Securing Vehicular Communications

Panos Papadimitratos and Jean-Pierre Hubaux
Ecole Polytechnique Fédéral de Lausanne (EPFL)
Lausanne, Switzerland
{panos.papadimitratos, jean-pierre.hubaux}@epfl.ch

Abstract

Vehicular communication (*VC*) systems are an emerging technology that has recently drawn the increased interest of governments, industry, and academia. *VC* will enable a variety of applications for safety, transportation efficiency, and infotainment. For example, warnings for environmental hazards (e.g., ice on the pavement) or abrupt vehicle kinetic changes (e.g., emergency breaking), traffic and road conditions (e.g., congestion or construction sites), and tourist information downloads will be provided by these systems.

A number of on-going efforts in industry and academia seek to address a wide range of technical challenges, before the technology is deployed in the near future. To name a few, sensing, processing and communication units that will be on-board the vehicles and mounted on the road-side infrastructure units, as well as the applications and networking protocols for vehicle-to-vehicle (*V2V*) and vehicle-to-infrastructure (*V2I*) communication are currently under development.

The unique features of *VC* systems make them vulnerable to a formidable set of abuses and attacks. Consider, for example, network nodes that 'contaminate' large portions of the vehicular network with false information: a single vehicle can transmit false hazard warnings that can then be taken up by all vehicles in both traffic streams. Or, similarly, a vehicle that meaningfully modifies messages of other vehicles. Or, even, a vehicle that forges messages in order to masquerade an emergency vehicle and mislead other vehicles to slow down and yield.

These simple examples of exploits clue that vehicular communications must be secured. Thwarting attackers, which could tamper with on-board electronics and software or simply run a rogue version of the *VC* protocol stack on any wireless-enabled device, is paramount. If the *VC* operation, and thus transportation system operation, is not safeguarded, *VC* systems could make anti-social and criminal behavior easier, in ways that would actually jeopardize the benefits of their deployment.

In this talk, we discuss how to secure the operation of *VC* systems, a hard and multifaceted problem. We first outline vulnerabilities and challenges, and then building blocks of a secure *VC* architecture. More information on our on-going research efforts on this topic can be found at http://ivc.epfl.ch and http://www.sevecom.org.