In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Towards Resilient Autonomous Cyber-Physical Systems against Adversarial Examples

By

Dr. Qun SONG

A*STAR Institute, Singapore

Date : 2 September 2022 (Friday)

Time : 11:00am to 12:00nn

Venue : 801, Ho Sin Hang Engineering Building, CUHK

Zoom : https://cuhk.zoom.us/j/94609354007?pwd=Y2t1WG1OdnlpSG9wSUFJaXJPNTZNQT09

(Meeting ID: 946 0935 4007; Passcode: 739408]

Abstract

Deep learning is shown susceptible to adversarial examples, which are crafted inputs aiming to cause wrong classification outputs for deep models by adding minute perturbations on the clean inputs. Thus, deploying deep learning models on the safety-critical cyber-physical systems without incorporating effective countermeasures against adversarial examples raises security concerns. This talk is about the studies on the threat and countermeasures for the adversarial example attack as an ongoing concern for the safety-critical autonomous cyber-physical systems. This talk will introduce the dynamic ensemble-based defenses designed under the strategy of moving target defense that effectively counteract the adaptive adversarial example adversary for embedded deep visual sensing. This talk will also present the systematic requirement investigation and credibility analysis of adversarial example attack against the power grid voltage stability assessment and develops effective countermeasure.

Biography

Qun Song received Ph.D. from Nanyang Technological University, Singapore in 2022 and B.Eng. from Nankai University, China in 2018. She is currently a research scientist at the Singapore A*STAR Institute of High Performance Computing. She will be joining the Department of Software Technology, EEMCS, TU Delft as an assistant professor in Nov 2022. Her research focuses on building reliable, resource-efficient, and physic-aware AI-powered Cyber-Physical Systems and Internet of Things. She is the recipient of the 2021 IPSN Best Artifact Award Runner-up and NTU SCALE Best Demo Award.

**** ALL ARE WELCOME ****

Host: Prof. XING Guoliang (Tel: 3943-8474, Email: glxing@cuhk.edu.hk)

Enquiries: Department of Information Engineering, CUHK (Tel.: 3943-8385)