UTC Project Information – **Center for Transportation, Environment, and Community Health**	
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 Sources and Amount 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	04/01/2021 – 03/31/2022
Brief Description of Research Project	21st century transportation systems leverage intelligent learning agents and data-centric approaches to analyze information gathered with sensing (both vehicles and roadsides) or shared by users to improve transportation efficiency and safety. Numerous machine learning (ML) 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, associated security and privacy issues start to surface. This project studied the security of ML systems and data privacy associated with learning-based traffic signal controllers (TSCs). Preliminary work had demonstrated that deep reinforcement learning (DRL) based TSCs are vulnerable to both white-box and black-box cyber-attacks. Research goals included 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, differential privacy techniques were applied to the mobility datasets to protect user privacy while preserving the effectiveness of the prediction outcomes of traffic-actuated or learning-based TSC algorithms. Approaches were evaluated in vehicular simulators using real mobility data from San Francisco and other cities in California. By

	accomplishing these goals, learning-based transportation systems are more secure and reliable for real-time implementations.
Describe Implementation of Research Outcomes (or why not implemented) *Place Any Photos Here*	We have performed simulation experiments to study the vulnerabilities of DRL-TSC algorithms in the presence of black-box and white-box adversarial attacks for both single and multiple intersections. Our results showed that the performance of DRL learning agent decreases in both settings, resulting in higher levels of traffic congestion. We implemented and evaluated several sequential anomaly detection models. While sequential anomaly detection models minimize the detection delays, it also achieves lower false alarm rates due to cumulative anomaly inspection. We then proposed an ensemble model that works with all the attack models without any model assumption. The results of anomaly detectors indicated that low-cost ensemble model achieves the best anomaly detection performance in all attack models and DRL settings.
Impacts/Benefits of Implementation (actual, not anticipated)	Our study has clearly demonstrated the potential adverse impact of security attacks on deep reinforcement learning based traffic light controllers (DRL-TSC), despite its enhanced performance in improving system throughput and travel delay. By implementing our proposed ensemble anomaly detection, we will be able to make such DRL-TSC systems more secure and robust for real-time implementation. This will result in driver safety and traffic flow efficiency.
Web Links • *Reports* • *Project website*	http://ctech.cee.cornell.edu/final-project-reports