CENTER FOR CONNECTED AND AUTOMATED TRANSPORTATION

Project Title	Cybersecurity of Transportation Infrastructure in a Connected-Vehicle Environment	
PI (Up to 2)	Henry Liu	Morley Z. Mao
Telephone #	734-764-4354	734-763-5407
E-mail:	henryliu@umich.edu	zmao@umich.edu
Institution:	University of Michigan	University of Michigan
Department:	UMTRI	EECS-CSE
Industry or Government Principal, organization, and contact information	Mcity Huei Peng hpeng@umich.edu 734-936-0352	
Most relevant CCAT research thrusts (choose all applicable)	__X__Enabling Technology __X___ Planning and Policy _____Human Factors __X__ Infrastructure Design and Management _____ Control and Operations _____Models and Implementation	
Funding Request		
Matching Funds and Source (if any)	Mcity $334,865	
Total Project Cost	$334,865	
Contract Number	69A3551747105	
Project start/end dates	1/1/2017 – 12/3/2018	
Project Abstract	The objective of this project is to find cybersecurity vulnerabilities in transportation infrastructure and identify a set of strategies to prevent or reduce the damage from cyberattacks. A series of recommendations to improve infrastructure cybersecurity will be developed. This project will first analyze the security of the current transportation infrastructure at the protocol level (e.g., dedicated short range communications, National Transportation Communications for Intelligent Transportation Systems) and at traffic-control-system level (e.g., traffic signal policy and operation). Then, real-world penetration tests will be conducted at the Mcity Test Facility to determine possible security vulnerabilities. Based on the testing results, consequences of security breaches will be investigated. Finally, a set of recommendations will be developed for best security practice. The final report for this project will not be publicly available.	
High-level implementation plan	(1) Analysis of the current protocol and traffic-control-system security; (2) Models and algorithms to detect potential cyberattacks; (3) Investigation of consequences of security breaches; and (4) A set of recommendations for best security practice.	
Project Metrics	Compromised data from only one OBU can cause more than 33% greater delay than normal signal operation Cyber attacks can increase network delay up to 600% under actuated signal control	

	Identify 4 attack surfaced for transportation infrastructure
Web Links:	ccat.umtri.umich.edu