Cyber Security for Smart Grids

❖ *Module Outline*

Smart grid security is crucial to maintain stable and reliable power system operation during the contingency situation due to the failure of any critical power system component. Ensuring a secured smart grid involves with a less possibility of power grid collapse or equipment malfunction. Due to lack of the proper security measures, a major blackout may occur which can even lead to a cascading failure. Therefore, to protect this critical power system infrastructure and to ensure a reliable and an uninterrupted power supply to the end users, smart grid security issues must be addressed with high priority. In a smart grid environment, electric power infrastructure is modernized by incorporating the current and future requirements and advanced functionalities to its consumers. To make the smart grid happen, cyber system is integrated with the physical power system. Although adoption of cyber system has made the grid more energy efficient and modernized, it has introduced cyber-attack issues which are critical for national infrastructure security and customer satisfaction. Due to the cyber-attack, power grid may face operational failures and loss of synchronization. This operational failure may damage critical power system components which may interrupt the power supply and make the system unstable resulting high financial penalties. In this chapter, some recent cyber-attack related incidents into a smart grid environment are discussed. The requirements and the state of the art of cyber security issues of a critical power system infrastructure are illustrated elaborately.

Smart grid is referring to the next generation of power systems that should and will replace the existing power system grids through intelligent communication infrastructures, sensing technologies, advanced computing, smart meters, and renewable energy resources. Features of the smart grid must meet requirements as high efficiency, reliability, sustainability, flexibility, and market enabling. But, the growing dependency on information and communication technologies with its applications and uses has led to new threats to discuss and to try to resist against them.

A smart grid is an electrical grid that uses information and communications technology to gather and act on information, such as information about the behaviors of suppliers and consumers, in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity.Smart grids are now being used in electricity networks, from the power plants all the way to the consumers of electricity in homes and businesses. The “grid” amounts to the networks that carry electricity from the plants where it is generated to consumers. The grid includes wires, substations, transformers, switches etc. The major benefits are significant improvement in energy efficiency on the electricity grid as well as in the energy users’ homes and offices.

Communication and information technologies are taking an increasingly important role in monitoring and controlling physical systems. The smart grid is an example of a cyber-security (CS) 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.

This course is mainly including the following topics:

1. Cyber security and privacy.
2. Computation challenges in the smart grid/renewable energy.
3. Distributed approaches to data processing in the grid.
4. Large data sets: modeling, analysis, communication, compression, storage, and security.
5. ICS and SCADA is playing a vital role in a smart grid infrastructure.

Module Objectives

The Cyber Security for Smart Grids is designed to:

1. To understand and use different optimization methods to optimize the management in a smart grid.
2. To understand and use different algorithms to improve security and privacy in a smart grid.
3. To introduce communication, networking, and sensing technologies involved with the smart grid, and the main advantages:Self-healing , Motivates and includes the consumer, Resists attack, Increases power quality, Accommodates all generation and storage options, Enables electrical markets, Optimizes assets and operates efficiently
4. To understand and use different algorithms to improve security and privacy in a smart grid.
5. To introduce the computational techniques involved with the smart grid (decision support tools and optimization).
6. To understand the scientific and technical challenges in realizing the smart grid vision.
7. To be able to apply this knowledge in analysis and problem solving of smart grid architectures needs and challenges.

❖ *Learning Outcomes*

The learning outcomes of this course include understanding the main issues of smart grid development and the critical technologies that underpin such development, their principles, physical constraints, Cybersecurity, privacy and technological potentials. At the end of the module, students will be able to:

1. List and classify the basic terms of a Power System Grid.
2. Explain the importance and objectives of the various dispersed generation units as well as that of the various energy management policies.
3. Describe and classify the modern and innovative application fields of dispersed generation units.
4. Describe by drawing a block diagram and explain the operation of the basic part of a smart grid, quantify its operational, financial and environmental advantages using charts.
5. Identify the telecommunication infrastructure needed for its operation.
6. Identify the role of cyber security and privacy in smart grid.

❖ *Module Contents*

Chapter 1: Smart Grid Network Architecture

- Bulk and distributed generation architectures
- Transmission and distribution architecture
- Advanced metering architecture
- In-home systems
- Micro-grids
- System interdependencies
- Protocols

Chapter 2: Hacking the Smart Grid

- Identifying a target
- Vulnerability
- Attack tools
- Attack methods

- Introduce cyber-attack issues which are critical for national infrastructure security and customer satisfaction.
- State of the art of cyber security issues of a critical power system infrastructure are illustrated elaborately.

Chapter 3: Privacy Concerns with the Smart Grid

- Privacy risks associated with the Smart Grid
- Privacy impact assessment
- Mapping security requirements to Smart Grid environments
- NISTIR 7628 Smart Grid cyber security architecture
- EU M/490 and the SGCG reference architecture for the Smart Grid

Chapter 4: Security Models for SCADA, ICS, and Smart Grid

- Safe enablement through smart policies
- Application controls
- User Controls Network Control
- Remote user of smart grids

Chapter 5: Securing the Smart Grid

- Implementing security control within Smart Grid endpoints
- Establishing strong boundaries and zone separation
- Protecting data and applications within the Smart Grid
- Situational awareness

Chapter 6: The Future of Grid

- The challenge of making predictions
- Value of personal data
- Future cyber security considerations

❖ *References*

1. The Smart Grid Interoperability Panel –Cyber Security Working Group, "Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements", August 2010
2. Cyber Security of Smart Grid Infrastructure. Available from: https://www.researchgate.net/publication/259764406_Cyber_Security_of_Smart_Grid_Infrastructure [accessed Feb 23 2019].
3. Haoming Liu; Xingying Chen; Kun Yu; YunheHou; , "The Control and Analysis of Self-Healing Urban Power Grid," , IEEE Transactions on Smart Grid, vol.3, no.3, pp.1119-1129, Sept. 2012
4. Yilin Mo; Kim, T.H.-H.; Brancik, K.; Dickinson, D.; Heejo Lee; Perrig, A.; Sinopoli, B., "Cyber–Physical Security of a Smart Grid Infrastructure," Proceedings of the IEEE , vol.100, no.1, pp.195-209, Jan.
5. The Smart Grid Interoperability Panel Cyber Security Working Group, "Introduction to NISTIR7628 Guidelines for Smart Grid Cyber Security", September 2010, online:http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf
6. S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system", in Proc. Power Energy Soc. General Meeting, Jul. 2010
7. Wen-Long ChinChun-Hung LeeTaoJiangTao Jiang. Blind False Data Attacks Against AC State Estimation Based on Geometric Approach in Smart Grid Communications, November 2018, IEEE Transactions on Smart Grid 9(6):6298-6306.