COVER FEATURE **GUEST EDITORS' INTRODUCTION**

Cybersecurity for the Smart Grid

Charalambos Konstantinou, Florida State University

Saraju P. Mohanty, University of North Texas

Digital Object Identifier 10.1109/MC.2020.2975901
Date of current version: 7 May 2020

0018-9162/20©2020IEEE

Smart grid security measures have proven to be inadequate to deter costly malicious cyberattacks. The six articles in this theme issue focus on challenges in developing stronger cybersecurity measures for the smart grid.

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, the traditional electric grid is evolving toward an intelligent smart grid. A smart grid is essentially a cyberphysical system (CPS) that can be called an *energy CPS*, integrating computing, communication, and control capabilities with the physical world of the traditional grid. Despite the reliability and efficiency benefits, the inadequate level of security measures in the smart grid is leading to a greater threat landscape.

Securing a smart grid environment presents numerous challenges that need to be considered; smart grids are heterogeneous interconnected systems, and this heterogeneity and diversity necessitate nonstatic, application-specific methods able to capture the complex interrelationships of various elements. The financial loss to the U.S. economy caused by malicious cyberattacks is estimated to be between US$57 and US$109 billion in 2016. Despite existing efforts, more focus is required on interoperable, effective, cost-recovery, 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 that can address the interoperability issues between technical, management, and policy-oriented approaches.

The intent of this theme issue of *Computer* is to appraise recent developments in the smart grid cybersecurity field and address 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 articles are directed toward engineers, scientists, researchers, educators, students, industrial experts, and other stakeholders who are engaged in smart grid cybersecurity research and education.

[DUE TO THE ADVANCEMENTS OF INFORMATION AND COMMUNICATION TECHNOLOGIES, THE TRADITIONAL ELECTRIC GRID IS EVOLVING TOWARD AN INTELLIGENT SMART GRID.]

ABOUT THIS ISSUE

In "Denial-of-Service Resilient Frameworks for Synchrophasor-Based Wide Area Monitoring Systems," Chawla et al. present a cyberattack detection and resilient framework for the synchrophasor-based wide area monitoring system implemented on a testbed with a real-time digital simulator. The framework can assist in the detection and mitigation of the impact of data unavailability due to denial of service attacks or communication failure. It can also identify the root cause of data unavailability using a signature-based method.

The next article, "Privacy-Preserved Optimal Energy Trading, Statistics, and Forecasting for a Neighborhood Area Network," by Smith et al., 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.

"Data-Centric Edge Computing to Defend Power Grids Against IoT-Based Attacks," 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 systems.

The article "The Cyberphysical Power System Resilience Testbed: Architecture and Applications," by Khan et al., presents a testbed to implement, test, verify, and evaluate cyberphysical 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 analyzing the interdependency between the communication network and the physical power system operation.

In "Attacking Electricity Markets Through IoT Devices," Barreto et al. demonstrate 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.

In the last feature article, "Sensitive Detection of GPS Spoofing Attack in Phasor Measurement Units via Quasi-Dynamic State Estimation," Xie and Meliopoulos discuss how time-stamped measurements using 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 them. The estimator requires the grid topology, transmission-line models, and dynamic electromechanical models of generators and motors to reliably detect GPS spoofing.

We thank all of the authors for their valuable contributions to this theme issue. We would also like to thank the reviewers for their valuable and timely efforts to ensure the high quality of these articles. We hope that this issue of *Computer* will serve as a valuable resource for the research community.

ABOUT THE AUTHORS

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, Florida State University, Tallahassee. His research interests include cyberphysical and embedded systems security with a particular focus on power systems. Konstantinou received a Ph.D. in electrical engineering from New York University. He is the recipient of the SCEE Young Faculty Development Award 2019 as well as the best paper award at VLSI-SoC 2018. He is a Member of the IEEE. Contact him at konstantinou@caps.fsu.edu.

SARAJU P. MOHANTY is the editor-in-chief of *IEEE Consumer Electronics Magazine* and a professor in the Department of Computer Science and Engineering, University of North Texas, Denton. His research focus is in smart electronic systems. Mohanty received a Ph.D. in computer science and engineering from the University of South Florida. He has authored 300 research articles and four books and has four U.S. patents. He received 11 best paper awards. He is a Senior Member of the IEEE. Contact him at Saraju.Mohanty@unt.edu.