Cybersecurity for the Smart Grid

Charalambos Konstantinou
Florida State University
konstantinou@caps.fsu.edu

Saraju P. Mohanty
University of North Texas
saraju.mohanty@unt.edu

Introduction

The security and well-being of societies and economies are tied to the reliable operation of power systems. Due to the advancements of information and communication technologies (ICT), the traditional electric grid is evolving towards an intelligent smart grid. Smart grid is essentially a cyber-physical system (CPS) which can be called energy CPS (E-CPS) that integrates computing, communication, and control (3Cs) capabilities with the physical world of traditional grid. Despite the reliability and efficiency benefits, the inadequate level of security measures is leading to a greater threat landscape. Securing smart grid environments presents numerous challenges that need to be considered; smart grids are heterogeneous interconnected systems, and this heterogeneity and diversity necessitate non-static, application specific methods able to capture the complex interrelationships of various elements. It is estimated that the financial loss to the US economy cause by malicious cyberattacks is estimated between $57 and $109 billion in 2016. Despite existing efforts, more focus is required on interoperable, cost-recovery, effective, and insurance mechanisms able to help guide further regulations and standards in this area. Such strategies need to ensure that technical solutions can “understand” interdependencies, integrate expertise from the engineering and cybersecurity communities, reduce institutional and policy barriers, and prioritize specific recommendations which can address the interoperability issues between technical, management, and policy-oriented approaches.

Therefore, this special issue intends to appraise recent developments in the smart grid cybersecurity field and address related challenges related to the practical, theoretical and engineering aspects of developing and deploying smart grid cybersecurity mechanisms while ensuring integration into policy and management solutions. The special issue consists of a set of selected articles and is aimed at engineers, scientists, researchers, educators, students, industrial experts, and other stakeholders who are engaged in smart grid cybersecurity research and education.

Scanning Articles for the Special Issue

The article on “Denial of Service Resilient Framework for Synchrophasor Based Wide Area Monitoring Systems” by Chawla, Agrawal, Singh, Panigrahi, Paul, and Bhalja presents a cyber-attack detection and resilient framework for the synchrophasor based Wide Area Monitoring System (WAMS) implemented on a testbed with real time digital simulator. The framework can assist in detection and mitigation of the impact of the data unavailability due to denial of service (DoS) attacks or communication failure. It can also identify the root cause of data unavailability using a signature-based method.

The article on "Privacy-Preserved Optimal Energy Trading, Statistics and Forecasting for a Neighborhood Area Network" by Smith, Wang, Ding, Chan, Spak, Guan, Tyler, Rakotoarivelo, Lin, and Abbasi presents a Stackelberg game with equilibrium in a three-party neighborhood area network, with a further enabler of open access to residents and other operators of privacy preserved data. The system is demonstrated using real residential net energy usage data and a real-time user-interface prototype that the community storage operator could provide to prosumers, further incentivizing participation in the residential smart grid.

The article on "Leveraging Data-Centric Edge Computing to Defend IoT- based Attacks in Power Grids" by Shrestha and Lin introduces data-centric edge computing to deploy defenses in Internet-of-things (IoT) networks, integrating the knowledge of physical states within decentralized regions of Supervisory Control and Data Acquisition (SCADA) systems.

The article on "Cyber-Physical Power System Resilience Testbed: Architecture and Applications" by Khan, Palomino, Brugman, Giraldo, Kasera, and Parvania presents a testbed to implement, test, verify, and evaluate cyber-physical resilience solutions for power systems integrated with a software defined networking-based communication infrastructure. Different attack scenarios are demonstrated for testing anomaly detection in the testbed and to analyze the interdependency between the communication network and the physical power system operation.

The article on "Attacks on Electricity Markets" by Barreto, Neema, and Koutsoukos demonstrates how an adverse generator can compromise the bids of smart appliances to manipulate the market clearing price and profit. The authors also present a mitigation strategy that drops some of the bids to correct the impact of the attack.

The article on "Sensitive Detection of GPS Spoofing Attack in Phasor Measurement Units via Quasi-Dynamic State Estimation" by Xie and Meliopoulos discuss how time-stamped measurements using the global positioning system (GPS) can be spoofed by malicious attackers. The authors propose the use of a quasi-dynamic state estimator to detect GPS spoofing attacks and recover from the attack. The estimator requires the grid topology, transmission line models, and the dynamic electromechanical models of generators and motors in order to reliably detect GPS spoofing.

Acknowledgements

We would like to thank all the authors for their valuable contribution to this special issue. We would like also to acknowledge and thank the reviewers for their valuable and timely efforts to ensure the high quality of the papers. We hope that this special issue will serve as a valuable resource for the research community.

Guest Editors' Bio

Charalambos Konstantinou is an Assistant Professor in Electrical and Computer Engineering, at the FAMU-FSU College of Engineering and the Center for Advanced Power Systems (CAPS), Florida State University (FSU), Tallahassee, FL, USA. Contact him at konstantinou@caps.fsu.edu.

Saraju P. Mohanty is the Editor in Chief of the IEEE Consumer Electronics Magazine and Professor in the Department of Computer Science and Engineering (CSE), University of North Texas (UNT), Denton, TX, USA. Contact him at Saraju.Mohanty@unt.edu.