EESG
Electric Energy Systems Group

SEMINAR series

IN CONJUNCTION WITH ENERGY AND INFORMATION SEMINARS

Wednesday, November 12, 2014, 2:00 p.m. | Porter Hall B34

LALITHA SANKAR
ASSISTANT PROFESSOR OF ECEE
ARIZONA STATE UNIVERSITY

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. Prior to her doctoral studies, she was a Senior Member of Technical Staff at AT&T Shannon Laboratories. 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 received the IEEE Globecom 2011 Best Paper Award for her work on privacy of side-information in multi-user data systems. She is a recipient of the NSF CAREER award for 2014.

Hosted by: Prof. Marija Ilic
Prof. Pulkit Grover
Department of ECE

When Man-in-the-Middle Meets Woman-at-the-Control Center: Implications of Cyber Attacks on Distributed Power System Operations

The electric power system is a complex network that is monitored and controlled by a distributed cyber-network of human-machine interfaced control systems. In fact, this distributed cyber network is the backbone of the modern electric grid and enables highly reliable guarantees on the generation and distribution of electricity by ensuring distributed information sharing and processing across the grid. The complexity and size of the electric network has led to a hierarchical management of the grid wherein data collection, processing, and control occurs from local utility providers to systems operators that manage large parts of the network. These distributed cyber systems (often referred to as energy management systems, i.e., EMSs) are just as vulnerable to sophisticated cyberattacks as are traditional networked information systems; however, the consequences of such attacks can be much severe for such critical infrastructure.

In this talk, I will focus on a class of man-in-the-middle (MitM) attacks that can disrupt real-time data sharing between two distributed EMSs. Simple control-theoretic models of grid functionalities suggest that MitM attacks focused on specific cyber processing units (e.g., state estimation) can be unobservable; however, the physical consequences of such attacks on the grid cannot be studied with such simple models. Specifically, these models do not take into account the spatio-temporal behavior of EMSs and the numerous resiliency mechanisms built into the system including hard-to-model operator behavior. Using mathematical models for real-time interactions and data sharing between two distributed EMSs, we show that for an MitM attack that limits real-time topology information sharing, operator behavior and real-time system response determines whether the attacks consequences can be severe enough to mimic the Northeast blackout of 2003 or whether the attack can be detected

Carnegie Mellon