Misbehavior Detection for Cooperative Intelligent Transport Systems

Project

Topic proposed by: IRT-SystemX, Telecom ParisTech
Thesis advisor: To be defined
Co-advisor: To be defined
Research Unit: Secured Cooperative Autonomous systems (SCA) project, Autonomous Transport program, IRT-SystemX
Contact: Pierpaolo.cincilla@irt-systemx.fr

Research Context

Cooperative Intelligent Transport Systems (C-ITS) start to be a mature technology: standardization progress and pre-deployment projects are opening the way to smart mobility.

C-ITS offer innovative ways of wireless communication between Intelligent Transport Systems (ITS) stations and ITS road-side units. They favour the development of ITS applications to improve traffic management, road safety, mobility and other comfort services. C-ITS systems have to guarantee communication security, especially in heterogeneous network environments. Safety critical applications require authentication to avoid attackers to send spoofed or reforged information, nevertheless, cars and drivers privacy must be maintained.

In order to enhance cooperative awareness, ITS exchange relevant information about their speed, heading, position, etc., as well as emergency messages. Emergency messages (Decentralized Environmental Notification Messages (DENM)) and beaconing messages (Cooperative Awareness Messages (CAM)) will be used by ITS to understand their environment. Those safety messages are sensitive for safety and the system must be robust to faulty devices or malicious users that may sent erroneous or tampered information.
To this end, it is essential to have a misbehavior detection mechanism that permits to monitor the system and exclude misbehaving nodes.

Proposed research

The main goal of the Ph.D. thesis is to design a misbehavior detection mechanism for Cooperative Intelligent
Transport System (C-ITS). The system will monitor ITS communications and catch faulty or malicious ITS to identify and exclude them from the system.
The misbehavior detection system needs two components: one embedded in ITS (e.g. vehicles) that monitor exchanged information plausibility and the other in the cloud that receive misbehavior reports from ITS and analyze them.
The embedded misbehavior detection mechanism checks received data plausibility. The ITS can perform several kind of verification of different complexity, varying from simple checks

of the received speed or position to be under a certain threshold or within a certain range to more complex checks as for example neighborhoods speeds comparison or verify received information with its sensors. Once an anomaly is detected the ITS can take some countermeasures (e.g. discard further messages received from that ITS) and send a misbehavior report to the central Misbehavior Authority (MA).

The MA receives all the reports from the ITS and analyses them. For privacy reasons all safety messages are signed using pseudonym identities, so both reporter and reported ITS are identified by their pseudonym. The misbehavior reports analysis can be performed at several levels. For example, at a device level, the MA can looks for reports on the same ITS (i.e. on the same pseudonym). At an higher level, the MA can cross-check reports on different pseudonyms linked to the same identity, and at another level the MA can cross data from different reports on different ITS. Those three strategies (device-based, event-based and feature-based) can be useful to identify different scenarios as faulty devices, malicious devices and coordinated attacks.

The misbehavior detection arises several privacy issues: to send the misbehavior report can be threatening for both the reporter and the reported ITS. Moreover, the misbehavior authority needs a means to link pseudonym identities (or another mechanism) for both investigation and revocation purposes. The challenge is to have a misbehavior detection system that is effective without harm privacy.

International

- Internship mandatory (three or six months).
- Publication in international conferences.
- Participation in SystemX and EU projects.

Bibliography

1. Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems Full-text available · Article · Oct 2016 Rens W. van der Heijden Rens W. van der Heijden Stefan Dietzel Stefan Dietzel Tim Leinmüller Tim Leinmüller Frank Kargl Frank Kargl

2. Norbert Bißmeyer, Joël Njeukam, Jonathan Petit, and Kpatcha M. Bayarou. 2012. Central misbehavior evaluation for VANETs based on mobility data plausibility. In *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications* (VANET '12). ACM, New York

3. Liu, Bisheng, Jerry T. Chiang, and Yih-Chun Hu. "Limits on revocation in vanets." *8th international conference on applied cryptography and network security*. 2010.

4. Haas, Jason J., Yih-Chun Hu, and Kenneth P. Laberteaux. "Design and analysis of a lightweight certificate revocation mechanism for VANET." *Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking*. ACM, 2009.

5. Papadimitratos, Panagiotis Panos, Ghita Mezzour, and Jean-Pierre Hubaux. "Certificate revocation list distribution in vehicular communication systems." *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*. ACM, 2008.