Cyber-Physical Smart Grid Security Tool for Education and Training Purposes

Neetesh Saxena
Department of Computing and Informatics
Bournemouth University
Bournemouth, UK
nsaxena@ieee.org

Vasilis Katos
Department of Computing and Informatics
Bournemouth University
Bournemouth, UK
vkatos@bournemouth.ac.uk

Neeraj Kumar
Department of Computer Science and Engineering
Thapar University
Patiala, India
neeraj.kumar@thapar.edu

***Abstract*— Cyber security education is now an essential piece of information to understand the current challenges in utilizing the technology in a secure manner. In this paper, we highlight the need of improving the human factors role and cyber security awareness in better securing the systems. We discuss a simulation tool called CPSA that can be used for education and training purposes to understand the impact of cyber-attacks on the physical power system, and overall system monitoring. The tool supports attacks modeling, different communication network topologies, simulation of bad data and malicious command received over the insecure network. This tool is helpful for students and researchers' education to better understand the logics and prepare them with skills to evaluate the future cyber-physical system security. The tool can also be used for training purpose to the technical and non-technical staff at power utility.**

Keywords—cyber-attacks; cyber-physical system; cyber education; training and awareness programme; smart grid

I. INTRODUCTION

Nowadays, understanding cyber security is extremely important and is required due to the nature of attacks targeted on different systems in almost all sectors by the cyber criminals. The attackers in the cyber-world try to breach data stored in the modern systems [1]. Considering this threat environment, cyber security education has become an essential part of our life to conduct day-to-day activities. As we live in a society, which is reforming itself smarter day-to-day. In this so called "smart world", we are expecting billions of devices in the future connected to the Internet. This scenario invites security vulnerabilities and threats around the world [2]. Understanding and applying cyber security are becoming more and more difficult as these threats evolve with the advanced technologies. It is even harder to understand the impact of these cyber-attacks on the physical systems considering the fact that nowadays, we have several physical systems connected to the Internet exchanging information over the insecure network. A smart grid is an example of such systems.

Many times, these systems are compromised due to the weak security implementation or by human mistakes due to not having sufficient understanding. Human factor in cyber security places an important role that can prioritize solutions for users to improve the cyber resiliency. Federal Information Systems Security Educators' Association (FISSEA) highlighted that in order to have a secure infrastructure, an organization needs to address human factors of cyber security by the informed and proactive workforce [1]. The major cyber risks occur due to data breaches due to mostly human errors or negligence, which lead to data as well as financial losses. In order to improve human factor aspects to defeat cyber-attacks, we need to get involved in cyber workforce development, training and awareness, and stakeholder and leadership engagement.

The power industry has recently faced potential cyber-attacks around the world that impacted the power grid with serious implications. Some of these recent cyber-attacks targeted real power systems were: Ukraine attacks in December 2015 and February 2016 [3]. The Ukraine power grid was brought down by cyber-attacks, which left 80,000 people in dark for more than six hours, and more than two months post-attack, the control centers were still not fully operational [3]. The attacks targeted IT staff and system administrators of companies responsible for distributing electricity. They delivered email to workers with a malicious Word document attached. Clicking on and selecting the attachment enabled macros in the document, which actually injected BlackEnergy, a Trojan horse, (which have infected other systems in Europe and the US) into the workers' machines. The attackers accessed the Supervisory Control and Data Acquisition (SCADA) networks through the hijacked Virtual Private Networks (VPNs), sent commands to disable the Uninterruptible Power Supply (UPS) systems, and opened up transmission line breakers at several substations. This caused a broad power blackout. It is evident that well planned and well-executed cyber-attacks through malicious control commands can potentially disconnect power devices at substations and leave hundreds of thousands of energy consumers in the dark. This scenario reflects a strong need of improving the security awareness of the operator and other staff at utility to protect the overall system. Human mistakes are one of the major issues in security breach, therefore, we need an education, training, and awareness programme to train them and make them aware about the recent cyber-attacks and best practices. At the same time, we need to improve cyber security awareness to the general public through several events, as well as enhance education with latest technological advancements and future challenges at universities and schools. This will prepare university students and researchers with skills to develop new

tools and techniques to evaluate the impact of potential cyber-attack, especially on a physical system.

A reliable and secure smart grid system is required to build. This can be initiated by providing in-depth education related to cyber security and smart grid system operations to the university students and researchers. The other aspect is to develop new simulation tools to improve better understanding of the system behavior and provide a training and awareness to technical as well as non-technical staff of the power utilities to mitigate the risks and under attacks circumstances. We actually need to look at the tools that could provide a continuous, efficient and real-time monitoring along with cyber-physical security assessment for increased situational awareness. The ideal training should involve all three factors to think about: (i) how to prevent these attacks from happening, (ii) how can we detect these attacks and vulnerabilities, and (iii) what is the worst case consequence if we are not able to protect the system against (i) and (ii).

The rest of the paper is organized as follows. Section II describes objectives, existing solutions and contributions of cyber-physical security tool in education and training. Section III highlights the cyber-physical system security challenges in education and training. Section IV explains the contextual learning requirements, whereas the Section V describes utilizing simulation tool in education and training. Finally, Section VI concludes this paper.

II. Objectives, Existing Solutions, and Contributions

In order to clearly provide better understanding and required knowledge to the university students and training to the utility staff, we must have a tool that covers several aspects of the cyber-physical system. In fact, to evaluate the current security of the power system, a cyber-physical security assessment of the joint communication-power system is required, rather than simply examining the cyber-security concerns in only the communication network or the impact of physical events on the power system. However, research in this area has not been fully explored. In summary, we have set the following objectives for the required education and training:

1. Awareness for power operators who do not understand cyber security, but deal with the system under attack.
2. Training programme for utility staff, including electrical engineers and IT professionals for better understanding the nature of cyber-attacks and their impact on the power system.
3. Point (1) and (2) are required to include in the education system for university students and researchers to design new tools and develop better techniques to cover all said aspects of the integrated cyber-physical system.

In subsequent paragraphs, we discuss the existing solutions to defeat some of the cyber-attacks. This will reflect the current state of the art in the education system as well as in the training and awareness programme, and will help to find unresolved problems and security issues in the smart grid system.

Tran et al. proposed a detection scheme for a replay attack in the smart grid [4]. Chen et al. discussed different categories of attacks: vulnerability, data injection and intentional attacks, and analyzed communication network robustness [5]. Yang et al. discussed an Address Resolution Protocol (ARP) spoofing based Man-in-the-Middle (MITM) attack [6]. Wei et al. performed a study on modeling Denial-of-Service (DoS)-resilient communication routing in the smart grid [7]. Etigowni et al. presented a cyber-physical access control solution by using information flow analysis based on mathematical models of the physical grid to generate policies enforced through verifiable logic [8]. Furthermore, Sgouras et al. made an attempt to assess the impact of cyber-attacks on the Advanced Metering Infrastructure (AMI), specifically considering Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks [9]. Hahn et al. introduced a security model to represent privilege states and evaluated viable attack paths in the AMI network [10]. Liu et al. analyzed the impacts of a line outage attack, DoS attack, and MITM attack on the physical power grid using an integrated cyber-power modeling and simulation testbed [11].

The above mentioned solutions have limitations, which could be further improved. In [5], [6], [9], [10] and [8], the impact of attacks on the power system was not studied, whereas the scheme in [4] does not consider the source of the cyber-attacks as being from the communication network, rather directly injected into the power system. The simulation work in [7] only included a 3-generator system, which is small to fully understand the impact of these attacks on real power systems.

The studies of cyber-physical systems found in the literature are based on attacks, such as MITM, DoS, and DDoS. These attacks are achieved by injecting false data or targeting the device to stop its functionality. However, there is no study carried out for malicious/false command injection in the smart grid, where an adversary can potentially isolate the critical power components by disconnecting them from the rest of the power system [3].

We developed an integrated cyber-physical tool from our previous work [12] to tackle the issue of impact monitoring of the cyber-physical system. This simulation tool can contribute in academia as well as industry as follows:

1. The developed tool helps in learning and understanding the nature of cyber-attacks, and models them using the technology under smart grid environment consisting of several power and communication devices and components.
2. The tool provides a broad understanding of setting different network topologies to analyze communication network for the smart grid in a better way.
3. The tool supports understanding and evaluation of power system activities and routine operations, such as power flow and contingency analysis.
4. The tool maps the behavior of cyber-attacks into the dynamics of power system measurements, and can be used in effectively improving the understanding of integrated cyber-physical smart grid security.

5. The tool helps in monitoring and evaluating the impact of cyber-attacks on the physical power system. This provides a greater understanding of this impact on individual power component as well as on the power system as a whole. The tool maintains communication logs, received and sent power system measurement data, and triggered control commands as well as generates security metrics to understand the critical and non-critical components in the system.
6. The tool provides insight to offer a reasonably better training and awareness guidelines to the technical as well as non-technical people. It will enable the operators to further develop their decision making skills. So, we can better prepare the students for this role in the future.

III. Cyber-Physical System Security Challenges in Education and Training

The smart grid system is cyber-controlled through an integration of the communications networks, embedded systems and software applications. It is therefore important to understand the interdependencies in an integrated cyber-physical system environment. However, this is a big challenge to resolve due to the unavailability or shortage of cyber-physical simulation tools, and consequently difficult to analyze and include in for the education and training purposes.

Existing simulators on the market independently simulate either the power system or the communications network [12]. For example, PowerWorld [13] is a dedicated power system simulator that simulates power systems dynamics and operations, but assumes ideal communication conditions in the communications layer. NS2/3, on the other hand, is dedicated communication network simulator that simulates communication network dynamics, but is incapable of simulating power system [14]. An integrated cyber-physical co-simulator must be able to model and simulate the power system as well as the communication system simultaneously in addition to providing functionalities for assessing cyber-physical security.

Cyber-attacks can affect the normal operation of power system applications, such as demand response. These attacks can also affect the decision making capability of a system operator, which can lead to cascading failures and instability in the grid. Compromised confidential power system information can lead to perform inappropriate actions by the operators. Cyber-physical attacks can result in permanent physical damage to power devices in the field. We should be able to model the nature and behavior of these attacks, and learn from their simulation. Different attack situations need to be captured and analyzed underlying communication network. System misbehavior on the power or communication network system may compromise power system data and may disrupt control devices. The current state and overall health of the power system can also be affected by attacks over the communication network. During these attacks, the power system may undergo various state transitions and eventually become insecure.

In addition to this, there are certain specific challenges that make the study of cyber-physical system more difficult, which are (i) scalability: due to the involvement of a large number of devices, (ii) simulation tool: due to the limitations of the existing simulation tools and the shortage of integrated cyber-physical simulation tool, (iii) applying critical thinking: modeling and detecting changes in the physical system targeted from the cyberspace are not straight forward and require expertise in both domains, and (iv) human element: as we know humans are the weakest link in security, they can mistake in designing and understanding the complex systems. But in order to understand and analyze the cyber-physical system, integrated tools need to be developed. The university education needs to be upgraded with the latest attack scenarios and advancements in the cyber-physical system using such tools. Similarly, the staff training programmes also need to be revised for better understanding of the nature of recent attacks and the techniques used by the cyber criminals to trigger these attacks. This will surely improve the human aspect of the system, and users will learn from their or others' mistakes.

A typical example for understanding the complexity of cyber-physical smart grid system is given below, where a false but legitimate command can potentially damage the power system operations, and is difficult to catch the fact that the command sent was false [3].

Use Case: The attacker can impersonate the communication network and sends a false (unwanted) but a legitimate command to the circuit breaker of the largest generator at a substation. Here, we try to understand its potential impact on the power system, and design a solution that addresses the issue of injecting a malicious command or a legitimate but false command over the communication network.

Effects on the Communication Network: Under this attack, we can observe and monitor several effects on the communication network, such as: (a) the deployed Intrusion Detection System (IDS) notifies the control center operator the type of command it received and the operator verifies whether the command is legitimate, and (b) a false command was issued to the substation device connected to the breaker of the targeted generator.

Effects on the Power System: If this attack is successful, we can observe the following impact on the power system: (a) insecure operation(s) of the power system, and (b) possible shedding of electrical load.

Steps: The following steps are involved in the presented use case to address the issue:

1. The attacker sends a false but legitimate command from an external location to the generator breaker over an insecure network.
2. The IDS detects a suspicious malicious command (based on its rules engine, such as IP address, port number, etc.) and notifies the operator. The operator verifies that the control center did not issue this command.
3. The developed tool performs power flow and cyber-physical contingency analysis to evaluate the effect of the command on the power system if it was allowed to go through. The tool discovers that the system is in an

insecure state indicating that the command was malicious in the sense that it was not sent from the control center.

4. The operator discards the command, and the secure system operation is restored back.

IV. Contextual Learning Requirements

This section covers contextual learning requirements for both, education as well as training purposes. Following are the expected requirements from a simulation tool to provide a clear understanding of the cyber-physical system security. Technically, the tool must contribute to educational learning as well as technical and non-technical training to the utility staff. The tool should:

1. Be able to detect real-time cyber security situations. This can be achieved by comparing the normal system behavior with the situations under attack.
2. Provide monitoring and control capabilities to the operators and system administrators.
3. Detect possible contingencies that can occur in the system as a result of a specific cyber-attack and analyze them.
4. Enhance the security and resilience of the power system by suggesting appropriate operator actions under attack scenarios.
5. Generate historical logs and trust metrics for different power and communication components and identify weak elements in the system, which helps operators to respond quickly when a similar situation occurs at repeated locations.
6. Apply user-generated rules for the normal operating range to better understand the behavior and normal state of the integrated cyber-physical system.
7. Identify and assess the current health of the cyber-physical-system by performing cyber-physical contingency analysis, and suggest the appropriate actions to take into account.
8. Suggest and enable an extra layer of security, i.e., hashing or encrypting the commands or critical measurements [15].

V. Utilizing Simulation Tool in Education and Training

Simulation is an effective way of working with very large problems that would otherwise require involvement of a large number of active users, devices and other resources, which is difficult to coordinate and build in a large-scale research environment for the purpose of investigation. In this section, we discuss an integrated cyber-physical security co-simulator tool capable of Cyber-Physical Security Assessment (CPSA) [12] and address how can this tool be used in education and training to better understand the cyber-physical system security.

We cover both aspects of the learning: (i) education aspect that reflects how we can improvise the existing knowledge and understanding in academia (at universities and schools), and (ii) training and awareness aspect that improves the cyber security understanding of the technical and non-technical staff, such as electrical engineers, computer operators, and other staff at the substation.

Attacks modelling and the measurement simulation using CPSA tool are shown in Figure 1. Similarly, Figure 2 represents commands simulation using tool and understanding their impact on the power system.

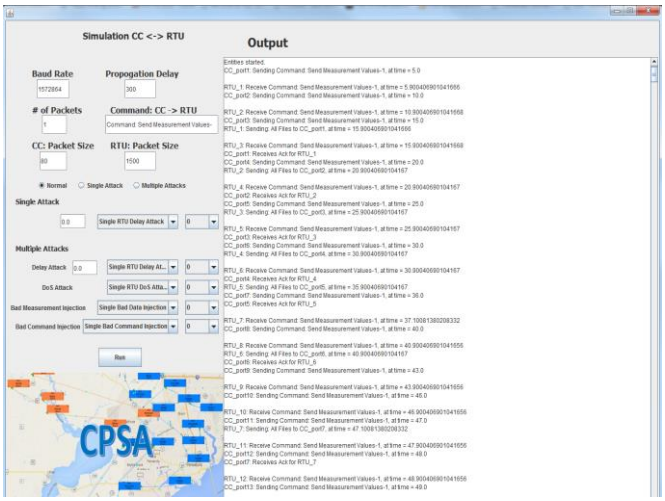

Fig. 1. CPSA tool for attacks modelling and data measurement simulation.

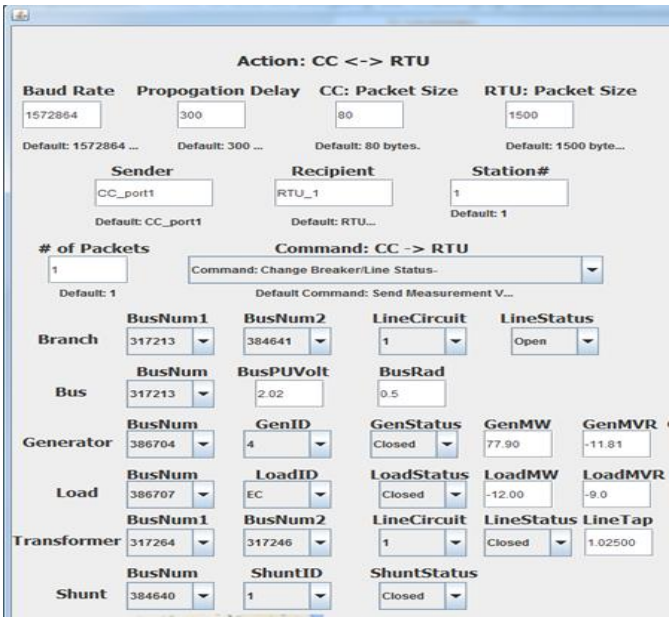

Fig. 2. Simulating commands and understanding their impact on the power system.

A. *How can we understand the behavior and nature of cyber-attacks?*

The tool models and helps to understand the possible cyber-attack scenarios. At present the tool works with four attack scenarios: bad data injection, malicious command injection,

DoS, and communication delay attacks. In addition to these attack scenarios, the simulation tool can be extended to model replay, impersonation, and other attacks. This covers not only the theoretical aspect of attack modeling and logical communication of data flow, but also provides an implementation aspect to model these attacks using technologies, such as Java, MATLAB, and PowerWorld. In order to gain insight and better understanding on the inter-dependencies in the system, the tool can be used to provide in-house training and awareness to the power utility staff. The tool models overall cyber-physical control loop including operator decisions under attack scenarios, which very much covers the training and awareness aspect to the technical staff.

B. How to understand security logs and forensic analysis to verify an attack footprint?

The tool provides the capabilities to aggregate, normalize and index the log files acquired from the different components. Upon successful detection of a security incident, the relevant Indicators of Compromise (IoC) are used to correlate and search the log files in order to allow the forensic analyst to construct a timeline of events and identify further indicators that will lead to attribution, that is, to identify the source of the attack and the impact the attack had upon the affected asset. The security incidents extracted from the log files can be also fed into Security Information and Event Management (SIEM) tools, such as Alienvault and Aplunk as well as general purpose analysis tools like Kibana and Elasticsearch. The educational aspect includes the understanding of these related tools and improving the accuracy to decide and detect indicators of compromise. The training aspect includes the detection of different attacks' footprint, i.e., source of the attack and its impact on the system, from the log files indicating the timeline of events, and then utilizing other tools for incident analysis.

C. How can we understand and evaluate the impact of cyber-attacks on the power system?

To better understand the impact of cyber-attacks on the power system, the tool maps communication network changed parameters (due to an attack) to power system dynamics through an interface. The tool supports the implementation of the communication network in Java, power system dynamics using PowerWorld, and the interface using MATLAB. This interface keeps a closed eye in the program segment where this mapping takes place and the parameters need to change and pass to the power system for evaluating the current state of the system with the changed values. The educational aspect includes the functionality and implementation details of this interface to map the received physical values from the communication network to the power system. The training aspect covers the generation of new files containing the power system dynamics before and after passing changed values to the PowerWorld.

D. What is an effective way and how can we perform power system monitoring?

The tool provides the operator with an interface to monitor the behavior of the power system. The tool also generates system residuals and Aggregate MW Contingency Overload (AMWCO) matrices in order to evaluate the security and health of the power system. The tool can support dynamic power system topology having power components ranged from several hundreds to a thousand. The education aspect improves the understanding of the functioning and details of global state estimation, power flow, and contingency analysis, whereas the training aspect covers functionalities and simulation details for global state estimation, power flow, and contingency analysis.

The purpose of state estimation is to identify the most likely state (bus voltage magnitudes and angles) of the power system using the measurements received from the devices in the field. Power flow determines the system state based on bus injections, and the obtained results serve as the base scenario for subsequent contingency analysis. Contingency analysis evaluates the impact of possible physical contingencies on the power system in terms of line thermal overload.

The tool can handle a small power system case with a few tens of buses to a large system with ten thousand buses. The tool is capable of monitoring the real-time system behavior (by comparing the current state of the system with the baseline under normal behavior) as well as the impact of cyber-attacks on the power system (by generating a couple of security metrics, and keeping history of communications logs).

E. How to understand and detect malicious measurement data?

The tool models a scenario of MITM attack under which an adversary can perform bad data injection attack on the power system. The education aspect involves the modeling and understanding of first performing MITM attack over the communication network to alter the measurement data, and then modify a specific or few values (within threshold or outside the range) of the measurements of a specific bus (with attached generators and loads), such as voltage, active power, reactive power, and angle. The tool supports Distributed Network Protocol (DNP3) packet format for transmitting the measurement data. The training aspect covers the understanding of system behavior when the malicious data are allowed vs. disallowed to the power system. The system generates output files to observe the changes in the final values for each bus in the system. Depending upon the outcomes, the operator makes a decision where to pass suspected malicious data into the real power system or just discard the received packets with such values.

F. How can the system detect malicious control command and ensure the transmission of legitimate command delivery?

Generally, the operator executes control commands to different power components at the substation as part of its routine and emergency operations. An attacker can modify the transmitted command over the insecure network to perform a specific action, such as opening a circuit breaker, detaching a generator, and shedding load. The education scenario involves the understanding of malicious command, which could be a legitimate but false (wanted) command. In order to detect a malicious command, the system deploys an IDS with filtering

rules based on different parameters, such as the IP address of the source, port number, and frequency of the same command triggered in a specific time interval. The IDS sends a notification to the operator, and the operator can decide whether to allow or disallow a command to execute on the real power system. The training scenario includes the awareness of such complex scenarios where a command is legitimate but unwanted or forged. It also includes the understanding of IDS filtering rules and understands the impact of suspicious command by simulating it using the tool, and depending upon the modified state of the power system, a command can be allowed or not. The tool can use digital signatures to ensure the authentic delivery of legitimate commands only [16].

G. How can the system understand and detect that a device is disabled (possibly due to a DoS attack) and is not functioning at a remote substation?

There could be situations where a device deployed in the field stopped working (possibly due to an attack, say, DoS), and does not send measurement data to the control center for some times. Hence, measurements from the substation are unavailable for state estimation. The tool may still provide global observability, since the system may have sufficient measurements in other parts. If several substation devices are under DoS attacks, the state estimator will lose observability into at least a portion of, if not the entire system. In this situation, it is difficult to provide any input to other energy functions, such as power flow, contingency analysis, and optimal power flow. The education aspect involves the understanding of such scenarios and techniques for observability analysis. The training aspect includes the detection of such as an attack using the tool and guide operators to take immediate action in order to mitigate the impact of such an attack on the power system.

VI. CONCLUSION

In this paper, we highlighted the need of understanding cyber-physical system security. We emphasize the role of human factors and their mistakes, which call the need for improvements in understanding the cyber security by the general public as well as technical and non-technical staff at utility. The understanding of cyber-physical system security can be enhanced by attacks modeling and evaluating the impact of cyber-attacks on the power system. We highlighted that CPSA tool can be used for educational purpose to improve the skills and knowledge of the university students and researchers. Subsequently, they can develop new tools and techniques for security analysis of the future cyber-physical systems. The CPSA tool can also be used for training purpose to the operators and other staff at utility. Much effort needs to be made in order to spread cyber security awareness and cyber-attack impact monitoring of the real physical system, such as the power grid.

REFERENCES

[1] Cybersecurity – the Human Factor, Federal Information Systems Security Educators' Association, FISSEA, 2017. [Online]. https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf.

[2] N. Saxena, B. J. Choi and R. Lu, "Authentication and authorization scheme for various user-roles and devices in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 907-921, May 2016.

[3] N. Saxena, L. Xiong V. Chukwuka, and S. Grijalva, "Impact evaluation of malicious control commands in cyber-physical smart grids," *IEEE Transactions on Sustainable Computing*, Special Issue on Sustainable Cyber Forensics and Threat Intelligence, 2017 (under review).

[4] T.-T. Tran, O.-S. Shin, and J.-H. Lee, "Detection of replay attacks in smart grid systems," In *Proc. International Conference on Computing, Management and Telecommunications*, 2013, pp. 298-302.

[5] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *IEEE Communications Magazine*, vol. 63, no. 1, pp. 3-18, 2014.

[6] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Q. Yao, B. Pranggono, and H. F. Wang, "Man-in-the-middle attack testbed investigating cyber-security vulnerabilities in smart grid SCADA systems," In *Proc. International Conference on Sustainable Power Generation and Supply (SUPERGEN)*, 2012, pp. 1-8.

[7] J. Wei and D. Kundur, "A flocking-based model for DoS-resilient communication routing in smart grid," In *Proc. Global Communications Conference (GLOBECOM)*, 2012, pp. 3519-3524.

[8] S. Etigowni, D. Tian, G. Hernandez, S. Zonouz, and K. Butler, "CPAC: Securing critical infrastructure with cyber-physical access control," In *Proc. 32nd Annual Conference on Computer Security Applications (ACSAC)*, 2016, pp. 139-152.

[9] K. I. Sgouras, A. D. Birda, and D. P. Labridis, "Cyber attack impact on critical smart grid infrastructures," In *Proc. IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, 2014, pp. 1-5.

[10] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 835-843, 2011.

[11] R. Liu, C. Vellaithurai, S. S. Biswas, and T. T. Gamage, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444-2453, 2015.

[12] N. Saxena, V. Chukwuka, L. Xiong and S. Grijalva, "CPSA: a cyber-physical security assessment tool for situational awareness in smart grid," In *Proc. 3rd Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC) in Conjunction with the ACM CCS*, Nov. 2017, Dallas, USA (accepted).

[13] The Visual Approach to Electric Power Systems, 2016. https://www.powerworld.com/.

[14] S. P. Leblanc, A. Partington, I. Chapman, and M. Bernier, "An overview of cyber attack and computer network operations simulation," In *Proc. Military Modeling & Simulation Symposium (MMS)*, 2011, pp. 92-100.

[15] N. Saxena and S. Grijalva, "Dynamic secrets and secret keys based scheme for securing last mile smart grid wireless communication," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1482-1491, Jun. 2017.

[16] N. Saxena and S. Grijalva, "Efficient Signature Scheme for Delivering Authentic Control Commands and Alert Messages in the Smart Grid," *IEEE Transactions on Smart Grid*, Jan. 2017 (online).