CENTER FOR CONNECTED AND AUTOMATED TRANSPORTATION

Project Title	Road-side based cybersecurity in connected and automated vehicle systems	
PI (Up to 2)	Neda Masoud, Henry Liu	
Telephone #	(734) 764-8230	
E-mail:	nmasoud@umich.edu	
Institution:	University of Michigan	
Department:	Civil and Environmental Engineering	
Industry or Government Principal, organization, and contact information	DENSO International America Inc.	
Government Principal, agency, and contact information		
Most relevant CCAT research thrusts (choose all applicable)	__Y___ Enabling Technology _____ Planning and Policy _____ Human Factors _____ Infrastructure Design and Management __Y___ Control and Operations __Y___ Models and Implementation	
Funding Request	$153,764	
Matching Funds and Source (if any)		
Total Project Cost	$153,764	
Contract Number	69A3551747105	
Project start/end dates	Jan. 2021-Jan. 2022	
Project Abstract	The objective of this research project is to further the knowledge on cybersecurity in connected and automated vehicles (CAVs). Specifically, we aim to develop a holistic framework that integrates physics-based data-driven modeling and dynamic decision making under uncertainty and partial information to improve cybersecurity in CAVs. CAVs are anticipated to enhance our current transportation system in terms of safety and mobility, and curb the environmental implications of the transportation sector. Despite these benefits, major concerns remain as to whether an interconnected network of CAVs and	

	infrastructure is vulnerable to malicious hackers or unintentional faults. In this proposed work, we aim to address open questions on cybersecurity of a network of connected CAVs. Our goal is to develop an integrated real-time, robust, and scalable context-aware framework to ensure safe navigation of CAVs and other road users. We will validate the framework using existing data from ongoing pilot studies as well as new simulated data which will be produced as part of this proposed work. The proposed framework contributes to the literature of anomaly detection/identification, data fusion, non-linear control, physics-based learning, and decision making under uncertainty in novel and important ways. It will build on the state-of-the-art filters, control algorithms, and machine learning methods to address scientific challenges with respect to incorporating `context' to improve learning and decision making under adversarial conditions. This context includes a vehicle's motion in relationship with its surrounding traffic, which is complicated by the stochastic time delay in receiving basic safety messages from the connected vehicles/infrastructure or in collecting and contextualizing data by the vehicle's on-board sensors.
High-level implementation plan	This project will adopt a two-level implementation plan. First, we will use an existing cybersecurity dataset to assess the performance of the developed cybersecurity solutions. Next, we will use an in-house simulation platform that is capable of modeling connected and automated vehicles in isolation and in platoons to assess the performance of our solutions on edge cases and scenarios for which naturalistic driving data does not exist.
Project Metrics	The metrics to show successful completion of the project include: successfully developing the cybersecurity solutions, assessing the performance of solutions on existing and new datasets, presenting the results of research at TRB and INFORMS conferences, publishing 1-2 journal papers in top peer-reviewed journals, and obtaining funding from external sources for expanding the research.
Web Links: [leave blank until project approval]	