Postdoctoral project

Title:
Cybersecurity Architecture for Transport Intelligent System (ITS)

Location: Télécom ParisTech (TPT)
Contacts:
- Rida Khatoun, rida.khatoun@telecom-paris.fr
- Mounira Msahli, mounira.msahli@telecom-paris.fr

Duration: 12-18 months
Begin at the earliest: September 15, 2019

Context

This postdoctoral position is in the context of a European project titled InDiD. It represents a real opportunity to see high impacted research results in the domain of intelligent transportation system.

InDiD is a pilot project aiming to evaluate how connected infrastructures will bring enhanced perception to road users. Building upon SCOOP@F (2014-EU-TA-0669-S), C-Roads France (2015-FR-TM-0378-S) and InterCor (2015-EU-TM-0159-S), experimentations will be carried out on a broad part of the country, to encompass a lot of configurations. InDiD includes representatives from Mobility, Digital and Telecommunication Industries as well as major public transport and urban node authorities. Strongly involved in the C-Roads Platform, InDiD initiative will bring together laboratory and closed experimentations with open road driving to assess interoperability impacts and deliver a mix of evidences on sustainability of EU strategy.

Description

The goal of this postdoc is to propose a novel approach based on machine learning to prevent and detect cyberattacks such as Jamming, Denial of Service (DoS), Sybil attacks, etc. in the used infrastructure. In this work, we rely on the C-ITS architecture specified in SCOOP@F, C-Roads France and InterCor projects. In the latter, the PKI hierarchy is composed of an Enrolment Authority (EA), Authorization Authority (AA) and a Root CA, Long Term Certificate Authority (LTCA) and Pseudonym Certificate Authority (PCA) used for distribution and maintenance of trust relationships between ITS stations and authorities or other ITS stations. In this context, vehicles communicate their own condition by using Cooperative Awareness Message (CAM) and report road condition by using Decentralized Environmental Notification Message (DENM.

The main idea of this postdoc is to design and validate a prevention and detection module in the used C-ITS architecture. The postdoc candidate will be involved in the following tasks:

- Definition of criterion to detect some specified attacks (Jamming, DoS, Sybil). As for example, for the Sybil attack, we evaluate the similarity of vehicle driving patterns, and then based on the variation of vehicles' driving pattern to distinguish the malicious nodes from the benign ones.
- Model of the problems

- Performance evaluation (Analytical and simulation analysis)

Background of the candidate

We are looking for a candidate with a PhD in Computer Sciences with very good background in cybersecurity in mobile networks especially in vehicular networks. A background in Machine learning is essential. She/He must have a good knowledge of vulnerabilities and attacks in such networks. Knowledge in performance evaluation, optimization, and modeling will be greatly appreciated as well as programming and simulation skills.