Lightweight Security Protocols for IP-based Wireless Sensor Networks and the Internet of Things

Mots clés :

● Directeur de thèse : Maryline Laurent
● Co-encadrant(s) :
● Unité de recherche : Services répartis Architectures MOdélisation Validation Administration des Réseaux
● Ecole doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
● Domaine scientifique principal: Divers

Résumé du projet de recherche (Langue 1)

Wireless sensor networks (WSNs) are increasingly used in several industrial domains, such as industrial process monitoring and control, e-health monitoring, and smart grid. Such networks are composed of resource-limited devices equipped with radio communication units and sensing/actuating capability. Conversely, their resource limitations (e.g. in terms of energy, processing power, memory) and the lack of communication reliability make it challenging to use existing cryptographic techniques and common standard protocols for their security. With the aim to reinforce the trend of future networks toward all-IP, the focus of thesis efforts will be to adapt legacy security standards (e.g., EAP, TLS, IPsec) to run in WSNs, and to extend standardized solutions proposed for IP constrained environments (e.g., RPL, CoAP) with security features. Considered security services in WSNs will cover multiple layers: hop-by-hop frame protection, as well as network authentication and access control, and end-to-end data security. In order to evaluate and validate the design, security, and performance of the proposed solutions, a testing framework will be devised to examine the behavior of the secure WSN under realistic attacks.

Résumé du projet de recherche (Langue 2)

Resource-efficiency, Scalability, Autonomy of sensors, Heterogeneity, End-to-end IP connectivity, Intermittent connectivity and mobility of sensors