Anomaly Detection Against GPS Spoofing Attacks on Connected and Autonomous Vehicles Using Learning from Demonstration

Abstract

GPS spoofing attacks pose great challenges to safety applications of connected vehicles (CVs) and localization of autonomous vehicles (AVs). In this paper, we propose to utilize transportation and vehicle engineering domain knowledge to detect GPS spoofing attacks towards CVs and AVs. A novel detection method using learning from demonstration is developed, which can be implemented in both vehicles and at the transportation infrastructure. A computational-efficient driving model, which can be learned from the historical trajectories of the vehicles, is constructed to predict normal driving behaviors. Then a statistical method is developed to measure the dissimilarities between the observed trajectory with the predicted optimal trajectory for anomaly detection. We validate the proposed method using two threat models (i.e., attacks targeting the multi-sensor fusion of the AV and attacks targeting the forward collision warning system of the CV) on two real world datasets (i.e., KAIST and NGSIM). Results show a satisfactory detection performance with both low false positive and false negative rates.