Guest Editorial: Privacy and Security in Smart Grids

Originally published in:
IET Smart Grid 3(5), https://doi.org/10.1049/iet-stg.2020.0209

IET Smart Grid

Special Section: Privacy and Security in Smart Grids

IET Journals
The Institution of Engineering and Technology

Guest Editorial: Privacy and Security in Smart Grids

eISSN 2515-2947
E-First on 15th October 2020
doi: 10.1049/iet-stg.2020.0209
www.ietdl.org

A smart grid is an advanced electricity network that tightly couples cyber and physical aspects through advanced monitoring, information processing and bi-directional communication technologies. While advanced monitoring and communication technologies make the grid 'smarter', they also introduce new vulnerabilities. Smart grids are complex and extensive critical infrastructures and they are under constant threat from a wide range of attacks, including data theft, false data injection, denial of service attacks, malware attacks, energy theft, as well as coordinated and distributed versions of these attacks. Successful attacks on smart grids can cause significant economic and social damage through power outages, damage to infrastructure, energy theft and waste. Therefore, it is essential to detect physical as well as cyber attacks before they result in cascading failures in the network. Privacy is another growing concern for the future of smart grids. The smart aspect of the grid requires near real time monitoring of the grid state, including consumer demand and response behaviour through smart meters, to increase the resilience and reliability of the grid. However, with advances in machine learning and data mining technologies, such fine-grained information about user activity can easily provide sensitive information about individual consumers, threatening their privacy. Consumer privacy must be protected not only against third-party attackers, but also against the legitimate energy providers and grid operators, making it a highly difficult challenge.

This Special Section brings together papers that study security and privacy issues in smart grids with the goal of developing information technologies that can provide the necessary security and reliability to the grid without sacrificing consumer privacy. Aligned with the interdisciplinary nature of security and privacy challenges in smart grids, we bring together papers from a wide range of research areas including power systems, machine learning, statistical estimation and optimisation.

Papers in this Special Section

In 'Detecting load redistribution attacks via support vector models', Chu *et al.* investigate an emerging and important problem in smart grids, the detection of cyberattacks. While traditional model-based detection techniques have been proven inadequate in identifying stealthy type attacks, the authors propose a machine-learning based detection framework by combining a support vector regression load predictor with a support vector machine attack detector, which is demonstrated to be effective in detecting both random and intelligently designed load redistribution attacks. Along with other recent publications, this paper highlights the opportunity of applying machine learning-based methods for cybersecurity enhancement in smart grids.

In the paper 'Modern power system reliability assessment with cyber-intrusion on heat pump systems', Gunduz and Jayaweera develop a novel framework to extend traditional physical-only power system reliability assessment to explicitly consider the growing interactions between cyber and physical networks. Case studies demonstrate that the cyber-intrusion, detection, and recovery processes can significantly affect the overall system reliability, which highlights the need to include cyber-physical interactions in the quantitative assessment of system reliability in smart grid.

Another paper dealing with the limitations of classical physics-based data detection methods in detecting cyber attacks on smart grids is 'Ensemble CorrDet with adaptive statistics for bad data detection' by Nagaraj *et al.* Existing data-driven methods are based on learning the statistics of a 'normal' grid operation to detect anomalies. However, these statistics continuously change in smart grids with the variations of loads and generation. To tackle these variations, they propose an adaptive data-driven anomaly detection method, by using a IEEE118-bus system. Their experimental results show that the proposed adaptive technique outperforms the current state of the art for bad data detection.

In 'Survey of machine learning methods for detecting false data injection attacks in power systems', Sayghe *et al.* focus on false data injection attacks that can compromise state estimation in smart grid monitoring systems, and provide a comprehensive overview of recent machine learning based methods for detecting false data injection attacks. The paper provides background on smart grid state estimation, common false data injection attack, and their potential impacts on power systems. The authors also identify limitations of the existing machine learning techniques, and provide future research directions to remedy these limitations.

In 'Privacy-cost trade-offs in smart electricity metering systems', Giaconi *et al.* consider exploiting an energy storage device for the dual purposes of energy cost optimisation and privacy by demand shaping. While the goal in cost optimisation is to shift the demand to off-peak periods with lower energy cost, privacy is achieved by obtaining a fixed demand profile that is as independent as possible from the real consumption profile. An analytical optimisation framework is introduced to solve for the optimal energy management policy, and numerical results are presented characterising the optimal cost-privacy trade-off under various assumptions on the available information about the future energy demand profile.

This Special Section also includes a comprehensive survey paper on smart meter privacy by Farokhi titled 'Review of results on smart-meter privacy by data manipulation, demand shaping, and load scheduling'. In this survey paper, Farokhi classifies mechanisms to ensure smart-meter privacy into three categories: data manipulation, demand shaping, and load scheduling. The first category refers to methods that focus on manipulating smart meter readings before being communicated to utility providers and retailers. These include non-stochastic methods, such as aggregation, binning, and down sampling, as well as stochastic noise addition. Demand shaping and load scheduling refer to physical privacy enabling techniques, where smart-meter readings are communicated without any manipulation, but instead the consumption is altered by exploiting renewable energy sources, batteries, or by shifting loads with the intention to confuse an attacker that may try to infer consumer behaviour based on smart meter data. This survey paper not only reviews a comprehensive list of privacy-enabling techniques within each of these categories, but also provides a thorough survey and comparison of smart meter privacy measures adopted in the literature.

We hope that this collection of papers contributes to the ongoing research activities in this active research area. We also envisage that the papers in this Special Section will find applications in industry and contribute to policy discussions. A secure and reliable smart grid is essential for the future of our society, and we hope that this collection will help us achieve this critical goal.

Guest Editors Biographies

Deniz Gündüz is a Professor in the Electrical and Electronic Engineering Department of Imperial College London, UK. He serves as the Deputy Head of the Intelligent Systems and Networks Group, and leads the Information Processing and Communications Laboratory (IPC-Lab). He is also a part-time faculty member at the University of Modena and Reggio Emilia, and held visiting positions at University of Padova (2018–2020) and Princeton University (2009–2012). His research interests lie in the areas of communications and information theory, machine learning, and privacy. Dr. Gündüz is a Distinguished Lecturer for the IEEE Information Theory Society (2020–22). He has served in various editorial roles, including *IEEE Transactions on Communications*, *IEEE Journal on Selected Areas in Communications*, *IEEE Transactions on Wireless Communications*, and *IEEE Transactions on Green Communications and Networking*. He is the recipient of the IEEE Communications Society – Communication Theory Technical Committee (CTTC) Early Achievement Award in 2017, a Starting Grant of the European Research Council (ERC) in 2016, IEEE Communications Society Best Young Researcher Award for the Europe, Middle East, and Africa Region in 2014, Best Paper Award at the 2019 IEEE Global Conference on Signal and Information Processing (GlobalSIP) and the 2016 IEEE Wireless Communications and Networking Conference (WCNC), and the Best Student Paper Awards at the 2018 IEEE Wireless Communications and Networking Conference (WCNC) and the 2007 IEEE International Symposium on Information Theory (ISIT).

Tobias Oechtering is Professor in Information Science and Engineering at KTH Royal Institute of Technology, Stockholm, Sweden, and is also director of KTH research platform on Digitalization. He received his Dipl.-Ing in Electrical Engineering and Information Technology in 2002 from RWTH Aachen and Dr-Ing in Electrical Engineering in 2007 from TU Berlin, Germany. His research interests include communication and information theory, physical layer privacy and security, statistical signal processing and learning as well as networked control. Dr. Oechtering is currently senior editor of *IEEE Transactions Information Forensic and Security* and editor of MDPI journal *Entropy*. He was previously associate editor of *IEEE Transaction Forensic and Security* between 2016–20 and *IEEE Communication Letters* 2012–15. In 2019, he was general chair of IEEE Information Theory Workshop in Visby, Gotland. He received the 2009 Advancement Award from the Vodafone Foundation.

Gabriela Hug received an M.Sc. degree in Electrical Engineering in 2004 and the Ph.D. degree in 2008, both from the Swiss Federal Institute of Technology (ETH), Zurich, Switzerland. After the Ph.D. degree, she worked in the Special Studies Group of Hydro One, Toronto, ON, Canada, and from 2009 to 2015, she was an Assistant Professor in Carnegie Mellon University, Pittsburgh, PA, USA. She is currently an Associate Professor in the Power Systems Laboratory, ETH Zurich. Her research is dedicated to control and optimization of electric power systems.

Deepa Kundur is Professor & Chair of The Edward S. Rogers Sr. Department of Electrical & Computer Engineering at the University of Toronto. Her research interests lie at the interface of cybersecurity, signal processing and complex dynamical networks. She is an author of over 200 journal and conference papers and is also a recognized authority on cyber security issues. She has served in numerous conference executive organization roles including General Chair of the 2018 GlobalSIP Symposium on Information Processing, Learning and Optimization for Smart Energy Infrastructures, TPC Co-Chair for IEEE SmartGridComm 2018, Symposium Co-Chair for the Communications for the Smart Grid Track of ICC 2017, and General Chair for the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems at ACM e-Energy 2016. Professor Kundur's research has received best paper recognitions at numerous venues including the 2015 IEEE Smart Grid Communications Conference, the 2015 IEEE Electrical Power and Energy Conference, the 2012 IEEE Canadian Conference on Electrical & Computer Engineering, the 2011 Cyber Security and Information Intelligence Research Workshop and the 2008 IEEE INFOCOM Workshop on Mission Critical Networks. She has also been the recipient of teaching awards at both the University of Toronto and Texas A&M University. She is a Fellow of the IEEE, a Fellow of the Canadian Academy of Engineering, and a Senior Fellow of Massey College.

Mohammadreza Arani received his B.Sc. degree from Sharif University of Technology, Tehran, Iran (2009), his M.Sc. degree from the University of Waterloo, Waterloo, Canada (2012), and his Ph.D. degree from the University of Alberta, Edmonton, Canada (2017), all in Electrical Engineering. From 2012 to 2013, he worked as a research associate at the University of Waterloo. He was a NSERC post-doctoral fellow at the University of Toronto, Toronto, Canada from 2017 to 2019. He joined Ryerson University as an Assistant Professor in July 2019.

Fei Teng is a lecturer at the Imperial College London, Department of Electrical and Electronic Engineering within the Control and Power Research Group. He is currently serving as the education director of Energy Futures Lab and the deputy director of Imperial – Tsinghua Joint Research Centre for Intelligent Power and Energy Systems. He is also holding a visiting position at MINES ParisTech. His research focuses on the secure and resilient operation of the future cyber-physical energy systems. He is an Associate Editor for *IEEE Open Access Journal of Power and Energy*, *IET Energy Conversion*, and *Economics and Control Engineering Practice*.