Electric Power and Power Electronics Institute

INVITED SEMINAR

Wednesday, December 2nd, 2015, 3:00pm – 4:00pm, Fishbowl, 333 WEB

CONSEQUENCES OF UNOBSERVABLE CYBER AND CYBER-PHYSICAL FALSE DATA INJECTION ATTACKS ON THE ELECTRIC POWER SYSTEM

Dr. Lalitha Sankar
Assistant Professor in the ECEE Department at Arizona State University

Abstract

The electric power system (EPS) is a complex network that is monitored and controlled by a distributed network of human-machine interfaced control (cyber) systems. These cyber systems are just as vulnerable to sophisticated cyber-attacks as are traditional networked information systems; however, the consequences of well-designed attacks that can actively change data can be much more severe for such critical infrastructure. Recent results on false data injection (FDI) attacks on the EPS have revealed the design of unobservable attacks within the context of specific (cyber) processing units, notably state estimators (SE). However, very little is known about the consequences of sophisticated, well-designed, and unobservable (within SE) FDI attacks on the electric power system as a whole. In this talk I will present recent work identifying a class of limited resource FDI attacks designed to cause a specific physical impact (line overflows) on the physical system while remaining unobservable to the cyber monitoring system (assuming an non-linear measurement and estimation model). We propose to do so via a bi-level optimization problem wherein the first level problem captures the attacker's goal of causing a line overflow subject to constraints on the attacker's resources (size of sub-network to attack) and the desire to be remain undetected (limit on load measurement changes). The second level problem captures the response of the system to FDI attacks (within SE) via a DC optimal power flow. Such a bi-level problem captures the sequential and modular aspect of computation in EPSs as a time-progression from obtaining measurements, followed by state estimation, and culminating in computation of the optimal power flow and redispatch while incorporating the attacker's (limited) information about the system. I will describe the results of our work for both cyber-only state-based and a cyber-physical topology-and-state-based FDI attacks.

This is joint work with Jingwen Liang, Jiazi Zhang, and Oliver Kosut.

Biography

Lalitha Sankar received the B.Tech degree from the Indian Institute of Technology, Bombay, the M.S. degree from the University of Maryland, and the Ph.D degree from Rutgers University. She is presently an Assistant Professor in the ECEE department at Arizona State University. Prior to this, she was an Associate Research Scholar at Princeton University. Following her doctorate, Dr Sankar was a recipient of a three year Science and Technology teaching postdoctoral fellowship from the Council on Science and Technology at Princeton University. Her research interests include information privacy and security in distributed and cyber-physical systems. For her doctoral work, she received the 2007-2008 Electrical Engineering Academic Achievement Award from Rutgers University. She is a recipient of a NSF CAREER award for 2014.