Encadrants : Nicolas Stouls et Lionel Morel

Contact : nicolas.stouls@insa-lyon.fr

Titre : extraction d'informations concernant la consommation d'énergie des protocoles cryptographique

Contexte : Les réseaux de capteurs sont des réseaux ayant de très fortes contraintes aussi bien au niveau de la consommation d'énergie, que de la sécurité des informations transmises ou que de la minimalité des espaces mémoire. Chaque noeud du réseau embarque principalement 4 composants : (1) un capteur (qui va varier en fonction du cas d'utilisation du réseau), (2) un composant de gestion des communications, (3) un service d'agrégation des données et (4) un service de cryptographie (chiffrement / déchiffrement / authentification). Dans une approche de développement de capteurs répondant à des contraintes de qualité de service, nous nous intéressons à l'évaluation de la consommation des différentes parties logicielles d'un capteur, y compris de son protocole cryptographique. L'objectif final est de proposer une méthode de développement top-down qui favoriserait la validation, par raffinement, du logiciel réalisé par assemblage de blocs existants.

Problématique : L'objectif de ce sujet est de proposer une ou plusieurs méthodes dévaluation de la consommation d'énergie d'un protocole cryptographique dans un capteur. Il existe différentes approches probabilistes permettant d'évaluer le WCET (Worst case execution time) d'un logiciel. En se basant sur les résultats existants, nous voulons identifier les critères principaux influant sur le coût énergétique d'un protocole cryptographique et intégrer ces résultats dans un langage de description de composants. Il serait intéressant d'exploiter comme outil intermédiaire l'outil Frama-C. Ce dernier permet la manipulation de code C annoté et notamment sa vérification.

Résultats attendus : (1) Proposition théorique de méthodes d'extraction d'informations concernant la consommation énergétique de protocoles de cryptographie (2) Proposition d'un langage de description basé sur les besoins mis en évidence (3) Réalisation d'un plugin Frama-C mettant en oeuvre au moins une partie des heuristiques proposées.