Network Delay Caused by Cyber Attacks on SVC and its Impact on Transient Stability of Smart Grids

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

Sruti Nuthalapati
Department of Electrical and Computer Engineering
University of Texas at Austin
Austin, TX, USA
nsruti@utexas.edu

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

***Abstract*—A smart grid is a typical cyber-physical system, which presents a tight coupling between cyber communications and a physical power network. Cyber security of smart grid is becoming a major concern throughout design and implementation of smart grid applications and technology. Therefore, it is essential to study the impact of cyber attacks on smart grids. This paper discusses cyber attacks that induce communication network delays and their impact on transient stability. Cyber attacks are launched on measured data for a FACTS device (static var compensator – SVC) that connects to the IEEE 39 bus benchmark system. Case studies are presented which analyze the impact of two types of communication delays, fixed and random, on transient angle stability and transient voltage stability on the benchmark system. The test system and cyber attacks are modeled with DSATools^{TM}. Simulation results show that some network delays induced by cyber attacks can make the system unstable.**

***Index Terms* – cyber security, smart grid, cyber attack, SVC, transient stability, communication network delay**

I. INTRODUCTION

To meet the requirements for the future energy infrastructure, modern power systems are increasingly incorporating communication technologies into advanced monitoring and control applications. This motivates the development of smart grids, which are designed to integrate large penetration of distributed energy, reduce carbon emissions, and provide energy services in an efficient and reliable way [1].

Some smart grid applications, such as Demand Response (DR), Wide Area Measurement System (WAMS), Flexible AC Transmission System (FACTS), and Advanced Metering Infrastructure (AMI), are widely deployed to facilitate smart grid operations. An essential feature of these applications is their dependency on advanced two-way communication, which inevitably introduces vulnerabilities to cyber attacks [2]. Furthermore, geographical dispersion of smart grids also presents potential attackers opportunities to launch a cyber or physical attack. Therefore, the cyber-physical security of smart grids is becoming a major concern throughout design and implementation of smart grid applications and technology.

Efforts have been taken to analyze the impact of cyber attacks on power systems, in terms of vulnerability analysis, framework design, test bed development, and cyber attack simulation. Cyber vulnerabilities in power systems have been identified in [3],[4]. Reference [5] proposed a framework for impact analysis of cyber attacks, using directed graphs to represent the cyber and physical entities. To analyze the impact of cyber attacks, some researchers have focused on network delay induced by Denial-of-Service (DoS) attacks. Reference [6] applied a series of fixed delay to a logic-controlled braking resistor. Simulation results in the paper showed that a big delay could make the test system unstable.

In order to better study the interaction between cyber communications and physical power systems, many test beds that use "co-simulation" technology were developed during recent years. Researchers in [7] developed a test bed for SCADA security research, and launched a Distributed DoS attack on SCADA, resulting in overloading of a transmission line. Another test bed was developed by researchers in [8], in which a coordinated DoS attack was launched on control center. A line was overloaded due to the network delay.

The authors have performed some earlier work in analyzing the impact on power system transient stability of cyber attacks launched on a static var compensator (SVC) and a static synchronous compensator (STATCOM) [9],[10]. A modification attack was launched on a SVC and a STATCOM in [9]; simulation results showed that the generators could lose synchronization when large positive biases were applied. An extended study was conducted in [10] while considering three cyber attack scenarios. The earlier work neglects the typical network delays that are present during data transmission and assumes network delay due only to cyber attacks. The work reported in this paper studies the impact of network delays due to cyber attacks along with typical network delays. Transient stability analysis results from several cyber attack studies on the IEEE 39 bus test system are presented.

In this paper, section II discusses cyber attacks and network delay models used in this paper. Section III introduces power system voltage control and transient stability indices. Section IV introduces the test system used in this

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

978-1-4799-6415-4/14/$31.00 ©2014 IEEE

paper. Case studies results are presented in section V. Finally conclusions are given in section VI.

II. Cyber Attacks on Communicaton Network

Smart grids are increasingly incorporating communication techniques that enable operators and customers to access the information in real time. This requires data exchange between control center and end users, hence greatly facilitates smart grid by operating efficiently and reliably. Meanwhile, cyber vulnerabilities are introduced inevitably. A potential attacker with knowledge of communication protocols can easily perform a cyber attack, such as Denial-of-Service attack, common gateway interface (CGI) attack, DNS spoofing attack, authentication server attack, man-in-the-middle (MITM) attack and manipulation attack [2]. Among all the possible consequences of cyber attacks, network delay is most commonly discussed and therefore is the focus of this paper. In this section, cyber attacks on communication protocols that cause network delays are introduced.

A. Cyber Attacks Causing Network Delay

Network delay consists of propagation delay, transmission delay, queuing delay, and processing delay. Successful cyber attacks can 1) increase the length of queue to prolong the queuing delay and transmission delay; and 2) consume the computation resource to prolong the processing delay.

Since many protocols used in current power system are not well protected [11], various cyber attacks can be potentially launched by attackers. Popular cyber attacks that cause network delay are introduced as follows.

1) Denial-of-Service Attack

Denial-of-Service (DoS) attack refers to a set of attacks that slow network performance, or make network unavailable to perform intended functionalities [12]. Several most commonly happened DoS attacks are introduced as follows.

a) Smurf attack: an attacker broadcasts echo requests through large number of packets with victim's spoofed IP. Any devices that defaulted to response to the request will issue replies to the victim, causing victim's device be flooded, slow down or out of order [13].

b) SYN flood attack: an attacker sends a sequence of SYN requests to victim's device, causing victim's resources consumed, and unresponsive to legitimate traffic.

c) Distributed DoS attack (DDoS): an attacker uses multiple computers to launch DoS attack [12]. Popular DDoS attacks include UDP flood, ICMP flood and Ping of Death.

2) Common Gateway Interface Attack

Common gateway interface (CGI) attack refers to an attacker can make the server prone to many kinds of attacks by investigating CGI scripts. For example, attacker would know what operation system the victim use, then the attacker can use the deficiency to access the server, modify or delete files. Also, by sending multiple CGI requests to the victim server, the CPU resources of the victim server will be consumed quickly, since the victim server needs to fork a new process for each request, and forking a process is an extremely expensive operation [14].

3) Authentication Server Attack

Authentication server attacks are targeting authentication server, by sending signatures to the server. Because it takes time to check the signature, multiple requests will consume the resources of the server.

4) Domain Name System Spoofing Attack

Domain name system (DNS) spoofing attack intends to direct diverting traffic to a fake IP address. By modifying the name server's cache database, the name server will return an incorrect IP address, so that the traffic is redirected and usually fake IP corresponds to phishing websites [15].

5) Man-In-The-Middle Attack

Man-In-The-Middle (MITM) attack refers to the attacker intercepts messages between two victims. By doing so, the attacker must be able to be protocol compliant for both ends.

6) Modification Attack

Modification attack refers to an attacker changes messages in transit. A network delay can be generated by changing time stamps. Because the induced messages is compliant to protocols, the attack is hard to detect. Most times a single manipulative act is insufficient to mount an effective attack, multiple manipulations may need to be repeated to have significant impact [16].

B. Network Delay Modeling

In this paper, the network delay is modeled as fixed delay and exponentially distributed delay, which are two commonly used delay models in sensor network analysis [17].

Fixed delay can be easily modeled by applying different constant values to the communication link. And exponential distributed delay can be randomly generated by a pseudo random seed. We call it "random delay" because it is randomly generated. The probability density function (pdf) of an exponential distributed delay [18] can be defined as:

$$f(x;\beta)=\begin{cases}\frac{1}{\beta}e^{-x/\beta}, & x\geq 0\\ 0, & x<0\end{cases} \tag{1}$$

Where $\beta>0$ is a scale parameter of the distribution, and it equals to the mean value of the exponential distribution. When increasing β, more large delays may appear.

III. Power System Voltage Control and Transient Stability

A. Power System Voltage Control

Power system stability of the modern interconnected power system is a major concern in power system security operation [19]. Bus voltages play an important role in power system stability. Bad voltage profiles can induce system instability and even a voltage collapse. Therefore, it's essential to keep bus voltage within an acceptable range for power system operation and voltage control.

Reactive power compensation is known as an efficient voltage control method to improve power system voltage stability. Besides the excitation control in generators, FACTS devices are gaining popularity recently, due to their fast control of reactive power.

B. Cyber Attacks on SVC

Typically an SVC comprises one or more actuators, i.e. thyristor controlled reactor (TCR) and thyristor switched capacitor (TSC), and an SVC controller [20]. The SVC controller receives measurement signals from a wired or wireless distributed sensor network. The signal may come from local measurement devices in the same substation, or/and from remote bus, depending on the control strategy implemented in the SVC controller. A potential attacker can launch cyber attacks, such as those introduced in section II, to cause a network delay when transmitting signals from sensors to the controller, and from the controller to the actuator. For example, an attacker can perform a DoS attack by broadcasting echo request packets containing a SVC controller's IP, causing many other network devices to respond to the IP address. Large data volume increases the queuing delay and processing delay. Man-In-The-Middle attack can also be used to delay traffic between sensor and controller by manipulating time stamp of packets [21].

C. Power System Transient Stability

Power system transient stability is the ability of an interconnected synchronous system to regain synchronization and a state of operation equilibrium after being subjected to a physical disturbance [19]. Power system stability can be classified based on the system variables observed, such as angle, voltage and frequency. In this paper, the impact of cyber attacks on angle stability and voltage stability are studied. Two stability indices, angle stability index and voltage stability index, were used to quantify the impact of cyber attacks on power system transient stability.

1) Angle Stability and Angle Stability Index

Angle stability refers to the ability of power system to maintain synchronization when subjected to a disturbance, by maintaining or restoring the equilibrium between the mechanical and the electromagnetic torque [22]. A simplified swing equation as shown in (2) can be used to study the motion of a single synchronous generators.

$$J\frac{d^2\theta}{dt^2} = T_m - T_e \qquad (2)$$

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

To quantify the impact of cyber attacks on angle stability, an angle stability index [22] is introduced as shown in (3).

$$\eta = \frac{360^o-\delta_{max}}{360^o+\delta_{max}} \times 100\%, -100 < \eta < 100 \qquad (3)$$

Where δ_{max} is the maximum angle separation of any two generators in the post-contingency system. Note that $\eta > 0$ and $\eta \leq 0$ denote stable and unstable conditions.

2) Voltage Stability and Voltage Stability Index

Voltage stability refers to the ability of power system to maintain the voltage at all buses within a certain level when subjected to a disturbance [22]. A deteriorated voltage profile may cause circuit breaker to be tripped by protective relays, or even cause cascading failures.

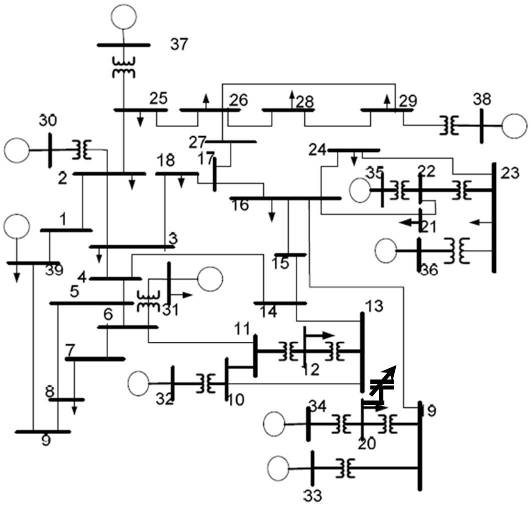

Figure 1. IEEE 39 bus test system

According to the Western Electricity Coordinating Council (WECC) standards [23], after an event or fault leading to the loss of a single power system element, load bus voltages must satisfy the following two requirements: 1) the voltage dip/sag should not exceed 25%; 2) the voltage dip/sag must not exceed 20% for more than 20 cycles (330 milli-seconds in 60 Hz systems). Based on these requirements and since all the contingencies studied in this paper lead to voltage drops, the voltage stability index was defined to be the maximum time a load bus voltage remains below 0.8pu, among all load buses.

IV. Simulation Setup

A. Test System

The IEEE 39 bus benchmark system was used to analyze the impact of cyber attacks on transient stability. The single line diagram shown in Fig. 1 comprises 10 generators, 16 loads, 13 transformers and 34 lines. The system parameters can be found in [24].

B. System Modeling

This system was modeled in Transient Security Assessment Tool (TSAT) of DSATools^{TM} package version 13 [25]. TSAT is a time-domain simulation tool designed for power system dynamic behavior assessment. Each generator was modeled as a round rotor synchronous generator with an exciter and a power system stabilizer (PSS). The loads in the system were modeled as constant PQ loads. Transformers and transmission lines were modeled as Pi models.

UDM allows a user to implement a customized control function using blocks available in the element library. A lookup table was used to store a number string that contained random delays. The string was randomly generated by MATLAB. During simulation, TSAT read the number from the lookup table sequentially, and applied the delay to the SVC controller.

SVC was allocated at bus 20, according to the optimized allocation given in [26]. The capacity ranges from -400 MVAr to 400 MVAr with a fixed 100 MVar capacitor bank. So the adjustable capacity ranges from -300 MVAr to 500 MVAr.

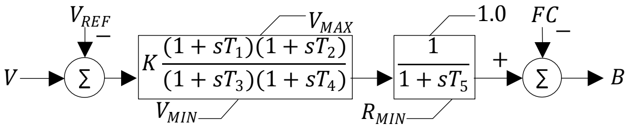

Figure 2. SVC control system block diagram

TABLE I Transient Stability Indices for cases without and with SVC when subjected to a contingency

Case Description	Transient Stability Indices	
	Angle Stability Index	*Voltage Stability Index*
Without SVC	36.57%	0.804s
With SVC	45.19%	0.024s

The control blocks for the SVC are depicted in Fig. 2. The voltage at bus 20 is compared with the reference value, and then the error is passed through a PI controller to determine the shunt capacitance. Two case studies were performed by applying a three-phase bolted fault to bus 16. The fault was cleared after 0.1s by opening line 16-17.

The angle and voltage stability indices for these two cases are shown in TABLE I. It can be seen that for the case without SVC, although the system was angle stable, the voltage stability criterion was violated. Because the voltage stability index (0.804s) was more than the maximum acceptable threshold (0.330s). Whereas for the case with SVC, both angle and voltage stability indices were improved.

Two types of network delays, fixed delay and exponentially distributed delay, were modeled. This paper focuses on the impact of attack-induced network delay on power system transient stability. The impact on controller stability when exposed to propagation delay is neglected. However, the cases simulated in this paper can be seen as an extensive study on a wide range of propagation delays.

C. Cyber Attack Scenarios

The attacker can launch cyber attacks whenever the power system is operating in normal, alert, emergency, extreme or restorative state. Therefore, multiple scenarios should be considered based on the timing that cyber attacks are launched. Due to the space limitation, this paper studies the scenario that cyber attacks launched at the same time with contingency.

V. Case Studies

This section presents the results of 11 case studies conducted in TSAT. In cases 1 to 6, the system equipped with an SVC was subjected to a fixed delay induced by cyber attacks. No network delay was considered in case 1 for comparison purposes. Fixed delays ranged from 100 ms to 500 ms with a step of 100 ms for cases 2 to 6. In cases 7 to 11, the same system was subjected to an exponentially distributed random delay induced by a cyber attack.. The mean value β defined in (1) was 2, 5, 10, 15, and 20, respectively. For each case, the random delays in the lookup table ranged from 100 ms to 500 ms. All of these 11 cases simulated the same contingency, which was a 3-phase bolted fault at bus 16 at time 1.0s, and cleared by opening line 16-17 after 6 cycles (0.1s). The cyber attacks were launched on the SVC controller at the same time with the contingency.

A. Impact of Fixed Network Delay

The angle and voltage stability indices for cases 1 to 7 are shown in TABLE II. When compared to case 1 (with no delay), cases 2 to 6 (with fixed delays) had deteriorations of both angle stability index and voltage stability index. In cases 2 to 4, increases in delay duration gradually decreased both indices, but the system remained stable ($\eta > 0$). Whereas in cases 5 and 6, fixed delays of 400 ms and 500 ms, respectively, caused the system to go unstable ($\eta < 0$).

Fig. 3 and Fig. 4 show the generator angles (relative to slack bus), voltage at bus 20 and the output of SVC of cases 1, 3, and 5. In Fig. 3, the SVC controller always received measurement value with a delay of 200 ms. This caused a lag in the output of SVC. As a result, the voltage at bus 20 (V_{20}) fluctuated with a higher magnitude, and made relative generator angles take longer time to settle down. In Fig. 4, output of SVC in case 5 boosted V_{20} to 1.2 p.u. at 2.5 second, and reduced V_{20} to 0.4 p.u. at 3.1 second. Compare to case 1, we can find that SVC in case 5 absorbed reactive power when bus 20 needed it most. This is the worst case. Generator angles were departing from each other, then system went unstable.

B. Impact of Randomly Generated Network Delay

The exponentially distributed network delays for cases 7 to 11 were generated randomly using different β values. TABLE II shows angle and voltage stability indices for cases 7 to 11. Each case was repeated 20 times using different sets of random relays with respect to the same value of β. For all the cases with random delay, the system remained stable ($\eta > 0$). However, as β increased, the indices started to deteriorate because the large delay segments tended to appear more frequently as β got larger.

Generator angles, voltage at bus 20 (V_{20}), voltage that was received by SVC (V_{20}') and output of SVC (Q_{SVC}) in case 10 ($\beta = 15$) are shown in Fig. 5. Generally the random delay did not affect system stability too much. $V_{20}^{'}$ contained small and large delay segments compared to V_{20}. Q_{SVC} in case 10 was similar to that in case 1. In addition, a large delay segment at 6.5s resulted in a difference in reactive power output.

To summarize, network delays caused by cyber attacks can deteriorate the transient stability margin, or possibly make the system unstable. Large fixed delays can make the system unstable. Whereas exponentially distributed delay has less effect on transient stability.

TABLE II Angle and voltage stability indices for cases 1 to 11

Delay Type	Case No.	Delay / β	Stability Indices	
			Angle (%)	*Voltage (s)*
Fixed Delay	1	0	45.19	0.024
	2	100 ms	44.78	0.024
	3	200 ms	41.08	0.040
	4	300 ms	31.34	0.628
	5	400 ms	-74.46	1.440
	6	500 ms	-72.96	1.752
Randomly Generated Delay	7	2	42.74	0.024
	8	5	41.90	0.024
	9	10	41.67	0.024
	10	15	42.87	0.024
	11	20	37.99	0.492

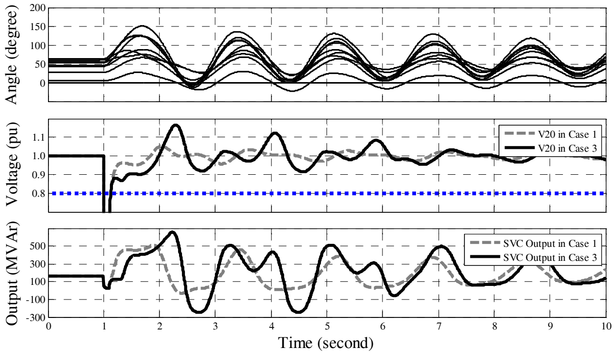

Figure 3. Generator angles, V_{20} and SVC output in case 1 and 3

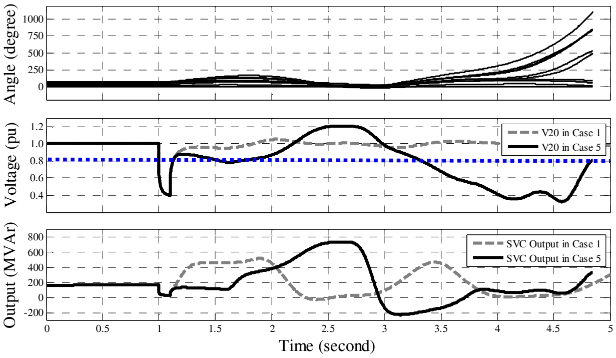

Figure 4. Generator angles, V_{20} and SVC output in case 1 and 5

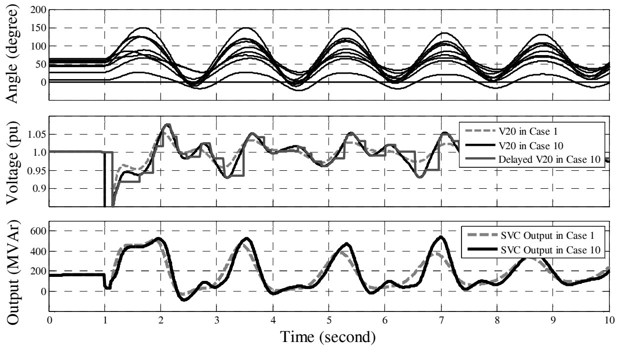

Figure 5. Generator angles, V_{20}, V_{20}' and SVC output in case 1 and 10

VI. Conclusions and Future Work

This paper discussed cyber attacks that can cause network delay in power system sensor networks. Two types of network delays, fixed delay and exponentially distributed delay, were modeled. Their impact on power system transient stability was studied. Simulation results showed that both fixed delay and exponentially distributed delay can deteriorate transient stability margin. Future work includes developing a cyber-physical test bed for further cyber security research.

References

[1] "The Smart Grid: An Introduction," U.S. Department of Energy [Online]. Available: http://energy.gov/

[2] M. Govindarasu, A. Hahn, and P. Sauer, "Cyber-Physical Systems Security for Smart Grid," Power Systems Engineering Research Center May 2012. [Online]. Available: http://www.pserc.wisc.edu

[3] M. Yilin, T. H. J. Kim, K. Brancik, D. Dickinson, L. Heejo, A. Perrig, and B. Sinopoli, "Cyber Physical Security of a Smart Grid Infrastructure," *Proceedings of the IEEE,* vol. 100, pp. 195-209, 2012.

[4] 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.

[5] 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 1st IEEE International Conference on Smart Grid Communications,* pp. 244-249, 4-6 Oct. 2010

[6] M. H. Ali, T. Murata, and J. Tamura, "Influence of Communication Delay on the Performance of Fuzzy Logic-Controlled Braking Resistor Against Transient Stability," *IEEE Trans. on Control Systems Technology,* vol. 16, pp. 1232-1241, 2008.

[7] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "SCADA Cyber Security Testbed Development," in *Proc. 2006 North American Power Symposium,* pp. 483-488, 17-19 Sept. 2006

[8] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," *IEEE Trans. on Smart Grid,* vol. 4, pp. 847-855, 2013.

[9] B. Chen, S. Mashayekh, K. L. Butler-Purry, and D. Kundur, "Impact of Cyber Attacks on Transient Stability of Smart Grids with Voltage Support Devices," in *Proc. 2013 IEEE/PES General Meeting* Vancouver, Canada, 2013.

[10] B. Chen, K. L. Butler-Purry, and D. Kundur, "Impact Analysis of Transient Stability Due to Cyber Attack on FACTS Devices," in *Proc. 2013 North American Power Symposium* Mahhatan, Kansas, 2013.

[11] I. H. Lim, S. Hong, M. S. Choi, S. J. Lee, T. W. Kim, S. W. Lee, and B. N. Ha, "Security Protocols Against Cyber Attacks in the Distribution Automation System," *IEEE Trans. on Power Delivery,* vol. 25, pp. 448-455, 2010.

[12] "Understanding Denial-of-Service Attacks," Web Page: http://www.us-cert.gov/ncas/tips/ST04-015

[13] S. Kumar, "Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet," in *Proc. 2007 International Conference on Internet Monitoring and Protection,* pp. 25-25, 1-5 July 2007

[14] M. Cross. (2006). *Developer's Guide to Web Application Security.* Burlington: Syngress.

[15] M. Anagnostopoulos, G. Kambourakis, P. Kopanos, G. Louloudakis, and S. Gritzalis, "DNS amplification attack revisited," *Computers & Security,* vol. 39, Part B, pp. 475-485, 2013.

[16] N. Kothari, R. Mahajan, T. Millstein, R. Govindan, and M. Musuvathi, "Finding protocol manipulation attacks," *SIGCOMM Comput. Commun. Rev.,* vol. 41, pp. 26-37, 2011.

[17] L. Victor, T. Milind, and L. O. Charles. (2003). *Distributed Sensor Networks: A Multiagent Perspective.* Kluwer Academic Publishers.

[18] W. Sun, F. Brannstrom, and E. G. Strom, "On clock offset and skew estimation with exponentially distributed delays," in *Proc. 2013 IEEE International Conference on Communications,* pp. 1872-1877, 9-13 June 2013

[19] P. Kundur. (1994). *Power System Stability And Control.* New York: McGraw-Hill.

[20] I. S. S. C. W. Group, "Static VAr compensator models for power flow and dynamic performance simulation," *IEEE Trans. on Power Systems,* vol. 9, pp. 229-240, 1994.

[21] J. T. Chiang, J. J. Haas, H. Yih-Chun, P. R. Kumar, and J. Choi, "Fundamental Limits on Secure Clock Synchronization and Man-In-The-Middle Detection in Fixed Wireless Networks," in *Proc. 2009 IEEE INFOCOM,* pp. 1962-1970, 19-25 April 2009

[22] 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 stability," *IEEE Trans. on Power Systems,* vol. 19, pp. 1387-1401, 2004.

[23] *WECC WECC-NERC Planning Standards*, WECC Standard 2007.

[24] A. Pai. (1989). *Energy Function Analysis for Power System Stability.* Springer.

[25] "DSATools Overview," Web Page: http://www.dsatools.com

[26] L. Xijuan and B. Jeyasurya, "Static VAR compensator allocation by simplified sensitivity analysis and its influence on transient voltage performance improvement," in *Proc. 2012 North American Power Symposium,* pp. 1-6, 9-11 Sept. 2012