Internet of things security: review from communication to sensor

Cédric Marchand
Université de Lyon, ECL, INSA Lyon, UCBL, CPE
INL, UMR5270
F-69134, Ecully, France
cedric.marchand@ec-lyon.fr

The Internet of Things (IoT) is today a well-known ecosystem, continuously growing at an impressive speed (from about 500 million connected things in 2016 to more than 6.5 billion in 2018), where small and smart objects interact through communicating networks. At this rate, there will be 6 times more connected things than human on earth by 2025. Consequently, the amount of collected and transmitted data is becoming enormous and depending on the application, these data will be sensitive and require protection. However, it is important to remember that the very first constraint in the IoT context is the energy consumption of the devices. Thus, it is a great challenge to combine security and energy consumption in this context.

Concerning security, an effort has been done to identify risks and challenges resulting from a lack of security but also in order enhance the security of communication protocols used in the IoT. Another solution is to add security features externally using either hardware accelerators or hardware secure elements to encrypt collected data just before the communication. However, these solutions require important area and power consumption overhead. Thus, it is necessary to find new ultra-lightweight solutions that make it possible to bring the security as close as possible to sensor in order to enhance the security in the IoT context.

In this presentation, we will first present some statistic and public concern about IoT security. Then, we will review security solutions proposed to increase IoT security from communication to sensor. Finally, we will discuss about non-volatile computing perspectives to bring security at the sensor closest possible point and how this will enhance the security of sensor node in the IoT context.