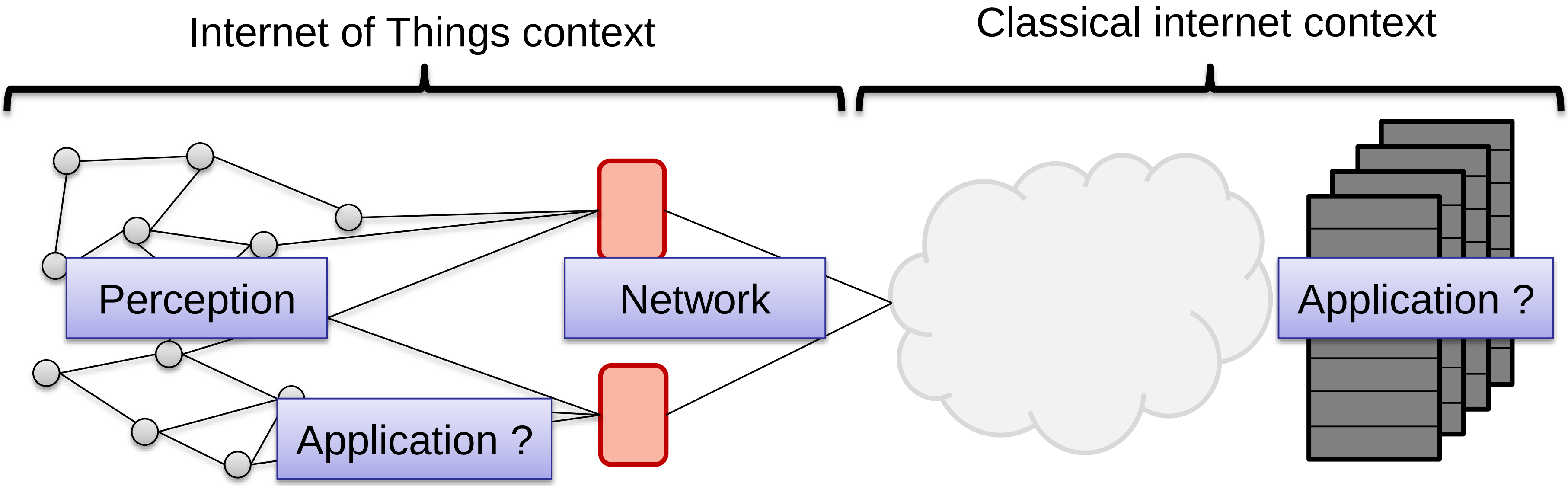
Source : Statista

Introduction: A lot of surveys from 2008 to 2015

- 2008 [1]:
  - Computation power and energy limitations
  - No dedicated cryptographic standard
  - Key management and routing tricks to enhance robustness
- 2011 [2]:
  - Propose to combine software and hardware to enhance IoT security
  - No concrete solutions provided
- 2013 [3]:
  - Present risks and challenges
  - Propose a three layers description for IoT (perception, network and application
- 2015 [4]:
  - Conclusion: proposed solutions are too complex and too expensive to be really integrated in the IoT context.

Introduction: Difficulty to include security in IoT

- Various context to secure with various constraints



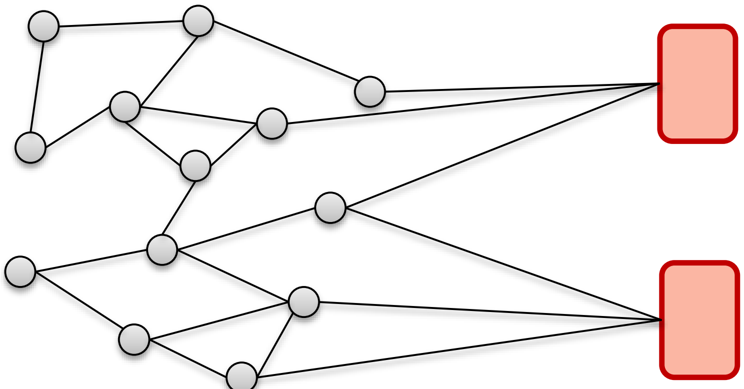
- Recent
- Security has to take into account:
  - Communications
  - Software
  - Hardware

- Long history
- Security features exist and are part of standards
- Regular update applied
- Attack vs countermeasure game

Communication protocols for IoT

- 802.15.4 [5]:
  - Basic protocol standard
  - Proposes security with different AES mode of operations
- ZigBee [6]:
  - Add Network and Application security layers using AES
- LoraWan [7]:
  - 2 keys (NwkSkey, AppSkey) used to derive a keystream
  - 2 activation methods (ABP, OTAA)
- MQTT [8]:
  - Proposes security through MQTTS
  - Lack of authentication
  - Lack of user partitionning

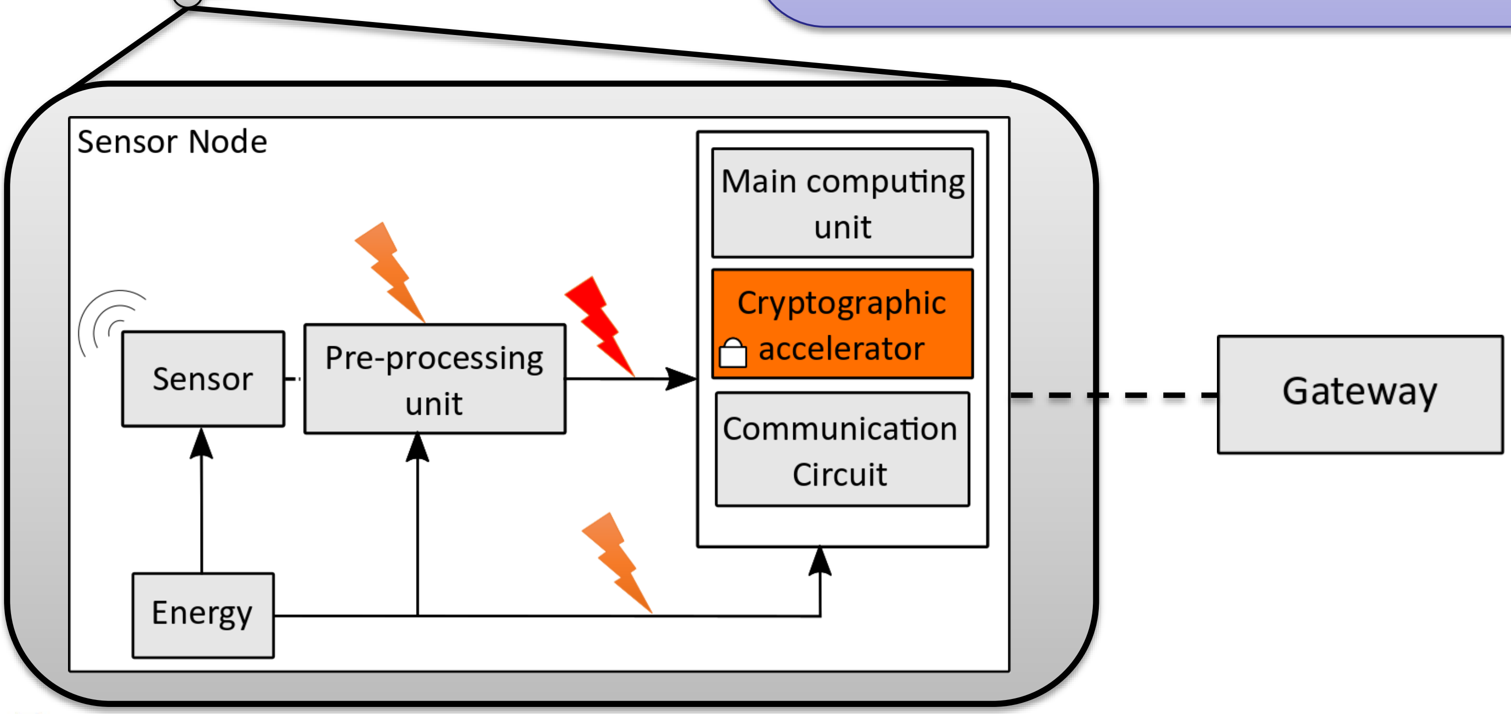
Sensor node security



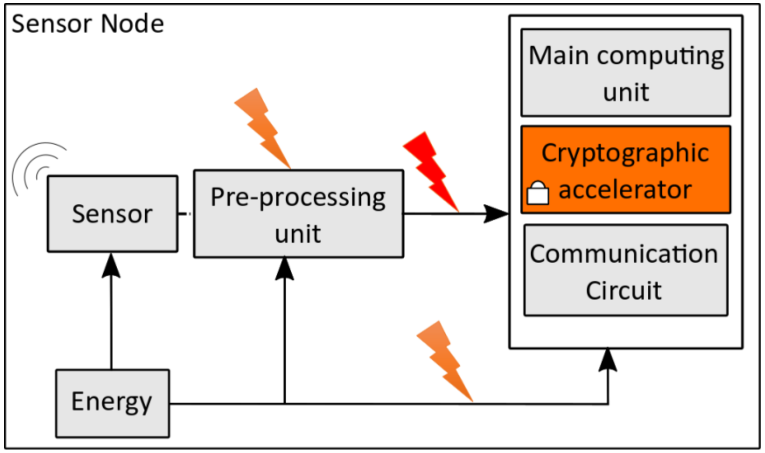
Secure communication possible thanks to dedicated protocols

BUT

A large vulnerable space still exist



Sensor node security



- A lot of surveys since 2008
- Specific constraints in term of area and energy consumption [9]:
  - 4000 GE for encryption circuit
  - 10µW per encryption

- Implement security inside the main computing unit:
  - Software → Increase execution time (energy consumption)
    → Lead to possible cache attacks [10]
  - Hardware → Increase area (26%) and energy consumption (18%) [11]
    → Without countermeasure, wide range of possible attacks (SCA, fault injection, …)

It is required to protect collected data as close as possible to the sensor

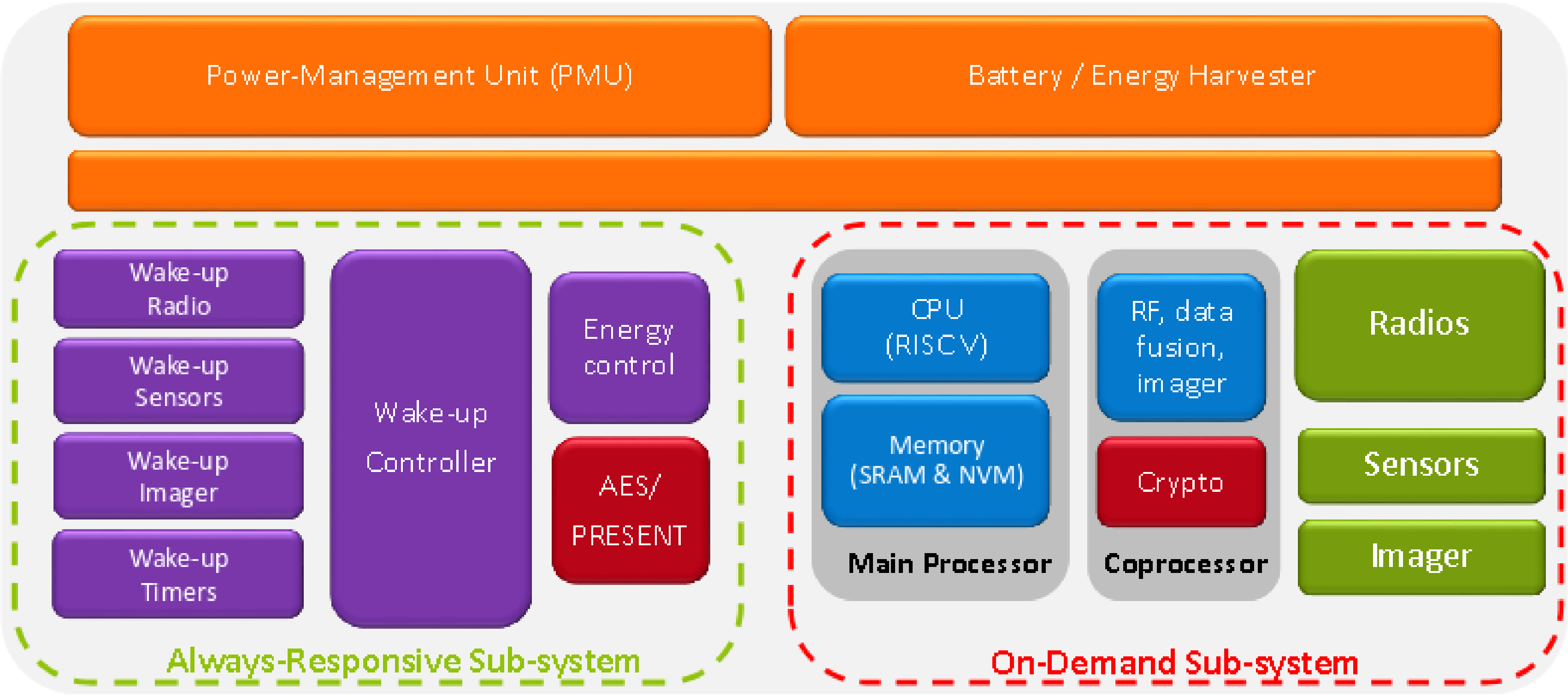
Sensor node security

- To decrease the cost of security in this IoT context:
  - Lightweight cryptography ? (Trivium [12], Present, Klein, …)
  - Change Computation paragidm ? (Near Sensor processing [13-14], In memory computing [15])
- A new NIST competition has been launch in 2018 to find the new lightweight standard[1]

[1] https://www.nist.gov/news-events/news/2018/04/nist-issues-first-call-lightweight-cryptography-protect-small-electronics

Sensor node security

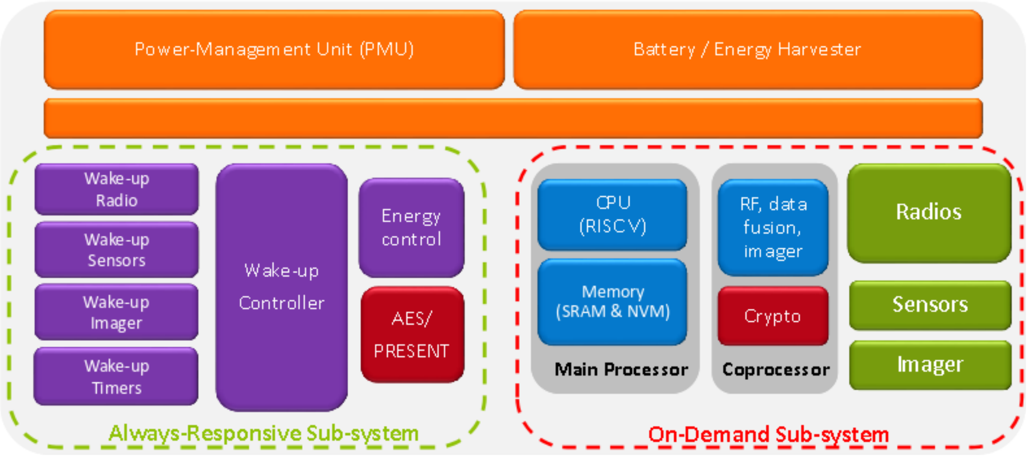
- L-IoT platform[1]

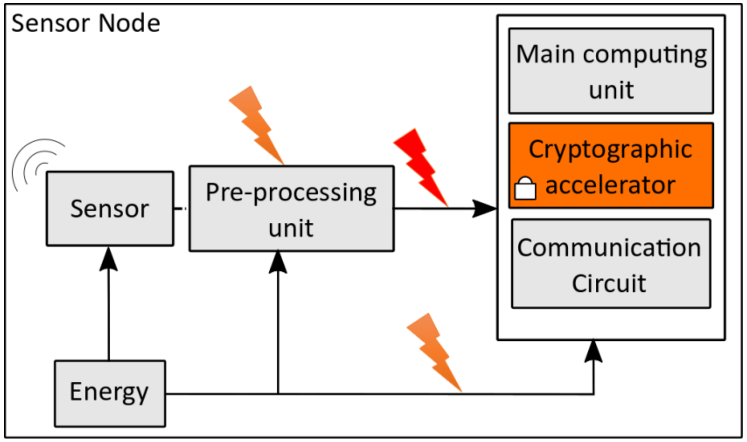


- High energy efficiency thanks to wake up possibilities
- 2 cryptographic cores implemented in Hardware

[1] http://damien.courousse.fr/pdf/DAC2017-LIOT-IPtrack.pdf

Sensor node security





Energy Consumption	+ + +	- - -
Area overhead	- -	- -
Security capability	+ +	+
Reconfigurability of security features	- - -	- - -

Conclusion

Secure commnication protocol fo IoT:

- Various standard protocols (802.15.4, Zigbee, Lora, MQTT)
- Each one proposes security recommandations

- Security depends on the implementation and uses of these protocols

Sensor node security:

- Currently implemented in the communication or main computing unit
  - Lead to high energy consumption
  - Lead to area overhead to acheive good robustness (hardware accelerator)

- The trend is to bring security closer to the sensor
  - Near sensor processing unit
  - New computation paradigm (in Memory for exemple)
  - Wake up capabilities → lead to lower energy consumption

Thank you for your attention

References

[1] MARTINS, David et GUYENNET, Herve. Etat de l'art-Sécurité dans les réseaux de capteurs sans fil. In : SAR-SSI 2008: 3rd conference on Security of Network Architectures and Information Systems. 2008.

[2] BABAR, Sachin, STANGO, Antonietta, PRASAD, Neeli, et al. Proposed embedded security framework for internet of things (iot). In : 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE). IEEE, 2011.

[3] ZHAO, Kai et GE, Lina. A survey on the internet of things security. In : 2013 Ninth international conference on computational intelligence and security. IEEE, 2013.

[4] SADEGHI, Ahmad-Reza, WACHSMANN, Christian, et WAIDNER, Michael. Security and privacy challenges in industrial internet of things. In : 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC). IEEE, 2015.

[5] SALEEM, Shahnaz, ULLAH, Sana, et KWAK, Kyung Sup. A study of IEEE 802.15. 4 security framework for wireless body area networks. *Sensors*, 2011, vol. 11.

[6] VIDGREN, Niko, HAATAJA, Keijo, PATINO-ANDRES, Jose Luis, et al. Security threats in zigbee-enabled systems: Vulnerability evaluation, practical experiments, countermeasures, and lessons learned. Hawaii International Conference on System Sciences. IEEE, 2013.

[7] Roy, S. Étude du chiffrement dans un réseaux IoT: le cas de LoraWan, MISC Hors Série n° 15

[8] Lifchitz, R. MQTT : Le protocol qui distribuevos données personelles à tous ?, MISC Hors Série n° 15

References

[9] Armknecht, F., Hamann, M., & Mikhalev, V. Lightweight authentication protocols on ultra-constrained RFIDs-myths and facts. In International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer, (2015)

[10] SEPULVEDA, Johanna, ZANKL, Andreas, et MISCHKE, Oliver. Cache attacks and countermeasures for NTRUEncrypt on MPSoCs: Post-quantum resistance for the IoT. IEEE International System-on-Chip Conference (SOCC). IEEE, 2017

[11] A. Singh, N. Chawla, J. H. Ko, M. Kar and S. Mukhopadhyay, "Energy Efficient and Side-Channel Secure Cryptographic Hardware for IoT-edge Nodes," in IEEE Internet of Things Journal

[12] MORA-GUTIÉRREZ, J. M., JIMÉNEZ-FERNÁNDEZ, C. J., et VALENCIA-BARRERO, M. Multiradix Trivium Implementations for Low-Power IoT Hardware. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017.

[13] DAS, Satyajit, MARTIN, Kevin JM, ROSSI, Davide, et al. An Energy-Efficient Integrated Programmable Array Accelerator and Compilation flow for Near-Sensor Ultra-low Power Processing. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018.

[14] CONTI, Francesco, SCHILLING, Robert, SCHIAVONE, Pasquale Davide, et al. An IoT endpoint system-on-chip for secure and energy-efficient near-sensor analytics. IEEE Transactions on Circuits and Systems I: Regular Papers, 2017.

[15] ZHANG, Yiqun, XU, Li, YANG, Kaiyuan, et al. Recryptor: A reconfigurable in-memory cryptographic Cortex-M0 processor for IoT. In : 2017 Symposium on VLSI Circuits. IEEE, 2017.