Integrated Learning Environment for Smart Grid Security

Kewen Wang, Yi Pan, Wen-Zhan Song
Department of Computer Science
Georgia State University
Atlanta, USA
kwang12@student.gsu.edu, {yipan, wsong}@gsu.edu

Weichao Wang
Department of SIS
UNC Charlotte
Charlotte, USA
weichaowang@uncc.edu

Le Xie
Department of Electrical and Computer Engineering
Texas A&M University
College Station, USA
Lxie@ece.tamu.edu

***Abstract*— Cyber Security of smart grids becomes more and more important to our everyday life for its wide implication in power systems, a critical infrastructure in a modern society. Many universities and corporations have put efforts in this field. However, there has been lack of emphasis on educational front of this important area. We believe that simulation systems designed for research purposes in the smart grid security should also be incorporated in education. Hence, this paper presents an integrated learning environment for the education of smart grid security. The core components of this environment are smart grid simulator and a learning website. Based on this learning environment, we design course projects and learning materials in teaching, so that students can better grasp the knowledge of smart grid security.**

Keywords-Cyber Security; Smart Grid Education; Learning Environment.

I. INTRODUCTION

With the widespread applications of smart grid, its security has raised significant interest and concerns among industries and academia [1]. A Department of Homeland Security report [2] shows that the vulnerability in smart meters and smart controllers could allow attackers to remotely compromise thousands of such devices and cause rolling blackout, which is a great threat to our everyday life. Significant efforts have been put on the research of such critical infrastructure services, with the example of several critical infrastructure research centers being established nationwide [3].

In contrast with strong emphasis on research in smart grid cyber security, the education programs fall behind in many aspects. For example, there is a lack of smart grid simulation software which provides a platform covering the essential components of corresponding security educational programs for teachers and students. Although some systems about the cyber security of smart grid become available for research purposes [4][5][6][7], few of them are suitable for education purposes because their software environment and programming interfaces are not available to students and instructors. The lack of this learning environment brings a huge difficulty for the education on smart grid security, which could train many people into fast developing industry [8][9] of smart grid and teach students necessary knowledge in this field.

Thus, it will be beneficial to solve this problem by developing a learning environment for the security of smart grid. In this paper, we propose an integrated smart grid learning environment for the purpose of smart grid security education and describe several course projects and learning materials using this learning environment. Section II presents the overview of this learning environment; Section III describes the details of the course projects using this learning environment; Section IV illustrates the learning materials available in the environment; Section V concludes the paper.

II. OVERVIEW OF LEARNING ENVIRONMENT

This learning environment mainly consists of two components: smart grid emulator and a learning website. This smart grid emulator is named Smart-Grid Common Open Research Emulator (SCORE). It provides a platform for emulating smart grid environment [10], and running real smart grid applications by applying virtualization techniques. This emulator SCORE needs to be installed in Linux environment, and operated by some related commands.

This process of installation and operation may be not easy for the students without computer science background, so we design a website for users to facilitate the access to this smart grid emulator. This website shown in Figure 1 provides an easy interface for user to practice in smart grid environment without considering complicated software environment. It is convenient for students to apply smart grid simulation environment to run specified power grid model and obtain related power and communication security knowledge under this model. After registration through the website shown in Figure 2, users can access the emulator that need be installed in Linux environment. It presents the registration information required.

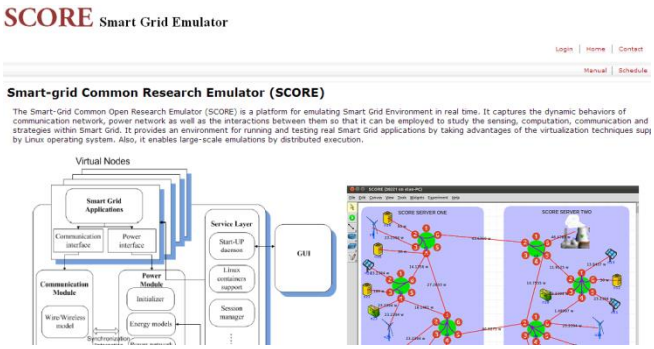

Figure 1. Website Display.

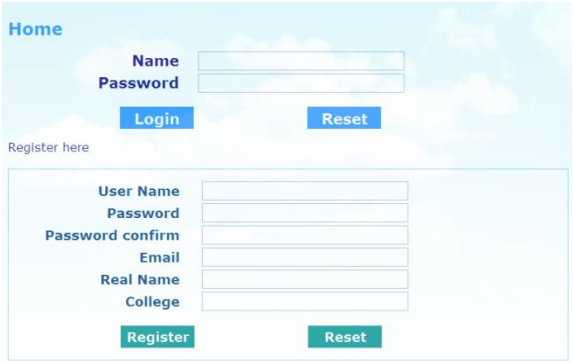

Figure 2. User Registration.

III. COURSE PROJECTS DESIGN

In this learning environment, we design several course projects to help students grasp related knowledge. In the projects, students are required to modify or write programs in the smart grid emulator to simulate the malicious attacks and obtain the resulting files showing the power network information. Moreover, in some projects, students are required to design counter attack plan to defend against such attacks.

A. Grid Topology Attack Project

After registering, user can access the schedule webpage shown in Figure 3. By clicking a time slot grid in this page, a new window will pop up to let user input some related information about reservation shown in Figure 4. After clicking "save" button, this task specified by the user will run in access the grid emulator during the time slot.

In this reservation window shown in Figure 4, a user can upload a configuration by clicking the "Choose File" button. If the user does not specify a file to upload, the system will use a default configuration file to run the smart grid emulator. Actually, this configuration file is *.imn type file. It is used to specify the grid topology information including node, power line and communication link information.

The alteration of this file could result in the change of the topology of the power grid, which is also the consequence of grid topology attack. In this project, we simulate the attack of damaging the current smart grid topology [11], by changing its topology configuration files. This project is shown in Figure 6. A new topology configuration of smart grid will result in a new smart grid topology.

During the running of smart grid, user can download the resulting log files, which display the dynamic power flow and network information. By clicking the reserved job in the schedule webpage shown in Figure 3, a new window will pop up to show the information of this running task shown in Figure 5. It displays the information about the task, and provides a link "ResultFile" to download the resulting log files.

Because a power system needs to balance demand and supply, some alterations of such configuration files may lead to the fluctuation of the whole power grid, which could be observed from its resulting log files.

Students are required to tamper with some topology configuration files and find out its impact on the stability of the whole power grid through comparing resulting log files before and after configuration files changing.

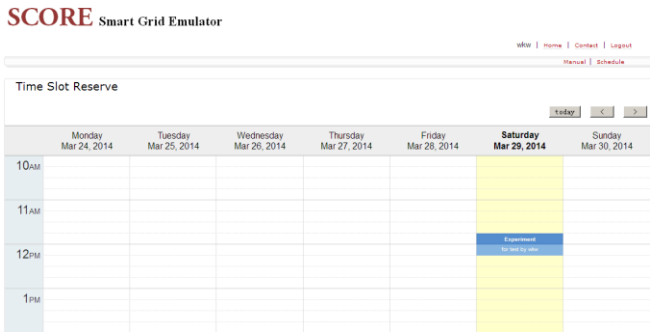

Figure 3. Schedule.

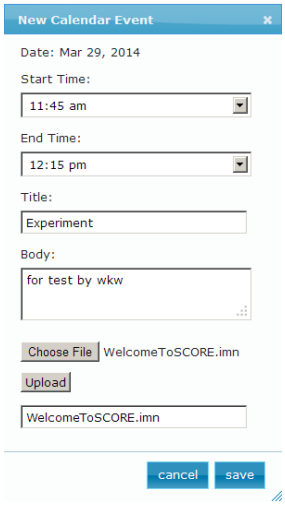

Figure 4. Time Slot Reserve.

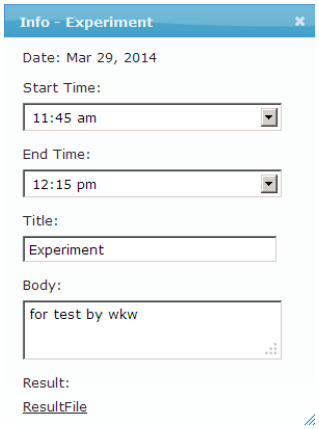

Figure 5. Result Information.

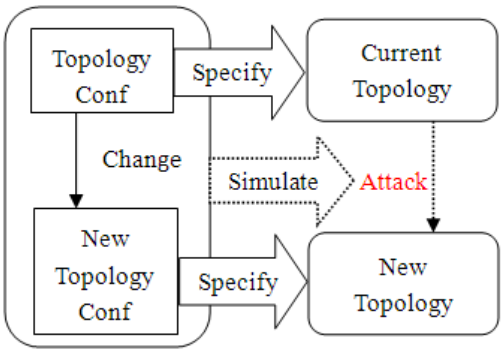

Figure 6. Topology Attack Project.

B. *Energy Model Attack Project*

Energy model specifies how the electrical appliances consume or supply the electrical power. Furthermore, user can customize energy model and run the system with your specified energy model by writing energy model programs and adding it to smart grid programs. It is possible to execute the energy model attack by overwriting the current energy model programs with the customized energy model programs. For example, modify the energy model to increase the power consumption of some electrical appliances may lead the whole power out of supply.

In this project, we implement the attack of altering the energy model of smart grid elements such as generator by modifying current energy model. This process is shown in Figure 8. Students are required to modify the sample program written in C++ to implement a new energy model. The main part of the sample program is shown in Figure 7. This sample program is running in the Smart grid emulator SCORE, and it specifies the energy model for appliances in the Smart Grid. Users can modify this sample code to implement their customozed energy model.

```
int main(intargc, char**argv) {
stringself_id = string(argv[1]); //use this to get the node id.
pid_tpid;
pid = getpid();
EnergyDaemoned(self_id); // init aenergydaemon using the node id.
        while (1){
        /* You can use the interfaces in EnergyDaemon.h
        * to implement your energy modeland interact with
    * the emulation environmenthere
  * The following is just a simple example.*/
                srand ( pid+ time(NULL) );
                intupdateInterval=rand() % 10 + 1;
                sleep(updateInterval);
                srand(updateInterval+pid+time(NULL));
                doubledesiredEnergy=rand()%50+1;
   //This sets the desired energy rate of the energy model.

        ed.setDesiredEnergy(desiredEnergy);sleep(5);

        ed.setDesiredEnergy(desiredEnergy);sleep(10);}
                return 0;
                }
```

Figure 7. Energy Model Sample Program.

Because the programs written by students may not execute correctly, instructors need correct the errors in the programs and submit it to the emulator. Similarly to the previous project, students can reserve a time slot and submit a task by specifying the topology configuration file containing customized energy model. And user can also download the resulting log files to observe the differences of the real-time power flow information between using previous and customized energy model.

Moreover, carefully designed alterations on selected energy models could keep the whole power system stable, which makes this attack not easy to be detected. In this project, students are required to design two suits of attack plans: one need change energy models of some elements to make the power grid system instable, and the other plan need change some energy models of a few elements and keep the system stable. Also, students are required to download the corresponding resulting log files to analyze the power flow and network information.

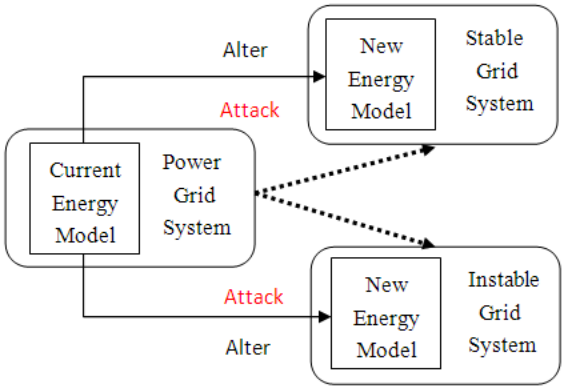

Figure 8. Energy Model Attack Project.

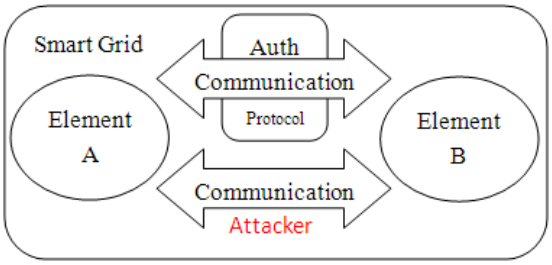

Figure 9. Authentication Protocol Project.

C. *Authentication Protocol Project*

Besides, we design an authentication protocol project to help students understand how authentication works in the smart grid environment. This project is shown in Figure 8.

Authentication is a critical component in network security, and it is widely taught in the course of network security. The authentication protocol in smart grid could be used to protect user data in the advanced smart meters to be safely collected by power corporations. And authentication is critical to prevent attackers to remotely control users' intelligent electrical appliances. Most important is the protection of the power grid control system, which needs authentication to access. It is necessary to apply authentication protocol to prevent malicious attack of the power grid control system.

In smart grid, authentication process can be skipped to reduce communication overhead, and this property could be used by attackers to bypass the authentication protocol. In Figure 8, attacker could get the communication between element A and element B in smart grid without authentication.

In this project, students are required to finish a search survey about the authentication in smart grid, and choose a senior to design a plan to execute such kind of attack. Moreover, students are taught the method to defend such attack from the experience of common network security and the features of smart grid. Students are required to propose a plan to defend against this kind of attack, and demonstrate why it could be feasible under the circumstance of smart grid.

IV. LEARNING MATERIALS

In addition, this website provides a platform to share learning materials like course presentation slides, related documents and source codes. We also design some flash videos in the web pages to introduce the overview of smart grid and its security; to explain complicated security policies, infrastructure stability and data privacy in smart grid; and to show how attacks and counter-attack work in smart grid environment. Students can access this website to obtain an in-depth grasp of smart grid security. Based on these learning materials, we have developed some course topics to cover the main aspects of smart grid security.

A. *Overview of Smart Grid and Its Cyber Security*

This is the introduction to the overall architecture of the smart grid including both the physical power system and the communication system. For power system, we will introduce the functions of the energy generation components, the distribution and transmission mechanisms, and the load control and demand response algorithms. For the communication system, we will cover various communication networks in smart grid, the Advanced Metering Infrastructure (AMI), and major smart grid industry standards.

The mutual impacts between the power system and the communication system will the emphasized in the materials. The cyber security of smart grid will provide the discussion of the problems such as the attacks in power system and communication system. Since many traditional security measures such as authentication, authorization, and accounting demonstrate unique properties in smart grid, we will re-introduce these concepts based on the new application environments.

Moreover, students can access the website to run the specified task and download the resulting log files. By observing these log files, students will have a clearer picture about the dynamical power flow information in smart grid. As a special emphasis, we will demonstrate how cyber attacks can lead to catastrophic results in physical power systems.

B. *Network Security and Infrastructure Stability in Smart Gird*

This section provides an in-depth coverage of the information network infrastructure in smart grid and its security. We will first describe the roles of wide area (WAN), local area (LAN), and home area networks (HAN) in smart grid. The advantages and disadvantages of different techniques to provide last-mile access connection to end users through power line communication, wireless networks, or cellular systems will be presented. Many network attacks in Internet have their companions in smart grid, and we will these kinds of attacks in details.

Since the power system needs to maintain a balance between the demands and supply in real-time, we will demonstrate how network attacks in the cyber system can impact the infrastructure stability of the whole power grids.

Moreover, the course projects of grid topology attack and energy model attack could assist the understanding of the attacks in smart grid. From these two projects, students could practice the simulated attack in smart grid and analyze these attacks' impact on the stability of power grid system.

C. *Data Security and Privacy in Smart Grid*

This section provides an in-depth coverage of the threats to confidentiality and privacy of the data in smart grid. We will first describe the data collection, aggregation, processing, transmission, and storage procedures in the AMI. Since different network protocols may be used at different stages of data processing, we will discuss the vulnerabilities during the data format transformation procedures.

In this section, we will introduce several concrete examples of data manipulation [12][13][14], such as data injection attacks [15][16]. Since data transmitted in smart grid without sanitization may lead to disclosure of sensitive information of end users, we will also introduce the countermeasures to preserve user privacy. Besides, the course project of authentication protocol will help students better understand the data privacy in smart grid and the importance of authentication in smart gird.

D. Examples. False data injection attack

We present a potential class of cyber attack, named false data injection attack, against the state estimation in deregulated electricity markets. With the knowledge of the system configuration, we show that such attacks will circumvent the bad data measurement detection equipped in present Supervisory Control and Data Acquisition (SCADA) systems, and lead to profitable financial misconduct such as virtual bidding the ex-post Locational Marginal Price (LMP).

An attacker could manipulate the nodal price of Ex-Post market while being undetected by the system operator. Combining with virtual bidding, such attack could bring financial profit to the attacker. A heuristic is developed to compute the optimal injection of the attacker, which can be formulated as a convex optimization problem and thus solved efficiently by the attacker.

We illustrate examples of financial virtual bidding misconducts, which are direct consequences of false data injection attack against the EMS state estimators. Figure 10 shows the topology of the IEEE 14-bus system. There are a total of five generators in this system. Table I describes two scenarios that are simulated. In both cases, a small subset of transmission line flow sensors are compromised by false data injection attack.

A malicious attacker aims at gaining profit from virtual bidding. At the pair of the nodes that are pre-specified in the third column of Table I, an attacker purchases and sells the same amount of virtual power in Day-ahead market at nodes j_1 and j_2, respectively. Based on historical trends, the attacker purchases at the lower price node and sells at the higher price node 3. In real-time market, the attacker then executes false data injection attacks on the selected sensors in order to remove a subset of congested lines. To illustrate the effect of the attacks on ex-post market clearing prices, we assume that the load forecast at day-ahead is perfect. In other words, if there were no cyber attacks, the day-ahead LMP will be the same as the ex-post LMP.

In Case I, only one transmission line (from bus 1 to bus 2) is congested. The attacker chooses to buy virtual power at bus4 and sells virtual power at bus 3 in day-ahead market. By compromising two line flow sensors with false data injection, the transmission line congestion gets relieved, leading to a system-wide uniform ex-post market price. Figure 11 shows the LMPs with and without the cyber attacks. Based on (12), the profit of such transaction is about \$1/MWh.

In Case II, there are three congested lines in the day-ahead market in Figure 12. By compromising three line flow sensors, the desired attack pair of nodes (buses 1 and 2) result in the same LMP in ex-post market. The reason is that the cyber attacks maliciously lower the estimated line flow information, thereby setting the shadow prices of the actual congested lines to be zero. The profit of such transaction is about \$8/MWh. In Table II, we compare the attack efforts and expected financial profits for both cases. We use the norm infinity of z_a with respect to the norm infinity of z as an indicator of the attack efforts. As the system congestion becomes more complex, the potential of gaining financial profits by maliciously placing false data attack is also higher.

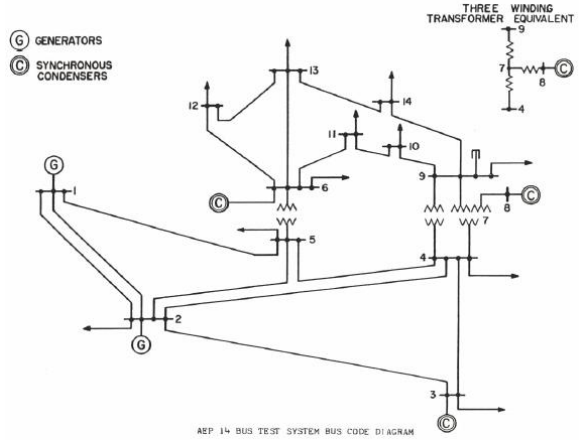

Figure 10. IEEE standard 14-bus system.

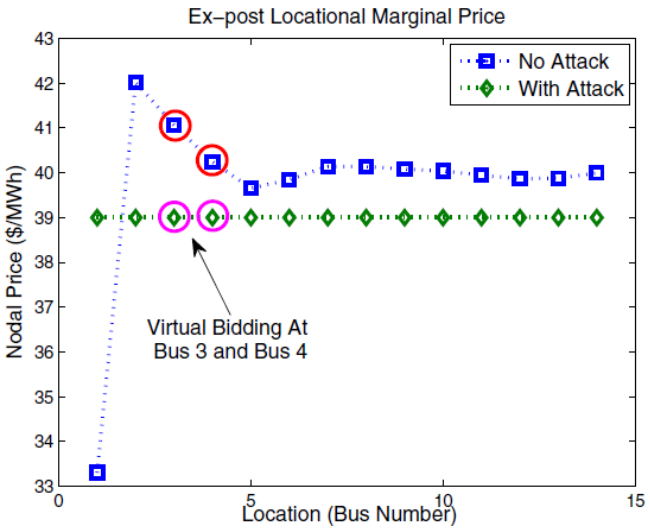

Figure 11. LMP with and without cyber attacks (only one line congestion).

TABLE I. CASE DESCRIPTION

	congested lines in day-ahead (from bus-to bus)	**virtual bidding nodes**	**compromised sensors**
Case I	1-2	3 and 4	line flow sensors 1-2, 3-4
Case II	1-2, 2-4, 2-5	1 and 2	line flow sensors 1-2, 2-3, 2-4

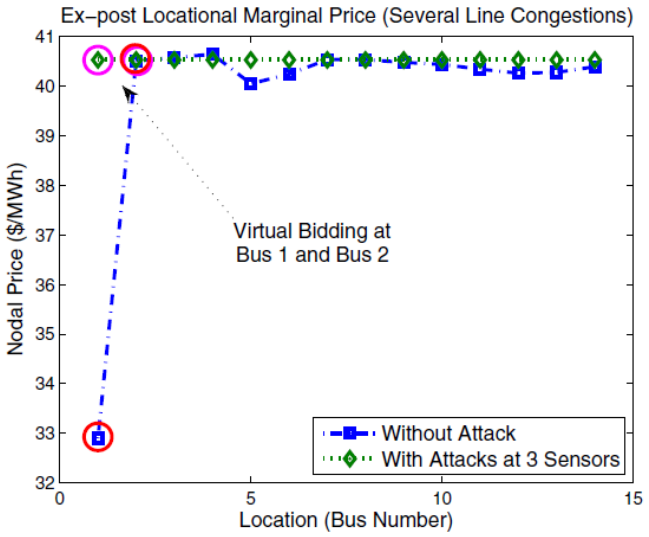

Figure 12. LMP with and without cyber attacks (three congested lines).

TABLE II. ATTACK EFFORTS AND PROFITS ($\varepsilon = 1MW_H$)

	relative efforts $\frac{\| z_a \|_\infty}{\| z \|_\infty}$	**profits (% of transaction cost)**
Case I	1.53%	2.50%
Case II	1.21%	9.76%

V. CONCLUSION AND FUTURE WORK

In this paper, we proposed a web-based smart grid learning module for students. It is shown to be beneficial for students to grasp the knowledge of security measures in smart grids and participate in the practice of smart grid security through instructive learning materials and delicately designed course projects in this learning environment.

Currently, we are working to provide friendly user interface and display course project results in graphics, especially the interaction parts in this website that provide the interface for students to access this learning environment. For example, the design of the reminding windows during the operations in the website will be improved for students to more easily apply the course project in this platform.

Moreover, an ongoing effort is to evaluate the student feedback and learning outcome from this proposed new module for smart grid security. This part will include designing the evaluation questions to measure the effect of the platform after practice of students, analyzing the feedback from students' answers to these questions to find out the defects and of this platform and improve the whole learning environment based these feedbacks.

REFERENCES

[1] Subcommittee on Smart Grid of the National Science and Technology Council. A policy framework for the 21st century grid: Enabling our secure energy future. Executive Office of the President, National Science and Technology Council, 2011.

[2] DHS Industrial Control System Cyber Emergency Response Team (ICS-CERT). Schneider electric quantum ethernet module multiple vulnerabilities.ICS-ALERT-11-346-01,2011.

[3] DHS. National infrastructure protection plan: Partening to enhance protection and resiliency. Department of Homeland Security, 2009.

[4] T. Godfrey, et al. "Modeling smart grid applications with co-simulation." Smart Grid Communications (SmartGrid -Comm), 2010 First IEEE International Conference on. IEEE, 2010, pp. 291-296.

[5] V. Liberatore and A. Al-Hammouri. Smart grid communicat- ion and co-simulation. In IEEE Energy Tech, 2011, pp. 1-5.

[6] H. Lin, S. Sambamoorthy, S. Shukla, J. Thorp, and L. Mili, "Power system and communication network co-simulation for smart grid applications." Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES. IEEE, 2011, pp. 1-6.

[7] J. Nutaro, P. Kuruganti, M. Shankar, L. Miller, and S. Mullen, "Intergrated modeling of theelectric grid, communications, and control." International Journal of Energy Sector Management, 2(3), pp. 420-438, 2008.

[8] KEMA. The u.s. smart grid revolution: Kema's perspectives for job creation. Prepared for the GridWise Alliance, 2009.

[9] M. Lowe, H. Fan, and G. Gereffi, "US Smart Grid: Finding New Ways to Cut Carbon and Create Jobs." Centre on Globalization, Governance and Competitiveness, Duke University (2011).

[10] S. Tan, W. Song, Q. Dong, And L. Tong, "Score: Smart-grid common open research emulator." Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on. IEEE, 2012, pp. 282-287.

[11] D. Choi, L. Xie, "Impact analysis of locational marginal price subject to power system topology errors." SmartGridComm 2013, pp. 55-60.

[12] S. Cui, et al. "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions." Signal Processing Magazine, IEEE 29.5 (2012), pp. 106-115.

[13] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid." Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on. IEEE, 2011, pp. 244-248.

[14] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid." Cyber-Physical Systems (ICCPS), 2012 IEEE/ACM Third International Conference on. IEEE, 2012, pp. 183-192.

[15] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets." Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on. IEEE, 2010, pp. 226-231.

[16] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations." Smart Grid, IEEE Transactions on 2.4 (2011), pp. 659-666.