DRT : Sujet de thèse SL-DRT-19-0515

DOMAINE DE RECHERCHE

Electronique et microélectronique - Optoélectronique / Sciences pour l'ingénieur

INTITULÉ DU SUJET

Renforcement de la sécurité inter-couches des protocoles de communication sans fil véhiculaires

RÉSUMÉ DU SUJET

La connectivité véhiculaire sans fil (ou V2X pour Vehicle to Everything) apparaît aujourd'hui comme un ingrédient essentiel des futurs systèmes de transport intelligents connectés (C-ITS) (ex. véhicule autonome, sécurité des usagers vulnérables de la route, coordination de flotte, cartographie et Internet des Objets véhiculaire…). A titre d'exemple, on pourra citer la technologie ITS-G5, qui repose sur le standard radio IEEE 802.11p à 5.9 GHz, ou encore la technologie C-V2X/LTE-V, qui se présente comme une adaptation de solutions cellulaires 4G au contexte véhiculaire (standard en cours de définition). Mais les modes de transmission V2X envisagés reposent le plus souvent sur une diffusion indifférenciée d'information (c.-à-d., destinée à toucher le plus grand nombre de véhicules alentours) et se trouvent ainsi naturellement exposées (ex. avec des canaux fréquentiels de contrôle fixes et connus publiquement). Aussi, de nombreux types d'attaque sont aujourd'hui envisagés, allant jusqu'au déni de service (ex. brouillage, injection/interception de messages, usurpation d'identité…).

Jusqu'à présent, les méthodes de sécurisation mises en avant dans ce contexte s'appuient pour l'essentiel sur des approches conventionnelles à base de cryptographie (c.-à-d., utilisant des clés, des pseudonymes, des signatures non-spécifiques). D'une part, les fonctions et paramètres de base (i.e., primitives, graines, algorithmes…), qui sont sélectionnées de manière statique, peuvent s'avérer mal dimensionnées en fonction du contexte d'usage. D'autre part, le surcoût cryptographique engendré (en termes de complexité calculatoire et d'accès au réseau cœur) est de nature à dégrader fortement la latence -pourtant critique- des systèmes véhiculaires à protéger, ce qui peut s'avérer rédhibitoire pour certaines applications.

Dans le cadre de cette thèse, on se propose donc de définir de nouveaux mécanismes de sécurité tirant conjointement profit des différentes couches du protocole radio V2X et du contexte applicatif véhiculaire (ex. « furtivité » de l'allocation de ressources radio et/ou ordonnancement pseudo-aléatoire de l'accès, pseudo-périodicité des messages par le biais de modèles de trafic réduisant la prédictibilité des paquets over-the-air, évaluation de la confiance des tiers via un contrôle de la cohérence/conformité d'informations applicatives échangées...), tout en complétant/renforçant les schémas sécuritaires actuels. L'étude comprendra une première phase d'analyse du risque au regard des spécifications V2X actuelles. Certaines des méthodes proposées pour contrecarrer les attaques les plus critiques seront évaluées à partir de simulations et de données expérimentales.

FORMATION NIVEAU MASTER RECOMMANDÉ

Master 2 Recherche (Systèmes et protocoles de communication sans fil, Télécoms, Cyber sécurité...)

INFORMATIONS PRATIQUES

Département Systèmes
Service Technologigies Sans Fils
Laboratoire Communication des Objets Intelligents

Centre : Grenoble

Date souhaitée pour le début de la thèse : 01/10/2019

PERSONNE À CONTACTER PAR LE CANDIDAT

Benoît DENIS
CEA
DRT/DSIS/STSF/LCOI
CEA-Leti Minatec
Bât. 51D, p. D440
17, rue des Martyrs
38054 Grenoble Cedex 9
France
Téléphone : 00438780990
Email : benoit.denis@cea.fr

UNIVERSITÉ / ÉCOLE DOCTORALE

Grenoble INP

Mathématiques, Sciences et Technologies de l'Information, Informatique (MSTII)

DIRECTEUR DE THÈSE

Mathieu CUNCHE
INRIA / INSA Lyon
INRIA PRIVATICS
INRIA Rhône-Alpes
Antenne Lyon la Doua
Bâtiment CEI-2
56, Boulevard Niels Bohr
CS 52132
69603 Villeurbanne