Impact of Cyber Attacks on Transient Stability of Smart Grids with Voltage Support Devices

Bo Chen, Salman Mashayekh, Karen L. Butler-Purry
Electrical and Computer Engineering Department
Texas A&M University
College Station, TX, USA
{boboychn, s.mashayekh, klbutler}@tamu.edu

Deepa Kundur
Electrical and Computer Engineering Department
University of Toronto
Toronto, ON, Canada
dkundur@comm.utoronto.ca

***Abstract*—Cyber security is becoming a major concern of smart grids, as the functionality of a smart grid is highly dependent on the cyber communication. Therefore, it is important to study the impact of cyber attacks on smart grids. This paper discusses several types of cyber attacks. Then, it presents results of studies of impacts on transient angle and transient voltage stability due to cyber attacks on two voltage support devices, SVC and STATCOM, in an 8-bus test system. The 8 bus system and voltage devices are simulated and the stability analysis is performed with DSA*Tools*™. The results showed that some modification cyber attacks can make the system angle or voltage unstable, following a physical fault in the system.**

***Index Terms*—cyber attack, cyber security, smart grids, SVC, STATCOM, FACTS, transient stability, voltage support device**

I. Introduction

In modern power systems, the increasing demand for reliable energy and integration of advanced technologies has motivated the concept of smart grid. Smart grid is an infrastructure capable of meeting the requirements for the future power system framework, by integrating distributed energy resources, plug-in hybrid vehicles, and energy storage devices, and providing advanced load management strategies.

To meet these requirements, some technologies such as Phasor Measurement Unit (PMU), Flexible AC Transmission System (FACTS), distributed control, and smart meters are widely deployed to facilitate smart grid operation in monitoring, voltage regulation, and economic dispatch. The functionalities of these technologies highly depend on cyber communications, which may be vulnerable to attacks. Thus, cyber security is becoming a major concern in smart grids [1].

The features of smart grids are implemented based on two-way communication. Therefore, cyber physical security is vitally important for smart grid infrastructure. The data representing the operating states, measurements, and control commands are intended to be shared among multiple devices and control centers. Therefore, smart grids grow potential cyber vulnerabilities as millions of interfaced devices and software are installed. The vulnerable points in the cyber system of smart grids can be used for performing cyber attacks by corrupted personnel and unauthorized parties [2].

Numerous cyber attacks and their resulting financial losses have been reported in the past several years [3]. The number of cyber attacks on the U.S. infrastructure increased 17-fold from 2009 to 2011 [4]. The Supervisory Control and Data Acquisition (SCADA) system is normally the main target of cyber attacks. Most utilities are struggling to identify the critical cyber assets [5]. Therefore, to protect smart grids from cyber attacks, it is essential to identify the vulnerabilities [6] and perform corresponding impact analysis [7],[8].

Several types of cyber attacks and their impacts have been studied in literature. Reference [9] studied cyber attacks on the automatic generation control loop which targeted integrity of information security. These attacks resulted in an increase in system frequency and tie-line flow. Reference [10] showed that a cyber attack may cause device restoration delays. Data integrity attacks were also performed on a load management system in [6], in which a graph based dynamic system model was used to analyze the impact of the cyber attack. A coordinated switching attack was studied in [8]. The results showed how switching a load in and out along a certain sliding mode could lead to system instability. Two data attack strategies on smart meters were studied in [11]. The results showed that the network state became unobservable when a certain set of meters were compromised. False data injection attacks on state estimator were studied in [12], which showed that it may be possible for attackers to make profits from real-time markets without being detected.

Voltage support devices, e.g. SVC and STATCOM, play a vital role in maintaining bus voltages and keeping system stability. Since a cyber attack can target these devices and due to their role in system stability, it is necessary to study impact of cyber attacks targeting these devices. This research fills this gap in literature by analyzing impact of cyber attacks on transient stability of smart grids with voltage support devices.

In this paper, section II reviews several classes of cyber attacks. Then, section III discusses the stability indices used in this paper to quantify the impacts. Section IV introduces the test system used in this paper and discusses system modeling. Section V reports the cyber attack simulation results from several cases. Finally, this paper is concluded in section VI.

II. Cyber Attack Classification

A. Vulnerabilities of Smart Grid Sensor Networks

Vulnerability is known as a weakness in the security of the system which might be attacked to cause loss or harm [13].

This work was supported in part by Norman Hackerman Advanced Research Program Project 000512-0111-2009 and NSF grants EECS-1028246 and EEC-1062603.

978-1-4799-1303-9/13/$31.00 ©2013 IEEE

Smart grids are vulnerable in communication, hardware and software. On the communication side, a wide variety of data communication protocols have been used to connect utility operation centers with system operation centers. Most of the existing protocols have vulnerabilities, including SCADA system [14]. On the hardware side, remote controllable elements are deployed among substation devices such as circuit breakers, capacitors, or measurement units. These remote controlled elements increase smart grid vulnerabilities to cyber attacks. And on the software side, vulnerabilities exist in the programs and applications installed on the computers within utility enterprises or operation centers. This vulnerability would cause a top-down attack.

B. Classification [13]

The CIA triad (Confidentiality, Integrity and Availability) is one of the core principles of information security [15]. Cyber attacks can be classified based on which of these three security goals they comprise. This section explains four types of cyber attacks.

1) Interception

Interception refers to a category of attacks on confidentiality in which an unauthorized party gains access to a cyber asset. This attack cannot be detected, but can be prevented with cryptography, which is a technology to secure information from third parties. Typical interception attacks are eavesdropping, wiretapping, fiber-tapping, packet sniffing, keystroke logging, surveillance, and traffic monitoring.

2) Interruption

Interruption refers to an attack on availability in which an unauthorized party destroys a cyber asset or makes it unavailable. Usually, it cannot be prevented and the general strategy is to detect the Denial-of-Service and react. Some examples are communication link jamming, software modification to prevent accurate execution, and data erasure.

3) Modification

Modification refers to an attack in which an unauthorized party gains access to and tampers with a cyber asset. Modification targets the integrity of information security and is an active attack. It can be prevented with cryptography. Typical modification attacks are control signal modification, sensor data modification, and modification of energy usage.

4) Fabrication

Fabrication refers to an attack in which an unauthorized party inserts counterfeit objects into system. Fabrication is an active attack on authentication. It can be detected with cryptography. Typical fabrication attacks are flooding attacks, insertion of fake control signals, and insertion of fake financial transactions for profit.

An attack from any of these categories can target a cyber device in a smart grid. This paper focuses on modification attacks and explores how they impact transient stability of a smart grid.

III. Power System Transient Stability

Power system stability is the ability of an interconnected system to regain a state of operating equilibrium after being subjected to a physical disturbance. It is always a great concern for secure system operation. Power system stability can be classified based on the time pan (long term, short term), size of disturbance (large disturbance, small disturbance), and system variables in which instability can be observed (rotor angle, voltage, frequency) [16]. In this paper, impact of cyber attacks on angle stability and voltage stability are studied.

A. Angle Stability

Angle stability refers to the ability of an interconnected power system to maintain synchronism when subjected to a disturbance [16]. It depends on the ability of the system to maintain or restore the equilibrium between the mechanical and the electromagnetic torque. To study transient angle stability, the equation of motion for synchronous generators, shown in (1), is used.

$$J\frac{d^2\theta}{dt^2} = T_m - T_e \tag{1}$$

In this equation, θ is the angular position of the rotor, J is the total moment of inertia of the coupled turbine and generator rotor mass, and T_m and T_e are the mechanical and the electromagnetic torques, respectively.

B. Voltage Stability

Voltage stability refers to the ability of an interconnected system to maintain the voltage at all buses within a certain level, when subjected to a disturbance [16]. It depends on the ability of the system to maintain or restore the equilibrium of supply and demand at load buses. Voltage instability may cause tripping of system elements (loads or lines), due to operation of protective devices. In a worse case scenario, voltage stability may trigger a progressive fall or rise of voltages at some buses and lead to a cascading outage.

C. Stability Indices

A stability index is a measure of how stable the system is, concerning an aspect of stability. Thus, stability indices can be used in impact analysis for comparison purposes. To assess the impact of cyber attacks on transient stability in smart grids, this paper uses the following indices for transient angle stability and transient voltage stability.

1) Angle Stability Index

Reference [17] defines an angle stability index by

$$\eta = \frac{360° - \delta_{max}}{360° + \delta_{max}} \times 100\% , \tag{2}$$

where δ_{max} is the maximum angle separation of any two generators in the same island in the post-contingency system. This index varies between -100% and $+100\%$ and $\eta > 0$ and $\eta \leq 0$ denote stable and unstable conditions, respectively. Also, a bigger η corresponds to a more stable system.

2) Voltage Stability Index

According to The Western Electricity Coordinating Council (WECC) standards, after an event or fault leading to the loss of a single power system element, load bus voltages must satisfy the following two constraints [18]. Firstly, the voltage dip/sag should not exceed 25%. Secondly, the voltage dip/sag must not exceed 20% for more than 20 cycles (330 milli-seconds in 60 Hz systems).

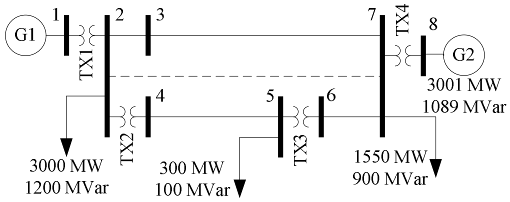

Figure 1. Test System with 2 generators 8 buses

TABLE I. DYNAMIC DATA OF GENERATORS

	$Base$ (MVA)	H (s)	x_d (pu)	x'_d (pu)	x''_d (pu)	t'_{do} (s)	t''_{do} (s)	x_q (pu)	x'_q (pu)	t'_{qo} (s)	t''_{qo} (s)	D
G1	2200	6.50	1.80	0.30	0.25	8.00	0.03	1.70	0.55	0.40	0.05	0
G2	4000	5.45	--	0.26	--	--	--	--	--	--	--	3

TABLE II. DATA OF LINES AND TRANSFORMERS

	TX1	TX2	TX3	TX4	L2-3	L2-7	L3-7	L4-5	L6-7
$R\ (pu)$	0	0	0	0	0	0	1.0e-4	1.0e-4	0
$X\ (pu)$	5.0e-4	5.0e-4	5.0e-4	5.0e-4	1.0e-2	8.6e-3	1.3e-3	5.0e-2	1.0e-2

Based on these requirements and since all the cases in this paper study contingencies which lead to voltage drops, the voltage stability index for the studies conducted in this paper is defined to be the maximum time a load bus voltage remains below 0.8pu, among all system load buses. For instance, consider a fault which causes the bus voltages at buses 2, 5, and 7 to stay below 0.8pu for 400ms, 500ms, and 350ms, respectively. In this case, the defined voltage stability index would be 500ms, which is the maximum time among all load buses. This index, i.e. 500ms, denotes an unacceptable voltage behavior, since it is greater than 330ms.

It is worth mentioning that the above voltage criteria are defined for load buses following single contingencies and the steady state threshold for load bus voltages are much tighter, usually about ±5% [16].

IV. SIMULATION SETUP

A. Test System

To study the impact of cyber attacks on a smart grid, the 8 bus transmission-level system shown in Figure 1 [17] was used. It includes 2 generators, 3 loads, 4 transformers, and 5 lines. The system parameters are listed in Tables I and II [17].

B. System Modeling

This system was modeled in Transient Security Assessment Tool (TSAT) of DSA*Tools*™ package. TSAT is a time-domain simulation tool designed for power system dynamic behavior assessment [19]. To model G2, the classical model, i.e. constant voltage behind transient reactance, was used. Also, G1 was modeled as a round rotor synchronous generator (GENROU) with an exciter and a Power System Stabilizer (PSS). The loads in the system were modeled as constant PQ loads. Also, pi models were used for transformers and transmission lines and line 2-7 was out of service.

C. Need for Voltage Support Devices

To demonstrate the need of this test system for voltage support devices, three case studies were performed. These

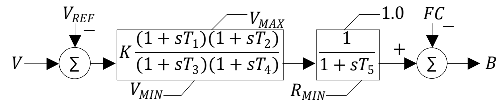

Figure 2. SVC control system block diagram

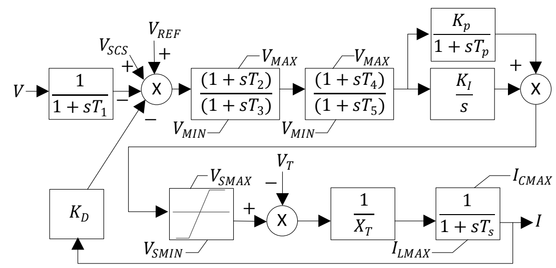

Figure 3. STATCOM control system block diagram

case studies are denoted with A, B, and C. In case A, the system was modeled without any voltage support device. In contrast, cases B and C modeled the system with an SVC and a STATCOM connected to bus 5, respectively.

Case A studied a 3-phase bolted fault at bus 7 at 0.5s which was cleared after 67ms by opening line 3-7. Note that this line fault was chosen, since it appeared to be the most severe line fault disturbance in the system, because the active power transferred over this line was the largest among all the lines in the system. It is emphasized again that for this case study, the system was modeled without any voltage support devices. The angle and voltage stability indices for this case are shown in the first row in Table III. It can be seen that although the system was angle stable, the voltage stability criterion was violated, since the voltage stability index (0.804s) was more than the maximum acceptable threshold (0.330s).

To demonstrate how a voltage support device can fix this problem, the system was modeled with an SVC and a STATCOM connected to bus 5 in cases B and C, respectively. It is worth mentioning that these two cases studied the same fault contingency. The models depicted in Figures 2 and 3 were used for the SVC and the STATCOM, respectively [17],[20]. In Figure 2, the voltage at bus 5 is compared with the reference value, and then the error is passed through a PI controller to determine the shunt capacitance. In Figure 3, the voltage at bus 5 is brought through a low-pass filter, first. Then, it is compared to the reference value which is adjusted by some corrective feedbacks. Finally, it proceeds to a PI controller which determines the output current. It is worth mentioning that both the SVC and the STATCOM controller were suspended, if the input voltage (v_5) dropped below 0.7pu. This mechanism is not shown in the block diagrams due to space limitation.

The angle and voltage stability indices for cases B and C are listed in Table III. In contrast with case A which was voltage unstable, the rows associated with cases B and C in this table show that a voltage support device connected to bus 5 in this system not only improved transient angle index, but also fixed the violated criterion on the voltage stability index.

Figure 4(a) compares the voltage at bus 5 in cases A, B, and C. It can be seen that the voltage dropped below the threshold (0.8pu) in case A and stayed there for 0.804s. Figure

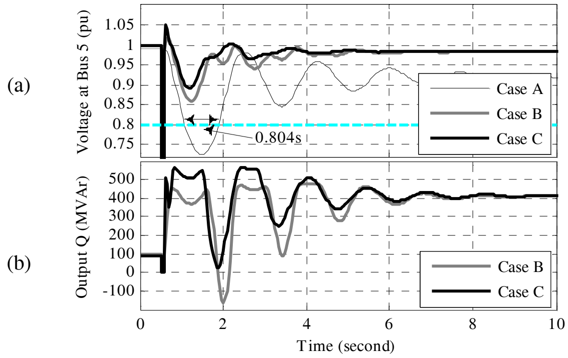

Figure 4. Comparison of the bus voltage magnitude and reactive power output with and without SVC and STATCOM in cases A, B, and C

TABLE III. TRANSIENT STABILITY INDICES FOR CASES A, B, AND C

Case No	*Case Description*	*Stability Index*	
		Angle	*Voltage*
A	Without SVC or STATCOM	59.98%	0.804s
B	With SVC	67.92%	0.000s
C	With STATCOM	69.46%	0.000s

4(b) shows the contribution of the SVC and STATCOM in cases B and C, in order to maintain the voltage at bus 5. It can be seen that with the presence of the SVC or the STATCOM, the voltage did not fall below 0.8pu. Comparison of cases B and C with case A shows that this system requires a voltage support device, in order to maintain transient voltage requirement following large disturbances. Thus, in the case studies presented in the next section, this system is equipped with either an SVC or a STATCOM connected to bus 5.

V. CYBER ATTACK CASE STUDIES

This section presents the results of 14 case studies conducted in TSAT. In cases 1 to 7, the system was equipped with an SVC connected to bus 5. In cases 8 to 14, the SVC was replaced by a STATCOM. All of these 14 cases simulated the same contingency, which was a 3-phase bolted fault at bus 7 at time 0.5s cleared by opening line 3-7 at 567ms. Except for cases 1 and 8, all of the other 14 cases simulated modification cyber attacks. In all of these 12 cases, an attacker gained unauthorized access to the communication link between the SVC's (or the STATCOM's) measurement and controller, and tampered it by adding positive or negative biases. These modification attacks can be characterized by (3), where $v'_5(t)$ and $v_5(t)$ denote modified and un-modified voltages at bus 5, respectively, and Δv is the bias value. Note that cases 1 and 8 simulated the system without any cyber attacks (or $\Delta v = 0$) and were the base cases for cases 2-7, and 9-14, respectively.

$$v'_5(t) = \begin{cases} v_5(t) & t < 0.567s \\ v_5(t) + \Delta v & t \geq 0.567s \end{cases} \quad (3)$$

A. *Cyber Attacks on the SVC (Cases 1-7)*

Cases 1-7 studied the system with an SVC connected to bus 5. In case 1, the added bias was zero. In other words, this case did not model any cyber attacks on the system. In contrast, cases 2-7 studied cyber attacks with bias values from -0.3pu to +0.3pu. Table IV lists the angle and the voltage stability indices for all of these cases. The row associated with case 1 in this table indicates that the SVC base case (no cyber attack) was angle stable and also satisfied the criterion on

TABLE IV. ANGLE AND VOLTAGE STABILITY INDICES FOR CASES 1 TO 14

Voltage Support Device	*Case No*	*Bias (pu)*	*Stability Index*	
			Angle (%)	*Voltage (s)*
SVC	1	0	67.90	0
	2	-0.3	60.53	0.708
	3	-0.2	67.95	0
	4	-0.1	67.95	0
	5	+0.1	66.15	0
	6	+0.2	59.83	0.696
	7	+0.3	-97.07	1.320
STATCOM	8	0	69.46	0
	9	-0.3	69.48	0.712
	10	-0.2	70.13	0
	11	-0.1	70.12	0
	12	+0.1	65.07	0
	13	+0.2	51.63	1.392
	14	+0.3	-97.34	0.828

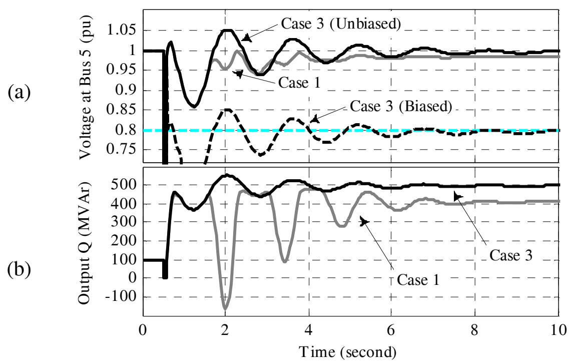

Figure 5. v_5, v'_5, and Q_{SVC} in case 1 and case 3

transient voltage. In case 2 the -0.3pu bias made v'_5 drop below 0.7pu, quickly. As a result, the SVC controller was suspended and could not inject reactive power to support the voltage at this bus. Thus, this attack was successful and made the system voltage unstable. In contrast, the negative biases in cases 3 and 4 did not result in SVC controller suspension. On the other hand, they caused the SVC to inject more reactive power to the system. These two attacks were unsuccessful and even improved the angle stability index.

Among the attacks with positive biases, the cyber attack of case 5 with +0.1pu bias resulted in ~2% decrease in the angle index and did not affect the voltage index. In case 6, the attack successfully violated the voltage criterion. It can be seen that the voltage index for this case was 0.696s which was more than the 0.330s threshold. Finally, the attack in case 7 was the only attack that made the system angle unstable. It can be seen that the angle stability index for this case was negative. This attack violated the voltage stability criterion, too.

To clarify the attack impact, consider case 3. Figure 6 compares Q_{SVC}, v_5, and v'_5 for cases 1 and 3. In case 3, the SVC controller sensed a biased voltage below the setting value (0.95pu), and thus increased the SVC's reactive power output. It can be seen that the reactive power output hit the upper limit (500MVar) in this case. Note that the voltage at bus 5 could have kept increasing and caused an overvoltage protective tripping, if the capacity of SVC was large enough.

B. *Cyber Attacks on the STATCOM (Cases 8-14)*

Cases 8-14 are analogous to cases 1-7, except that they study the system with a STATCOM instead of an SVC. Table

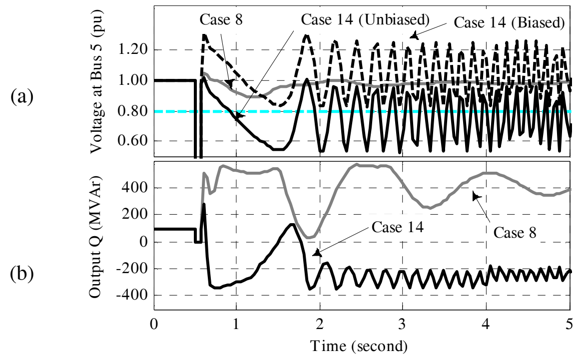

Figure 6. v_5, v_5', and $Q_{STATCOM}$ in case 8 and case 14

III shows that the base case, i.e. case 8, was angle stable and satisfied the voltage constraint, too. Similar to case 2 with SVC, the STATCOM controller was suspended in case 9, since the modified voltage dropped below 0.7pu. As a result, this attack violated the voltage index. In contrast, the negative biases in cases 10 and 11 did not result in STATCOM's suspension. These attacks not only did not violate the voltage constraint, but also improved the angle index by ~1%. In case 12, the positive bias resulted in a slight degradation of angle index, but did not affect the voltage index. In case 13, the attack could decrease the angle index by ~20% and could result in the violation of the voltage index, too. Finally, the attack in case 14 successfully made the system angle unstable. This attack also violated the voltage index.

Figure 6 depicts the contribution of the STATCOM along with the voltage at bus 5 for cases 8 and 14. Figure 6(a) shows that the biased voltage in case 14 was above the setting value (1.05pu), and made the STATCOM reduce its reactive power output. Figure 6(b) depicts that it eventually absorbed reactive power from the system, which worsened the voltage profile at bus 5 and also made the system angle unstable.

To summarize, the above case studies showed that the modification attacks can deteriorate the transient stability margin, or even make the system unstable. As previously shown in Table IV, SVC cases 2, 6, and 7 and STATCOM cases 9, 13, and 14 which took advantage of bigger bias magnitudes, all violated the voltage stability index. Regarding the bias sign, it can be concluded that the positive biases are more dangers compared to the negative biases, especially shortly after the fault is cleared. The reason is that the system is more vulnerable in this period, due to insufficient reactive power support. Examples of effective positive bias attacks were cases 7 and 14. In these cases, positive biases boosted up the modified voltages. Therefore, voltage support devices injected less reactive power into the system, or even absorbed reactive power from the system.

VI. Conclusions and Future Work

This paper discussed cyber security issues in smart grids. Then, it presented results of studies of modification cyber attacks impact on transient stability of smart grids with voltage support devices, such as SVC or STATCOM. In the studies, the attacker gained access to the communication link between the sensor and the controller of the voltage support device, and modified it by adding a bias to the measurement data. To study the impact of the attacks on system transient stability, two stability indices for angle and voltage stability were used. Simulation results showed that cyber attacks on SVC or STATCOM could cause a deterioration of the stability margin, or even make the system unstable. It was observed that the effectiveness of the attacks highly depended on the bias magnitude and sign. Future work includes further impact analysis of cyber attacks on other smart grids, investigation of mitigation strategies, and development of frameworks to identify cyber physical system vulnerabilities.

References

[1] "Guidelines for smart grid cyber security," National Institute for Standards and Technology, NISTIR 7628, 2010.
[2] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber physical system security for the electric power grid," *Proceedings of the IEEE,* vol. 100, pp. 210-224, 2012.
[3] S. Baker, S. Waterman, and G. Ivanov, "In the crossfire: Critical infrastructure in the age of cyber war," Center for Strategic and International Studies (CSIS) McAfee Inc., 2009.
[4] "Cyber attacks against infrastructure jump 17-fold warns National Security Agency," [Online]. Available: http://www.smartgridnews.com
[5] M. Mertz, "NERC CIP compliance: We've identified our critical assets, now what?," in *Proc. 2008 IEEE Power and Energy Society General Meeting,* pp. 1-2, July, 2008.
[6] D. Kundur, F. Xianyong, L. Shan, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Proc. 2010 First IEEE International Conference on Smart Grid Communications,* pp. 244-249, 4-6 October, 2010.
[7] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A smart grid vulnerability analysis framework for coordinated variable structure switching attacks," in *Proc. 2012 IEEE Power and Energy Society General Meeting,* pp. 1-6, 22-26 July, 2012.
[8] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Switched system models for coordinated cyber-physical attack construction and simulation," in *Proc. 2011 IEEE International Workshop on Smart Grid Modeling and Simulation,* pp. 49-54, 2011.
[9] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *Proc. 2010 IEEE Power and Energy Society General Meeting,* pp. 1-6, 25-29 July, 2010.
[10] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," in *Proc. 2009 IEEE/PES Power Systems Conference and Exposition,* pp. 1-8, March, 2009.
[11] O. Kosut, J. Liyan, R. Thomas, and T. Lang, "Malicious data attacks on the smart grid," *IEEE Trans. on Smart Grid,* vol. 2, pp. 645-658, 2011.
[12] X. Le, M. Yilin, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. on Smart Grid,* vol. 2, pp. 659-666, 2011.
[13] D. Kundur, "Cyber Security of the Smart Grid." Class Handouts: Texas A&M University, 2012.
[14] M. T. O. Amanullah, A. Kalam, and A. Zayegh, "Network security vulnerabilities in SCADA and EMS," in *Proc. 2005 IEEE Transmission and Distribution Conference and Exhibition,* pp. 1-6, 2005.
[15] T. Flick, J. Morehouse, and C. Veltsos, *Securing the Smart Grid : Next Generation Power Grid Security.* Burlington, MA: Syngress, 2011.
[16] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, and V. Vittal, "Definition and classification of power system," *IEEE Trans. on Power Systems,* vol. 19, 2004.
[17] "TSAT User Manual," Powertech Labs Inc., Canada, 2012.
[18] "Western Electricity Coordinating Council planning standards," NERC/WECC, 2003.
[19] "DSA*Tools* Overview," [Online]. Available: http://www.dsatools.com
[20] Y. J. Zhang, C. Chen, Y. Li, and G. B. Wu, "Dynamic voltage support planning for receiving end power systems based on evaluation of state separating and transferring risks," *Electric Power Systems Research,* vol. 80, pp. 1520-1527, 2010.