Disclaimer
This syllabus is to be used as a guideline only. The information provided is a summary of topics to be covered in the class.
Information contained in this document such as assignments, grading scales, due dates, office hours, required books and materials may be from a previous semester and are subject to change. Please refer to your instructor for the most recent version of the syllabus.

EEE 598: Smart Grid Operations, Cybersecurity, and Analytics – Spring 2019

Classroom: BYAC 210
Class timings: Tu-Th: 1:30 – 2:45 pm
Credits: 3

Instructor:
Dr. Lalitha Sankar
School of Electrical, Computer, and Energy Engineering
Arizona State University
PO Box 875706
Tempe, AZ 85287-5706

Office: Engineering Research Center 585
Email: lsankar@asu.edu
Phone: 480-965-4953 **Fax:** 480-965-0745

Office Hours:
Tuesday: 2:45 – 3:45 pm
Thursday: 10 – 11:30 am

Email questions at any time for prompt replies.

Required Textbook: None (Class Notes & Papers: All reading materials on Blackboard/Canvas).
References:

- Power System State Estimation: Theory and Implementation, *A. Abur and A. G. Exposito*.
- Probability and Stochastic Processes: A Friendly Introduction for Electrical and Computer Engineers, 2nd Edition, *Yates & Goodman*

Offered: Every other year since 2013

Prerequisites / co-requisites: graduate standing and a background in either power/communications engineering or computer science

Course Description: Communication and information technologies have taken an increasingly important role in monitoring and controlling physical systems. The electric power grid is a canonical example of a cyber-physical system in which the physical electrical grid is monitored by a network of sensors and other intelligent devices to continuously monitor, control, and dynamically manage the network to ensure near-perfect reliability. In contrast to the traditional grid in which generation, transmission, and distribution were 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 an array 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 an end-to-end communications, control, and computation (cyber) architecture integrated with the physical network.

In this course we will learn about electric power system operations specifically the core operations implemented in current state-of-the-art Energy Management Systems and evaluate their vulnerability to cyberattacks. We will also use an existing software platform with core EMS functionalities to test attacks. The second part of the course will focus on machine learning based methods to design better anomaly detectors that go beyond state of the art to enable both event-based and malicious data changes. The course will involve several guest lecturers with expertise in SCADA systems, cyberattacks, distributions systems, PMUs, and data analytics.

The material for the course will be based on reading current literature and class discussions. **A background in either power systems or communication systems is desirable but not required**. The aim is to introduce the appropriate concepts to both audiences and enable interactions and discussions. **This is a project-based course and will involve Matlab-based implementations.**

Topical Coverage:

- Introduction to Cyber-Physical Systems (CPS)
- The Power Grid
- Grid Sensing and Data collection Methods: SCADA, PMU
- What is Cybersecurity in the context of power systems? Is this a real threat?
- Operations: Computation/Cyber Aspects of the Grid –State Estimation (SE), Real-time Contingency Analysis, Security-constrained Economic Dispatch
- Cyber-Security in the Smart Grid: Network attacks: STUXNET, Ukraine, False data injection attacks on SE, effect of attacks on grid operations
    - Attack design
    - Vulnerability analysis
- Countering Data Issues: Machine Learning Countermeasures/Analytics: the need for better bad data detectors, **using machine learning methods** such as SVM, nearest neighbor, recurrent neural networks, and LSTMs to design enhanced BDDS that include anomaly detectors for real-time situational awareness