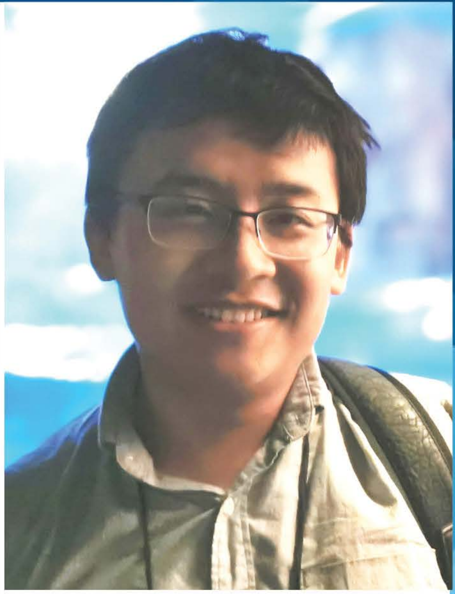
COLLEGE OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

Dissertation Defense

Chaowei Xiao



Machine Learning in Adversarial Environments

Friday, June 12, 2020
11:00 am – 1:00 pm
umich.zoom.us/j/7886942853

ABSTRACT: Deep Learning (DL) has achieved great success these days. It has been used in many applications in the real world, even in safety-critical applications such as autonomous driving systems. It seems that we are ready for DL now. However, is DL ready for us? In this talk, I will answer this question by exploring threats of current DL systems in adversarial environments where adversaries could manipulate inputs. To raise awareness of this threat and motivate the investigation of defense, I will show the feasibility to apply this threat to the real-world. In the end, I will introduce a principled method to mitigate this threat by exploring the properties of the learning model or the data.

Chair: Prof. Mingyan Liu