2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)

Impact of Malicious SCADA Commands on Power Grids' Dynamic Responses

Hui Lin*, Zbigniew Kalbarczyk†, Ravishankar K. Iyer†
*Department of Computer Science and Engineering, University of Nevada at Reno
†Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign,
*hlin2@unr.edu, †{kalbarcz, rkiyer}@illinois.edu

Abstract **Control-related attacks can use malicious commands crafted in legitimate formats to initiate perturbations to power systems. Our previous work used the steady state of power systems (e.g., through power flow analysis) to estimate the consequences of such commands [1]. However, when power systems move from one steady state to another, their physical components go through a transient period, during which the system state can experience oscillations. An anomaly in an oscillation can make power systems lose synchronisms and experience catastrophic consequences. Analysis based on the steady state cannot understand and predict those harmful oscillations. In this paper, we study the impacts of control-related attacks on the dynamic responses of a power grid, by mapping malicious commands (e.g., that disconnect transmission lines) delivered via communication networks to power systems' electromechanical models. Based on theoretical analysis and numerical simulations, we find that it is challenging for attackers to destabilize a power system, but they can introduce large oscillations in the transient period and thereby cause physical damage.**

SUMMARY OF NOTATION

n	The number of generators in a power system
m	The number of buses in a power system
$\bar{V}_k = V_k \angle \theta_k$	The voltage at bus k, including magnitude V_k and angle θ_k
δ_k	The rotor deviation angle of the generator at bus k
f_k	The rotor frequency of the generator at bus k (in Hz)
ω_k	The rotor angular frequency of the generator at bus k (in rad/s)
H_k	The inertia constant of the generator at bus k
D_k	The damping coefficient of the generator at bus k
P_k^M	The mechanical power of the generator at bus k
P_k^E, Q_k^E	The electrical power of the generator at bus k
P_k^D, Q_k^D	The demand of real or reactive power at bus k
z_k	The internal impedance of the generator at bus k
$Y = G + \mathrm{j}B$	The admittance matrix, which can be decomposed into two real-valued matrices: $Y = G + \mathrm{j}B$
x	State variable for a control system

I. INTRODUCTION

Control-related attacks on SCADA (supervisory control and data acquisition) systems used by power grids can use malicious commands crafted in legitimate formats to initiate physical perturbations. Previous research work has used the steady state of power systems to estimate the consequences of those physical perturbations, e.g., overloading of transmission lines [1].

When power systems move from one steady state to another, their physical components go through a transient period, during which the system state can experience oscillations. Compared to physical violations in the steady state, anomalous oscillations during the transient period can have different security concerns related to power systems' operations. For example, an out-of-band oscillation of a generator's mechanical rotors can trip a relay and isolate the generator from the power system, causing further imbalance between generation and consumption. Unfortunately, anomalies during a power system's transient period cannot be foreseen and detected by the steady-state analysis, which always assumes that a power system can move to a stable steady state following perturbations.

In this paper, we determine the impact of control-related attacks on power systems' dynamic responses (e.g., the oscillations of generators' rotor frequency) by mapping malicious commands (e.g., that disconnect transmission lines or change generations or load demands) delivered via communication networks to power systems' electromechanical models. We demonstrate that it is possible for attackers to follow the proposed analysis to identify malicious perturbations at runtime. We go beyond our previous work, which analyzed the impact of attacks on the steady state, by identifying the control-related attacks that (i) reveal no physical violations when subjected to steady-state analysis, and (ii) introduce out-of-band oscillations that cause security violations during the system's transient period.

To achieve those objectives, we make the following contributions:

- ***Theoretical analysis of control-related attacks.*** We use electromechanical models of generators to formulate a power system as a linear time-invariant system. Based on the mathematical representations, we illustrate how the compromises of network packets propagate step by step in a power system and ultimately cause physical perturbations.

  Through the analysis, we find that it is challenging, if not impossible, for control-related attacks to destabilize power systems. However, the linearized model can successfully identify big perturbations that cause significant oscillations for generators, including ones that cannot be detected by steady-state analysis.
- ***Identify discrepancies between steady-state and transient stability analysis.*** We use the aforementioned theoretic approach to identify multiple cases in which steady-state analysis reveals no physical damage, but the system experiences out-of-band oscillations during the transient period.

  Such discrepancies reveal that existing intrusion detection systems that rely on steady-state analysis can be ineffective against control-related attacks that aim to introduce large transient oscillations. To accurately detect such malicious activities, we need to consider a power system's dynamic models and also use them efficiently.

978-1-5386-7954-8/18/$31.00 ©2018 IEEE

Here, we *discuss the role of the proposed method in the hierarchy of current power system dynamic performance analysis approaches* [2]. On one hand, the objective of *small signal stability analysis* is to evaluate systems' dynamic responses under small variations in load and generation. On the other hand, the objective of *transient stability analysis* is to evaluate systems' capability to maintain stability when subjected to severe disturbances, e.g., short-circuit faults in transmission lines. The severity of disturbances caused by control-related attacks sits in between the levels of disturbance considered in those two traditional analyses. The analyses we present here can complement those prior analyses by characterizing dynamic responses of power systems against malicious activities that can be performed through existing IT infrastructures.

II. Preliminaries

A. Power system dynamic model

In this section, we present our approach for transient analysis based on a power system's dynamic model to evaluate the impact of control-related attacks. The transient analysis describes the trajectory of system state when it moves from one steady state to another; it is closely related to the topology of transmission networks and the mechanical model used for generators and load units.

For each generator, we formulate the electromechanical behavior of rotors with algebraic differential equations (DAEs). In this paper, we use the "classical model," which models a generator as a voltage source of constant magnitude connected in series with a constant reactance. In the classical model, two DAEs, known as *swing equations* and shown in equations (1) and (2), model the electromechanical behavior of each generator. While the classical model contains two DAEs, the proposed analysis methods can be applied to more complicated models. As we focus on the transient activities of generators, we use a single constant impedance to simulate a load unit.

$$\dot{\delta}_k = \omega_k - \omega_s \tag{1}$$

$$\frac{2H_k}{\omega_s}\dot{\omega}_k = P_k^M - P_k^E - D_k(\omega_k - \omega_s) \tag{2}$$

In equations (1) and (2), we use ω_s to represent synchronous angular frequency of rotors, e.g., $\omega_s = 2\pi f_s$ with $f_s = 60$ Hz in the United States. The meaning of other parameters can be found in the Summary of Notation.

On each generator, the swing equations and power flow equations are correlated by the electrical power generated on that bus (denoted by P_k^E for bus k). Consequently, when a perturbation that causes a change in generated electrical power happens, it can introduce oscillations of generators' rotor angular frequency (denoted by δ_k). For example, if the topology of transmission networks is changed, we can calculate the new power flow injected at each bus based on the solution of power flow equations. The updated power flows are used in swing equations to estimate accurately the trajectory of power flows changing from old values to these new values.

B. Linearization

It can take a long time to directly solve nonlinear DAEs. To identify malicious perturbations at runtime, we linearize equations (1) and (2) based on the same assumptions used for the DC power flow analysis: (i) the system states are close to nominal values, i.e., $V_i \approx 1$, $|\theta_i - \theta_k| \approx 0$; and (ii) the power network is lossless, i.e., $G_{ik} \approx 0$.

When we linearize swing equations for generators and group them together, we can represent those equations in the following matrix formulation:

$$\begin{bmatrix}\Delta\dot{\delta}(t)\\ \Delta\dot{\omega}(t)\end{bmatrix} = A\begin{bmatrix}\Delta\delta(t)\\ \Delta\omega(t)\end{bmatrix} + \boldsymbol{u} + \Delta P_0. \tag{3}$$

The derivations of equation (3)'s parameters and variables are shown in Table 1. Equation (3) is related only to the rotor frequency/angle of each generator. Note that matrix A, which is referred to as the *state transition matrix*, hides the detailed topological aspects (e.g., the line's conductance and susceptance), but it establishes the mathematical relations between generators' rotors and facilitates power systems' transient analysis.

TABLE 1. VARIABLES AND PARAMETERS USED IN EQUATION (3)

$\Delta\delta(t) = [\Delta\delta_1(t), \dots, \Delta\delta_n(t)]^T$
$\Delta\omega(t) = [\Delta\omega_1(t), \dots, \Delta\omega_n(t)]^T$
$A = \begin{bmatrix}I & 0\\ 0 & M\end{bmatrix}^{-1}\begin{bmatrix}0 & I\\ L_{gg} - L_{gl}L_{ll}^{-1}L_{lg} & -D\end{bmatrix}$
$\Delta P_0 = \begin{bmatrix}I & 0\\ 0 & M\end{bmatrix}^{-1}\left(\begin{bmatrix}0\\ L_{gl}\end{bmatrix}L_{ll}^{-1}[\Delta P_1^D, \dots, \Delta P_m^D]^T + [0_n^T, \Delta P_1^M, \dots, \Delta P_n^M]^T\right)$
$M = diag\left(\frac{2H_1}{\omega_s}, \dots, \frac{2H_n}{\omega_s}\right)$
$D = diag(D_1, \dots, D_n)$
$L_{gg} = -diag(z_1^{-1}, \dots, z_n^{-1})$
$L_{ll} = B - diag\left((z_1^{-1}, \dots, z_n^{-1}, \mathbf{0}_{m-n}^T)\right)$
$L_{gl} = L_{lg}^T = \left[diag(z_1^{-1}, \dots, z_n^{-1}), \mathbf{0}_{n\times(m-n)}\right]$

Current power systems use feedback control (e.g., automatic generation control or turbine governor control) to ensure that the state converges to a stable value after encountering disturbances. In this paper, the impact of the control is described by variable u in equation (3). This variable is a vector of $2n$, which describes the linear feedback control based on the state variable, i.e., $u = -E\begin{bmatrix}\Delta\delta\\ \Delta\omega\end{bmatrix}$. To simplify the discussion, we consider E to be a *diagonal* matrix. The minus sign is added to indicate that a negative feedback control is applied. In other words, we can have $E = diag(e_1, \dots, e_{2n})$, where $e_k > 0$ with $1 \le k \le 2n$. After we add the control inputs, the LTI model of the power system becomes:

$$\begin{bmatrix}\Delta\dot{\delta}(t)\\ \Delta\dot{\omega}(t)\end{bmatrix} = (A - E)\begin{bmatrix}\Delta\delta(t)\\ \Delta\omega(t)\end{bmatrix} + \Delta P_0 \tag{4}$$

III. Threat Model

In this paper, we consider the remote insider threat model, based on attacks that occurred in Ukrainian power plants [3]. We assume that attackers can bypass the barrier (or perimeter protection) between corporate networks and control networks and establish footholds in the control network that connects the control center and relay devices. In our threat model, we assume that the attackers can penetrate computing devices on the communication path that connects the control center and relay devices. Those computing devices, such as human-machine interfaces (HMIs) or RTUs, are often installed at substations that are distributed over a large geographical area. Because it is challenging to maintain computing devices across a wide area,

we often find unpatched vulnerabilities in those devices, e.g., an old TCP vulnerability found in substation devices [4].

In our threat model, control-related attacks can use malicious commands crafted in legitimate network packets. The compromised commands lead to the modification of the power system's physical configuration and changes in the system's dynamic responses.

In today's power systems, it is possible to perform many control operations (e.g., scheduled line outages, generation control, and load shedding [5][6]) by issuing network packets based on protocols like DNP3 or Modbus from compromised computing devices (such as human-machine interfaces or laptops brought in by system operators) within the control network. Consequently, attackers can maliciously modify the physical configurations of the power system by penetrating the control network. Because the physical configuration determines the parameters of the swing equations that describe the electromechanical behavior of a power system, control-related attacks can modify the system's transient activities.

To quantify the consequences of control-related attacks, we propose the following properties related to the behavior of state variables during the transient period.

***Definition 1* (Stability property).** The state variables, i.e., $\Delta\delta$ and $\Delta\omega$, are bounded with the bounded input.

***Definition 2* (Security index).** To measure the severity of the generator frequency deviation (or oscillations), we define the security index (proposed in [7]) as $S_{dev} = \sum_{k=1}^{n} \left(\frac{\Delta\omega_k}{\omega_s} \times 100\right)^2$.

***Definition 3* (Physical violation).** When the rotor frequency of at least one generator at its stable state deviates by more than 0.5 Hz, i.e.,$|\Delta\omega_k| > 2\pi \times 0.5\ rad/s$, the corresponding generator is regarded as having a physical violation.

A. Related work

We classify malicious attacks that target the *feedback control loop* into two types. The first type is false or bad data injection attacks, in which attackers introduce malicious measurements that affect the outcome of state estimation [8]. In this type of attack, incorrect system states are estimated and can have a negative impact on power grids. However, there has not been sufficient research on how the incorrect system states can lead to damage to the physical infrastructure. The second type is discussed in [9], in which DeMarco et al. exploit a control-theoretic approach to study the impact of malicious feedback control on a power system. The paper assumes that the attackers have full control over a generator, which can be challenging to achieve in practice through control networks.

Attacks that perturb the feedback control loop of a power system can indirectly impact the issued control commands. However, in today's power grid, commands are more frequently transmitted over the IP-based control network. Consequently, after gaining access to the control network, the attackers have more incentives to compromise control commands, which can directly change the state of the power system. This is not to say that attacks on sensor measurements are not important. Quite the opposite: compromised measurements can be used to hide the real (potentially anomalous) state of the power grid to delay detection of an attack until after the system has been damaged (as seen in the case of Stuxnet [10]).

Cascading outages of multiple physical components of a power grid, such as substations and transmission lines, have drawn much research attention. The efforts have been proposed to identify and rank the vulnerable physical components in the power grid. To achieve that goal, the metrics of a power system's electrical characteristics, e.g., the load of a substation or transmission lines, can be used [11][12]. In addition, researchers use the characteristics of the transmission network, e.g., its connectivity or the length of the shortest path between substations, to identify the vulnerable components [13][14]. The control-related attacks considered in this paper also target physical components. However, we specifically focus on the physical configurations that can be modified via communication networks.

IV. Attack Analysis

In this paper, we analyze two attack scenarios: the outage of multiple transmission lines, and malicious generation or load demand adjustment [5][6][15].

A. Scenario I: Outage of multiple transmission lines

By exploiting control commands to operate relays in substations, attackers can put multiple transmission lines out of service simultaneously. In our previous work, we showed that this attack goal can be achieved through a single network packet [1]. In this attack scenario, the outage of transmission lines is reflected in the values of the admittance matrix, which further impact matrix A in the LTI model. Notably, matrix A plays an important role in a system's control functionality, e.g., stability and controllability.

***Remark 1* (system stability).** If the transmission network of a power system is still connected after a malicious line outage, the system remains stable.

We could not find a strict proof of the property included in this remark. However, based on the mathematical model, we find that it would be impractical, if not impossible, for attackers to construct a specific line outage that could make the system unstable.

If the transmission network is still connected after a line outage, matrix B in Table 1 will be a negative definite matrix [16]. Because $L_{ll} = B - diag\left((z_1^{-1}, \dots, z_n^{-1}, \mathbf{0}_{m-n}^T)\right)$ and the matrix $\left[-diag\left((z_1^{-1}, \dots, z_n^{-1}, \mathbf{0}_{m-n}^T)\right)\right]$ is a negative semi-definite matrix, L_{ll} is also a negative definite matrix, which makes L_{ll} full rank; thus, L_{ll}^{-1} exists.

If we consider the LTI model in the Laplace domain, the pole of the system can be obtained by solving an equation: $\det\left(Is - (A - E)\right) = 0$, where $\det(\cdot)$ returns the determinant of a matrix:

$$Is - (A - E) = \begin{bmatrix} Is + E_1 & I \\ M^{-1}(L_{gg} - L_{gl}L_{ll}^{-1}L_{lg}) & Is - M^{-1}D + E_2 \end{bmatrix}, \quad (5)$$

where matrix E is partitioned to include two diagonal matrices E_1 and E_2 with appropriate dimensions.

If e_k (which is the k-th diagonal element of matrix E) is a system pole, then $s = e_k$ satisfies the equation $\det\left(Is - (A - E)\right) = 0$. Note that when $s = e_k$, we also have $\det(Is + E_1) = 0$.

This system pole is only related to the feedback control applied to the power grid. How its value is changed depends on how feedback control can be modified by attacks; we leave that topic to future work.

Other poles, for which $\det(Is + E_1) \neq 0$, satisfy the following equation:

$$\det\Big((Is - M^{-1}D + E_2)(sI + E_1) - M^{-1}\big(L_{gg} - L_{gl}L_{ll}^{-1}L_{lg}\big)\Big) = 0 \quad (6)$$

Based on equation (6), we can study how the line outage can impact the system poles. When the line outage does not disconnect the power network, L_{ll} is still full rank, and its inverse exists. When attackers introduce the outage of multiple transmission lines, they can affect the values of L_{ll}, which can impact only the constant part of the characteristic polynomial on the left side of equation (6). At that stage, there are no general closed-form relations between entries in L_{ll}^{-1} and L_{ll}. Consequently, we cannot establish a closed-form derivation to reflect the changes of system poles according to the change of L_{ll}. Furthermore, the changes made in L_{ll} because of the line outage are always distributed among all elements in L_{ll}^{-1}. Consequently, it is challenging, if not impossible, for an attacker to analytically construct a strategy that makes the system unstable.

Remark 2. The analysis above excludes the case in which a malicious line outage disconnects a power system into islands. When the power system network is connected after a multiple-line outage, the system load demand and generation remain unchanged and therefore can be balanced easily. Consequently, it is likely that the system remains stable.

When the power system network is disconnected into islands because of a line outage, we can repeat the analysis for each island. However, for each island, the power balance between the load and the generation is disturbed. That is equivalent to modifying ΔP_0 in the equation (4); ΔP_0's impact on a power system's dynamic responses is discussed in Section IV.B.

B. Scenario II: Change power generation & load demands

From equation (6), we can see that changes made to power generation and load demands can affect the value of ΔP_0, which can be regarded as an input variable to an LTI system. State feedback control is usually designed based on the type of inputs. For example, if the inputs are constant, then a proportional control is usually added in the feedback loop so that the state or the outputs can keep track of the input and reach a steady state.

ΔP_0 is a $2n$ vector for which the values of the first n elements are 0. If an attacker changes the power generation or load demand, only the values of the last n elements are changed. Because the last n elements correspond to a change of $\Delta\omega$, the security index proposed in *Definition 2* can be changed.

If attackers make ΔP_0 constant, then $\Delta\delta(t)$ and $\Delta\omega(t)$ will converge to other nonzero values. Consequently, system states, i.e., $\delta(t)$ and $\omega(t)$, will keep on increasing or decreasing, which can destabilize the power system. In practice, however, the power generation or the demand from load units can be adjusted only in a specific range. Under such constraints, it can be impractical to try to destabilize the power system based on changes in generation or load demands.

In addition to a power system's transient activities, its steady states can also be changed under this attack scenario. When a power system reaches a steady state, $\Delta\dot{\delta}$, $\Delta\dot{\omega}$ become 0, and then equation (6) becomes:

$$\mathbf{0} = (A - BK)\begin{bmatrix}\Delta\delta(t)\\ \Delta\omega(t)\end{bmatrix} + \Delta P_0 \quad (7)$$

Equation (7) provides the closed-form relations between the deviation of system steady states and ΔP_0, which is also related to L_{ll} and can be changed by the attacker correspondingly. As a result, we can see that attacking the system with a line outage can cause perturbations of generation and load demands that affect the system's steady-state values; this is consistent with the analysis in our previous work [1].

V. EVALUATIONS

We performed evaluations from an attacker's perspective to find a malicious strategy, i.e., ways to perturb the physical configuration of a power system, that can (i) put the system into unstable states, or (ii) violate physical constraints on rotor frequency deviation as specified in *Definition 3*.

In the evaluations, we used the IEEE 14-bus system and IEEE RTS-96 system. The case file for these two systems and the parameters of the dynamic characteristics of the generators can be found in [17][18]. Two attack scenarios were simulated: (i) random opening of 4 transmission lines, and (ii) random selection of load units or generators, and increasing or decreasing of the demands or outputs by at most 20%. We implemented the linear approximation of the power system, i.e., equation (4), in Matlab Simulink and used this linear model to calculate a security index and select malicious system changes.

A. Impact of line outage on system stability

For each combination of 4 transmission lines, we calculated the solution of equation (6) to see whether there were system poles whose real part was larger than zero. To simulate normal variation of generator models, we varied the parameter values in the range of −50% to 200% of the base values provided in [17][18]. We selected 30 sets of random values for the generator model; for each set of parameter values, we randomly analyzed 1000 combinations of outages of up to 4 transmission lines, where the outages did not disconnect the power system into isolated islands.

In all our experiments, we could not find any attack strategy that could directly destabilize the system. In other words, we could not find the solution of equation (6) on the open right-hand plane by opening multiple transmission lines. In addition, we further studied how much the solutions were changed under this attack scenario. We measured the average standard deviations ("SD") of all solutions from our experiments, as shown in Table 2. We can see that the impact of a line outage on the state variable is small, which makes it challenging for attackers to destabilize the system by disconnecting multiple transmission lines. These results are consistent with the analysis presented in *Remark 1*.

TABLE 2. STANDARD DEVIATION OF SYSTEM POLE AGAINST A MULTIPLE-LINE OUTAGE IN THE IEEE 14-BUS SYSTEM.

	Pole 1	**Pole 2**	**Pole 3**	**Pole 4**	**Pole 5**
SD	0.0113	0.0149	0.0134	0.0173	0.0112
	Pole 6	**Pole 7**	**Pole 8**	**Pole 9**	**Pole 10**
SD	0.0088	0.0165	0.0159	0.0129	0.0129

B. Impact of line outage on security index

In this section, we use the solution of equation (6) to evaluate how line outages can impact the security index calculated based on the peak value and steady-state values of $\Delta\omega$, which affects the range of oscillation during a system's transient activities. Note that the derivation in equation (6) is a linear approximation of the power system's nonlinear model; attackers can use such a derivation to quickly identify a critical line outage that introduces significant oscillations. We can use the power system's nonlinear model to validate the accuracy of such attack identifications.

In Figure 1, we show the variation of the security index against the line outages for the IEEE 14-bus system. The *x*-axis displays the index of 100 randomly selected combinations of 4-line outages, while the *y*-axis represents the value of the security index. The solid line shows the variation of the security index calculated based on the steady-state values of $\Delta\omega$, while the dotted line shows the variations based on their peak values. Figure 1 shows that the security index varies against different combinations of line outages. Compared to the security index calculated based on steady states, the variation is especially dramatic for the peak values.

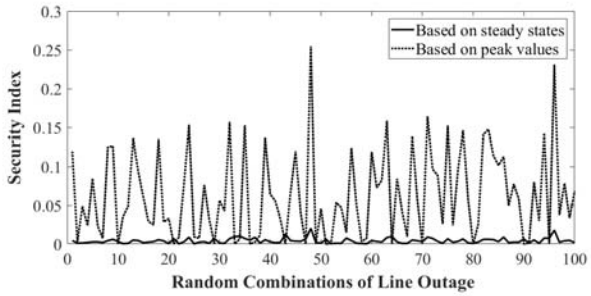

Figure 1. Variation of the security index based on the steady-state value and the peak value of $\Delta\omega$ against random line outages.

Based on the value of the security index, we could identify the relative severity levels of line outages that affect a power system's dynamic responses. To validate the analysis based on the derived LTI model, we selected the 10 line outages with the largest security indices and the 10 line outages with the smallest security indices, and evaluated them in the Transient Stability toolbox in PowerWorld [19]. For each generator, we added turbine governors, which can adjust mechanical power, i.e., P_k^M.

Based on the responses simulated in PowerWorld, we find that the security index and the LTI model can effectively identify severe system perturbations. For the 10 line outages with the smallest security indices, we usually observed 0.1~0.2 Hz deviation of the rotor frequency. However, for the 10 line outages with the largest security indices, the steady-state value of rotor frequency could increase to 0.4~0.5 Hz on average. The most severe frequency deviation for the IEEE 14-bus system was found when lines 2, 3, 4, and 12 were disconnected (based on the line index used in Matpower [17]), while the least severe frequency deviation occurred when lines 12, 15, 16, and 17 were disconnected. Figures 2(a) and 2(b) present the transient responses of these two cases for comparison. In the figure, the *x*-axis specifies a timeline from 0 to 20 seconds; the *y*-axis specifies the value of the rotor frequency in Hz. The responses of all five generators are represented by different colors. In Figure 2(a), after the line outage, the steady-state frequency of the rotor at all buses stays around 60.5 Hz, while the peak value of the rotor frequency can increase up to 61.5 Hz.

In practice, large deviations of rotor frequency can either directly damage a generator or trip physical devices. With the help of feedback controls, e.g., turbine governors, the steady state of the frequency deviation caused by the outage of lines 2, 3, 4, and 12 could be reduced. Even with the help of the feedback controls, the rotor frequency of the generators on buses 1 and 6 deviated out of the safe margin (e.g., 60±0.5 Hz) for almost 8 seconds.

Malicious line outage that avoids steady-state detection. In the IEEE RTS-96 system, we used the derived linearized model to identify malicious perturbations that introduce (i) significant oscillations during a power system's transient period, but (ii) no overloading of transmission lines based on steady-state power flow analysis. The transient responses of two such cases are shown in Figures 2(c) and 2(d). Because the RTS-96 system has 33 generators, we show in the figure the responses of five selected generators, which experience more oscillations than the others do. Disconnection of 4 transmission lines (out of a total of 120) is a small disturbance and introduced no safety violations on the system's steady state. However, these disturbances, which occurred in different locations, can disrupt the interactions among generators and cause significant oscillations for them. From the figure, we can see that rotor frequencies can be as large as 62 Hz after they become stable. In practice, such oscillations can immediately trip the generators. If no appropriate remedy responses are applied, the attacks can even cause some physical damage.

C. Impact of changing load demand and/or generation on the security index

Changing both load demand and power generation changes ΔP_0 in equation (4), and that further changes the values of a system's state variables. In this section, we change ΔP_0 with different constant values and study how the steady-state values of the system state vary accordingly.

Changes of load demand and/or power generation introduced dramatic variations of the security index, similar to what is shown in Figure 1. We validated the changes in PowerWorld. We selected two changes that give the maximum security index and the minimum security index. Specifically, when load demands at buses 2, 3, 4, 6, 9, 13, and 14 were increased by 20%, the maximum security index was found. When load demands at buses 5, 10, 11, and 12 were increased by 20%, the minimum security index was observed. For a less severe load demand change, shown in Figure 2(e), the steady-state value of the rotor frequency was around 59.9 Hz. On the other hand, for a severe load demand change, shown in Figure 2(f), the rotor frequency decreased to 59.4 Hz, which is also beyond the range of ±0.5 Hz.

VI. Discussions

Based on the analysis in this paper, we would like to highlight two points to be addressed in the future. First, we find that control-related attacks can impact the open-loop characteristics of power systems in ways that are different from the impacts on

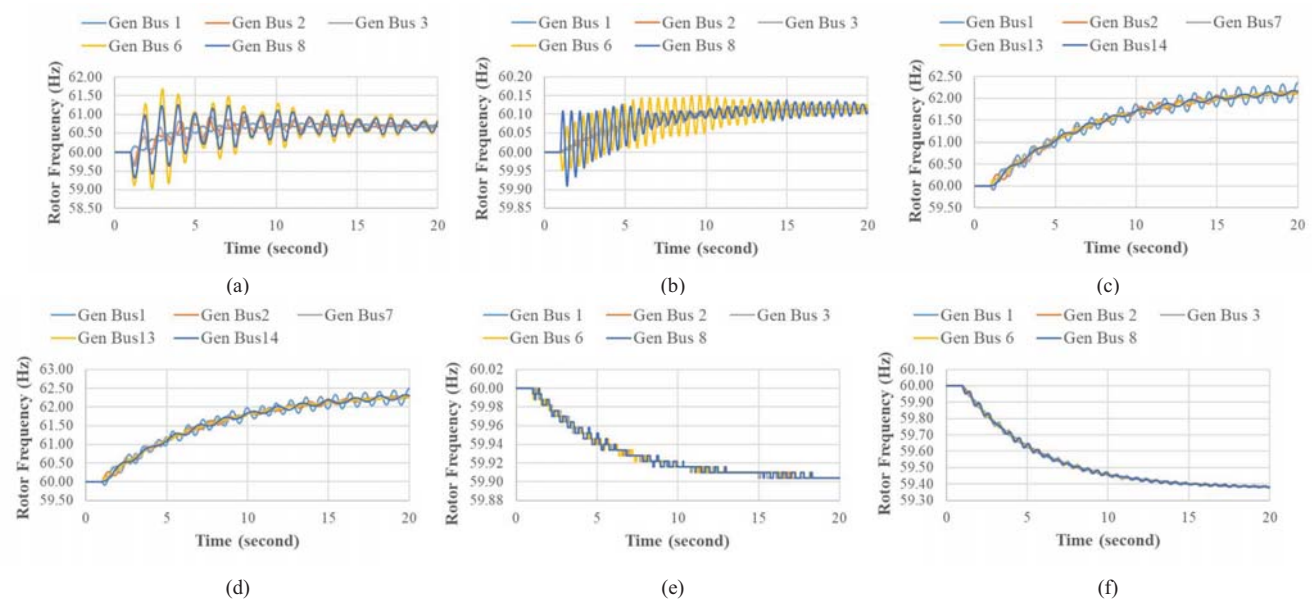

Figure 2. Transient responses for outages of (a) lines 2, 3, 4, and 12, and (b) lines 12, 15, 16, and 17 in the IEEE 14-bus system; transient responses for outages of (c) lines 1, 10, 102, and 109, and (d) lines 1, 10, 102, and 107 in the IEEE RTS-96 system; and transient responses for increasing load demands at (e) buses 5, 10, 11, and 12, and (f) buses 2, 3, 4, 6, 9, 13, and 14.

closed-loop performance that have previously been found via dynamic analysis. Because feedback control mechanisms are designed based on a system's open-loop characteristics, control-related attacks can potentially make those control mechanisms less effective and cause security violations on the control mechanisms; this impact needs further in-depth analysis in future work. Second, control-related attacks have a fundamental computation-asymmetry advantage over defenders. While we can use the linearized model to identify malicious attack strategies quickly, the model does not provide accurate solutions for a system's dynamic responses. Simulations based on the nonlinear model can accurately identify the dynamic responses and detect the attacks; however, these simulations can take a long time, making it difficult to apply them at run-time.

VII. Conclusion

In this paper, we use control-theoretic approaches to study the impact of control-related attacks in which a malicious command can change a power system's physical infrastructure, e.g., the network topology of a transmission network. Our study reveals that the considered attack scenarios (i.e., multiple-line outages and modification of generation and/or load demands) have limited capability to destabilize a power system, but can easily introduce physical violations on generators during a system's transient period. Our evaluations on the IEEE 14-bus system and the IEEE RTS-96 system validate the theoretic findings.

Acknowledgments

This material is based upon work supported in part by: (1) the National Science Foundation under award number CNS 1314891. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation; and (2) the Department of Energy under award number DE-OE0000780. Neither the United States Government not any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

References

[1] H. Lin, A. Slagell, Z. T. Kalbarczyk, P. W. Sauer, and R. K. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 163–178, Jan. 2018.

[2] P. Kundur, N. J. Balu, and M. G. Lauby, *Power System Stability and Control*. New York: McGraw-Hill, 1994.

[3] R. M. Lee, M. J. Assante, and T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*. SANS and E-ISAC technical report, March 2016. [Online] Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[4] D. Formby, S. Jung, J. Copeland, and R. Beyah, "An empirical study of TCIP vulnerabilities in critical power system devices," in *Proc. 2nd Workshop on Smart Energy Grid Security*, pp. 39–44, 2014.

[5] B. Qiu, Y. Liu, E. K. Chan, and L. J. Cao, "LAN-based control for load shedding," *IEEE Computer Applications in Power*, vol. 14, no. 3, pp. 38–43, July 2001.

[6] ABB, *Grid Automation Controller COM600 Product Guide*. 2014. [online] Available: http://www05.abb.com/global/scot/scot229.nsf/veritydisplay/04a937b04ea99cb3c1257aad0031463f/$file/COM600_pg_756764_ENe.pdf.

[7] J. Hazra, and K. S. Avinash, "Identification of catastrophic failures in power system using pattern recognition and fuzzy estimation," *IEEE Trans. Power Systems,* vol. 24, no. 1, pp. 378–387, 2009.

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

[9] C. L. DeMarco, J. V. Sariashkar, and F. Alvarado, "The potential for malicious control in a competitive power systems environment," in *Proc. IEEE Int. Conf. Control Applications*, 1996, pp. 462–467.
[10] N. Falliere, L. Murchu, and E. Chien, "W32.Stuxnet dossier," Symantec Security Response, 2011.
[11] A. O. Ekwue, "A review of automatic contingency selection algorithms for online security analysis," in *Proc. Int. Conf. Power System Monitoring and Control*, 1999, pp. 152–155.
[12] F. Albuyeh, A. Bose, and B. Heath, "Reactive power considerations in automatic contingency selection," *IEEE Trans. Power Apparatus and Systems*, vol. PAS-101, no. 1, pp. 107–112, Jan. 1982.
[13] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?" *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 20, no. 3, 2010.
[14] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Physical Review E,* vol. 69, no. 2, Feb. 2004.
[15] IEEE Power & Energy Society, "Object group 12: binary output commands," in *IEEE Standard for Electric Power Systems Communications – Distributed Network Protocol (DNP3)*, IEEE Std. 1815-2010, pp. 1,775, July 1, 2010.
[16] Z. Wang, A. Scaglione, and R. J. Thomas, "Generating statistically correct random topologies for testing smart grid communication and control networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 28–39, June 2010.
[17] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning and analysis tools for power systems research and education," *IEEE Trans. Power Systems*, vol. 26, no. 1, 2011.
[18] C. Grigg *et al*. "The IEEE Reliability Test System-1996. A report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee," *IEEE Trans. on Power Systems*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999.
[19] PowerWorld Corporation. PowerWorld: The Visual Approach to Electrical Power Systems. [online] Available: http://www.powerworld.com/.