On Using Energy Storage Systems in Switching Attacks That Destabilize Smart Grid Systems

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

***Abstract*—A new class of switching attacks in smart grid systems is investigated in this work. The proposed attack relies on calculated switchings of a fast-acting energy storage system (ESS) in order to drive the system state variable of the target generator beyond the stability boundary. Based on understanding the structure of the power system, an adversary uses the swing equation to find the stability boundary of the target generator. In order to conduct a successful switching attack, the adversary intercepts the power system's measurements and switches the circuit breaker of the ESS back-and-forth depending on the value of system state variable. Numerical results show the effectiveness of the proposed switching attack when applied to the New England power system.**

I. Introduction

Smart grid systems utilize advanced control, communications, and sensor technologies to improve the efficiency of the power system and help utility companies better manage and control the energy resources and meet the electricity demand. Moreover, the ongoing integration of the renewable energy sources and the energy storage systems into the power grid accelerates the interest of adopting smart grid technologies.

As the smart grid applications are getting implemented in various power systems, security and reliability issues of the cyber assets of the power grid have recently surfaced. Cyber assets of the smart grid include the communications networks, computing systems, and data storage. The introduction of the cyber infrastructure opens the door for potential hacking and cyber attacks on the smart grid. These attacks can yield financial loses for both the consumers and the utility company though compromising the integrity or confidentiality of the consumer data, the stability of the power grid (or part of it), or the availability of critical data for the control centers.

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.

Variable-structure systems are nonlinear control systems that are characterized by discontinuous dynamics [1]. In this case, the dynamics of the system are changed by a control signal (often called a switching signal) that switches the control system back-and-forth between its switched subsystems. Utilizing the concept of variable-structure control, a recent work in [2]–[7] investigated the effect of sliding-mode switching attacks on the stability of power systems. The proposed attack in [2]–[7] made use of load switching in the power grid to create a sliding-mode control system and consequently cause power system instability. However, the development of such attacks approximated the power system as a single-machine infinite-bus (SMIB) system with a small connected generator along with its load.

This work investigates the use of a fast-acting energy storage system (ESS) in conducting a switching attack in order to destabilize parts of the power grid. In order to successfully accomplish this mission, 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. Using these conditions, the adversary can build a variable-structure system model and design the switching signal accordingly.

The adversary relies on using the swing equation in order to find the stability regions of the target generator under the different states of the ESS. System state information is collected by different sensors scattered around the power grid and is transmitted through a communication network. 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.

Contributions of this work include proposing a new class of switching attacks that utilize fast-acting ESSs. Moreover, the conducted analysis does not assume an SMIB model, the swing equation model of the systems generators is used instead; consequently, the dynamics of the power system are better captured in this development. Further, the proposed attack is applied on the New England 10-generator 39-bus power system.

The rest of this paper is organized as follows. The problem setting is presented in Section II and the proposed switching attack is detailed in Section II. Section IV numerically investigates the effectiveness of the proposed switching attack. Conclusions are shown in Section V.

II. Problem Setup

Variable-structure systems are nonlinear control systems characterized by ordinary differential equations with discontinuous state functions [8]. 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

978-1-4799-1785-3/15/$31.00 ©2015 IEEE

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

where t is the time variable, $\dot{x}$ denotes the derivative of x with respect to time, and x (sometimes denoted as $x(t)$ to emphasize its time dependence) is the system state variable. Moreover, $f_1(x,t)$ is the system dynamics when $s(x) > 0$, and $f_2(x,t)$ is the system dynamics when $s(x) \leq 0$. Further, $s(x)$ is a state-dependent switching signal. The trajectory of the system often refers to the evolution of x in time through state space. This equation, as it models a dynamical change between two physical systems, can be useful to model a power system when a circuit breaker switches between two states.

Theoretical variable-structure switching systems can exhibit high-frequency oscillations in the state variable; this phenomenon is called chattering [8], which is unrealistic for real-life circuit breakers that display practical delays and hysteresis between consecutive switchings. Consequently, to overcome such issue for practical variable-structure switching attacks, a boundary layer, known as the hysteresis margin and termed as $\epsilon > 0$, is employed. This means that switching between the $f_1(x,t)$ and $f_2(x,t)$ subsystems occurs when $s(x)$ crosses the boundary between the lines of ϵ and $-\epsilon$.

A recent work of [2]–[6] investigated using sliding-mode control to design the switching signal. However, the development of the switching attack assumed the target generator is connected to a small switchable load and the rest of the power grid is approximated as an SMIB power system.

To shed light on a potential application of variable-structure control systems in a smart grid system, 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. However, in order to successfully accomplish this mission, the adversary needs to have a physical or cyber access to the circuit breaker, have an access to the system state variable (i.e., x), and have a working knowledge of the system model of the smart grid under the different states of the circuit breaker. Using these conditions, the adversary can build a variable-structure system model, design the switching signal (i.e., $s(x)$) accordingly, and switch the circuit breaker back-and-forth depending on the value of $s(x)$.

Specifically, to construct a switching attack on a smart grid system using an ESS, the adversary has to implement the following steps:

1) determine the system state variable;
2) model the power grid as a switched control system (i.e., find $f_1(x,t)$ and $f_2(x,t)$);
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.

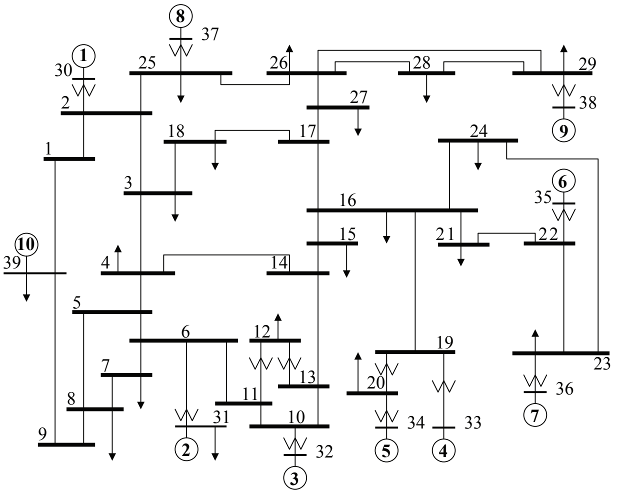


Fig. 1. New England power system

Parameter	Description
E_i	internal voltage of Generator i, $\forall\, i \in \{1,\ldots,N\}$
$P_{e,i}$	electrical power of Generator i
$P_{m,i}$	mechanical power of Generator i
δ_i	rotor angle of Generator i
ω_i	relative normalized rotor frequency of Generator i
X'_{di}	direct-axis transient reactance of Generator i
M_i	inertia of Generator i
D_i	damping coefficient of Generator i

Fig. 2. System parameters

The theme of the attack is to guide the system state variable outside the stability boundary of one of the switched systems by conducting calculated back-and-forth switchings; once that happens, switching can stop and the power system becomes unstable.

We consider the New England 10-generator 39-bus power system shown in Fig. 1. In this power system, Generator 10 at Bus 39 represents the aggregation of a large number of power generators. Let N denote the number of generators in the power system (i.e., $N = 10$). The parameters of the generators of the power system are defined in Fig. 2 and are expressed in per units, with the exception of M_i and D_i which are expressed in seconds and δ_i which is expressed in radians.

We employ the swing equation model to describe the dynamics of a physical synchronous generator. The time evolution of the rotor's angle and frequency in this model ideally enables the study of transient stability of the power system. We assume that the swing equation parameters are constant even when the power system undergoes instability. To address the physically networked nature of the power system, we make use of the Kron-reduction techniques to reduce the order of the interconnections and determine effective mutual couplings between the synchronous generators of the power system [9].

The relative normalized frequency of Generator i is defined in this work as $\omega_i = \frac{\omega_i^{act} - \omega^{nom}}{\omega^{nom}}$, where ω^{nom} is the nominal angular frequency of the power system and ω_i^{act} is the actual angular frequency of Generator i. Further, let the state variable of Generator i be defined as $x_i = [\delta_i, \omega_i]^T$, where $(\cdot)^t$ is the transpose operator. Let also $\dot{\delta}_i$ and $\dot{\omega}_i$ denote the derivatives of δ_i and ω_i with respect to time, respectively.

Synchronous generators are typically equipped with power control schemes (such as exciter and governor controls) that help the generator adjust its internal settings to respond to changes in the overall power grid. However, these local controllers are often insufficient due to their slow reaction to rapid system-wide changes. Consequently, assuming there is no power control in the power system, the swing equation for Generator i is expressed as [10], [11]

$$\begin{aligned} \dot{\delta}_i &= \omega_i \\ M_i\,\dot{\omega}_i &= -D_i\,\omega_i + (P_{m,i} - P_{e,i})\ , \end{aligned} \tag{2}$$

where the electrical power of Generator i is defined as [12]

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

where $G_{ik} = G_{ki} \geq 0$ and $B_{ik} = B_{ki} > 0$ are the Kron-reduced equivalent conductance and susceptance, respectively, between Generator i and Generator k, $\forall\, i, k \in \{1, \ldots, N\}$.

III. Switching Attack

The adversary has to specify a target generator out of the N generators in the power system, design the switching signal, and determine the hysteresis margin of the target circuit breaker. 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 $U_{\hat{i}}$. Further, the ESS is controlled by a circuit breaker. At any specific moment, the ESS at Generator $\hat{i}$ can be either injecting power, absorbing power, or disconnected from the grid. Thus, to reflect the incorporation of the ESS, the swing equation of Generator $\hat{i}$ appears as

$$\begin{aligned} \dot{\delta}_{\hat{i}} &= \omega_{\hat{i}} \\ M_{\hat{i}}\,\dot{\omega}_{\hat{i}} &= -D_{\hat{i}}\,\omega_{\hat{i}} + P_{a,\hat{i}} + \sigma_{\hat{i}}\,U_{\hat{i}}\,, \end{aligned} \tag{4}$$

where $\sigma_{\hat{i}}$ is the state of the circuit breaker that controls the ESS of Generator $\hat{i}$, and $P_{a,\hat{i}} = P_{m,\hat{i}} - P_{e,\hat{i}}$ denotes the accelerating power of Generator $\hat{i}$.

By controlling the value of $\sigma_{\hat{i}}$ through physical or cyber means, the adversary affects 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 is being absorbed from the generator bus, and the adversary is not taking any disturbing action when $\sigma_{\hat{i}} = 0$. Consequently, the different states of the circuit breaker affect the dynamics of Generator $\hat{i}$ as

$$M_{\hat{i}}\,\dot{\omega}_{\hat{i}} = \begin{cases} -D_{\hat{i}}\,\omega_{\hat{i}} + P_{a,\hat{i}} & \sigma_{\hat{i}} = 0 \\ -D_{\hat{i}}\,\omega_{\hat{i}} + P_{a,\hat{i}} + U_{\hat{i}} & \sigma_{\hat{i}} = 1 \\ -D_{\hat{i}}\,\omega_{\hat{i}} + P_{a,\hat{i}} - U_{\hat{i}} & \sigma_{\hat{i}} = -1\,. \end{cases} \tag{5}$$

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.

The following assumptions about the power system are used in this work:

- the ESS of Generator $\hat{i}$ is initially disconnected from the power grid (i.e., $\sigma_{\hat{i}}$ = 0);
- the model of the target generator does not include an exciter nor a governor control;
- the adversary is able to find the stability boundaries of the target generator for the three cases of $\sigma_{\hat{i}}$ (i.e., $f_{\hat{i},0}(x,t)$, $f_{\hat{i},1}(x,t)$, and $f_{\hat{i},2}(x,t)$); and
- the target generator is considered unstable if its system state variable is outside the stability boundary of the disconnected case.

The last assumption indicates that Generator $\hat{i}$ is termed unstable if the trajectory of $x_{\hat{i}}$ leaves the stability region of $f_{\hat{i},0}(x,t)$ of that generator.

The adversary conducts the variable-structure switching attack using the fast-acting ESS as outlined in Algorithm 1. The adversary first switches the target circuit breaker to connect the ESS to the power grid in the absorb mode. The adversary then tracks the state variable until the switching signal leaves the hysteresis margin; if $x_{\hat{i}}$ is inside the stability boundary of $f_{\hat{i},1}(x,t)$, the adversary switches the circuit breaker to make the ESS of Generator $\hat{i}$ inject power, otherwise, the adversary disconnects the ESS from the power grid. The adversary later tracks the value of $x_{\hat{i}}$ until $s(x_{\hat{i}}) < -\epsilon$, then switches the circuit breaker to $\sigma_{\hat{i}} = -1$ if $x_{\hat{i}}$ is inside the stability boundary of $f_{\hat{i},2}(x,t)$, and so on. The adversary repeats the previous steps until $x_{\hat{i}}$ is outside the stability region of $f_{\hat{i},0}(x,t)$, then

Algorithm 1 Switching Attack

```
switch the circuit breaker to absorb power (i.e., $\sigma_{\hat{i}} = -1$)
while $x_{\hat{i}}$ is inside the stability region of $f_{\hat{i},0}(x,t)$ do
    measure $\delta_{\hat{i}}$ and $\omega_{\hat{i}}$
    calculate the value of the switching signal $s(x_{\hat{i}})$
    track $x_{\hat{i}}$ till $s(x_{\hat{i}}) > \epsilon$
    if $x_{\hat{i}}$ is inside the stability boundary of $f_{\hat{i},1}(x,t)$ then
        $\sigma_{\hat{i}} = 1$ (i.e., switch ESS to inject power)
    else
        $\sigma_{\hat{i}} = 0$ (i.e., disconnect ESS from grid)
    end if
    measure $\delta_{\hat{i}}$ and $\omega_{\hat{i}}$
    calculate $s(x_{\hat{i}})$
    track $x_{\hat{i}}$ till $s(x_{\hat{i}}) < -\epsilon$
    if $x_{\hat{i}}$ is inside the stability boundary of $f_{\hat{i},2}(x,t)$ then
        $\sigma_{\hat{i}} = -1$
    else
        $\sigma_{\hat{i}} = 0$
    end if
end while
permanently switch the circuit breaker to $\sigma_{\hat{i}} = 0$
```

permanently switching the circuit breaker to $\sigma_{\hat{i}} = 0$ will drive the target generator's frequency and phase unbounded. Consequently, the switching attack is considered successful in destabilizing Generator $\hat{i}$.

IV. Numerical Results

The New England 10-generator 39-bus power system of Fig. 1 is considered. The values of M_i's and X'_{di}'s are found in [13], [14] and D_i is set to 20 msec for all generators. The power system is assumed to be running in normal state from $t = 0$ to $t = 0.5$ seconds. However, a switching attack targets Generator 9 (i.e., $\hat{i} = 9$) at $t = 0.5$ seconds.

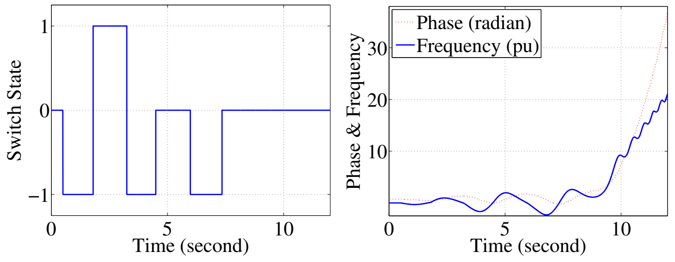
Before the occurrence of the switching attack, load flow analysis of the power system is conducted to find the values of $P_{e,i}$, δ_i, and E_i for each generator in the system. Because the power system is balanced and there are no transients, the mechanical power of each generator equals the electrical power of that generator before the occurrence of the switching attack.

Let the switching signal be defined as $s(\delta_9, \omega_9) = \omega_9$, and let the hysteresis margin be $\epsilon = 0.1$. Further, let the power of the ESS at Generator 9 be selected as 10% of the mechanical power of that generator before the switching attack (i.e., $U_9 = 0.8292$ pu). Then, assuming the phases of the different generators, other than the target one, remain constant during the switching attack, the equilibrium points of Generator 9 are $[0.7073, 0]^T$ for $\sigma_9 = 0$, $[0.8472, 0]^T$ for $\sigma_9 = 1$, and $[0.5265, 0]^T$ for $\sigma_9 = -1$.

The time evolution of the switch state and the phase and frequency of Generator 9 during the switching attack are shown in Fig. 3. It is observed that the generator becomes unstable after only five switchings. As the adversary switches the circuit breaker to the disconnect mode (i.e., $\sigma_9 = 0$) for the last time, both the phase and frequency of Generator 9 rapidly become unbounded.

The system trajectory during and after the variable-structure switching attack is shown in Fig 4. The stability boundaries and the equilibrium points of Generator 9 under the three states of σ_9 are also shown. It is noted that the phase and frequency of the target generator fluctuate during the attack; the attack stops when the system state variable is outside the boundary region of $f_{9,0}(x,t)$, and the frequency and phase become unbounded after that. Consequently, Generator 9 becomes unstable and the variable-structure switching attack is said to be successful.

Next, an actual simulation of the New England power system, where the phase and frequency of all generators change according to the swing equation, is considered. The switching attack lasts 5 seconds from $t = 0.5$ to $t = 5.5$ seconds, and the simulation time is 20 seconds. Further, the governor control is not activated in this case. Fig. 5 shows the phase portrait, frequency, and phase of Generator 9, and the phase and frequency of Generators 1–4. It is noted that even though the switching attack targets only Generator 9, the other generators in the power system are negatively affected because the dynamics of the different components of the interconnected power system are interdependent as shown in Eq. 2. Results of this figure show that a 5-second switching attack can destabilize the power system.



(a) Switch state

(b) Phase and frequency of Generator 9

Fig. 3. Attack details

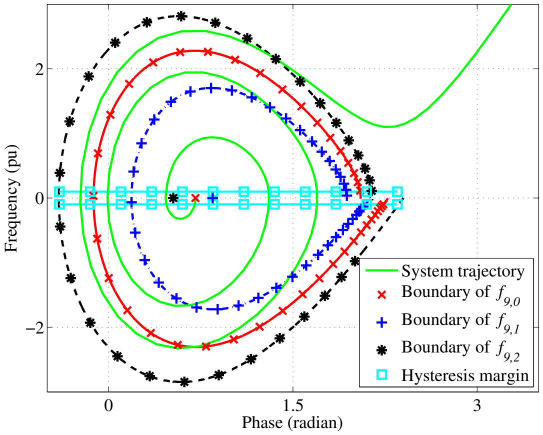


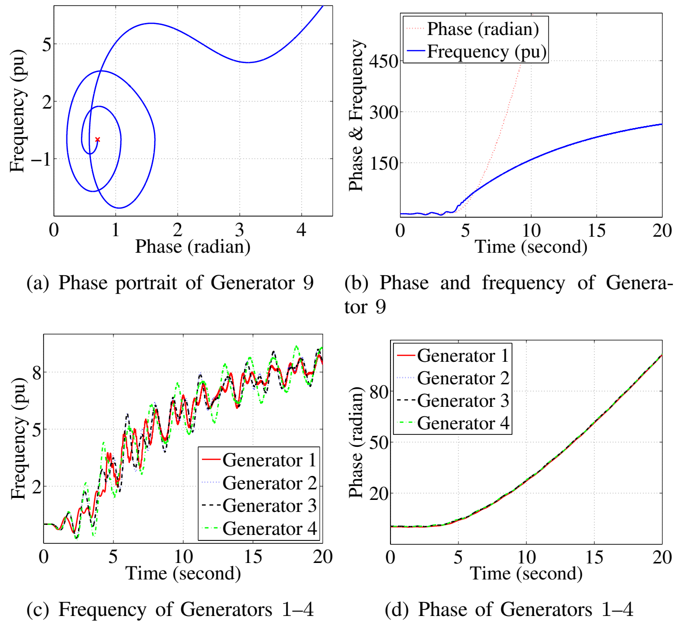
Fig. 4. Phase portrait of Generator 9

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

$$\dot{P}_{m,i} = \kappa_i \left(P_{e,i} - P_{m,i} \right), \tag{6}$$

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. 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.

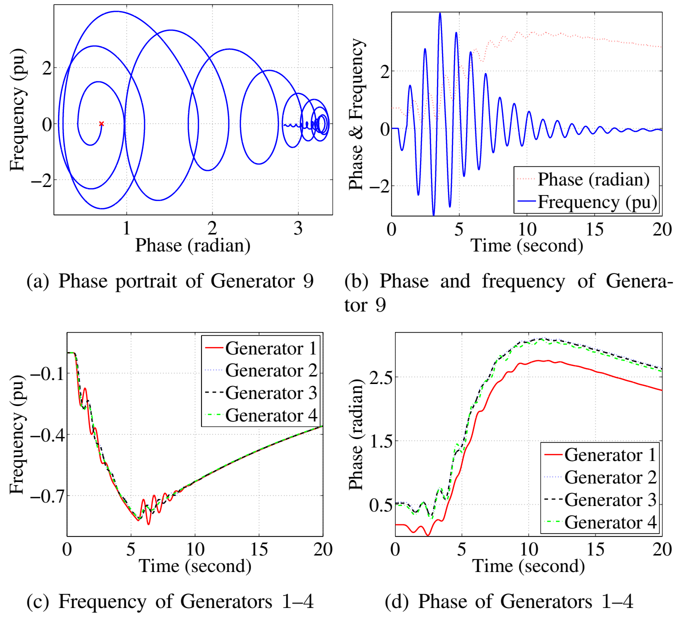
Fig. 6 illustrates the effect of the switching attack on Generator 9 and on Generators 1–4 when the governor control is activated. Let the stability time of a generator be defined as the time it takes the governor control to permanently restrict the frequency of the generator to within the ±0.01-pu range. The stability time of the system generators is found to be around 49 seconds when the value of the governor's update rate is set to $\kappa_i = 0.5$, $\forall\, i \in \{1, \ldots, N\}$. Although the switching attack lasts for 5 seconds, the governor control



(a) Phase portrait of Generator 9 (b) Phase and frequency of Generator 9

(c) Frequency of Generators 1–4 (d) Phase of Generators 1–4

Fig. 5. Effect of attack on Generators 9 and 1–4



(a) Phase portrait of Generator 9 (b) Phase and frequency of Generator 9

(c) Frequency of Generators 1–4 (d) Phase of Generators 1–4

Fig. 6. Effect of attack on Generators 9 and 1–4 (governor control is activated)

needs extra 44 seconds to stabilize the frequency of the system generators. Further, the governor control cannot stabilize the phase of the system generators.

V. Conclusions

This paper investigates a new class of switching attacks on smart grid systems using fast-acting energy storage system. In order for an adversary to build a variable-structure system model and design the appropriate switching signal, the adversary needs to have an access to the target circuit breaker, can intercept the system state variables, and have a working knowledge of the system model of the smart grid for the different states of the circuit breaker. System state variables are collected by different sensors around the power gird and are transmitted through a communication network. The adversary intercepts the system measurements and affects the circuit breaker's switch that controls the energy storage system depending on the value of the system state variable of the target generator.

Performance measures are investigated when the switching attack is applied to the New England 39-bus 10-generator power system. Further, the performance is investigated when the governor control in activated in the power system. Results of this work show the effectiveness of the proposed switching attack in destabilizing the power grid.

Acknowledgments

This work was supported by the National Science Foundation under grant ECCS-1028246 and the Natural Sciences and Engineering Research Council of Canada.

References

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

[2] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A Class of Cyber-Physical Switching Attacks for Power System Disruption," in *Cyber Security and Information Intelligence Research Workshop (CSIIRW)*, pp. 1–4, October 2011.

[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] 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.

[5] S. Liu, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Coordinated Variable Structure Switching in Smart Power Systems: Attacks and Mitigation," in *International Conference on High Confidence Network Systems (HiCoNS) at Cyber Physical Systems Week (CPS Week)*, pp. 21–30, April 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. K. Farraj, E. M. Hammad, D. Kundur, and K. L. 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.

[8] 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.

[9] 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.

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

[11] 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.

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

[13] 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.

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