Coordinated Variable Structure Switching Attack in the Presence of Model Error and State Estimation

Shan Liu, Deepa Kundur, Takis Zourntos and Karen L. Butler-Purry
Department of Electrical and Computer Engineering
Texas A&M University
College Station, Texas 77843-3128, USA
{liu2712, dkundur, takis, klbutler}@tamu.edu

***Abstract*—Coordinated variable structure switching attacks have been recently proposed as a class of cyber-physical attacks on future smart grid systems. In the traditional formulation of this assault, the opponent is assumed to have a local model of the power system and knowledge of the state (rotor angle and frequency) of a target generator under attack. In this paper, we study the performance of this attack when the opponent has imperfect knowledge of the local system dynamics and partial knowledge of the generator state. In such a situation, we demonstrate how the attacker can make use of Luenberger-based state estimation techniques that are robust to model error to still achieve power system disruption via rotor angle instability.**

I. Introduction

One of the critical challenges in the design and deployment of smart grid systems is that of ensuring system security. Given the increasing dependence of these emerging power systems on information technology, cyber security issues, in particular, become of crucial importance. Government initiatives around the world are providing resources to aid in addressing system security. As a result, a spectrum of smart grid stakeholders ranging from electric power utilities to device vendors are aligning their visions to include cyber protection.

Within this climate of rapid decision-making and focused integration, a fundamental need arises to better understand overall system vulnerabilities as a result of cyber-physical integration. Recent work focused on false data injection attacks has demonstrated the vulnerabilities in residual-based bad data detection approaches used for state estimation [1], [2], and other work has founded on integrity attacks [3]. In this work, we focus on studying the parallel problem of vulnerabilities stemming from cyber-enablement of circuit breakers and the associated variability in system architecture.

Recently, the authors identified a class of attacks termed *coordinated variable switching attacks* for smart grid systems that exploit a somewhat "emergent" property in switched dynamical systems called the *sliding mode* to destabilize target synchronous generators [4]–[7]. To apply the attack, an opponent must have knowledge of the local dynamics of the power system as well as the rotor angle and frequency state of the target generator(s). In this work we assess the feasibility of such an attack under:

1) *model error*; here we assume the opponent has an understanding of the structure of the dynamics, but has biased parameter values; and
2) *incomplete state information*; we focus on the situation whereby the opponent has knowledge of the frequency, but not phase of the target generator and must estimate the former via knowledge of the terminal voltage and current of an associate transmission line.

In the next section, we summarize our coordinated switching attack. Section III studies the effect of model error on attack identification. Section IV introduces a Luenberger-based approach for estimating system state from other known signal quantities. Simulations demonstrate the effectiveness of the attack under error and partial knowledge. Final remarks are provided in Section V.

II. Coordinated Switching Attacks

A. Attack Construction and Existence Condition

Switched systems are a type of variable structure system that consist of a family of subsystems and a rule that governs the switching among them. For example, consider the following single-switch system consisting of two possible dynamics:

$$\dot{x}(t) = \begin{cases} A_1(x,t), & s(x) > 0 \text{ (switch closed)} \\ A_2(x,t), & s(x) < 0 \text{ (switch open)} \end{cases} \quad (1)$$

where $x(t) \in \mathbb{R}^n$ is the state vector, $A_i(x,t) \in \mathbb{R}^n$ is the subsystem dynamics when the switch is either open/closed, and $s(x) \in \mathbb{R}$; $s(x) = 0$ is called the *switching surface*. For certain system parameters and selection of $s(x)$ it can be shown that Eq. 1 exhibits a form of emergent behavior known as a *sliding mode* [4], [5]. Here, the trajectory of the state $x(t)$ is attracted and subsequently confined to the $s(x) = 0$ manifold, which in the case of a sliding mode is also termed the *sliding surface*.

Coordinated variable structure switching attacks are a new class of cyber-physical attacks that employ a variable structure systems theory model of a smart grid. The attack is designed to achieve a form of physical disruption through cyber corruptions of the associated communication channels or control signals of target switch(es). Attack execution requires use of local state-dependent information of the physical power system (possibly attackable by eavesdropping on communication links of appropriate measurement devices). The existence of such vulnerabilities can be found through both visual inspection [4],

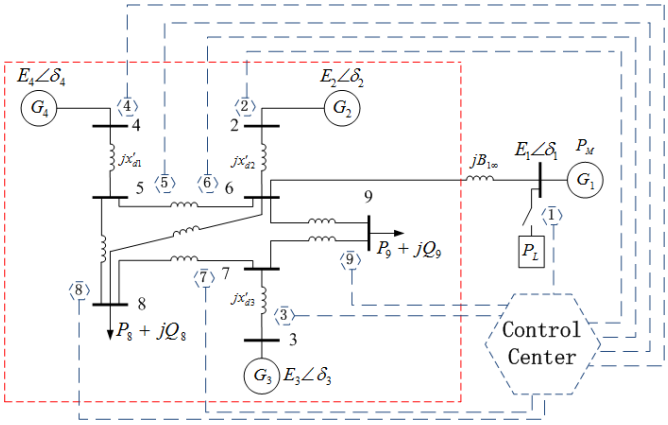


Fig. 1: One line diagram of revised Western Electricity Coordinating Council (WECC) 3-machine, 9-bus system. The (red) dashed rectangle is approximated as a SMIB system.

[5] and mathematical analysis employing the following theorem on a linearized model of the system [6], [7].

Theorem 1 (Existence of a Sliding Mode)**.** *Given the variable structure system:*

$$\dot{x} = \begin{cases} A_1 x + b_1, & s(x) > 0 \\ A_2 x + b_2, & s(x) \leq 0 \end{cases} \tag{2}$$

where $x \in \mathbb{R}^{n\times 1}$, $A_i \in \mathbb{R}^{n\times n}$, $b_i \in \mathbb{R}^{n\times 1}$ *and*

$$s(x) = Cx \in \mathbb{R} \tag{3}$$

for constant row vector $C = [c_1 \ c_2 \ \cdots \ c_n] \in \mathbb{R}^{1\times n}$ *the necessary and sufficient conditions for the existence of a sliding mode are:*

$$\begin{cases} C(A_1 x + b_1) < 0, & s(x) > 0 \\ C(A_2 x + b_2) > 0, & s(x) < 0 \end{cases}. \tag{4}$$

In this paper we study the effect of model error and state estimation on the identification and performance of such an attack. We will focus our results on the test system discussed in the next section.

B. System Modeling and Variable Structure Representation

We consider the Western Electricity Coordinating Council (WECC) 3-machine, 9-bus system of Fig. 1. The (blue) dashed lines represent the cyber components, which correspond to communication channels, sensors, breaker actuators and the control center. The (black) solid lines illustrate physical power system elements including generators, loads, switches, transmission lines.

We approximate this system by using the following second order nonlinear single-machine infinite bus (SMIB) model:

$$\begin{cases} \dot{\delta}_1 &= \omega_1 \\ M_1\dot{\omega}_1 &= P_{M1} - E_1^2 G_{11} - s_L P_L \\ & \quad -E_1 E_\infty B_{1\infty}\sin\delta_1 - D_1\omega_1 \end{cases} \tag{5}$$

where δ_1 and ω_1 are the rotor angle and rotor speed deviation of Generator G_1, respectively, and collectively form the system state vector $x = [\delta_1 \ \omega_1]^T$. The parameters M_1, D_1 and E_1 represent the moment of inertia, damping coefficient, and internal voltage of Generator G_1, respectively, E_∞ is the voltage magnitude at the infinite bus, P_L is the local load at Bus 1, s_L is the load switch status ($s_L = 1$, if the load is connected; $s_L = 0$, otherwise), and $B_{1\infty}$ is the transfer susceptance of the line between Bus 1 and infinite bus.

Assuming $P_1 = P_{M1} - E_1^2 G_{11} - s_L P_L$ and $C_{1\infty} = E_1 E_\infty B_{1\infty}$ where $C_{1\infty} = 1, D_1 = 0.1, M_1 = 0.1$, $P_{M1} - E_1^2 G_{11} - P_L = 0$, $P_{M1} - E_1^2 G_{11} = 0.9$, the overall variable structure system can be represented in linearized form as [8]:

$$\begin{aligned} A_1 &: \begin{cases} \dot{\delta}_1 = \omega_1 \\ \dot{\omega}_1 = -10\delta_1 - \omega_1 \end{cases} && \text{if } P_L \text{ connected} \\ A_2 &: \begin{cases} \dot{\delta}_1 = \omega_1 \\ \dot{\omega}_1 = 9 - 10\delta_1 - \omega_1 \end{cases} && \text{if } P_L \text{ not connected} \end{aligned}. \tag{6}$$

where the system state $[\delta_1 \ \omega_1]^T$ represents the rotor phase angle and frequency of Generator G_1.

III. System Modeling Error

Our focus in this section is on representing modeling error and its effect on the switching attack. We specifically model errors as biases to system parameter coefficients. For the linearized model of our test system of Eq. 6 the errors are represented as:

$$A_1 : \begin{cases} \dot{\delta}_1 = 0(1+\varepsilon_{11}) + (1+\varepsilon_{12})\omega_1 \\ \dot{\omega}_1 = -10(1+\varepsilon_{13})\delta_1 - (1+\varepsilon_{14})\omega_1 \end{cases}. \tag{7}$$

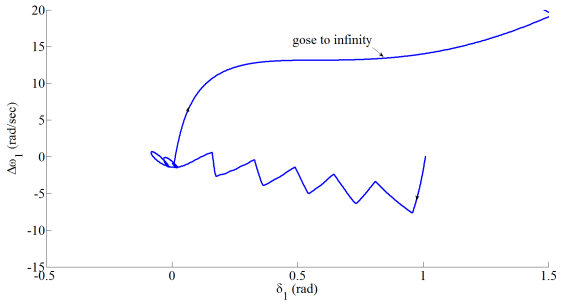
$$A_2 : \begin{cases} \dot{\delta}_1 = 0(1+\varepsilon_{21}) + (1+\varepsilon_{22})\omega_1 \\ \dot{\omega}_1 = 9 - 10(1+\varepsilon_{23})\delta_1 - (1+\varepsilon_{24})\omega_1 \end{cases}. \tag{8}$$

A. Effect of Model Error on Attack Existence Region

Assuming $s > 0$ and $s < 0$ correspond to the load switch being closed (subsystem A_1) and open (subsystem A_2), respectively, our system of Eq. 7-8 corresponds to $A_1 = \begin{bmatrix} 0 & 1+\varepsilon_{12} \\ -10(1+\varepsilon_{13}) & -(1+\varepsilon_{14}) \end{bmatrix}$, $A_2 = \begin{bmatrix} 0 & 1+\varepsilon_{22} \\ -10(1+\varepsilon_{23}) & -(1+\varepsilon_{24}) \end{bmatrix}$, $b_1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and $b_2 = \begin{bmatrix} 0 \\ 9 \end{bmatrix}$ of Eq. 2. Eq. 4 of Theorem 1 provides the following existence conditions for the sliding mode $s = c_1\delta_1 + c_2\omega_1$:

$$\begin{cases} \begin{cases} c_1(1+\varepsilon_{12})\omega_1 - 10c_2(1+\varepsilon_{13})\delta_1 - c_2(1+\varepsilon_{14})\omega_1 < 0 \\ \qquad \text{for } c_1\delta_1 + c_2\omega_1 > 0 \end{cases} \\ \begin{cases} c_1(1+\varepsilon_{22})\omega_1 - 10c_2(1+\varepsilon_{23})\delta_1 - c_2(1+\varepsilon_{24})\omega_1 + 9c_2 > 0 \\ \qquad \text{for } c_1\delta_1 + c_2\omega_1 < 0 \end{cases} \end{cases}. \tag{9}$$

The inequalities above enable the attacker to identify parameters $C = [c_1 \ c_2]$ for execution of the attack. As is observed from Fig. 2, the existence of ε_{ij} creates two possible forms of error: first, false negative or *missed* values for C, and, second, false positive values for C. Fig. 2(b) demonstrates how parameter error creates false negative and positive existence regions. We observe that for "small" errors (i.e., less than 10% deviation in parameter value) and significant existence



(a) State trajectory for $s = 6\delta_1 + \omega_1$.

Fig. 3: State trajectory for $s = 6\delta_1 + \omega_1$.

regions in $[c_1\ c_2]$-parameter space as in Fig. 2, selecting values of $[c_1\ c_2]$ for attack execution is best done using *internal* values within the $[c_1\ c_2]$-existence region. For instance, if we constrain $c_2 = 1$ (to avoid scale ambiguity) then the parameter value for c_1 must be selecting somewhere along the horizontal line of Fig. 2(b). We select $C = [6\ 1]$ corresponding to $s = 6\delta_1 + \omega_1$ for our test case which lies in a region fairly distinct from the boundary of our existence region.

B. WECC 3-Generator, 9-Bus Simulation Study

To verify that the selected $s = 6\delta_1 + \omega_1$ (based on the linear and error-prone system) represents a valid sliding surface in a more realistic test system, we demonstrate the execution of the switching attack on a PSCAD simulation of the WECC 3-generator, 9-bus system in Fig 1. Here, the base MVA is 100, the system normal frequency is 60 Hz and the generator parameters are shown in Table I. The transmission line connecting Generator G_1 and the infinite bus are modeled using an inductor of 0.014 H. The local load P_L is chosen to be 32.4 MW modeled using a constant resistor. The PSCAD step size was chosen to be 50 μs.

The initial state of the WECC system is set to to the stable focus of $(1.1198, 0)$. If $s > 0$, the system dynamics switch to system A_1 and if $s < 0$, they switch to A_2. The switching attack is applied from 0 to 2.5 seconds that drives the system trajectory across the stability boundary of A_2 at which point the switch is permanently set to A_2 making the system unstable. PSCAD simulations demonstrate in Fig. 3 how at time 2.5 seconds, the system trajectory goes to unstable.

Table II presents results on the attack existence range of $C = [c_1\ 1]$ (note: $c_2 = 1$ is fixed as discussed above) for different system models: linearized SMIB of Eq. 6 with no parameter error, nonlinear SMIB of Eq. 5 with and without parameter error (random errors of $\varepsilon_{ij} = \pm 0.1$ were considered) and the high-order WECC test system of Fig. 1 and Table I. It is clear that there is a large overlap in the existence of a sliding mode in both the nonlinear and linearized versions. Thus we conclude that our approach to attack identification is robust to both linearization of the system model and parameter error of approximately $\pm 10\%$. In the next section we discuss the effects of model error on system state estimation.

TABLE I: Generator parameters for WECC system.

Name	Parameter	Gen 1	Gen 2
Rated RMS Line-Line Volatge	V_{gl-l}	13.8 kV	16.5 kV
Active Power	P_g	36 MW	100 MW
Power Factor	p_{fg}	0.8	0.8
Frequency	f	60 Hz	60 Hz
Direct axis unsaturated reactance	Xd	1.55	0.146
D axis unsaturated transient reactance	Xd'	0.22	0.0608
D axis open circuit unsaturated transient time constant	Tdo'	8.95 sec	8.96
Q axis unsaturated reactance	Xq	0.76	0.0969
Q axis unsaturated transient reactance	Xq'	N.A	0.0969
Q axis open circuit unsaturated transient time constant	Tqo'	N.A	0.31
Inertia Constant	H	0.5 sec	23.64
Name	Parameter	Gen 3	Gen 4
Rated RMS Line-Line Volatge	V_{gl-l}	18.0 kV	13.8 kV
Active Power	P_g	163 MW	85MW
Power Factor	p_{fg}	0.8	0.8
Frequency	f	60 Hz	60 Hz
Direct axis unsaturated reactance	Xd	0.8958	1.3125
D axis unsaturated transient reactance	Xd'	0.1198	0.1813
D axis open circuit unsaturated transient time constant	Tdo'	6.0	5.89
Q axis unsaturated reactance	Xq	0.8645	1.2578
Q axis unsaturated transient reactance	Xq'	0.1969	0.25
Q axis open circuit unsaturated transient time constant	Tqo'	0.539	0.6
Inertia Constant	H	6.4	3.01

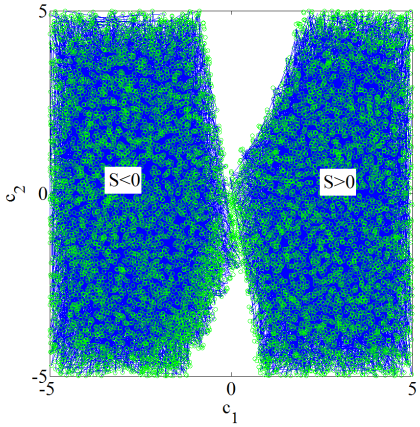
TABLE II: Empirical existence of sliding surface $s = c_1\delta_1 + \omega_1$ for linearized SMIB, nonlinear SMIB, nonlinear SMIB with parameter errors and WECC test system. Simulation tests were conducted for $-20 \leq c_1 \leq 20$.

	Linearized SMIB	Nonlinear SMIB
No sliding mode	$-20 \leq c_1 < 0.7$	$-20 \leq c_1 < 0.6$
Sliding mode exists	$0.7 \leq c_1 \leq 20$	$0.6 \leq c_1 \leq 20$
	Nonlinear SMIB with parameter error	WECC
No sliding mode	$-20 \leq c_1 < 0.6$	$-20 \leq c_1 < 0.7$
Sliding mode exists	$0.6 \leq c_1 \leq 20$	$0.7 \leq c_1 \leq 20$

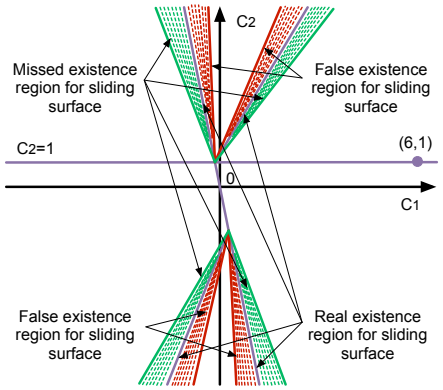
IV. Dynamic State Estimation

A. State Estimator with Model Parameter Error

Power systems need to be continuously monitored in order to keep the system in a normal and secure state, thus knowing the system state is necessary and important. When the physical state of the system cannot be observed directly, a state estimator is employed using input-output measurements of the real system. Coordinated variable structure switching attacks require local state information of the target generator. This can be obtained by an attacker through eavesdropping.



(a) Attack existence range, no error.



(b) False positive/negative regions.

Fig. 2: The effect of model parameter error on identification and execution of attack parameters.

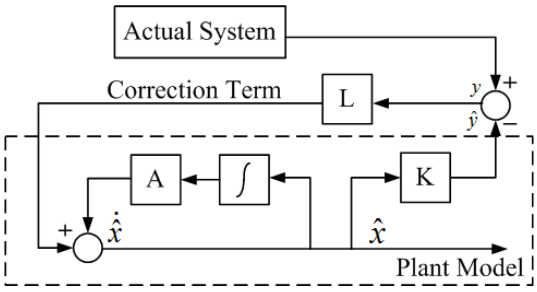


Fig. 4: Luenberger observer for state estimation.

The feasibility of this depends on the communication media and protocols used and its discussion is beyond the scope of this paper. To ensure that the coordinated variable structure switching attack can be implemented with limited state information (in this paper we assume that the frequency ω_1 is known but phase δ_1 must be estimated), we introduce a method that makes use of a Luenberger observer to estimate δ_1. The architecture of a Luenberger observer for state estimation is shown in Fig. 4.

Consider the subsystem dynamics of the actual variable-structure system with known output $y(t)$:

$$\begin{cases} \dot{x}(t) = A_i x(t) + b_i \\ y(t) = Kx(t) \end{cases} \tag{10}$$

where $i = 1$ (for $s > 0$) or $i = 2$ (for $s < 0$), $x(t) \in \mathbb{R}^{n\times 1}$ is the state vector, $y(t) \in \mathbb{R}^{n\times 1}$ is the output, $A_i \in \mathbb{R}^{n\times n}$, $b_i \in \mathbb{R}^{n\times 1}$ and $K \in \mathbb{R}^{1\times n}$. The state estimator makes use of $y(t)$ to determine an estimate of the state $\hat{x}(t)$ assuming the actual system parameters A_i, b_i and K are known; since these values are typically estimated they are distinctively denoted by $\hat{A}_i = A_i + E_{A_i}, \hat{b}_i = b_i + E_{b_i}$ and $\hat{K} = K + E_K$ where E_x denotes the corresponding additive error matrix/vector. The estimator dynamics are given by:

$$\begin{cases} \dot{\hat{x}}(t) = \hat{A}_i \hat{x}(t) + \hat{b}_i + L(y(t) - \hat{y}(t)) \\ \hat{y}(t) = \hat{K}\hat{x}(t) \end{cases} \tag{11}$$

where $x(t) \in \mathbb{R}^{n\times 1}$ is the state vector, $y(t) \in \mathbb{R}^{n\times 1}$ is the system output, $A_i \in \mathbb{R}^{n\times n}$, $b_i \in \mathbb{R}^{n\times 1}$, $K \in \mathbb{R}^{1\times n}$ and $i = 1, 2$. It is well known that for $\hat{A}_i = A_i, \hat{b}_i = b_i$ and $\hat{K} = K$ the estimator error $e(t) = x(t) - \hat{x}(t)$ dynamics satisfies:

$$\dot{e}(t) \;=\; \dot{x}(t) - \dot{\hat{x}}(t) = (A_i - LK)e(t) \tag{12}$$

whereby if the pair (A_i, K) is observable, the estimation error $e(t)$ will decay to zero for any initial condition $e(t_0)$. The observer dynamical behavior can be adjusted by adjusting the observer gain $L = [l_1\ l_2]^T$. In particular, the initial observer state need not match the initial system state as long as the observer gain L is chosen such that all eigenvalues of the matrix $A_i - LK$ are placed to the left in the complex plane. Applying this principle to our variable structure system, we propose the following theorem.

Theorem 2 (State Estimator with Model Parameter Error)**.** *Consider the variable structure system of Eq. 10 with state estimator dynamics of Eq. 11. For* $\hat{A}_i = \begin{bmatrix} a_{i1}(1+\varepsilon_{i1}) & a_{i2}(1+\varepsilon_{i2}) \\ a_{i3}(1+\varepsilon_{i3}) & a_{i4}(1+\varepsilon_{i4}) \end{bmatrix}$ *and* $\hat{K} = \begin{bmatrix} k_1(1+\gamma_1)\ k_2(1+\gamma_2) \end{bmatrix}$, *assuming* $|\varepsilon_{ij}|, |\gamma_i| \ll 1$, *the convergence of the state estimator depends only on the errors of the main diagonal of* $\hat{A}_i$ *and the errors of* $\hat{K}$ *while* $x(t)$ *is bounded. To guarantee error convergence, we require* $l_1k_1(1+\gamma_1) + l_2k_2(1+\gamma_2) - a_{i1}(1+\varepsilon_{i1}) - a_{i4}(1+\varepsilon_{i4}) > 0$.

Proof: The error dynamics in general are:

$$\begin{aligned} \dot{e}(t) \;&=\; \dot{x}(t) - \dot{\hat{x}}(t) \\ &=\; (A_i - LK)x(t) - (\hat{A}_i - L\hat{K})\hat{x}(t) + (b_i - \hat{b}_i) \\ &=\; (\hat{A}_i - L\hat{K})e(t) - (E_{A_i} - LE_K)x(t) + E_{b_i}. \end{aligned}$$

While the switched system is stable, the system state $x(t)$ is bounded and $|x(t)| \le B_x < \infty$. Given the bounded errors of $|\varepsilon_{ij}| \le B_{ij} \ll 1$, $|\gamma_i| \le B_K \ll 1$ and $\|E_{b_i}\| \le B_{b_i} < \infty$, we have a bounded term $(E_{A_i} - LE_K)x(t) + E_{b_i} \le (B_{A_i} - LB_K)B_x + B_{b_i}$. Thus, the error dynamics will converge to $\mathcal{N}$, a neighborhood of $x(t)$, whose size is dependent on the

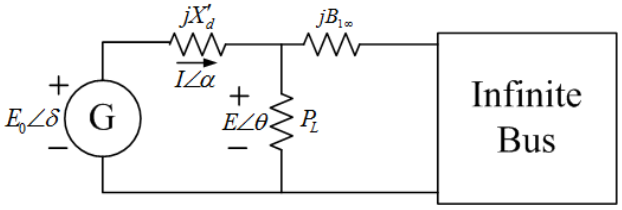


Fig. 5: SMIB System Model

magnitude of the bound on $(E_{A_i} - LE_K)x(t) + E_{b_i}$. Therefore, the estimation error $e(t)$ will decay to $\mathcal{N}$ for any initial condition $e(t_0)$ if the pair $(\hat{A}_i, \hat{K})$ is observable.

$$\hat{A}_i - L\hat{K} = \begin{bmatrix} a_{i1}(1+\varepsilon_{i1}) - l_1k_1(1+\gamma_1) & a_{i2}(1+\varepsilon_{i2}) - l_1k_2(1+\gamma_2) \\ a_{i3}(1+\varepsilon_{i3}) - l_2k_1(1+\gamma_1) & a_{i4}(1+\varepsilon_{i4}) - l_2k_2(1+\gamma_2) \end{bmatrix}$$

The eigenvalues of the matrix $\hat{A}_i - L\hat{K}$ are given by:

$$\begin{aligned} & det(\lambda I - (\hat{A}_i - L\hat{K})) \\ = \; & \lambda^2 + (l_1k_1(1+\gamma_1) + l_2k_2(1+\gamma_2) - a_{i1}(1+\varepsilon_{i1}) - a_{i4}(1+\varepsilon_{i4}))\lambda \\ & + (a_{i1}(1+\varepsilon_{i1})a_{i4}(1+\varepsilon_{i4}) - a_{i2}(1+\varepsilon_{i2})a_{i3}(1+\varepsilon_{i3}) \\ & - a_{i1}(1+\varepsilon_{i1})l_2k_2(1+\gamma_2) - a_{i4}(1+\varepsilon_{i4})l_1k_1(1+\gamma_1) \\ & + a_{i2}(1+\varepsilon_{i2})l_2k_1(1+\gamma_1) + a_{i3}(1+\varepsilon_{i3})l_1k_2(1+\gamma_2)) \end{aligned}$$

Based on the equations above, the real part of the eigenvalues are given by

$$Re(\lambda_i) = -\frac{l_1k_1(1+\gamma_1) + l_2k_2(1+\gamma_2) - a_{i1}(1+\varepsilon_{i1}) - a_{i4}(1+\varepsilon_{i4})}{2} \tag{13}$$

To guarantee $Re(\lambda_i) < 0$, we require

$$l_1k_1(1+\gamma_1) + l_2k_2(1+\gamma_2) - a_{i1}(1+\varepsilon_{i1}) - a_{i4}(1+\varepsilon_{i4}) > 0. \tag{14}$$

Thus, the convergence of the state estimator depends only on the errors $\varepsilon_{i1}, \varepsilon_{i4}, \gamma_1$ and γ_2 found along the main diagonal of $\hat{A}_i$ and in $\hat{K}$. ■

It is clear that appropriate design of L can compensate for model error if error bounds are known.

B. Case Study

We empirically study state estimation in the context of variable structure system attacks in the presence of model error using our WECC test system. We assume that the generator frequency is known to the attacker, but the rotor phase angle must be estimated from terminal voltage and current of the associate transmission line. Specifically, we employ the SMIB model of Fig. 5; according to the Kirchoff's Voltage Law:

$$\begin{aligned} E_0\angle\delta &= jX'_dI\angle\alpha + E\angle\theta \\ &= (E\cos\theta - X'_dI\cdot\sin\alpha) + j(E\sin\theta - X'_dI\cos\alpha) \end{aligned}$$

where $E_0\angle\delta$ is the generator internal voltage, jX'_d is the impedance of transmission line, $I\angle\alpha$ is the current of transmission line and $E\angle\theta$ is the terminal voltage. Thus, the generator internal voltage E_0 and phase angle δ can be estimated using the following equations:

$$E_0 = \sqrt{(E\cos\theta - X'_dI\cdot\sin\alpha)^2 + (E\sin\theta - X'_dI\cos\alpha)^2} \tag{15}$$

and $\tan\delta = \frac{E\sin\theta + X'_dI\cos\alpha}{E\cos\theta - X'_dI\sin\alpha}$. Given the approximation that $\tan\delta \approx \delta$ when δ is small, we have

$$\delta \approx \tan\delta = \frac{E\sin\theta + X'_dI\cos\alpha}{E\cos\theta - X'_dI\sin\alpha}. \tag{16}$$

Therefore, δ can be estimated via the terminal voltage $E\angle\theta$ and current $I\angle\alpha$ of transmission line as follows:

$$\begin{bmatrix} \frac{E\sin\theta + X'_dI\cos\alpha}{E\cos\theta - X'_dI\sin\alpha} \\ \omega \end{bmatrix} \Rightarrow \begin{bmatrix} \delta \\ \omega \end{bmatrix} \tag{17}$$

According to Theorem 2, we must choose the observer gain L such that all eigenvalues of the matrix $(\hat{A}_i - L\hat{K})$ are placed to the left in the complex plane when giving the WECC system model with errors.

Given the system model of Eq. 7-8 we consider the case in which $x(t) = [\delta\ \omega]^T \in \mathbb{R}^{n\times 1}$, $y(t) = [\frac{E\sin\theta + X'_dI\cos\alpha}{E\cos\theta - X'_dI\sin\alpha}\ \omega]^T \in \mathbb{R}^{n\times 1}$, and $\hat{A}_1 = \begin{bmatrix} 0 & 1+\varepsilon_{12} \\ -10(1+\varepsilon_{13}) & -(1+\varepsilon_{14}) \end{bmatrix}$, $\hat{A}_2 = \begin{bmatrix} 0 & 1+\varepsilon_{22} \\ -10(1+\varepsilon_{23}) & -(1+\varepsilon_{24}) \end{bmatrix}$, $b_1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and $b_2 = \begin{bmatrix} 0 \\ 9 \end{bmatrix}$, $\hat{K} = [1, 1]$ (assuming no error).

Applying Theorem 2, we have

$$\begin{aligned} & det(\lambda I - (\hat{A}_i - L\hat{K})) \\ = \; & \lambda^2 + (l_1 + l_2 + (1+\varepsilon_{i4}))\lambda + (10(1+\varepsilon_{i2})(1+\varepsilon_{i3}) \\ & + (1+\varepsilon_{i4})l_1 + (1+\varepsilon_{i2})l_2 - 10(1+\varepsilon_{i3})l_1) \end{aligned}$$

For $Re(\lambda_i) < 0$, we therefore require:

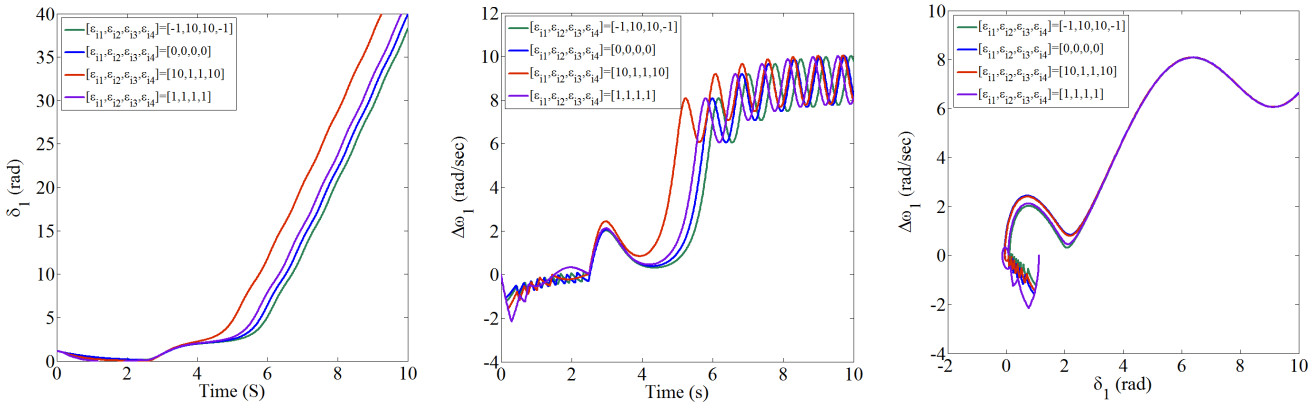
$$l_1 + l_2 + (1+\varepsilon_{i4}) > 0 \tag{18}$$

Thus, in this case the behavior of the state estimator only depends on ε_{i4}, $i = 1, 2$. Assuming, all errors are within the range ± 10, in order to make sure the eigenvalues are in the left hand plane, our our observer gain L is chosen as $L = [1\ 10]$.

We tested the observer with the attack $s = 6\delta_1 + \omega_1$ discussed in previous section. The system dynamics travel along with the sliding mode and still achieve the instability and disruption as shown in Fig. 6; the phase angel and frequency deviations between the estimate state and real state with different set of error are shown. Different model errors have been tested leading to the following observations:

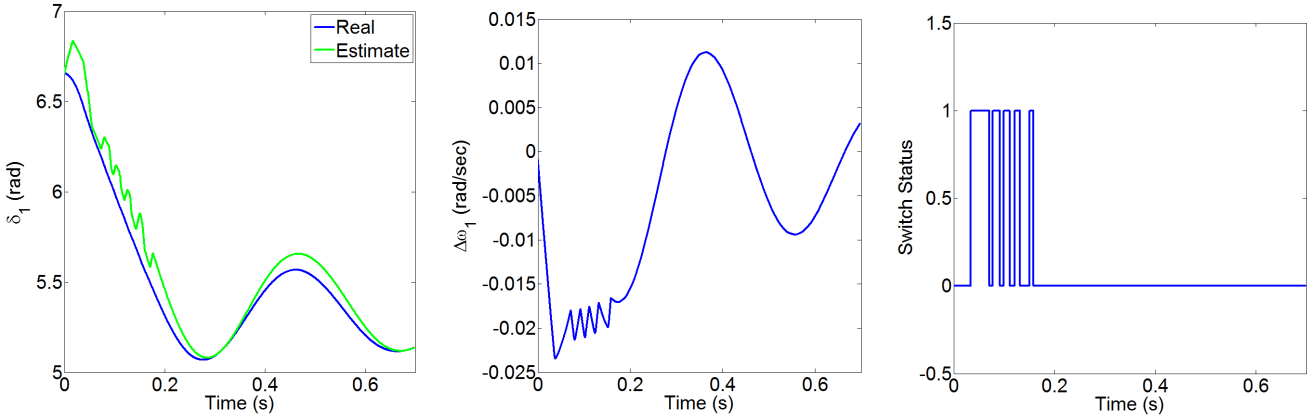
1) As predicted by our analysis, as the error values increase, so does the deviation between $\hat{x}(t)$ and $x(t)$.
2) As stated in Theorem 2, the performance of the estimator is only dependent on the error values $\varepsilon_{i1}, \varepsilon_{i4}, \gamma_1$ and γ_2 and not on ε_{i2} or ε_{i3}.

In order to demonstrate our results on a more realistic test system, we applying our attack $s = 6\delta_1 + \omega_1$ to a higher order model of the WECC system in PSCAD. Even in the presence of model error, the state estimator can track the real state with reasonable accuracy within 0.7 seconds. The corresponding simulation results for the rotor angle, deviation from the nominal frequency of G_1 and the switch status are shown in Fig. 7.



(a) G_1 phase angle. (b) G_1 deviation from nominal frequency. (c) System trajectory.

Fig. 6: Comparison of model errors in WECC system with Luenberger Observer.



(a) G_1 phase angle. (b) G_1 deviation from nominal frequency. (c) Switch Status.

Fig. 7: PSCAD simulation results of WECC system with Luenberger Observer.

V. Conclusions

In this paper, we studied the performance of coordinated variable structure switching attacks in the presence of both model error and state estimation. We demonstrated the potential of the traditional Luenberger observer for coordinated switching attacks when the system state is only partially known to the attacker. Moreover, we identified that the rate of convergence of the state estimator is a function of only specific error terms on the observer system model. Future work focuses on different strategies that exploit the existence of stable sliding modes and identifying inherently secure smart grid topologies.

Acknowledgment

Funding for this work was provided through the Norman Hackerman Advanced Research Program Project 000512-0111-2009 and NSF grants EEC-1062603 and ECCS-1028246.

References

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conference on Computer and Communications Security*, Chicago, IL, November 2009, pp. 21–32.

[2] A. Ashok and M. Govindarasu, "Cyber attacks on power system state estimation through topology errors," in *2012 IEEE Power & Energy Society General Meeting*, San Diego, California, July 22-26 2012.

[3] A. Giani, E. Bitar, M. Garcia, and M. McQueen, "Smart grid data integrity attacks: characterizations and countermeasures," in *Second IEEE International Conference on Smart Grid Communications*, October 17-20 2011, pp. 232–237.

[4] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. Butler-Purry, "A class of cyber-physical switching attacks for power system disruption," in *7th ACM Annual Cyber Security and Information Intelligence Research Workshop*, October 12-14 2011.

[5] ——, "Switched system models for coordinated cyber-physical attack construction and simulation," in *First IEEE International Workshop on Smart Grid Modeling and Simulation*, Brussels, Belgium, October 17 2011, pp. 49–54.

[6] S. Liu, D. Kundur, T. Zourntos, and K. Butler-Purry, "Coordinated variable structure switching in smart power systems: Attacks and mitigation," in *1st International Conference on High Confidence Networked Systems*, Beijing, China, April 17-18 2012.

[7] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A smart grid vulnerability analysis framework for coordinated variable structure switching attacks," in *2012 IEEE Power & Energy Society General Meeting*, San Diego, California, July 22-26 2012.

[8] ——, "A smart grid vulnerability analysis framework for coordinated variable structure switching attacks," in *Proc. IEEE Power Engineering Society General Meeting*, San Diego, CA, July 2012.