Titre : Sécurité des communications orientée couche physique

Mot-clés : réseaux de capteurs sans-fil, sécurité, radio-communications

Organisme d'acceuil : LaBRI

Encadrants : Stéphane Delbruel (stephane.delbruel@labri.fr), Joachim Bruneaux-Queyreix (joachim.bruneau-queyreix@u-bordeaux.fr)

Contexte : L'usage d'objets communicants sans-fil est devenu inséparable de notre quotidien. L'accroissement continu du nombre d'appareils partageant de l'information dans le cadre de l'Internet des objets a été fortement porté par la multiplication des réseaux capteurs, que ce soit dans le cadre des villes connectées, des usines intelligentes ou des établissements de santé intelligents. Ces petits objets pervasifs et hétérogènes dans leurs tâches sont destinés à être déployés pour accomplir soit la remontée d'information relatives à l'environnement soit une action physique précise.

Un grand pan de recherche concerne la sécurité des communications relatives à ces objets, et beaucoup d'efforts ont été faits pour étendre les principes d'authentification des équipements et de chiffrement des échanges à ces objets en particulier. Cependant, les performances réduites et l'exigence d'une consommation électrique restreinte ont montrés les limites de la transposition des outils de sécurité standards vers ces objets embarqués connectés.

Le développement d'une approche de la sécurité qui se base sur la couche physique et non plus sur la couche applicative est très prometteuse pour vaincre les limitations inhérentes à ce domaine et apporte avec elle son lot de solutions, permettant une consommation énergétique réduite, l'indépendance vis-à-vis d'une infrastructure et une approche indépendante des capacités de calcul. Pour cela, elle se base sur des principes physiques des communications radio – à savoir les informations propres à un canal de communication entre deux objets et le principe de réciprocité d'un canal – pour favoriser l'émergence de techniques nouvelles pour authentifier un émetteur, établir une clé secrète partagée ou dégrader la capacité d'un observateur à intercepter du trafic. L'authentification d'un objet communiquant via cette nouvelle approche éveille un très grand intérêt et de premiers efforts ont été fait pour appliquer ces solutions à l'Internet des objets et notamment pour des technologies basse-consommation et longue distance. Cependant, l'implémentation de ces solutions dans les réseaux de capteurs sans-fil connaît des manquements dans le passage de la théorie à la pratique, manquements auxquels nous allons nous intéresser.

L'objectif de ce stage sera d'analyser les limitations de l'authentification via la couche physique pour ensuite proposer des solutions pour l'application de ces concepts dans les réseaux de communication sans-fil basse consommation et longue distance.

Pour cela, cet objectif sera décomposé en deux axes de travail :

- Analyser la faisabilité et les limitations de l'authentification par couche physique dans des environnements limités en énergie.

- Étendre cette solution d'authentification au-delà de son schéma point à point vers une authentification collaborative impliquant différents nœuds du réseau.