***Editorial Article***

**Information Integrity in Smart Grid Systems**

**Al-Sakib Khan Pathan1, Zubair Muhammad Fadlullah2, Mostafa M. Fouda3, Muhammad Mostafa Monowar4, and Philip Korn5**

*1Computer Science Department, International Islamic University Malaysia, Malaysia*

*2Graduate School of Information Sciences (GSIS), Tohoku University, Japan*

*3Faculty of Engineering at Shoubra, Benha University, Egypt*

*4Faculty of Computing and Information Technology, King AbdulAziz University, Saudi Arabia*

*5Google Research, USA*

[sakib@iium.edu.my](mailto:sakib@iium.edu.my), [zfadlullah@ieee.org](mailto:zfadlullah@ieee.org), [mfouda@feng.bu.edu.eg](mailto:mfouda@feng.bu.edu.eg), [hemal.cu@gmail.com](mailto:hemal.cu@gmail.com), [flip@google.com](mailto:flip@google.com)

The smart grid is a modernized electrical grid that connects power generation, transmission, distribution, and consumers using information and communication technology. One of the key characteristics of the smart grid is its support for bi-directional information flow between the consumers of electricity and the utility provider. A critical twist on the current electrical grid system is that this kind of two-way interaction would allow electricity to be generated in real-time based on consumer demand and power requests. While the system would give users more control over electricity use and supply, many security issues are raised to ensure the information privacy of the users as well as authorization procedures for electricity use. Security loopholes in the system could, in fact, aggravate the electricity supply system instead of improving it. The quality of the information from the perspective of billing and accounting is also a major concern. In this special issue, our objective was to compile the latest advances in the fields of information assurance and information integrity in smart grid systems.

Though information integrity is a pillar of information security for many systems, a unified definition of information integrity does not exist. From a general point of view, it could be defined as ensuring reliable information output irrespective of any type of input. That is, the information produced by a system should be accurate enough to be relied on for the normal operation of the system. As 100% information integrity may not be guaranteed for any system, most of the companies and systems today try to adopt what is referred to as the *reasonable assurance*. In any smart grid system, an electricity provider must create accurate billing statements for users and supply electricity to users based on demand. Hence, accuracy in supply, billing, and usage demand must be ensured in some way. In the literature, the terms, *data* and *information* are often used interchangeably. However, while dealing with actual usage of electricity and billing issues, we have to differentiate among the terms: *data*, *information*, and *knowledge*. While data means the raw readings or numbers or values, information would be the processed meaning of that. Knowledge in this context is the interpreted information as it should be understood for a particular case. Knowledge about the entire smart grid system is essential for the company to operate with efficiency.

As the smart grid system is sensitive in the sense that the users’ privacy must be maintained in the entire process while some data should be made available to the law enforcement agencies to ensure national security, the critical questions that arise in such a system are:

* Who are the people responsible to store and manage the master files, sales information, and account information of the users?
* Who is in charge of coordinating and reconciling data for the entire system? Is it a distributed task or centralized? If distributed, how is the integrity maintained within the system?
* Who ensures appropriate control and management of data to be made public or to be kept secret?
* If the users control their own data and usage information, are they parts of the system? Then, who ensures the integrity of the users in the process? If not, how does the system manage the balance between data privacy and user accountability?

Our intention for this special issue was to encourage researchers to discuss all these issues related to information integrity and security services in the smart grid. Given these objectives, after our initial call for papers, we received 22 submissions from around the globe. After a rigorous review process, keeping the theme of the special issue intact, we have accepted only 9 of these submissions. Below, we present the summary of the contributions selected for this special issue:

Detecting the lack of a reference system security model for smart grid, Suleiman, H. et al. in their paper, “*Integrated Smart Grid Systems Security Threat Model*”, present an integrated approach of various reference models. They perform an extensive analysis of system security requirements, threats, and vulnerabilities, and present a comprehensive Systems Security Threat Model (SSTM) for the smart grid environment.

The paper entitled, “*Short Term Power Load Prediction with Knowledge Transfer*” by Zhang, Y. and Luo, G. proposes a novel transfer learning method to solve the power load forecast problems in the smart grid. Forecasting power load is a vital issue for smart grid management as accurate forecast can greatly reduce the operational cost of power systems. The authors in this work claim to improve the prediction accuracies by using the knowledge transferred from nearby cities, avoiding negative knowledge transfers by correct source task selection, and reducing the time complexity of the prediction inferences.

Kessler, S. et al. in their paper, “*Allocative and Strategic Effects of Privacy Enhancement in Smart Grids*” characterize both theoretically and numerically the effect of privacy mechanisms applied in a local energy market scenario. The model presented in the work considers demand side flexibility as well as energy storage systems. The core finding is that privacy enhancement methods are applicable in local energy markets including private households. The authors note as a conclusion, “*From an economic perspective, the negative allocative effects are low and controllable while privacy enhancement significantly increases the privacy protection of participating individuals. From a computer science perspective, these markets are a meaningful performance indicator for the utility of privacy enhancement methods.*”

Shafiei, H.et al. in their contribution entitled, “*An Effective Countermeasure Against Traffic Analysis Attacks in Wide Area Measurement Systems*” look into the various effective countermeasures against severe kinds of security attacks with a particular focus on traffic analysis attacks in a wide area measurement system like smart grid. The core idea is to obfuscate the network traffic to make it undetectable by the adversary. The authors present a mathematical model to point out the effects of various contributing parameters and show the efficiency of their approach through simulation experiments.

The paper, “*A Hierarchical Optimization Model for Energy Data Flow in Smart Grid Power Systems*” by Jarrah, M. et al., as understood from its title, presents a hierarchical optimization model for energy data flow in the smart grid environment. The proposed approach has mainly three levels of hierarchy where at level one, a single home or a group of homes are combined to form an Optimized Power Entity (OPE) that may satisfy its load demand from its own renewable energy sources. At level two, a group of OPEs satisfies energy requirements of all OPEs within the group. And finally at level three, any surplus renewable energy from different groups along with the energy from the grid is used to fulfill unsatisfied demands, and the remaining energy is sent to other storage devices.

Anwar A. et al.’s work entitled, “*Identification of Vulnerable Node Clusters against False Data Injection Attack in an AMI based Smart Grid*” presents a study of the physical characteristics of the power system, and shows the relationship between the system stability indices and the false data injection attacks. The authors investigate the interdependent nature of nodes in the power grids and utilize a method based on the voltage stability index to identify node characteristics in terms of voltage collapse.

Nabeel, M. et al.’s work, “*Scalable End-to-End Security for Advanced Metering Infrastructures*” presents a basic key management scheme and a broadcast group key management scheme based on PUF (Physically Unclonable Function) devices for secure end-to-end communication in AMIs (Advanced Metering Infrastructures) – that is to assure confidentiality and integrity of messages and strong authentication of smart meters. PUF is basically a physical entity that is embodied in a physical structure and is usually easy to evaluate but hard to predict.

Abuadbba, A. and Khalil, I. contribute the paper entitled, “*Wavelet Based Steganographic Technique to Protect Household Confidential Information and Seal the Transmitted Smart Grid Readings*” in which, they propose a novel secure steganographic algorithm to protect confidential smart grid information by hiding them randomly bit-by-bit inside the transmitted normal readings using a generated key.

Finally, Lee, B. et al. note in their paper, “*Role-Based Access Control for Substation Automation Systems Using XACML*” that there is a genuine need for accessing data of internal equipment and devices of a substation system from external systems as power grids continue to evolve. Hence, they propose a novel approach for implementing role-based access control based on IEC 62351standard for substation automation using eXtensible Access Control Markup Language (XACML).

There is a very balanced contribution of different aspects of information integrity in the papers included in the special issue. Hence, we hope that the works would be of interest to the researchers working on the relevant areas.

**The Guest Editors**

**Al-Sakib Khan Pathan, Ph.D.**

Computer Science Department, International Islamic University Malaysia, Malaysia

Email: sakib.pathan@gmail.com, spathan@ieee.org

**Zubair Muhammad Fadlullah, Ph.D.**

Graduate School of Information Sciences (GSIS), Tohoku University, Japan

Email: zfadlullah@ieee.org

**Mostafa M. Fouda, Ph.D.**

Faculty of Engineering at Shoubra, Benha University, Egypt

Email: mfouda@feng.bu.edu.eg, mfouda@ieee.org

**Muhammad Mostafa Monowar, Ph.D.**

Faculty of Computing and Information Technology, King AbdulAziz University, Saudi Arabia

Email: hemal.cu@gmail.com

**Philip Korn, Ph.D.**

Google Research, USA

Email: flip@google.com