Exploring the effect of cyber-attacks on traffic condition in a partially or fully automated and connected environment

Context
With recent communication and built-in vehicle technologies, automated vehicles will be soon appearing in the traffic network. Since automated and connected vehicles use communication protocol in a corresponding media to exchange data or receive commands, this may provide tendency for potential cyber attackers trying to influence driving behavior of each individual vehicle or traffic condition in an area. The goal of this project is to first implementation Cooperative Adaptive Cruise Control (CACC) in a traffic simulator. The next step is to model a feasible scenario of a possible cyber attach and explore the related consequences on the traffic condition.

Tasks
The main tasks for this project are:

- Constructing a test-bed model in a traffic simulator such as Aimsun.
- Implementing the ready API code for CACC strategy.
- Designing and Implementing a feasible scenario for a possible and relevant cyber-attack.
- Exploring the effect of such attacks in the driving behavior or traffic condition.

Requirements
- Knowledge of cyber-attack scenarios
- Good programming knowledge in Python
- Basic knowledge of motion dynamics
- Basic understanding of traffic network and traffic control is beneficial but not required
Contact:
Chair of Traffic Engineering and Control
Majid Rostami
majid.rostami@tum.de