DRT: Thesis SL-DRT-19-0515

RESEARCH FIELD

Electronics and microelectronics - Optoelectronics / Engineering science

TITLE

Cross-layer security reinforcement of vehicular wireless communication protocols

ABSTRACT

Vehicular wireless connectivity (also referred to as V2X for Vehicle to Everything) is seen today as a core enabler of future cooperative intelligent transport systems (C-ITS) (ex. highly autonomous driving, vulnerable users safety, fleet/trajectories coordination, vehicular mapping and vehicular Internet of Things…). ITS-G5, which relies on the IEEE 802.11p radio standard operating at 5.9 GHz, or C-V2X/LTE-V, which is an adaptation of 4G cellular solutions into the vehicular context (standard under definition), are two examples of relevant technologies frequently promoted in this context. However, related « open » V2X transmission modes are most often based on information broadcast (i.e., to reach the highest numbers of neighboring vehicles around) and as such, they are highly vulnerable (ex. with public control frequency channels). Accordingly, many kinds of attacks must be considered, including critical services denial (ex. through jamming, messages injection/interception, impersonations…).

So far, most of the security schemes put forward in this context rely on conventional cryptographic techniques and tools (i.e., using non-specific keys, pseudonyms or signatures). On the one hand, the main security features (i.e., primitives, seeds and algorithms…), which are determined in a static way, can be over-sized in some particular vehicular use cases. On the other hand, the resulting cryptographic overhead (in terms of computational complexity and access to the core network) contribute to strongly increase the latency of protected systems, what may be not compliant with safety applications.

In the frame of these PhD studies, we thus propose to define and evaluate new security mechanisms that could take benefits from different layers of the V2X protocol stack, as well as from the specificities of the vehicular application context itself (ex. « stealth » radio resource allocation, pseudo-random access and/or messages periodicity reducing the predictability of over-the-air data traffic, neighbors' trust assessment by cross-checking the consistency of exchanged application data...), while completing and reinforcing existing security schemes. A first step of these investigations with consist in conducting an in-depth risk analysis with respect to the specifications of current V2X standards. Then, some of the counter-measures proposed to mitigate most critical attacks will be validated by means of both simulations and field experimental data.

LOCATION

Département Systèmes
Service Technologigies Sans Fils
Laboratoire Communication des Objets Intelligents
Place: Grenoble
Start date of the thesis: 01/10/2019

CONTACT PERSON

Benoît DENIS

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

UNIVERSITY / GRADUATE SCHOOL

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

THESIS SUPERVISOR

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