Grant Deliverables and Reporting Requirements for UTC Grants

UTC Project Information	
Project Title	Improving Security and User Privacy in Learning-Based Traffic Signal Controllers (TSC)
University	University of California Davis
Principal Investigator	Chen-Nee Chuah
PI Contact Information	chuah@ucdavis.edu 530-752-5825
Funding Source(s) and Amounts Provided (by each agency or organization)	USDOT: $45,000 UCD: $26,357
Total Project Cost	$71,357
Agency ID or Contract Number	Sponsor Source: Federal Government CFDA #: 20.701 Agreement ID: 69A3551747119
Start and End Dates	Start date: 04/01/2021 End date: 03/31/2022
Brief Description of Research Project	The 21st century of transportation systems leverages intelligent learning agents and data-centric approaches to analyze information gathered with sensing (both vehicles & road sides) or shared by users to improve transportation efficiency and safety. Numerous machine learning models have been incorporated to make control decisions (e.g., traffic light control schedules) based on mining mobility data sets and real-time input from vehicles via vehicle-to-vehicle and vehicle-to-infrastructure communications. However, in such situations, where ML models are used for automation by leveraging external inputs, the associated security and privacy issues start to surface. This project aims to study the security of machine learning systems and data privacy associated with learning-based traffic signal controllers (TSCs). Our preliminary work has demonstrated that deep reinforcement learning (DRL) based TSCs are vulnerable to both white-box and black-box cyber-attacks. Our research goals include (1) quantifying the impact of such security vulnerabilities on the safety and efficiency of the TSC operation, and (2) developing effective detection and mitigation mechanisms for such attacks. In learning based TSCs, vehicles share their messages with the DRL agents at TSCs,

	which will then analyze the data and take action. Sharing vehicular mobility data with a network of TSCs may cause privacy leakage. To address this problem, we propose to apply differential privacy techniques to the mobility datasets to protect user privacy while preserving the effectiveness of the prediction outcomes of traffic-actuated or learning-based TSC algorithms. We will evaluate our approaches in vehicular simulator using real mobility data from San Francisco and other cities in California. By accomplishing these goals, learning-based transportation systems will be more secure and reliable for real-time implementations.
Describe Implementation of Research Outcomes (or why not implemented) Place Any Photos Here	
Impacts/Benefits of Implementation (actual, not anticipated)	
Web Links • Reports • Project Website	http://ctech.cee.cornell.edu/final-project-reports/