Detection of misbehavior and anomalous activities in VSNs

Motived by the increasing momentum gained by the integration of the Internet-of-Vehicles (IoV) and social networks, Vehicular Social Networking (VSN) are promising to enable smart mobility in modern cities. In VSNs, individuals communicate by exploiting social behavior. They utilize sensors embedded into smart devices, onboard units, roadside units (RSUs), and vehicles to measure real-world conditions and communicate over a ubiquitous network which support various wireless communication technologies. In this respect, VSNs present new security challenges, one of them is the integrity of data transmitted and exchanged between the connected devices. Successful exploitations can happen though various attack vectors such as jamming, data injection, replay, routing, and Sybil attacks. The implications of these attacks can severely impact the safety of the connected vehicles. Motivated by the increasing momentum of big data analytics and machine learning (ML) in the security field, this project aims at mainly leveraging advanced ML algorithms to detect anomalous activities indicating security breaches in VSNs.