Proposal for ISIE 2021 Tutorial

Title of Tutorial:

Cyber Security for Smart Grids

Contact Information of Speakers:

Dr. Shantanu Chakrabarty
Affiliation: Department of Computer Science, National University of Singapore, Singapore
Address: 3 Research Link, #03-02, Singapore 117602
TEL: +65 9359 5377
e-mail: dcsshch@nus.edu.sg

Dr. Biplab Sikdar (corresponding speaker)
Affiliation: Department of Electrical Engineering, University of A, Country
Address: 4 Engineering Drive 3, E4-05-32, Singapore 117583
TEL: +65 6516 2291
e-mail: bsikdar@nus.edu.sg
personal website: https://www.ece.nus.edu.sg/stfpage/bsikdar

Background of Speakers:

Shantanu Chakrabarty
- Cybersecurity of smart grids
- Power systems and smart grid analysis and planning
- Critical infrastructure cybersecurity

Biplab Sikdar
- Cyber-physical system security
- Internet of Things
- Computer network protocols

Brief description of the tutorial (500 words max):

Power grids around the world have embarked on a modernization process to transform themselves into "smart" grids by integrating a wide range of advanced computing, communications and industrial control technologies. The resulting integration of information technology (IT) and operation technology (OT) networks also open up power grids to cyber threats, and recent cyber-security incidents that have caused large-scale power outages have highlighted the importance and urgency of securing power grids against cyber-attacks. This tutorial is intended to provide the attendees with a

comprehensive overview of the cyber-security issues faced by smart girds, techniques and solutions for addressing them, and future research directions. This tutorial will start with an overview of cyber-threats faced by smart grids, the nature of adversaries, and common vulnerabilities. Next, the tutorial will focus on securing power grid control and operation against false data and malicious command injection attacks, and present defence mechanisms against such attacks. Finally, the tutorial will discuss practical aspects of securing smart grids as well as open problem and the future possibilities in attacks and countermeasures.

This is divided into three parts. The topics covered in each part are listed below.

- Part 1 (30 min + 5 min Q&A): Introduction to security for smart grids (Dr. B. Sikdar)
  - Attacks, motives, and vulnerabilities
  - Security models for SCADA, ICS, and smart grids
  - Case study: Attacks on the Ukrainian power grid
- Part 2 (35 min + 5 min Q&A): Securing power grid operation and control (Dr. S. Chakrabarty)
  - Taxonomy of attacks on grid operation and control
  - False data injection attacks and methods to detect them
  - Malicious command injection attacks and methods to detect them
- Part 3 (30 min + 5 min Q&A): Applied cyber security for smart grids (Dr. B. Sikdar)
  - Implementing security control within a smart grid
  - Protecting data and applications
  - Case study: defending against Shamoon
  - Future directions in cyber security considerations and countermeasures

Each of the parts will be followed by a question and answer session.

Biography:

Dr. Shantanu Chakrabarty obtained B.E degree in Electrical Engineering from University College of Engineering (Autonomous), Osmania University in 2010 and M.E degree in Electrical Engineering from Indian Institute of Science Bangalore in 2012 with Power Systems as the specialization. He then obtained Ph.D. from Indian Institute of Science Bangalore in 2018. The thesis was concerned with the development of algorithms for adjusted load flow solutions which comes under the area of power systems analysis and planning. Currently, he is working as a research fellow in the Department of Computer Science, National University of Singapore. His present research is centered around cybersecurity of smart grids. The research broadly covers analysis of vulnerabilities of smart grids to cyber-attacks and the subsequent development of protection schemes to protect smart grids from such threats. His areas of interest presently include power systems and smart grid analysis, cybersecurity of smart grids, and critical infrastructure cybersecurity.

Prof. Biplab Sikdar is currently a vice-dean in the Faculty of Engineering at the National University of Singapore and is a member of the Department of Electrical and Computer Engineering. He received the B. Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He was an Assistant Professor from 2001-2007 and Associate Professor from 2007-2013 in the Department of Electrical, Computer, and Systems Engineering at Rensselaer Polytechnic Institute from 2001 to 2013. He is a recipient of the

NSF CAREER award, the Tan Chin Tuan fellowship from NTU Singapore, the Japan Society for Promotion of Science fellowship, and the Leiv Eiriksson fellowship from the Research Council of Norway. His research interests include IoT and cyber-physical system security, network security, and network performance evaluation. Dr. Sikdar is a member of Eta Kappa Nu and Tau Beta Pi. He served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012 and as an Associate Editor for the IEEE Transactions on Mobile Computing from 2014-2017.

Brief description of the intended audience

The intended audiences for this tutorial includes practitioners and academics in the broad area of power grids. The tutorial intends to provide the audience with an overview of security issues faced by power grids as they modernize and familiarize them with the best practice in defense strategies. It will also provide students and young researchers in the audience with possible

Support technical committee in IES (if any)

Support from the TC on Resilience and Security for Industrial Applications has been sought and we are awaiting a reply.