Proceeding of the IEEE 28th
Canadian Conference on Electrical and Computer Engineering
Halifax, Canada, May 3-6, 2015

On Using Distributed Control Schemes to Mitigate Switching Attacks in Smart Grids

Abdallah Farraj, Eman Hammad, Deepa Kundur
Department of Electrical and Computer Engineering, University of Toronto, Ontario, Canada
Email: {abdallah, ehammad, dkundur}@ece.utoronto.ca

***Abstract*—This work investigates the performance of distributed control schemes in mitigating the effects of a switching attack in smart grid systems. The control schemes use feedback linearization to inject and absorb power in order to achieve transient stability. On the other hand, an adversary utilizes fast-acting energy storage systems in conducting a switching attack in order to destabilize parts of the power grid. Numerical results demonstrate the performance of the control schemes during a switching attack that targets the New England 10-generator 39-bus power system.**

I. Introduction

Interest in smart grid systems has surged recently. Smart grid systems use advanced control, communications, and sensor technologies to improve the efficiency and resilience of the power grid. Moreover, the ongoing integration of the renewable energy sources and the energy storage systems into the traditional power grid accelerates the interest of adopting smart grid technologies and opens the door to new research opportunities.

The timely availability of power system's measurements can help in designing advanced control schemes that help protect the system against disturbances. Parametric feedback linearization (PFL) controller was proposed in [1], [2] to achieve transient stability of a smart grid system by utilizing an external power source at the system generators. Feedback linearization control theory is used in the PFL scheme to convert the nonlinear power system into an equivalent linear system. To achieve stability, sensor measurements are periodically communicated to controllers that then actuate change through calculated power injection and absorption actions.

As the smart grid applications are getting implemented in various power systems, reliability and cyber security issues have recently surfaced. The introduction of the cyber component of the grid can lead to potential cyber attacks on the smart grid. Specifically, switching attacks on smart grid systems have gained recent attention from the research community. Based on understanding the structure of the power system and accessing the system state variables, effective switching attacks can be constructed to disrupt the normal operation of the power system.

Utilizing the concept of variable-structure control, a recent work in [3]–[6] investigated the effect of sliding-mode switching attacks on the stability of power systems. The proposed attack in such works made use of load switching in the power grid to create a sliding-mode control system and consequently cause power system instability. Further, a recent work in [7], [8] proposed using a fast-acting energy storage system (ESS) in conducting a switching attack in order to destabilize parts of the power grid. In such works, an adversary needs to have a physical or cyber access to the circuit breaker, have an access to the system state variable, and have a working knowledge of the system model of the smart grid under the different states of the circuit breaker. Specifically, the adversary intercepts the system measurements before calculating the switching signal in order to switch the circuit breaker of the ESS back-and-forth depending on the value of system state variable.

This work investigates the performance of the PFL control schemes when the power system is under a switching attack that utilizes the energy storage systems (see [7], [8]). The difference between this work and that investigated in [1], [2] is that the disturbance in this paper is a switching attack while it was a physical fault in [1], [2]. Consequently, the PFL controller is proposed in this work to mitigate the effect of the switching attacks that target the system generators using the energy storage systems.

The rest of this paper is organized as follows. The problem setting is presented in Section II, and Section III investigates the properties of the feedback linearization control scheme. The switching attack is detailed in Section IV. Section V numerically investigates the effectiveness of the controller in mitigating the switching attack. Conclusions are shown in Section VI.

II. Problem Setup

Variable-structure systems are nonlinear control systems characterized by ordinary differential equations with discontinuous state functions [9], [10]. Such systems are found useful in modeling and analyzing the behavior of smart grid systems. For example, a variable-structure system can be modelled as

$$\dot{x} = \begin{cases} f_1(x,t), & s(x) > 0 \\ f_2(x,t), & s(x) \leq 0\,, \end{cases} \tag{1}$$

where t is the time variable, $\dot{x}$ denotes the derivative of x with respect to time, x is the system state variable, $f_1(x,t)$ is the system dynamics when $s(x) > 0$, $f_2(x,t)$ is the system dynamics when $s(x) \leq 0$, and $s(x)$ is a state-dependent switching signal. Because it models a dynamical change between two physical systems, Eq. (1) can be useful to model a power system when a circuit breaker switches between two states.

978-1-4799-5829-0/15/$31.00 ©2015 IEEE

An adversary is assumed to be interested in destabilizing part of the power grid by switching a circuit breaker that controls a fast-acting ESS back-and-forth. In order to successfully accomplish this mission, the adversary needs to have a (physical and/or cyber) access to the circuit breaker, develop a knowledge of the model of the power grid under the different states of the circuit breaker, and be able to access the system state variable (through intercepting the cyber infrastructure). The adversary can consequently build a variable-structure system model, design the switching signal, and switch the circuit breaker back-and-forth depending on the value of switching signal.

A. System Model

The New England 10-generator 39-bus physical power system (shown in Fig. 1) is considered in this work. Let N denote the number of generators in the power system. Every Generator i, $\forall i \in \{1, \ldots, N\}$, is described by its internal voltage (E_i), rotor angle (δ_i), relative normalized rotor frequency (ω_i), inertia (M_i), damping coefficient (D_i), electrical power ($P_{e,i}$), and mechanical power ($P_{m,i}$). The relative normalized frequency of Generator i is defined as $\omega_i = \frac{\omega_i^{act} - \omega^{nom}}{\omega^{nom}}$, where ω^{nom} is the nominal angular frequency (in radians per second) of the power system and ω_i^{act} is the actual angular frequency of Generator i.

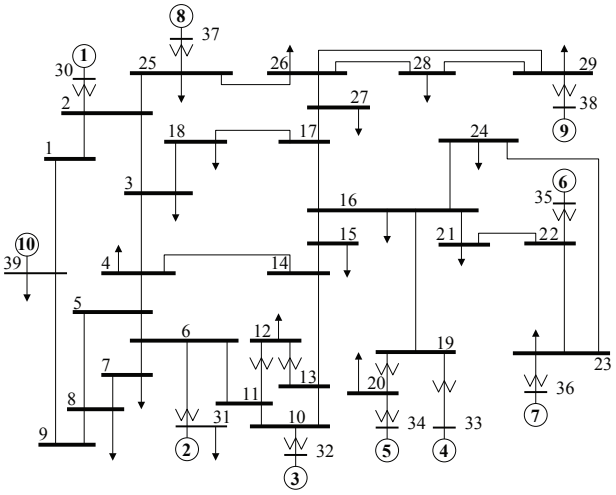

Fig. 1. New England power system

B. Transient Stability

The swing equation links the system parameters in a differential equation, and this model can be used to describe the dynamics of the system generators. The values of the rotor angle and frequency of the system generators can enable the study of transient stability. The swing equation parameters are assumed to be constant even when the system undergoes instability. Further, the Kron-reduction technique [11] is used to reduce the order of the interconnections between the synchronous generators in the power system.

Let $\dot{\delta}_i$ and $\dot{\omega}_i$ denote the derivatives of δ_i and ω_i with respect to time, respectively. Assuming that there is no power control in the system (both the governor and exciter controls are disabled) and that there are no protection schemes to safeguard the generators against frequency fluctuations, the swing equation of Generator i is expressed as [12], [13]

$$\begin{aligned} \dot{\delta}_i &= \omega_i \\ \dot{\omega}_i &= \tfrac{1}{M_i}\left[-D_i\,\omega_i + P_{a,i}\right], \end{aligned} \tag{2}$$

where $P_{a,i} = P_{m,i} - P_{e,i}$ denotes the accelerating power of Generator i. The electrical power of Generator i is defined as [14]

$$\begin{aligned} P_{e,i} = \sum_{k=1}^{N} \; & |E_i|\,|E_k|\,[G_{ik}\cos(\delta_i - \delta_k) + \\ & B_{ik}\sin(\delta_i - \delta_k)], \end{aligned} \tag{3}$$

where $G_{ik} = G_{ki} \geq 0$ is the Kron-reduced equivalent conductance between Generators i and k and $B_{ik} = B_{ki} > 0$ is the Kron-reduced equivalent susceptance between Generators i and k.

Transient stability describes the ability of a power system to remain in synchronism when subjected to disturbances. Through an application of control strategies, transient stability during the presence of a disturbance can be achieved by maintaining both exponential frequency synchronization and phase angle cohesiveness. Exponential frequency synchronization requires the frequencies of all the generators to agree asymptotically with a common value typically set to 60 Hz and normalized in this work to 0. Phase angle cohesiveness mandates that the difference between the phase angle of the different generators in the power system should be below a predefined threshold.

III. Feedback Linearization Control

Synchronous generators in the power system are typically equipped with power control schemes (such as exciter and governor controls) that help to adjust the internal settings of the generators in order to respond to changes and disturbances in the power grid. However, these local power control schemes have slow reaction to rapid changes in the power system. As such, without external power control schemes, the synchronous generators cannot alone achieve transient stability in the presence of a disturbance. Consequently, the use of external control schemes can help in achieving transient stability.

A multi-agent framework that incorporates both cyber and physical elements of a smart grid system is considered [1]. Each cyber-physical agent consists of a synchronous generator, a sensor that measures the rotor phase angle and frequency of the generator, and a local distributed controller that obtains information from the sensors in order to compute a control signal that is applied on an ESS at the synchronous generator's bus.

Applying an external power source at the bus of Generator i, termed as U_i, modifies the swing equation of Generator i to

$$\begin{aligned} \dot{\delta}_i &= \omega_i \\ \dot{\omega}_i &= \tfrac{1}{M_i}\left[-D_i\,\omega_i + P_{a,i} + U_i\right] . \end{aligned} \tag{4}$$

As such, the controller affects the dynamics of the power system by absorbing or injecting a specified amount of real power through the application of a fast-acting ESS at the designated generator's bus. A positive value of U_i means that the controller injects power at the bus of Generator i, and a negative value implies that real power is being absorbed from the bus of Generator i.

A. Centralized PFL

A centralized parametric feedback linearization (CPFL) control scheme relies on receiving timely measurements of the frequency and phase of all synchronous generators in the power system in order to calculate the control signal. Mathematically, the CPFL control for frequency stability and phase cohesion is expressed as [2]

$$U_i = -P_{a,i} - \alpha_i\,\omega_i - \beta_i\left[\delta_i - \delta_i^*\right] , \tag{5}$$

where $\alpha_i \geq 0$ is called the frequency stability parameter of Generator i, $\beta_i \geq 0$ is the phase stability parameter of Generator i, and $\boldsymbol{\delta}^* = [\delta_1^*, \delta_2^*, \ldots, \delta_N^*]^T$ is the desired phase of the system generators. The $\alpha_i\omega_i$ term will asymptotically drive the normalized frequency of Generator i to 0, and the $\beta_i\left(\delta_i - \delta_i^*\right)$ term will drive the CPFL controller to settle the phase of the system generators on $\boldsymbol{\delta}^*$. Consequently, frequency synchronization and phase cohesiveness are maintained after the activation of the controller.

The CPFL controller fully cancels the nonlinear terms in the swing equation of Generator i provided that all system measurements are obtained. Consequently, the swing equation of the interconnected power system reduces into decoupled linear equations after implementing the CPFL controller.

B. Decentralized PFL

The communication channels relaying the system measurements from the sensors to the controllers are vulnerable to cyber attacks (such as denial of service attacks). Consequently, the decentralized parametric feedback linearization (DPFL) controller only utilizes the measurements from the sensors situated near the local generator bus. As a result, the accelerating power term ($P_{a,i}$) cannot be estimated and consequently cannot be cancelled. Mathematically, the DPFL control is expressed as [1]

$$U_i = -\alpha_i\omega_i - \beta_i\left[\delta_i - \delta_i^*\right] . \tag{6}$$

IV. Switching Attack

Before conducting the switching attack, the adversary has to specify the target generator(s) out of the N generators in the power system and design the appropriate switching signal. Let the target generator be denoted as Generator $\hat{i}$, $\forall\,\hat{i} \in \{1, \ldots, N\}$. A fast-acting ESS is assumed to be installed at Generator $\hat{i}$. The value of real power the ESS can inject or absorb at the bus of Generator $\hat{i}$ is termed $U_{\hat{i}}$. The ESS is controlled by a circuit breaker, and the ESS at Generator $\hat{i}$, at any specific moment, can be either injecting power, absorbing power, or disconnected from the grid. Thus, to reflect the incorporation of $U_{\hat{i}}$, the swing equation of Generator $\hat{i}$ becomes

$$\begin{aligned} \dot{\delta}_{\hat{i}} &= \omega_{\hat{i}} \\ \dot{\omega}_{\hat{i}} &= \tfrac{1}{M_{\hat{i}}}\left[-D_{\hat{i}}\,\omega_{\hat{i}} + P_{a,\hat{i}} + \sigma_{\hat{i}}\,U_{\hat{i}}\right] , \end{aligned} \tag{7}$$

where $\sigma_{\hat{i}}$ is the state of the circuit breaker that controls the ESS of Generator $\hat{i}$.

By controlling the value of $\sigma_{\hat{i}}$ through physical or cyber means, the adversary can affect the dynamics of the power system by absorbing or injecting a specified amount of real power. Specifically, when $\sigma_{\hat{i}} = 1$ the ESS of Generator $\hat{i}$ injects power of magnitude $U_{\hat{i}}$ into the generator bus, a value of $\sigma_{\hat{i}} = -1$ indicates that power of $U_{\hat{i}}$ is being absorbed from the generator bus, and the adversary is not actively disturbing the power system when $\sigma_{\hat{i}} = 0$.

Let $f_{\hat{i},0}(x,t)$, $f_{\hat{i},1}(x,t)$, and $f_{\hat{i},2}(x,t)$ denote the system dynamics of Generator $\hat{i}$ when $\sigma_{\hat{i}} = 0$, $\sigma_{\hat{i}} = 1$, and $\sigma_{\hat{i}} = -1$, respectively. To construct a switching attack on Generator $\hat{i}$ using its corresponding ESS, the adversary has to implement the following [7]:

1) determine the system state variable;
2) model the power grid as a switched control system (i.e., find $f_{\hat{i},0}(x,t)$, $f_{\hat{i},1}(x,t)$, and $f_{\hat{i},2}(x,t)$);
3) determine the phase portrait of each subsystem and overlap them on the same plot;
4) find a suitable switching signal using the phase portraits;
5) intercept the system measurements to determine the value of $x(t)$;
6) control the state of the circuit breaker's switch depending on the value of $s(x)$; and
7) drive the system state variable outside the stability region of one of the subsystems.

V. Numerical Results

The New England 10-generator 39-bus power system is considered. The values of M_i's and X'_{di}'s are found in [15], [16] and D_i is set to 20 ms for all generators. The power system is assumed to be running in normal state. However, a switching attack targets the power system at $t = 0.5$ second for 15 seconds.

In the following numerical results, the adversary switches a 0.1-pu (i.e., 10 MVA) power storage at the target generator. The adversary measures the frequency of the target generator (i.e., $\omega_{\hat{i}}$). If $\omega_{\hat{i}} \geq 0$, then $\sigma_{\hat{i}} = 1$, and the attacker injects 0.1-pu real power at the bus of the target generator. However, if $\omega_{\hat{i}} < 0$, then $\sigma_{\hat{i}} = -1$, and the attacker absorbs 0.1-pu real power from the target generator's bus.

The PFL control scheme is activated on all generators at $t = 0.7$ second (i.e., after 200 ms after the start of the switching attack). Further, it is assumed that the power of the ESS that the PFL has access to at each generator is limited to 10% of the mechanical power of the corresponding generator before

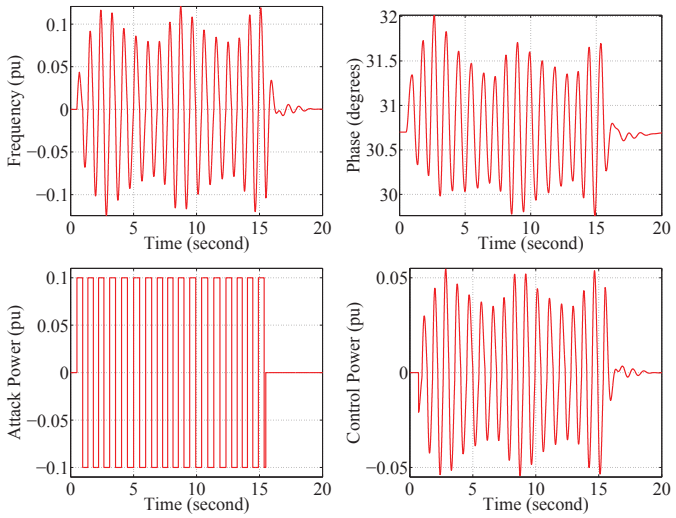

Fig. 2. DPFL controller of Generator 2 vs. switching attack

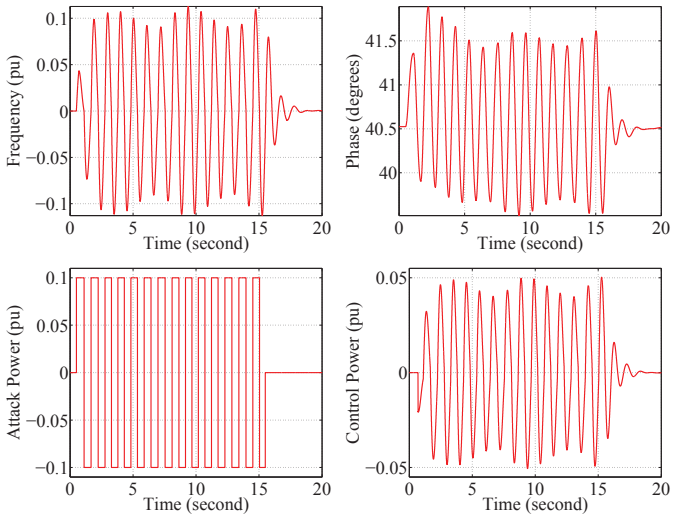

Fig. 3. DPFL controller of Generator 9 vs. switching attack

the beginning of switching attack. For example, U_9 is limited to 0.8292 pu, which is 10% of $P_{m,9}$. In addition, because the DPFL controller is more robust to cyber attacks and that it uses less average control power than the CPFL control scheme, the following numerical results display the performance of the DPFL control scheme in mitigating the switching attack.

Stability time of a generator is measured by finding the difference between the time after which the frequency of the generator is restricted to a 0.8333% threshold (i.e., the time when the frequency of the generator is limited to $\pm$ 0.5 Hz) and the time when the PFL stabilizing controller is activated. Further, the frequency stability parameter (α) is set to 0.45 and the phase stability parameter (β_i) is set to $\alpha/2$.

A. Fixed Attack

In this case, the adversary targets both Generator 2 and Generator 9 during the 15-second switching attack. Consequently, the adversary measures ω_2 and ω_9 and switches the corresponding circuit breakers depending on the signs of ω_2 and ω_9.

Figs. 2 and 3 display the frequency and phase of Generators 2 and 9 along with the details of the switching attack and the output of the PFL control scheme. Even though the control scheme is activated 200 ms after the start of the switching attack, it is noted that the DPFL controller efficiently stabilizes the target generators. It is observed that the average stability time of the system generators (excluding Generator 10) is around 16.0043 seconds and the average external power that is utilized by the DPFL control scheme is about 0.012 pu.

B. Random Attack

The adversary targets two randomly-selected generators (other than Generator 10) every 50 ms in this case. The adversary randomly selects two target generators to conduct the switching attack on at the beginning of the 50-ms period, and the frequencies of the target generators are found in order to determine if the adversary needs to inject or absorb power on each of the target generators. At the end of the 50-ms period, the attacker selects other target generators, and so on.

The performance of the DPFL control scheme is detailed in Table I. It is observed that the controller stabilizes the generators of the power system within about 1 second from the end of the random switching attack. It is also noted that the average external power that is used by the control scheme to stabilize the power system is less than tenth of the attack power.

Let the governor control be activated for the following numerical result. One way to implement a governor controller is to slowly close the gap between the mechanical and the electrical powers of the generator. Let $\dot{P}_{m,i}$ denote the derivative of $P_{m,i}$ with respect to time, then this implementation can be mathematically represented for Generator i as

$$\dot{P}_{m,i} = \kappa_i \left(P_{e,i} - P_{m,i} \right), \tag{8}$$

where $\kappa_i \geq 0$ is the governor's update rate. A value of $\kappa_i = 0$ indicates that the governor control is not activated on Generator i.

Table II shows the performance of the control scheme when the governor control is activated for a value of $\kappa_i = 0.5$. The implemented nonlinear governor closes 90% and 99% of the gap between $P_{m,i}$ and $P_{e,i}$ in 4.6 and 9.1 seconds, respectively. It is seen that there is a reduction (i.e., a save) in both average stability time and control power when the governor control is activated. Results of this table confirm the findings of [2] where it is mentioned that the operation of the PFL controller aligned naturally with that of the governor control.

Results of this section demonstrate that the PFL control scheme can effectively mitigate the effects of the switching attacks. Moreover, it is observed that the power system is stabilized within a short time after the end of the switching attack and that the controller uses a relatively small amount

of power to counter the effects of the adversary.

TABLE I
SYSTEM PERFORMANCE

Generator	Stability Time (s)	Control Power (pu)
1	15.8739	0.0081
2	15.7208	0.0091
3	15.8364	0.0084
4	15.8423	0.0093
5	15.8185	0.0095
6	15.8235	0.0085
7	15.8382	0.0098
8	15.9071	0.0105
9	15.7987	0.0089
Average	15.8288	0.0091

TABLE II
SYSTEM PERFORMANCE: DPFL AND GOVERNOR CONTROL

Generator	Stability Time (s)	Control Power (pu)
1	15.4693	0.0070
2	15.3645	0.0087
3	15.3980	0.0078
4	15.4855	0.0082
5	15.3446	0.0090
6	15.2742	0.0073
7	15.3346	0.0086
8	15.5653	0.0090
9	15.3935	0.0079
Average	15.4033	0.0082

VI. CONCLUSIONS

This paper investigates the performance of distributed control schemes in mitigating switching attacks in smart grid systems. The adversary utilizes fast-acting energy storage systems in conducting a switching attack by intercepting the system measurements and affecting the circuit breaker's switch that controls the energy storage system depending on the value of the system state variable of the target generator. Further, the control schemes use feedback linearization techniques to inject and absorb real power in the power system in order to achieve transient stability.

Performance of the distributed controller is investigated when switching attacks are applied to the New England 39-bus 10-generator power system. Numerical results demonstrate the effectiveness of the feedback linearization control schemes in mitigating the switching attacks and stabilizing the power system.

ACKNOWLEDGMENTS

This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

REFERENCES

[1] E. Hammad, A. Farraj, and D. Kundur, "A Resilient Feedback Linearization Control Scheme for Smart Grids under Cyber-Physical Disturbances," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, pp. 1–5, February 2015.

[2] A. Farraj, E. Hammad, and D. Kundur, "A Cyber-Enabled Stabilizing Controller for Resilient Smart Grid Systems," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, pp. 1–5, February 2015.

[3] 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 *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 49–54, October 2011.

[4] A. Farraj, E. Hammad, D. Kundur, and K. Butler-Purry, "Practical Limitations of Sliding-Mode Switching Attacks on Smart Grid Systems," in *IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–5, July 2014.

[5] S. Liu, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Coordinated Variable Structure Switching Attack in the Presence of Model Error and State Estimation," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 318–323, November 2012.

[6] 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 *IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–6, July 2012.

[7] A. Farraj and D. Kundur, "On Using Energy Storage Systems in Switching Attacks That Destabilize Smart Grid Systems," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, pp. 1–5, February 2015.

[8] A. Farraj, E. Hammad, A. Al Daoud, and D. Kundur, "A Game-Theoretic Control Approach to Mitigate Cyber Switching Attacks in Smart Grid Systems," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 964–969, November 2014.

[9] D. Liberzon, *Switching in Systems and Control*. Systems & Control: Foundations & Applications Series, Birkhäuser, 2003.

[10] A. Sabanovic, L. Fridman, and S. Spurgeon, *Variable Structure Systems: From Principles to Implementation*. IET Control Engineering Series 66, The Institution of Engineering and Technology, 2004.

[11] F. Dörfler and F. Bullo, "Kron Reduction of Graphs With Applications to Electrical Networks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 60, pp. 150–163, January 2013.

[12] P. M. Anderson and A. A. Fouad, *Power System Control and Stability*. IEEE Power Systems Engineering Series, IEEE Press, 1994.

[13] F. Dörfler and F. Bullo, "Synchronization and Transient Stability in Power Networks and Non-Uniform Kuramoto Oscillators," in *American Control Conference (ACC)*, pp. 930–937, June/July 2010.

[14] A. R. Bergen and V. Vittal, *Power Systems Analysis*. Prentice-Hall, second ed., 2000.

[15] T. Athay, R. Podmore, and S. Virmani, "A Practical Method for the Direct Analysis of Transient Stability," *IEEE Transactions on Power Apparatus and Systems*, vol. 98, pp. 573–584, March/April 1979.

[16] B. Pal and B. Chaudhuri, *Robust Control in Power Systems*. Power Electronics and Power Systems Series, Springer, 2006.