DEPARTMENT OF
COMPUTER SCIENCE
TEXAS TECH
Whitacre College of Engineering

Perception Security of Autonomous Systems

Ming Li, Ph.D.
University of Arizona
Tuesday, November 5, 2024
3:30 p.m.
Zoom:
https://texastech.zoom.us/j/98378510928?pwd=LCzeblQN80tTQDDxRajezJXXAKfrXN.1
Meeting ID: 983 7851 0928
Passcode: 996165

Abstract: Autonomous Systems (AS), such as self-driving cars, robotic agents, and surveillance systems, rely heavily on sensors to perceive their surroundings and make informed, autonomous decisions. However, the security of these systems has become increasingly critical, as malicious actors can exploit vulnerabilities in the perception pipeline, leading to potentially catastrophic consequences. This talk delves into the security challenges posed by sensor perception modules in autonomous systems.

We will explore how adversaries can remotely inject deceptive patterns into camera feeds, creating or altering objects in the perceived environment. These attacks exploit weaknesses in both the sensing mechanism and machine learning-based object detection algorithms. To counter such threats, we will introduce a novel defense framework that leverages spatiotemporal consistency checks, which is agnostic to the specific sensing modality or attack technique. Finally, we will discuss future research directions in this field, aiming to further strengthen the security and robustness of autonomous systems.

Bio: Ming Li is a Professor in the Department of Electrical and Computer Engineering of University of Arizona and affiliated with the Computer Science Department. He was an Associate Professor in the same department from 2015-2024. He was an Assistant Professor in the Computer Science Department at Utah State University from 2011 to 2015. He received his Ph.D. in ECE from Worcester Polytechnic Institute, MA, in 2011. His main research interests are wireless and cyber security, with current emphases on security and privacy for next-generation wireless networks, physical layer security, privacy-preserving data analysis, and cyber-physical system security. He received the NSF Early Faculty Development (CAREER) Award in 2014, and the ONR Young Investigator Program (YIP) Award in 2016. His works have been published in major security and networking conferences, including ACM CCS, USENIX Security, NDSS, IEEE S&P, IEEE INFOCOM, ACM Mobihoc, etc. He has published more than 130 journal and conference papers and received six best paper/poster awards, including a best paper award from ACM WiSec 2020. Currently he serves on the editorial board of IEEE TIFS and served as an associate editor for TMC and TDSC. He is a Fellow of IEEE (class of 2024), and a member of ACM.