Tuning Out of Phase: Resonance Attacks

Eman Hammad, Ahmed M. Khalil, Abdallah Farraj, Deepa Kundur, and Reza Iravani
Department of Electrical and Computer Engineering, University of Toronto, Canada
Email: {{ehammad, abdallah, dkundur}@ece, ahmed.mohammedmohammed@mail, iravani@ecf}.utoronto.ca

***Abstract*—This work presents a new class of cyber-physical switching attacks of power transmission systems. The proposed resonance attack relies on enhancing inter-area oscillation modes to drive groups of system generators out of step. This switching attack targets inter-area oscillations by switching a relatively small part of the system load at a (low) frequency that resonates with one of the inter-area oscillation modes observed in the power system. The targeted frequency of the attack is chosen through measurement-based analysis of the frequency deviation at a targeted bus that is observable by the adversary. Numerical results show the effectiveness of the proposed switching attack when applied to a two-area system.**

I. Introduction

Smart grid systems employ advanced control, communications, and sensor technologies to improve the reliability and efficiency of the power delivery system. Information about system operation is collected using sensors placed in specific locations. This cyber data is then transmitted through a communication network to distributed controllers where it is analyzed to determine if any actions must be applied to enhance system operation.

Cyber security concerns of the smart grid have recently surfaced as more smart grid applications are getting implemented in various power systems. Specifically, the introduction of the cyber component of the grid can lead to potential cyber and physical attacks on the smart grid. For example, based on understanding the structure of the power system and accessing the system information, effective switching attacks can be constructed by an adversary to disrupt the normal operation of the power system.

Recent work in [1]–[4] investigate the effect of sliding-mode switching attacks on the stability of power systems, where the switched power system is modeled as a variable-structure control system [5]. Such attacks use calculated switchings of a load in the power grid to create a sliding-mode control system and consequently cause power system instability. However, the development of such attacks assumes a linear system model and full knowledge of the system states.

Further, a fast-acting energy storage system (ESS) is proposed in [6] to be used in conducting switching attacks that destabilize parts of the power grid. An adversary is proposed to have a physical or cyber access to a circuit breaker, have an access to the system state variable, and have a knowledge of the system model of the power system 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.

In addition, an Idaho National Laboratory's Aurora experiment [7] presents the threat of switching a synchronous machine from the power system out of synchronism. The threat model assumed by the Aurora attack places an adversary at the capacity of gaining control on one of the most protected components in a power system. This assumption decreases the possibility of such attack in a practical power system.

However, some mitigation frameworks are developed recently [8], [9]. For example, the utility counteracts switching attacks using an external ESS through a game-theoretic based control in [8] and a feedback-linearization based control in [9].

This paper presents a new class of switching attacks, termed *resonance attacks*, that can be staged stealthily without full knowledge of the system states or its detailed properties. Small signal analysis on any power system usually uncovers the local and inter-area mode oscillations that would appear in that system under small disturbances. In this work we are interested in the inter-area mode oscillations which are related to how a group of coherent synchronous generators swing against another group. The proposed resonance attack switches a relatively small part of the load located near an inter-area link. The low switching frequency is selected to over-impose (resonate) with one of the system inter-area oscillation modes and thus enhancing it; hence, with sufficient switching the attack will resonate with the targeted mode resulting in driving a group of generators to instability.

The proposed class of attacks relies on estimating the inter-area modes of oscillation characterizing the system under attack. Several measurement-based approaches exist in literature to provide an estimate of the frequency of the different inter-area modes. A review of such methods is presented in [10]. Examples of such methods are masking signal-based empirical mode decomposition [10], spectral Independent Component Analysis (ICA) [11], [12], Prony analysis [13], Yule-Walker methods [14], least squares algorithms [15], and subspace methods [16]. In this paper we adopt the spectral ICA approach to estimate the frequencies of the different inter-area modes; nevertheless, other methods could be applied easily. The proposed class of attack is applied to a two-area four machine system [17] to show its effectiveness.

The remainder of this paper is organized as follows. Resonance attacks and the threat model are presented in Section II. Section III provides a brief review of the small signal analysis and inter-area oscillations in power systems. The estimation of the inter-area modes oscillating frequencies using the spectral ICA approach is discussed in Section IV. In Section V the simulation setup and analysis of the results are discussed.

978-1-4673-8289-2/15/$31.00 ©2015 IEEE

Conclusions and final remarks are discussed in Section VI.

II. Resonance Attacks

Studies of switching attacks in the context of smart grids try to evaluate the impact of threat models where an adversary exploits cyber-enabled components to gain access to the physical power system. It is tempting for an adversary with bad intentions to manipulate the different degrees of freedom in the smart grid system. Therefore, the main function of the existing protection and monitoring schemes is to mitigate these endless possibilities of such attacks through a comprehensive survivability framework. The main goal of this paper is to further elaborate that power systems remain very vulnerable to switching attacks with current detection and protection schemes.

Resonance switching attacks combine three properties that enable them to be of serious threat to power systems:

1) low switching frequency that can easily go undetected,
2) low switching power that cannot be easily distinguished from regular load changes, and
3) no full system model is required.

A. Threat Model

Power systems with multiple synchronous machines exhibit many interesting properties and phenomena, among which is the coherency between the different generators. Synchronous machines coherency is often mapped as the problem of coupled oscillators [18]. This work considers global small-signal stability problems in power systems, such problems are often a result of the interactions between groups of generators in the system. Inter-area mode oscillations is one manifestation of such interactions typically observed when the two or three groups of generators are interconnected by weak lines [17].

There are two distinct types of inter-area oscillations; very low frequency modes ($0.1-0.3$ Hz) involving all generators of the power system, and higher frequency modes ($0.4-0.7$ Hz) involving subgroups of generators swinging against each other. An inter-area oscillation mode(s) is characteristic of a specific power system under certain operating conditions. A detailed representation of the interconnected power system enables the analysis of inter-area oscillations as will be detailed in Section III.

The adversary in a resonance attack relies on the fact that a disturbance in a power system, e.g. a fault, will excite different inter-area modes. Typically, the generators in a given area will oscillate in phase for inter-area modes [17]. To conduct this attack, an adversary needs to gain access to part of the system load (denoted L_{sw}).

Typically loads are of three types; constant current, constant power, and constant impendence. For an effective resonance attack, the best candidate as a switching load is probably a constant impedance load. Other types of load would suffer adverse effects as a result of switching, hindering them useless for the adversary. The reason is that constant impedance loads are usually heating loads. Therefore, switching part of a constant-impedance load will not get the attention of the consumers whose loads are being controlled; thus, the attack can go unnoticed by the system operator and the consumers. However, the constant power loads and constant current loads are, in most cases, motor loads and converter-based loads, respectively. Therefore, switching part of such loads will intervene with their normal mode of operation and this will get the attention of both the consumers and the system operator. Therefore, constant impedance loads are considered to be the best candidate of the proposed class of attacks especially in the winter when the percentages of such loads are relatively high.

Further, in addition to an access to line measurements on the bus connected to the switching load L_{sw}, the adversary would need a mechanism to gain access and control that enables him/her to excite the different inter-area modes. A possible scenario is where the adversary obtains a limited access to a substation, specifically access to the de-energization circuit breaker of the line connected to the load. The adversary intentionally causes a transient short circuit and collects line measurements for few seconds. An alternative scenario enables an adversary with limited resources to cause a transient fault from the switching load side and then collect line measurements on the same line for few seconds.

The collected measurements are then analyzed by the adversary to deduce characteristic inter-area oscillation frequencies of the system (termed f_m). It is important to note that no previous system knowledge (i.e., the $\boldsymbol{A}$ matrix) is required to construct this attack. The adversary then selects one of higher frequency modes ($0.4-0.7$ Hz), and at the time of his/her choice, the adversary can start switching the load under control at the same frequency (termed f_{sw}) of the targeted inter-area mode. This switching will cause coherent generators in the system areas to swing against each other; the phase difference would eventually be outside the tolerated range, resulting in either tripping of the generators or islanding of the system areas if islanding mechanisms are installed.

B. Proposed Resonance Attack

To launch an effective resonance switching attack, the adversary has to conduct the following:

1) Gain access to:
   - Part of the constant-impendence load L_{sw} with the ability to switch that load on and off.
   - Line measurements at the bus where the load is connected.
   - Short circuiting control, such as the built-in de-energization circuit breaker or a method of imposing a fault at the load side.
2) Impose a transient short-circuit on the power system at time t_0 to excite system inter-area oscillation modes.
3) Record line measurements for few seconds following the fault till the system settles down.
4) Perform the spectral ICA analysis on the recorded data to extract the frequencies of the inter-area modes (i.e., f_m).
5) Choose the targeted mode frequency $f_{tm} \in f_m$.

6) At time $t_0 + T$, start switching L_{sw} at frequency $f_{sw} = f_{tm}$, where $T > 0$ is the time the adversary waits before launching the switching attack.
7) Stop the switching attack when the power system becomes instable.

III. Small Signal Stability and Inter-area Oscillations

Maintaining synchronism between synchronous machines when subjected to small disturbances is an important stability aspect of power systems, and is usually referred to as small signal stability. Small-signal stability problems in current power systems are related to insufficient damping of system electromechanical oscillations [17]. Although power systems are highly non-linear, under normal operating conditions those systems can be linearized around an operating point. Eigenvalue analysis is a well-known and commonly used approach to investigate the properties of inter-area oscillations in multi-machine power system models [17], [19], [20].

A. System Model

A multi-machine dynamic power system can be described using a nonlinear state-space representation as

$$\begin{aligned} \dot{\boldsymbol{x}} &= \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{u}) \\ \boldsymbol{y} &= \boldsymbol{g}(\boldsymbol{x}, \boldsymbol{u}) \end{aligned} \tag{1}$$

where $\boldsymbol{x} = [x_1, x_2, \ldots, x_n]^T$ is the state vector, $\boldsymbol{u} = [u_1, u_2, \ldots, u_n]^T$ is the system inputs vector, $\boldsymbol{y} = [y_1, y_2, \ldots, y_m]^T$ is the system outputs vector, and $\boldsymbol{g} = [g_1, g_2, \ldots, g_m]^T$ is a vector of nonlinear functions relating state and input variables to output variables.

Further, the state of the system is the minimum amount of information about the power system at any instant in time that is necessary to determine the future behavior of the system. As small-signal stability considers the stability of the power system under small perturbations, we can linearize the system dynamics around an equilibrium point using Taylor's series expansion.

Let $(\boldsymbol{x_0}, \boldsymbol{u_0})$ be the initial state vector and the initial input vector corresponding to the equilibrium point that is under study by the small-signal stability analysis; hence, $\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x_0}, \boldsymbol{u_0}) = \boldsymbol{0}$. For a small deviation $(\boldsymbol{\Delta x}, \boldsymbol{\Delta u})$, let the perturbed state be presented as

$$\begin{aligned} \boldsymbol{x} &= \boldsymbol{x_0} + \boldsymbol{\Delta x} \\ \boldsymbol{u} &= \boldsymbol{u_0} + \boldsymbol{\Delta u} \end{aligned} \tag{2}$$

based on which the linearized forms of (1) can be formulated as

$$\begin{aligned} \boldsymbol{\Delta \dot{x}} &= \boldsymbol{A \Delta x} + \boldsymbol{B \Delta u} \\ \boldsymbol{\Delta y} &= \boldsymbol{C \Delta x} + \boldsymbol{D \Delta u} \,. \end{aligned} \tag{3}$$

In this case, $\boldsymbol{A}$ is the state matrix of size $n \times n$, which is also the Jacobian matrix with elements a_{ij} corresponding to the partial derivatives $\partial f_i / \partial x_j$ evaluated at the equilibrium point of interest.

Next, we discuss how the eigenvalues of the state matrix $\boldsymbol{A}$ relate to system stability and the inter-area mode oscillations.

B. Eigenvalues and Stability

To study the small-signal stability of the power system, eigenvalue analysis is done on the state matrix $\boldsymbol{A}$ of the linearized system model. The result of this eigenvalue analysis is usually presented in the form of right and left eigenvectors $(\boldsymbol{\psi}, \boldsymbol{\phi})$, where

$$\begin{aligned} \boldsymbol{A\psi}_i &= \lambda_i \boldsymbol{\psi}_i \\ \boldsymbol{\phi}_i \boldsymbol{A} &= \lambda_i \boldsymbol{\phi}_i \,. \end{aligned} \tag{4}$$

Let $\boldsymbol{\Phi} = [\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \ldots, \boldsymbol{\phi}_n]$, then the following quadratic form results in

$$\boldsymbol{\Phi}^{-1} \boldsymbol{A \Phi} = \boldsymbol{\Lambda} \tag{5}$$

where $\boldsymbol{\Lambda}$ is a diagonal matrix with the eigenvalues λ_i as the diagonal elements.

A mode corresponding to an eigenvalue λ_i defines a time dependent characteristic given by $\mathrm{e}^{\lambda_i t}$ [17]. As such, stability of the power system is determined by those eigenvalues. A real eigenvalue would correspond to a non-oscillatory mode, where a negative real eigenvalue represents a decaying mode and positive real eigenvalue represents instability. However, complex eigenvalues, that usually occur in conjugate pairs, correspond to oscillatory modes.

For a complex pair of eigenvalues shown in (6), the frequency of oscillation f in Hz is calculated by (7) and the damping ratio ξ is given by (8) as

$$\lambda = \sigma \pm j\omega \tag{6}$$

$$f = \frac{\omega}{2\pi} \tag{7}$$

$$\xi = \frac{-\sigma}{\sqrt{\sigma^2 + \omega^2}} \,. \tag{8}$$

In small-signal stability literature, the eigenvalue sensitivity quantifies how an eigenvalue λ_i is affected by different elements of the state matrix $\boldsymbol{A}$. Further, the participation factor is defined as the sensitivity of the eigenvalue λ_i to the diagonal element a_{kk} of the state matrix $\boldsymbol{A}$. Specifically, let the participation factor p_{ki} be defined as

$$p_{ki} = \frac{\partial \lambda_i}{\partial a_{kk}} \,. \tag{9}$$

Hence, a participation factor quantifies the relative participation of the respective state in the corresponding mode.

IV. Probing the Targeted Inter-area Modes

The proposed class of attacks depends in its core on identifying the frequency of an inter-area mode of oscillation through an offline analysis of line measurements. This is the main challenge an adversary has to overcome in order to achieve the switching attack's goal of destabilizing the power system as described in the threat model above. In the technical literature, several methods are proposed to estimate the dominant mono-frequency components for the signals. In this paper, we adopt the spectral ICA method as introduced in [11], [12]. The required input data to this method is the frequency deviation signal recorded at the bus connecting the switching load L_{sw}. This data is gathered over the time

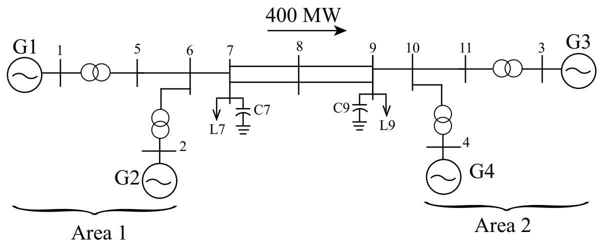

Fig. 1. The 2-area 4-machine system

following the induced fault by the adversary and until the system settles down without additional intervention from the adversary.

The ICA method is a technique that identifies the sources and the mixing parameters of a system that has the input data as its output. This is done without previous knowledge of the system properties or details [12]. There are two approaches of the ICA method: (*i*) time-domain ICA and (*ii*) spectral ICA. Both approaches aim at decomposing an input matrix $\boldsymbol{X}$ into independent non-Gaussian components (IC's) such that

$$\boldsymbol{X} = \boldsymbol{W} \times \boldsymbol{S} \tag{10}$$

where the rows of $\boldsymbol{S}$ are the IC's of the system and $\boldsymbol{W}$ is the mixing matrix that relates the IC's to the measured signal.

The rows of $\boldsymbol{X}$ are the time series of the measured data in the time-domain ICA approach. However, they are the power spectra of the measured data in the spectral ICA method, which can be determined using discrete Fourier transform. The main advantages of spectral ICA method over the time-domain approach are (*i*) time delays and phase lags invariant ability and (*ii*) immunity to noise in the measured data [11].

Define the Kurtosis of a zero-mean random variable v as

$$\text{kurt}(v) = \mathbb{E}(v^4) - 3(\mathbb{E}(v^2))^2 \tag{11}$$

where $\mathbb{E}$ is the expectation operator. To estimate the mixing matrix and the IC's, a fast fixed-point algorithm [21] is used. This algorithm arrives at the estimates by maximizing the Kurtosis of the different IC's. More details about the adopted method implementation can be found in [11], [21], [22].

V. Simulation and Numerical Results

A. Simulation Setup

To illustrate the analysis of the proposed resonance attacks, we consider the small-signal stability of a two-area four-generator power system [17], shown in Fig. 1. The system composes of two similar areas connected via a weak tie, and each area consists of two coupled synchronous generators. Each generator has a rating of 900 MVA and 20 kV.

Further, each generator circuitry is represented by a 4th-order rotor electrical dynamic model. The stator electrical circuit is represented in the network steady-state model. For each generator, the magnetic saturation effects of both axes are included in the model. Input mechanical power to each generator is assumed to remain unchanged and the governor system dynamics are not considered. All generators are equipped with DC excitation systems. The transmission system is represented by the network nodal equations. The system data is available in [17].

TABLE I
System oscillatory modes

No.	Eigenvalue		Frequency	Damping
	σ	ω	(Hz)	Ratio
1	-0.0447	±3.3256	0.5293	1.3%
2	-0.5575	±6.7107	1.0680	8.3%
3	-0.5638	±6.9352	1.1038	8.1%
4	-0.3793	±0.3334	0.0531	75.1%
5	-0.3984	±0.3300	0.0525	77.0%
6	-0.7400	±0.4663	0.0742	84.6%
7	-5.0527	±1.7660	0.2811	94.4%
8	-4.3874	±1.3211	0.2103	95.8%
9	-6.2695	±1.5562	0.2477	97.1%
10	-6.3100	±1.5564	0.2477	97.1%
11	-34.5597	±0.0817	0.0130	100%

Our simulation time-step is 1.667 msec and each simulation case provides 20 seconds of dynamic response of the system subsequent to a disturbance [23]. The simulated response is sampled at the rate of 120 Hz in compliance with the IEEE standard for synchrophasor measurements.

As discussed in Section II, the appropriate load model for the proposed attack is the constant impedance load. As such, an analytical eigenvalue analysis of the system, given the knowledge of the system state matrix $\boldsymbol{A}$, shows that the power system exhibits the eigenvalues and modes of oscillation shown in Table I.

Based on the above modes of oscillation, the first mode is the best candidate to use as the targeted mode of attack. The reasons for such claim are that

1) this mode is the least-damped mode of oscillation; therefore, it will be the easiest mode to drive the system to instability, and
2) it is an inter-area mode, therefore the attack switching frequency will be very low (specifically, 0.53 Hz), which achieves the stealth attack criterion.

B. Inter-Area Mode Frequency Estimation

Following the threat model described in Section II, a 3-phase fault is imposed at Bus 7 at which the switching load is connected for a duration of 80 msec. After the fault clearing, the power system is left to settle down with its own dynamics and the frequency deviation signal at Bus 7 is recorded. The frequency deviation signal can be calculated from the rate of change of the phase angle of the bus voltage as

$$\Delta f_7|_{t+\Delta t} = \frac{1}{\omega_0}\left(\frac{\theta_7|_{t+\Delta t} - \theta_7|_t}{\Delta t}\right) \tag{12}$$

where ω_0 is the system nominal frequency, θ_7 is the voltage phase angle of Bus 7, and t and $t + \Delta t$ are time instants. Fig. 2 shows the recorded signal used as the input data to the spectral ICA method.

Applying the spectral ICA method to the above signal resulted in identifying a dominant IC of frequency f_{tm} = 0.55 Hz. This value is very close to the frequency of the inter-area mode identified from the small signal analysis of the system. However, since the estimated frequency is not exactly

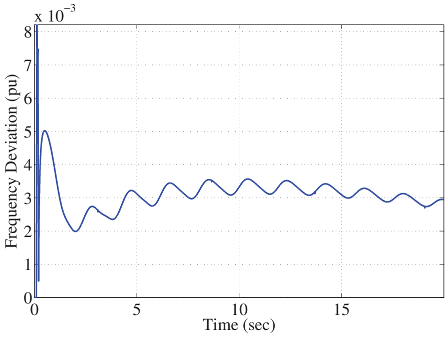

Fig. 2. Frequency deviation signal recorded at Bus 7

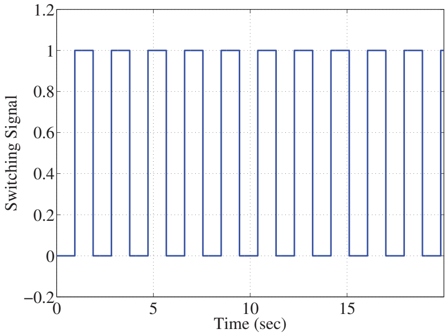

Fig. 3. Controlled load switching signal

the same as the calculated one, the sensitivity of the attack strength to the change of the estimated value of the inter-area mode is studied and the results are shown in the following subsections.

C. Simulation Results

Using the estimated value of the inter-area mode of oscillation, the switching attack is initiated on the test system. Fig. 3 shows the switching signal used in the resonance attack. This signal is the control signal to the circuit breaker of the controlled part of the switching load L_{sw}. The main characteristic of this signal is its low frequency which fulfills the stealth criterion of the attack.

Fig. 4 and Fig. 5 show the impact of the switching attack on the generators' angular speed ω and relative internal angle $\Delta\delta$. In this attack, 5% of the total system load is being switched (i.e., 14% of the load connected at Bus 7). It is clear that the proposed resonance attack is able to quickly drive the test power system to instability. Although we have not included the models of speed governors and turbines, it is important to state that the system was driven to instability before traditional speed governors and the turbines would have reacted. As shown, the resonance attack is able to destabilize the system at around 10 seconds, and this is typically less than the time constants of such devices. Thus, speed governors and turbines would begin to respond after the generators would have been disconnected by the out-of-step protection scheme.

D. Sensitivity Analysis

The sensitivities of the proposed attack to the switching frequency and the portion of the load being switched are

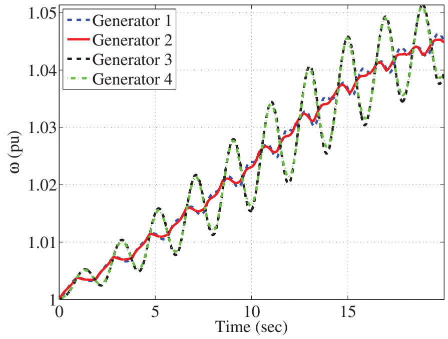

Fig. 4. Impact of the switching attack on angular speed of system generators

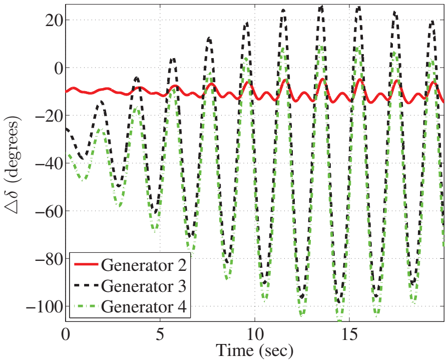

Fig. 5. Impact of the switching attack on internal angle of system generators

studied in this subsection. The index adopted for this study is the time to instability. This measure is defined as the time difference between starting the switching attack and the time one of the system generators' angular speed is strictly above 1.025 pu. The reason of adopting such threshold is that at this speed the over-speeding protection will be activated and the generator will be disconnected from the system. At this instant, the system will fail since huge generation-load mismatch will result.

Several simulation cases are considered where the load switching frequency f_{sw} is varied through the range of inter-area oscillations. Results of this study are shown in Fig. 6. It is clear that a very low time-to-instability is achieved at a switching frequency of $f_{sw} = 0.529$ Hz which is the same frequency as the inter-area mode extracted by the eigenvalue analysis of the system shown in Table I. Further, it is noted that an adversary with an estimated switching frequency of $f_{tm} = 0.55$ Hz, extracted through the ICA analysis, is able to successfully conduct the attack as confirmed in this figure.

Moreover, the lowest time-to-instability is achieved at $f_{sw} = 0.05$ Hz. This is actually a frequency of another oscillatory mode in the system as shown in Table I. However, the frequency of this mode is not estimated by the ICA method due to its high damping ratio ($\sim 75\%$) and since this mode is not an inter-area mode but a mode related to the flux linkage of the synchronous generators. Therefore, if the adversary, by any means, has access to some information about the parameters of the synchronous generators, he/she would have done better from the attack point of view.

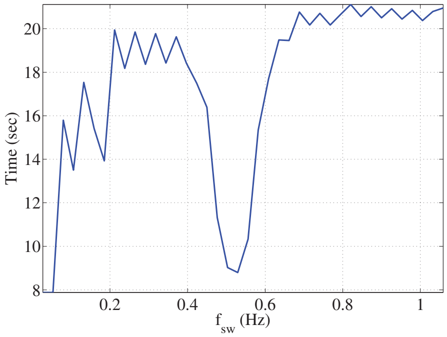

Fig. 6. Instability time vs. switching frequency

We further study the sensitivity of the attack through varying the percentage of switching load $\%L7_{sw}$ and the switching frequency f_{sw} while observing the time to instability. Fig. 7 illustrates these results as a contour map showing the time to instability curves as boundaries. While this figure emphasizes the previous observation, it further describes the relationship between time to instability and $\%L7_{sw}$, where it shows that to achieve instability in a shorter time the adversary would need to control and switch a higher percentage of the load.

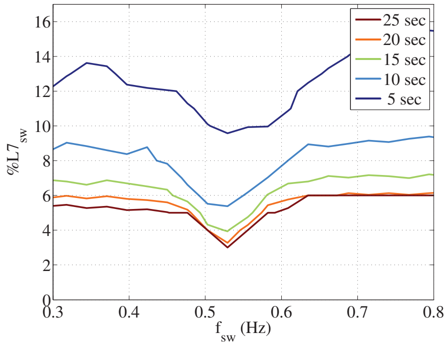

Fig. 7. Contour map of instability time of different switching loads vs. switching frequency

VI. Conclusions

A new class of cyber-physical attacks on smart grids is proposed in this paper. The resonance attack mainly depends on identifying the frequency of an inter-area mode of oscillation, which can be done using the spectral ICA method. This is followed by switching part of the system load on and off on that frequency which leads the power system to instability.

As an illustration, the proposed resonance attack is applied to a two-area system. Results of this work show that low-frequency switching of a small percentage of the load can quickly drive the power system to instability.

References

[1] 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.

[2] 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.

[3] 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.

[4] A. Farraj, E. 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.

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

[6] 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.

[7] Source: CNN, "Staged cyber attack reveals vulnerability in power grid."

[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] A. Farraj, E. Hammad, and D. Kundur, "On Using Distributed Control Schemes to Mitigate Switching Attacks in Smart Grids," in *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 1–5, May 2015.

[10] A. R. Messina, *Inter-area oscillations in power systems: a nonlinear and nonstationary perspective*. Springer Science & Business Media, 2009.

[11] M. Ariff and B. C. Pal, "Coherency identification in interconnected power systeman independent component analysis approach," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1747–1755, 2013.

[12] J. Thambirajah, N. F. Thornhill, and B. C. Pal, "A multivariate approach towards interarea oscillation damping estimation under ambient conditions via independent component analysis and random decrement," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 315–322, 2011.

[13] J. F. Hauer, C. Demeure, and L. Scharf, "Initial results in prony analysis of power system response signals," *IEEE Transactions on Power Systems*, vol. 5, no. 1, pp. 80–89, 1990.

[14] R. W. Wies, J. W. Pierre, and D. J. Trudnowski, "Use of arma block processing for estimating stationary low-frequency electromechanical modes of power systems," *IEEE Transactions on Power Systems*, vol. 18, no. 1, pp. 167–173, 2003.

[15] R. W. Wies, A. Balasubramanian, and J. W. Pierre, "Combining least mean squares adaptive filter and auto-regressive block processing techniques for estimating the low-frequency electromechanical modes in power systems," in *IEEE Power and Energy Society General Meeting (PESGM)*, pp. 8–pp, IEEE, 2006.

[16] M. Larsson and D. S. Laila, "Monitoring of inter-area oscillations under ambient conditions using subspace identification," in *IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–6, IEEE, 2009.

[17] P. Kundur, *Power System Stability and Control*. EPRI Power System Engineering Series, McGraw-Hill, 1994.

[18] F. Dörfler, M. Chertkov, and F. Bullo, "Synchronization in complex oscillator networks and smart grids," *Proceedings of the National Academy of Sciences*, vol. 110, no. 6, pp. 2005–2010, 2013.

[19] P. W. Sauer and M. A. Pai, *Power System Dynamics and Stability*. Prentice-Hall, 1998.

[20] Y. Chompoobutrgool, "Concepts for power system small signal stability analysis and feedback control design considering synchrophasor measurements." Licentiate Thesis, KTH Royal Institute of Technology, 2012.

[21] A. Hyvärinen and E. Oja, "A fast fixed-point algorithm for independent component analysis," *Neural computation*, vol. 9, no. 7, pp. 1483–1492, 1997.

[22] C. Xia and J. Howell, "Isolating multiple sources of plant-wide oscillations via independent component analysis," *Control Engineering Practice*, vol. 13, no. 8, pp. 1027–1035, 2005.

[23] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. V. Cutsem, and V. Vittal, "Definition and Classification of Power System Stability: IEEE/CIGRE Joint Task Force on Stability Terms and Definitions," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1387–1401, 2004.