SEMINAR ANNOUNCEMENT

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
COLLEGE OF DESIGN AND ENGINEERING
Website: https://cde.nus.edu.sg/ece

Area: Control, Intelligent Systems & Robotics

Host: Associate Professor Xiang Cheng

Research Webinar

TOPIC	:	**Security of Cyber-Physical Systems**
SPEAKER	:	**Dr. Bharadwaj Satchidanandan** **Postdoctoral Researcher, Laboratory for Information and Decision Systems** **Massachusetts Institute of Technology (MIT)**
DATE	:	**Thursday, 23 March 2023**
TIME	:	**9.00AM to 10.00AM**
WEBINAR	:	**Join Zoom Meeting** **https://nus-sg.zoom.us/j/4156763801?pwd=NUwzUWhwdlZlcGt3cmhyTzFld1V0QT09** **Meeting ID: 415 676 3801** **Passcode: 662108**

ABSTRACT

The coming decades may see the large-scale deployment of networked cyber-physical systems to address global needs in areas such as energy, water, healthcare, and transportation. However, as recent events have shown, such systems are vulnerable to cyber-attacks. They are not only economically important, but being safety critical, their disruption or misbehavior can also cause injuries and loss of life. It is therefore important to secure such networked cyber-physical systems against attacks. In the absence of credible security guarantees, there will be resistance to the proliferation of cyber-physical systems, which are much needed to meet global needs in critical infrastructures and services. This talk addresses the problem of secure control of cyber-physical systems. This problem is different from the problem of securing the communication network, since cyber-physical systems at their very essence need sensors and actuators that interface with the physical plant, and malicious agents may tamper with sensors or actuators, as recent attacks have shown.

We consider physical plants that are being controlled by multiple actuators and sensors communicating over a network, where some sensors and actuators could be "malicious." A malicious sensor may not report the measurement that it observes truthfully, while a malicious actuator may not apply actuation signals in accordance with the designed control policy. Against this backdrop, we present a general technique termed "Dynamic Watermarking" by which honest nodes in the system can detect the actions of malicious nodes and disable closed-loop control based on their information. Dynamic Watermarking employs the technique of honest actuators injecting a "small" random noise, known as private excitation, into the system which will reveal tampering of measurements by malicious sensors. We show how such an active defense can be used to secure networked systems of sensors and actuators.

BIOGRAPHY

Bharadwaj Satchidanandan is a postdoctoral researcher in the Laboratory for Information and Decision Systems at Massachusetts Institute of Technology (MIT), where he is hosted by Prof. Munther A. Dahleh. He obtained his Ph.D. from Texas A&M University in 2019 where he was advised by Prof. P. R. Kumar. His research interests include cyber-physical systems, security, renewable energy, mechanism design, control, communications, etc.