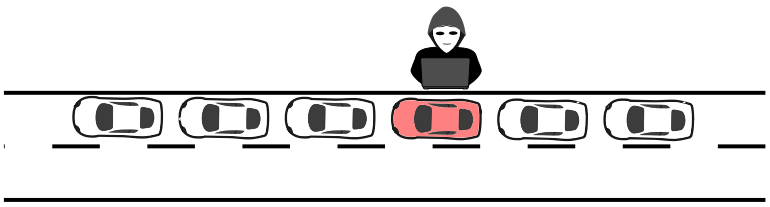
Bachelor / Master's Thesis

Secure platooning in attack scenarios



Vehicle-to-everything communication can serve as the basis for novel applications enabling cooperation among mobile systems of the future. An example application for this is *vehicle platooning* on different kind of streets. Vehicle platooning means a convoy or a platoon of vehicles travelling in close co-ordination under fully automated longitudinal and lateral control. In general, a platoon has a leader which is responsible for setting the trajectory and speed for all vehicles in the platoon. All other vehicles in the platoon are following one another with a very small headway spacing and they are linked to each other through control mechanisms. This control mechanism describes how the following vehicles have to react to steady-state operations or to disturbances. The small headway leads to an increased capacity of the road and reduced fuel consumption by using the reduced air drag.

We believe that a single and maliciously controlled vehicle in a platoon can destabilize a platoon with catastrophic effects. One example is an attacker that causes the platoon to oscillate and thus cause accidents or to leverage instabilities to target certain vehicles in a controlled manner with far greater effects. This could be done by misinforming other cars. For example, the attacker sends a beacon that causes vehicles to accelerate. In the next step, the attacker performs an aggressive break, which causes an accident at high speed, making this kind of attack especially dangerous. As the underlying platoon approach is based on trust, it is hard to counteract this kind of attack. However, it might be possible to mitigate the effect of an attack by introducing different countermeasures. One could use other input values besides the received DSRC input to validate the received information. The result would be to increase the headway time and to report this abnormality to other members in the platoon.

Goals of the thesis

Hence, in the scope of this thesis we want to investigate the consequences when one of the cars in the platoon does not behave according to the control law. In doing so, we want to address questions like: Is it possible to detect an attack and to implement countermeasures, which don't offset advantages of platooning? How would a platoon look like that is resistant against attacks and offers advantages of platooning?

The first step is to implement different threat models and attacks within SUMO and make them usable within OMNeT++ and Plexe.[1] We already have some platoon controllers implemented, which we will be using with the implemented attacks to destabilize or control the platoon. The controllers and the application logic will be changed later in order to detect and counteract the attacks. The results of this thesis will help make platoons more secure and more dynamic in realistic scenarios.

Keywords

C++, Platooning, Network Simulation, Vehicular Networking

[1] http://plexe.car2x.org/

Contact:
Tobias Hardes <hardes@ccs-labs.org>

Website:
http://www.ccs-labs.org/cms/