In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering
Seminar

Machine Learning for Cyber-Physical System Security

by

Prof. David Yau
The Singapore University of Technology and Design, Singapore

Date : 26 February 2025 (Wednesday)
Time : 3:30 pm – 4:30 pm
Venue : Rm 801, Ho Sin Hang Engineering Building, CUHK

Abstract

Mission-critical cyber-physical infrastructures such as power systems increasingly apply information and communication (ICT) technologies to improve their operations. However, the ICT integration introduces a new attack surface that subjects them to various powerful attacks, such as time-delay attacks and false data injection. In this talk, I will overview some of our recent experiences in applying machine learning and deep learning solutions for securing cyber-physical smart grids for purposes such as detecting and classifying attacks.

Biography

David Yau obtained the B.Sc. from CUHK, and M.S. and Ph.D. from UT Austin, all in computer science. Since 2013, he has been Professor at the Singapore University of Technology and Design (SUTD), after serving as Distinguished Scientist at Singapore ADSC. Before Singapore, he was Assistant Professor and then Associate Professor (Computer Science) at Purdue. His research interests are in networked computer systems, including the security and privacy of cyber-physical systems. He has served as TPC co-chair or in the organizing committees of several international conferences. He is currently an Associate Editor for ACM Trans. Sensor Networks. He was previously on the editorial boards of IEEE Trans. Network Science and Engineering (awarded Excellent Editor in 2022), IEEE/ACM Trans. Networking, and IEEE Trans. Smart Grid, Special Section on Smart Grid Cyber-Physical Security.

**** ALL ARE WELCOME ****

Host: Prof. YEUNG Wai Ho Raymond (Tel: 3943-8375, Email: raymond@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)