Systematic Investigation of Sensor Spoofing Attacks to Autonomous Systems

Abstract

Robotic Vehicles (RVs) have gained great popularity over the past few years. Meanwhile, they are also demonstrated to be vulnerable to sensor spoofing attacks. By injecting malicious fake data into the sensors, an external adversary is able to trick a victim RV into taking dangerous actions, which could cause severe security and safety consequences. In this talk, we will investigate sensor spoofing attacks from two perspectives. First, we propose a novel *action flow model* to systematically describe robotic function executions and unexplored sensor spoofing threats. Second, we introduce new defense frameworks, which leverage state-of-the-art deep learning technology to detect different types of sensor spoofing attacks in a holistic and unified manner.

Bio

Dr. Tianwei Zhang is currently an assistant professor at School of Computer Science and Engineering, Nanyang Technological University, Singapore. He received his Bachelor's degree at Peking University in 2011, and Ph.D degree at Princeton University in 2017. His research focuses on building efficient and trustworthy computer systems. He has been involved in the organization committee of numerous technical conferences, including serving as the general chair of KSEM'22. He serves on the editorial board of IEEE Transactions on Circuits and Systems for Video Technology (TCSVT) since 2021, and received the best associate editor award in 2022. He has published more than 100 papers in top-tier AI, system and security conferences and journals. He has received several best paper awards including ASPLOS'23, ICDIS'22 and ISPA'21.