EEE598: SECURITY AND PRIVACY IN CYBER-PHYSICAL SYSTEMS (THE SMART GRID)

Instructor: Dr. Lalitha Sankar
ERC 585

Communication and information technologies are taking an increasingly important role in monitoring and controlling physical systems. The smart grid is a canonical example of a cyber-physical system (CPS) in which the physical power grid is monitored by a network of sensors and other intelligent devices to dynamically track and control the network to ensure near-perfect reliability. In contrast to the traditional grid in which generation, transmission, and distribution are clearly distinct and managed by well-defined entities, the smart grid allows integration of renewables (e.g., solar, wind) at every layer of the grid (transmission and distribution). Furthermore, there is an increasing need to finely monitor the grid to better manage and conserve energy resources through a variety of devices from phasor management units (PMUs) at the transmission levels and Advanced Metering Infrastructure (AMI) such as smart meters at the distribution level. These requirements call for architecting an end-to-end communications, control, and computation (cyber) network that overlays and functions in synchrony with the physical network.

This course is aimed at students interested in doing research in any of the following topics:
(i) cyber-security and privacy;
(ii) computation and communication challenges in the smart grid;
(iii) distributed approaches to data processing in the grid; and
(iv) large data sets: modeling, analysis, communication, compression, storage, and security.

Topics:
In this course, we will focus on developing simple communication and computing models for the grid with specific emphasis on architecting such a network with strict security and privacy guarantees. The aim is to understand the data collection, modeling, and control challenges along with the security and privacy issues that arise in architecting such a network. Specific focus will be placed on the following topics:

- Introduction to CPSs and the smart grid
- Distributed data collection in complex networks (the smart grid)
- Cyber-security and privacy challenges in CPSs
- Topics in the Smart Grid:
    - Secure state estimation (monitor the state -- phase/voltage -- in the grid)
    - Distributed computation in the grid with privacy/confidentiality guarantees (focus on computational aspects in the grid such as unit commitment, economic dispatch, frequency control)
    - Tradeoff between privacy and utility (benefit) in sharing AMI measurements
- Large Data Challenges in the Grid:
    - How to develop (linear/non-linear) stochastic models for data in the grid
    - Centralized vs. distributed computation paradigms
    - How much data is needed? Compression/storage/communication challenges

Textbooks/Reading Materials/Exams:
The material for the course will be based on reading current literature. Guest lecturers will be invited for specific topics. A background in either power systems **or** communication systems is desirable. Background in control theory or probability theory is a plus but not needed. The aim is to introduce the appropriate concepts to both audiences and enable interactions and discussions.
Students should expect to read papers and make presentations throughout the course. All the necessary background will be introduced as needed. Students from power and communications systems are expected to team up and work on a final term project including a presentation.