Optimal False Data Injection Attack Against Load-Frequency Control in Power Systems

Mohamadsaleh Jafari, *Member, IEEE*, Mohammad Ashiqur Rahman, *Senior Member, IEEE,* and Sumit Paudyal, *Senior Member, IEEE*

***Abstract*—Intelligent false data injection on load measurements can trigger false relay operation (FRO) of frequency-based protection relays, affecting the power system frequency and thus threatening the security of power systems. In this paper, we propose an optimization-based formal model to find the optimal false data injection attack (OFDIA) with the minimum required time leading to an FRO. The proposed model considers the dynamic behavior of the power system in an optimization framework to find the optimal size of attacks over multiple generators' dispatching cycles to minimize the attack launch time. Using the proposed formal modeling, we study the impact of power system parameters, including inertia, governor's droop and time constant, and the attacker's accessibility to loads on the attack success and launch time. The results demonstrate that systems with low inertia are more vulnerable to FDIAs while systems with higher inertia are more secure as fewer generator protection relays are impacted by FRO. In addition, we show that securing more load meters can increase the time for launching an attack in the system. Moreover, our studies show that a combination of large values of the governor's time constants and small values of the governor's droops can raise the time of successful attacks, making the system more secure against FDIAs.**

***Index Terms*—False data injection attack, load-frequency control, frequency stability, optimization, protection relays.**

I. Introduction

With the adoption of advanced information and communication technologies, the traditional power grids are transforming into smart cyber-physical systems [1]. Although this transition to smart grids brings several benefits to system operations [2], [3], it also makes power grids vulnerable to cyber threats due to their increased dependency on communication and measurement technologies. Among the various types of cyberattacks, false data injection attack (FDIA) represents a major class of cyberattacks that have been extensively investigated recently in the literature [4]–[7]. In FDIA, an attacker sends wrong data into the existing measurement/communication systems in the power grids so that it can mislead the control center/controllers to make wrong control decisions. There are several real-world instances in that FDIA has been devised by the attackers to cause damage to the power grids. For example, FDIA on distribution grids in Ukraine in 2015 left more than 200 thousand customers without electricity for a few hours [5]. Besides, there are some attacks such as the Stuxnet [8] and Dragonfly [9] in which the attacker needed to have full knowledge about the system and full access to the real-time data in the control centers. The developed Stuxnet worm injected false data into control signals and attacked nuclear centrifuges. Despite the fact that these attacks were not launched in power systems, it is possible that such complicated attacks with full access to data easily target power systems as well. Access to such a high level of data can also be provided by insider attackers [10] via social engineering against employees in the control center [11]. Considering all of the abovementioned, in this paper, we study FDIAs on power systems while the attacker has full access to the power system data.

Grid frequency is one of the indicators of the normal operation of power systems. Any major fluctuations in the frequency need to be corrected so that it remains within the acceptable range; otherwise, there could be serious consequences, including blackouts. For example, the 2019 blackout in England and Wales was caused by the decline in the grid frequency that left around one million customers without electricity [12]. Following any disturbance in the power grids, the primary frequency response, which includes automatic decentralized control action of generators' active power output, instantaneously determines the grid frequency. However, in a bit slower time scale compared to the primary frequency response, the grid frequency is maintained by re-dispatching the generators. If the frequency fluctuates from the nominal value, re-dispatching the generators adjusts the reference set-points of the generators equipped with governors to bring the frequency back within the acceptable range.

Since the dispatching process relies on measurements and communication (see Fig. 1), any FDI in the closed-loop dispatching process may impact the frequency stability of the power system leading to false tripping of relays and system-wide consequences [13]. Among the several protection relays that could be impacted by FDI, the rate-of-change-of-frequency (RoCoF) relays, under-/over- frequency relays, and Load shedding relays are the ones directly impacted by FDI on the closed-loop control of the dispatching process. These relays are responsible for assisting in load-generation balance by disconnecting generators/loads at pre-defined locations as needed [14], [15], tripping the generators during excessive frequency excursion to protecting the system from frequency instability, and preventing synchronous generators from damage. Though most of the protection relays operate based on local measurements as shown in Fig. 1, the FDIA on the closed-loop control of the dispatching process can cause

This work is supported in part by National Science Foundation grant ECCS-2001732, Department of Energy award CR0000024, and Florida International University Graduate School Dissertation Year Fellowship. The authors are from Florida International University, Miami, FL, USA. Emails: mjafa006@fiu.edu, marahman@fiu.edu, spaudyal@fiu.edu

TABLE I
SUMMARY OF NOTATIONS

Symbol	Definition	Symbol	Definition
$\hat{(\cdot)}$	Parameter value after attack	$\overline{\varepsilon}^r$	Slack term for upper RoCoF threshold
$\check{(\cdot)}$	Parameter value from control center's viewpoint	$\underline{\varepsilon}^r$	Slack term for lower RoCoF threshold
$\mathcal{A}$	Set of accessible loads to the attacker	Δt	Simulation time step
i,j	Bus indices	ΔP^s	Governor reference set-point change in two subsequent time steps
k	Discrete step	a	Number of random sets of accessible loads
$\mathcal{C}$	Set of discrete steps of generators dispatching cycles $\{\frac{t^c}{\Delta t}, \frac{2t^c}{\Delta t}, ..., \frac{Ct^c}{\Delta t}\}$	$B_{i,j}$	Imaginary part of line admittance between bus i and bus j
$\mathcal{F}$	Set of dispatchable generators	C	Number of dispatch cycles
$\mathcal{G}$	Set of buses with generators	$\overline{C}$	Maximum number of dispatch cycles
$\mathcal{L}$	Set of buses with loads	f_o	Nominal frequency
$\mathcal{N}$	Set of buses	H	Synchronous generators' inertia constant
$\mathcal{O}$	Set of non-dispatchable generators	K_D	Generator's damping factor
$\mathcal{T}$	Set of simulation discrete steps $\{1,2,..., \frac{Ct^c}{\Delta t}\}$	n	Number of simulation discretized steps
$\alpha,\beta,\gamma,$ η,ζ	Weighting factors	P	Attack success possibility
$\widetilde{P}^l$	Load measurement attack value	$\widetilde{P}^l$	Load measurement attack value
δ	Generator's rotor angle and buses' voltage angle	$\widetilde{P}^l$	Load measurement attack value
$\dot{\delta}$	Rate of change of generator's rotor angle	$\widetilde{P}^l$	Load measurement attack value
ω	Instantaneous angular frequency	P^g	Generator's active power output
$\dot{\omega}$	Rate of change of instantaneous angular frequency	$\overline{P}^g$	The upper limit of generator active power
ω_o	Nominal angular frequency	$\underline{P}^g$	Lower limit of generator active power
$\dot{\omega}^r$	RoCoF	P^l	Load active power
$\overline{\tau}^f$	Over frequency threshold	P^m	Generator's mechanical input power
$\underline{\tau}^f$	Under frequency threshold	P^s	Governor's reference set-point
τ^g	Bad data detection threshold for generator power output changes in two subsequent discrete steps	r	Number of cycles in RoCoF calculation
τ^l	Bad data detection threshold for load measurements changes in two subsequent time steps	R	Governors' droop
τ^r	RoCoF threshold	S	Generator's apparent power
$\Delta\omega$	Angular frequency deviation	S^b	Base MVA
$\overline{\varepsilon}^f$	Slack term for over-frequency threshold	t^a	Average time minimally required for a successful attack
$\underline{\varepsilon}^f$	Slack term for under-frequency threshold	t^c	Time interval between two subsequent dispatch cycles
T	Governors' time constant	x	Attaker's accessibility to load measurements

unnecessary changes in frequency that ultimately leads to false relay operations (FRO) [16]. As a simple example of how FRO attacks can arise in power systems, assume an attacker injecting false data into the load measurements at dispatching cycle n to mislead the control center of a reduction in load consumption. This faulty data makes the control center have a wrong dispatch of power in the system and determines wrong reference set-points for the governors. Comparing the frequency deviation $\Delta\omega$ and P^s, the governor changes the mechanical input power of the generators, and consequently, the total power generation in the grid alters while the actual load in the grid is still the same as the pre-attack value (remember that the attacker just injects false data into the load measurements and does not alter the actual load consumption). This load-generation imbalance causes some fluctuations in the frequency. If the fluctuations are large enough so that at least one of the RoCoF and under-/over- frequency thresholds are met, FRO is considered as successful. Otherwise, the attacker needs to launch another attack at the subsequent dispatching cycle $n+1$. The summary of the notations used in this paper can be found in Table I.

A. Related Work

The impact of FDIAs on the frequency behavior of power grids and protection relay operation is studied in the literature. The effect of FDIAs on the generators' dispatching process

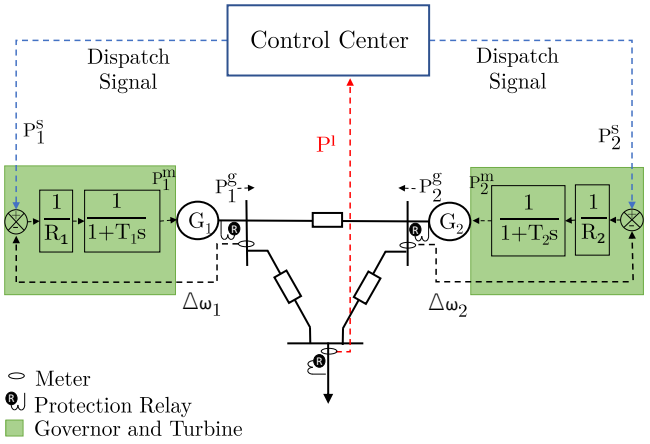


Fig. 1. An example of generators dispatching process in power grids to regulate grid frequency.

is studied in [17]–[19] while investigating different FDIA templates such as signal scaling, ramps, surges, and random noises. In [20], authors showed the impact of an attack on local controllers of loads (that emulate inertia) in power grid frequency. In [21], the authors showed that FDIAs could lead to unnecessary grid frequency deviation, which eventually triggers load shedding. The authors of [22] demonstrated the effect of random FDIA directed at loads to trigger RoCoF relays. The impact of some limited predefined templates of FDIA, such as constant or random packet delays, have also been investigated in [23], [24].

Detection and mitigation of FDIAs on load-frequency control of power systems also have been widely investigated in the literature. An automatic generation control (AGC) targeted FDIA detection and defense mechanism is proposed in [25] based on the generative adversarial network. The forecasted area control error (ACE) is utilized in [26] to identify and mitigate FDIA on AGC. Reference [27] considers FDIAs as unknown inputs and uses the estimated value of FDIAs to compensate for the associated impacts on AGC. A control mechanism is presented in [28] based on a Kalman filter and artificial neural network to detect and mitigate the impact of FDIAs. However, the FDIA model considered in [17]–[28] are based on random attacks or limited pre-defined attack templates which might not be of interest of attackers in real word.

Despite [19], [21], [22], [25]–[28], there are other relevant FDIA works, though not in the context of generators dispatching process, developing optimal attack in their studies. A mechanism to find the optimal attack to cause transmission line outages is proposed in [29], [30]. However, the scope of these papers (to cause overload in transmission lines) is different from the scope of this work (attack on load-frequency control). In [31], the authors present a Laplace-domain optimization framework to investigate the vulnerability and impact of AC/HVDC load frequency control on FDIAs. The authors in [11] and [32] aim at finding the optimal attack within a minimum amount of time. However, these works consider multi-area interconnected power systems wherein all the generators within one area are replaced with a single equivalent generator

whiles focusing on tie-line sensor measurements compromise. In addition, [11] is missing the operation of generator RoCoF relays as well as load shedding under-frequency relays.

An intelligent FDIA may defeat the control center's defense mechanism as it ensures stealthiness [33], [34]. Launching a successful arbitrary FDIA could be possible, but to ensure stealthiness, the arbitrary attack takes a substantial amount of launch time to be successful [35], [36]. Such an attack might not be of interest to the attackers. However, an optimal false data injection attack (OFDIA), as proposed in this work, that minimizes the number of compromised measurements and launch time can leave a very short time for remedial actions to the control centers [37]. Therefore, control centers should consider possible OFDIA in the defense mechanism to ensure power grids' secure operations.

B. Contributions

The contributions of this paper are as follows:

- We propose time-domain formal modeling to find the OFDIA while minimizing the time for a successful attack. We use an optimizer to find the optimal size of the load attack while implementing a sequential process to find the minimum time for a successful attack. However, due to the non-convexity of the problem, the proposed method might not return the global optimal. Moreover, the optimization model is formulated based on weighted objective functions; thus, the approach is sensitive to the selection of the weight.
- Unlike most literature, focusing on compromising tie-line sensor measurements, our proposed formal modeling aims at compromising the load measurements across the power grid. In other words, most of the current papers focus on control areas, while we consider the FDIA on load measurements within those control areas. This scenario seems more realistic since the number of load meters in a power grid is way more than the number of tie-line sensor measurements. Therefore, it is more probable to have unsecured load meters than unsecured tie-line sensor measurements.
- Thereafter, leveraging the proposed formal modeling, we analyze and present a comprehensive study of the impact of power system parameters, such as the generator's inertia, the governor's droop and time constant, and the attacker's accessibility to loads on the possibility of a successful attack and the minimum required time.

The rest of the paper is organized as follows: the load-frequency model of power grids is given in section II. In section V, we present the test system and the case studies. In section VI, we discuss the result of simulations, and ultimately, we conclude our work in section VII.

II. Load-Frequency Model of Power Grids

Load-frequency dynamics of power grids can be modeled using the swing equation of generators, power grid model, actions of controllers (i.e., governors), and operations of relays (i.e., RoCoF and under-/over- frequency relays). Fig. 1 shows typical power grid components, controllers, and relays that determine frequency dynamics in power systems. In the actual operation of power grids, the inertia of synchronous generators and governor actions continuously impact the frequency dynamics (i.e., primary frequency response), and at a regular interval (e.g., 2-4 s), grid measurements are obtained (e.g., grid frequency, tie line flow), and generators updated dispatch signals are sent to dispatchable generators to maintain the frequency (i.e., secondary frequency control) [38].

A. Primary Frequency Response

In this section, we model the dynamic behavior of power systems in a time-domain optimization framework. To do so, we consider the differential equations of synchronous generators and governors along with DC power flow to model the changes in rotor angles. DC power flow returns the new values of rotor angles for any changes in power systems, such as load fluctuations, that help us in the evaluation of the system's frequency behavior. Thereafter, in order to model these continuous-format questions in an optimization environment, we discretize them using the Backward Euler method [39]. Power system dynamics are represented by non-linear differential-algebraic equations (DAE), which can't be solved analytically. Thus, the equations need to be discretized for solving using numerical methods. Moreover, the Backward Euler method yields a linear model of the dynamics after the discretization, and hence the model exhibits scalability compared to a non-linear discretized model. However, the focus of the paper is not on the computational gain due to discretization, we used off-the-shelf solvers available in Julia to solve the model.

The frequency behavior of a multi-machine power system can be expressed using the Swing equation as [38],

$$\dot{\delta}_i = \omega_i - \omega_o = \Delta\omega_i, \quad \forall i \in \mathcal{N}, \tag{1}$$

$$\dot{\omega}_i = \frac{1}{2\,H_i}\left(P_i^m - P_i^g - K_{D_i}\,\Delta\omega_i\right), \quad \forall i \in \mathcal{G}. \tag{2}$$

All the notations used in the mathematical formulation are provided in Section I. For brevity, we dropped the time index. Without loss of generality, the governor is represented as the TGOV1 model, which is a simplified representation of steam turbine governors as [40],

$$P_i^m = \frac{1}{T_i}\int\left(\frac{P_i^s - \Delta\omega_i}{R_i} - P_i^m\right), \quad \forall i \in \mathcal{O}. \tag{3}$$

With the classical representation of a synchronous generator, its terminal voltage angle can be approximated by the rotor angles, and using the DC power flow formulations, the power grid model becomes,

$$P_i^g - P_i^l = \sum_{j\in\mathcal{N}} B_{i,j}\,(\delta_i - \delta_j), \quad \forall i \in \mathcal{N}. \tag{4}$$

The dynamic model (1)-(4) determines the primary frequency response of power grids.

B. Secondary Frequency Control

For secondary frequency control, the control center may run the DC power flow (4) based on measurements (e.g., P^l, as shown in Fig. 1), and obtain steady-state reference set-points (dispatch signals) P^s as,

$$P_i^s = R_i\, P_i^g, \quad \forall i \in \mathcal{F}. \tag{5}$$

C. Operation of Frequency-based Relays

Generators are typically equipped with RoCoF and over-frequency relays, and the loads (at bulk level) are equipped with under-frequency (or load shedding) relays to keep the load/generation balance by disconnecting excess loads/generation in case of large-frequency oscillations outside the pre-defined range. Under/over-frequency relays are triggered based on frequency measurements ω, and RoCoF relays are triggered based on the average rate of change of frequency $\dot{\omega}^r$ at the relay locations.

III. False Data Injection Attack

The false data injection attack (FDIA) model is developed considering the dynamics of the power grid and actions of the control center in case of any compromise made on the load measurements, as shown in Fig. 2. Consider that $\widetilde{P}_i^l, \forall i \in \mathcal{A}$ denotes the magnitude of the injected false data into the load measurements. We use $(\widehat{\cdot})$ to represent parameters/measurements after FDIA. Therefore, the compromised load measurements that the control center uses to update the dispatch signals are $\widehat{P}_i^l = P_i^l + \widetilde{P}_i^l, \forall i \in \mathcal{A}$. The outcome of the control center running dispatching process routine based on compromised load measurements $\widehat{P^l}$ is the compromised reference set-points for the governors, i.e., $\widehat{P}_i^s, \forall i \in \mathcal{F}$. When these compromised reference set-points are sent to the governors, it causes load-generation imbalance leading to frequency dynamics that possibly result in frequency instability. Therefore, the control center unknowingly participates in the attacker's goal of attacking the load-frequency control in power grids.

We use the Backward Euler method to discretize the continuous form of the power system dynamic model and control center actions described in Section III as,

Load Measurement Attack:

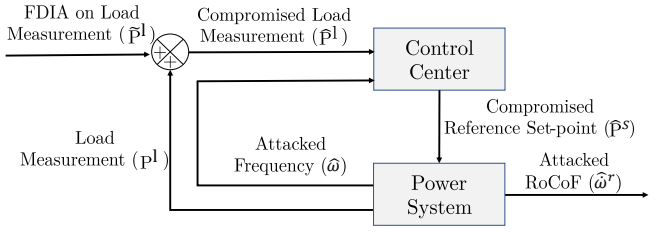


Fig. 2. A schematic of false data injection attack and its impacts on power grid's behavior.

$$\widetilde{P}_i^l[k] = \begin{cases} 0 & \forall i \notin \mathcal{A},\ \forall k \in \mathcal{T}, \\ \widetilde{P}_i^l[\,\mathcal{C}[z-1]\,] & \forall i \in \mathcal{A},\ \mathcal{C}[z-1] \le k < \mathcal{C}[z], \\ & \forall z \in \{2,3,...,C\}, \end{cases} \tag{6}$$

Power Grid Frequency Dynamics:

$$\widehat{\delta}_i[k+1] = \widehat{\delta}_i[k] + \Delta t\ \left(\widehat{\omega}_i[k+1] - \omega_o\right), \quad \forall i \in \mathcal{N}, \forall k \in \mathcal{T}, \tag{7}$$

$$\widehat{\omega}_i[k+1] = \widehat{\omega}_i[k] + \frac{\Delta t}{2H_i}\Big(\widehat{P}_i^m[k+1] - \widehat{P}_i^g[k+1] - K_{D_i}\left(\widehat{\omega}_i[k+1] - \omega_o\right)\Big), \quad \forall i \in \mathcal{G}, \forall k \in \mathcal{T}, \tag{8}$$

$$\widehat{P}_i^m[k+1] = \widehat{P}_i^m[k] - \frac{\Delta t}{T_i}\left(\widehat{P}_i^m[k+1] - \frac{\widehat{P}_i^s[k+1] - \left(\widehat{\omega}_i[k+1] - \omega_o\right)}{R_i}\right), \quad \forall i \in \mathcal{F}, \forall k \in \mathcal{T}, \tag{9}$$

$$P_i^g[k] - P_i^l[k] = \sum_{j \in \mathcal{N}} B_{i,j}\ \left(\widehat{\delta}_i[k] - \widehat{\delta}_j[k]\right), \quad \forall i \in \{\mathcal{O} - \mathcal{F}\}, \forall k \in \mathcal{T}, \tag{10}$$

$$\widehat{P}_i^g[k] - P_i^l[k] = \sum_{j \in \mathcal{N}} B_{i,j}\ \left(\widehat{\delta}_i[k] - \widehat{\delta}_j[k]\right), \quad \forall i \in \mathcal{F}, \forall k \in \mathcal{T}. \tag{11}$$

Control Center Actions:

$$\acute{P}_i^g[k] - (P_i^l[k] + \widetilde{P}_i^l[k]) = \sum_{j \in \mathcal{N}} B_{i,j}\ \left(\acute{\delta}_i[k] - \acute{\delta}_j[k]\right), \quad \forall i \in \mathcal{F}, \forall k \in \mathcal{C}, \tag{12}$$

$$P_i^s[k] = R_i\, \acute{P}_i^g[k], \quad \forall i \in \mathcal{F}, \forall k \in \mathcal{C}. \tag{13}$$

Equation (6) shows the load measurement attack where it is zero for measurements not included in accessible loads ($\mathcal{A}$) and remains constant within a dispatching cycle. Note that in (7)-(12), the grid dynamics are modeled based on actual loads and compromised set-points of governors obtained from the control center, which leads to compromised power system variables/parameters. In (13) and (14), the compromised dispatch signals are obtained based on the compromised load measurements. Note that in (13), $\widehat{P}^l = P^l + \widetilde{P}^l$ includes the amount of false data injection on the load measurements.

To model the operations of RoCoF relays, we compute $\dot{\omega}^r$ at relay location as following [41],

$$\dot{\omega}_i^r = \frac{1}{r\,\Delta t} \sum_{j=k-r}^{k-1} \big(\omega_i[k+1] - \omega_i[k]\big), \quad \forall i \in \mathcal{G} \tag{14}$$

Then, the FRO decision is made based on pre-defined thresholds for frequency and RoCoF as,

$$\text{FRO} = \begin{cases} 1 & \left(\widehat{\dot{\omega}}_i^r[k] \ge \tau^r\right) \vee \left(\widehat{\dot{\omega}}_i^r[k] \le -\tau^r\right), \quad \forall i \in \mathcal{G}, \\ 1 & \widehat{\omega}_i[k] \ge \overline{\tau}^f, \quad \forall i \in \mathcal{G}, \\ 1 & \widehat{\omega}_i[k] \le \underline{\tau}^f, \quad \forall i \in \mathcal{L}, \\ 0 & \text{otherwise.} \end{cases} \tag{15}$$

IV. Optimal False Data Injection Attack Model

In this section, we propose the OFDIA model, which optimizes the amount of the load attack in launching a RoCoF or frequency violations. The relay operation logics, as defined in (16) are non-smooth functions, which complicates the problem formulation as it requires integer variables to model. Using slack variables, we reformulate the OFDIA as follows, which makes the problem linear programming in nature; and, hence yields a tractable formulation. OFDIA optimizes the size of load attack, i.e., $\sum_{\substack{k\in\mathcal{C}\\ i\in\mathcal{A}}}(\widetilde{P}_i^l[k])^2$, subject to the constraints (7)-(16) for given dispatching cycle C.

OFDIA:

$$\textbf{Minimize}\quad \zeta\sum_{\substack{k\in\mathcal{C}\\ i\in\mathcal{A}}}(\widetilde{P}_i^l[k])^2+\eta\sum_{\substack{k\in\mathcal{T}\\ i\in\mathcal{L}}}\underline{\varepsilon}_i^f[k] + \sum_{\substack{k\in\mathcal{T}\\ i\in\mathcal{G}}}(\alpha\,\overline{\varepsilon}_i^r[k]+\beta\,\underline{\varepsilon}_i^r[k]+\gamma\,\overline{\varepsilon}_i^f[k]) \tag{17}$$

S. t.: Constraints $(7)-(15)$,

$$\widehat{\omega}_i^r[k]+\overline{\varepsilon}_i^r[k]\geq\tau^r,\quad \forall i\in\mathcal{G},\forall k\in\mathcal{T}, \tag{18}$$

$$\widehat{\omega}_i^r[k]-\underline{\varepsilon}_i^r[k]\leq-\tau^r,\quad \forall i\in\mathcal{G},\forall k\in\mathcal{T}, \tag{19}$$

$$\widehat{\omega}_i[k]+\overline{\varepsilon}_i^f[k]\geq\overline{\tau}^f,\quad \forall i\in\mathcal{G},\forall k\in\mathcal{T}, \tag{20}$$

$$\widehat{\omega}_i[k]-\underline{\varepsilon}_i^f[k]\leq\underline{\tau}^f,\quad \forall i\in\mathcal{L},\forall k\in\mathcal{T}, \tag{21}$$

$$\overline{\varepsilon}^r[k],\underline{\varepsilon}^r[k],\overline{\varepsilon}^f[k],\underline{\varepsilon}^f[k]\geq 0,\quad \forall k\in\mathcal{T}, \tag{22}$$

$$-\tau^l\,P_i^l\leq\widetilde{P}_i^l[k]\leq\tau^l\,P_i^l,\quad \forall i\in\mathcal{A},\forall k\in\mathcal{C}, \tag{23}$$

$$\underline{P}_i^g\leq P_i^g[k]\leq\overline{P}_i^g,\quad \forall i\in\mathcal{G},\forall k\in\mathcal{T}, \tag{24}$$

$$\underline{P}_i^g\leq\widehat{P}_i^g[k]\leq\overline{P}_i^g,\quad \forall i\in\mathcal{G},\forall k\in\mathcal{T}, \tag{25}$$

$$-\tau^g\,P_i^s[k]\leq\widehat{P}_i^s[k+1]-\widehat{P}_i^s[k]\leq\tau^g\,P_i^s[k],\quad \forall i\in\mathcal{F},\forall k\in\mathcal{C}, \tag{26}$$

where constraints (7)-(12) represent dynamic model of power grids, (13)-(14) represent action of control center, and (15) represents RoCoF calculation. Equations (18) and (19) implement the RoCoF relay operational logic as described in (16). Similarly, (20) and (21) model the operation of frequency relays defined in (16). Equation (22) ensures positive slack variables. In (23), we try to keep the load attack within $[-\tau^l,\tau^l]\%$ of the actual load at bus i. The main purpose of adding this constraint is to prevent OFDIA from attacking some of the load measurements only and leaving the rest unchanged. This might be mathematically possible and bring a minimum OFDIA value; however, this would not be a realistic attack scenario to have a large difference between subsequent time steps. The commonly employed bad data detection algorithms are the residue-based ones which deploy state estimate methods to find the operational state of the power system. When the residual exceeds the allowed range, the data is classified as bad data [42]. Conventionally, an attack is stealthy when the changes in (one or more) measurements keep the difference between the reported measurements and estimated measurements within a threshold value [43]. When this difference is zero, the stealthiness is at the best possible case. Therefore, in this paper, we consider an attack scenario in which the grid is fully visible. This means that there are enough measurements across the grid, and the control center does not need to perform any state estimation to obtain the visibility of the grid. Hence, any attack on the measurements by the attacker is directly transferred to the control center and affects the generators' dispatching process. Besides, we consider some thresholds in our attack modeling that help us to represent an attack with no observable changes. This ensures the stealthiness of the attack so that no bad data detection and FDIA detection algorithms detect the OFDIA. Equations (24)-(25) maintain the true and attacked values of the generator's active power within the permissible range, respectively. Equation (26) limits the generator power output changes in two subsequent dispatching cycles within the $[-\tau^g,\tau^g]\%$ of the generator's output power. α, β, η, ζ, and γ are weighting factors tuned so that each of the OFDIA components does not overweight the rest. This helps OFDIA to return the optimal attacks in the system regardless of their type (RoCoF/frequency). The objective function (17) optimizes the attack vector along with the slack variables to ensure the frequency/RoCoF is pushed towards the upper/lower threshold for relay operations. Note that, given the stealthiness constraint (23), generators' inertia, and time constant of equipment and controllers, the above model may not yield an optimal attack vector in one dispatching cycle; thus, the OFDIA models may need to be run for multiple dispatching cycles [37].

To run OFDIA in multiple dispatching cycles, we start the optimization with C = 1, run OFDIA, and check if there is a feasible attack that triggers FRO defined in (15). If so, the loop terminates, and the results are considered optimal. Otherwise, C is increased, and the process continues until we either find a successful attack or we reach $C=\overline{C}$ that indicates FRO is not feasible even in multiple dispatching cycles. The flowchart of this process is shown in Fig. 3. There is no limit on choosing the maximum number of dispatching cycles ($\overline{C}$). The proposed OFDIA in this paper can take any $\overline{C}$ and try to find the optimal attack within the desired time. However, if the $\overline{C}$ is not large enough, the solver might not be able to find a successful attack. Basically, the suitable $\overline{C}$ can vary for different power grids. For instance, if a power grid mostly contains generators with large inertia, the frequency in such a grid would take longer to oscillate. Therefore, a frequency/RoCoF attack takes a longer time to be successfully launched in such grids; that is, it requires a larger $\overline{C}$.

V. Numerical Studies

In this section, we present numerical case studies of our proposed FDIA model based on an IEEE test system. These studies are performed based on the attacker's accessibility to load measurements since the assumption of the attacker having access to all the load measurements across the power system is not realistic. Besides, when the attacker has access to all the loads, no matter how different the power system parameters are, the solver can find a feasible solution. Therefore, in our numerical studies, we consider that the attacker has limited access to a subset of loads (e.g., $x\%$ of all the loads). We will use $\mathcal{A}$ to denote this accessible set.

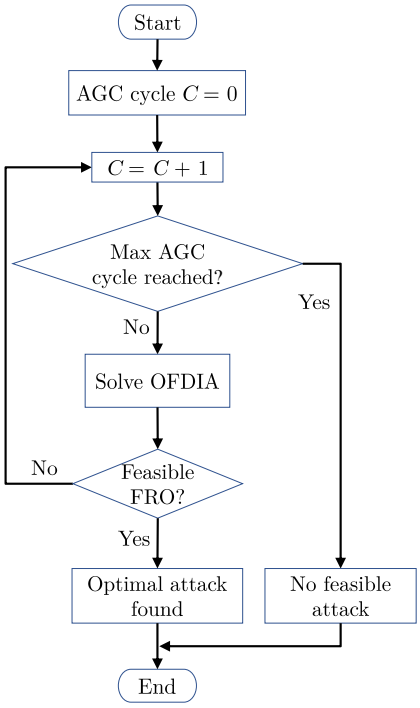


Fig. 3. Flowchart to run OFDIA in multiple dispatching cycles.

TABLE II
SYSTEM'S LOAD INFORMATION.

Bus	P^l (MW)	Q^l (MVAR)	Bus	P^l (MW)	Q^l (MVAR)
3	322.0	2.4	21	274.0	115.0
4	500.0	84.0	23	247.5	84.6
5	0	-200.0	24	308.6	-92.2
7	233.8	840.0	25	224.0	47.2
8	522.0	176.0	26	139.0	17.0
15	320.0	153.0	27	281.0	75.5
16	329.4	323.0	28	206.0	27.6
18	158.0	30.0	29	283.5	126.9
20	680.0	103.0	31	9.2	4.6
39	1104.0	250.0			

TABLE III
SIMULATION PARAMETERS.

Parameter	Value	Parameter	Value
f_o(Hz)	60	τ^l(%)	30.0
Δt(s)	1/60	τ^g(%)	40.0
t^c(s)	2	$\overline{\tau}^f$(Hz)	60.8
$\overline{C}$	30	$\underline{\tau}^f$(Hz)	59.2
r	12	τ^r(Hz/s)	1.5
S^b(MVA)	100	a	30.0

A. Test System

We consider the IEEE 39 bus system [38] shown in Fig. 4 as the case study to test the proposed formal attack model. This system has 10 synchronous generators where S_i = 1000MVA for $\forall i \in \mathcal{G}$. For simplicity, for all the generators, we consider K_D = 0. Moreover, we ignore the sub-transient reactances of the generators; therefore, the angle of bus voltages is equal to the generator rotor angles. All the generators are assumed to have over-frequency and RoCoF relays, and all the loads have under-frequency relays. The generators connected to buses 30 through 35 are considered to be equipped with governors participating in the frequency regulation in the dispatching process, i.e., $\mathcal{O} = \mathcal{F}$, and the remaining generators have a fixed mechanical input power. We assume that the actual values of the loads in the grid, i.e., P_i^l, $\forall i \in \mathcal{L}$, remain constant throughout the simulation (which is $\leq$ 60 s). However, our proposed formal model can capture the actual changes in loads along with the compromised measurements. The information on the loads and the simulation parameters used in the entire paper is given in Tables II and III, respectively.

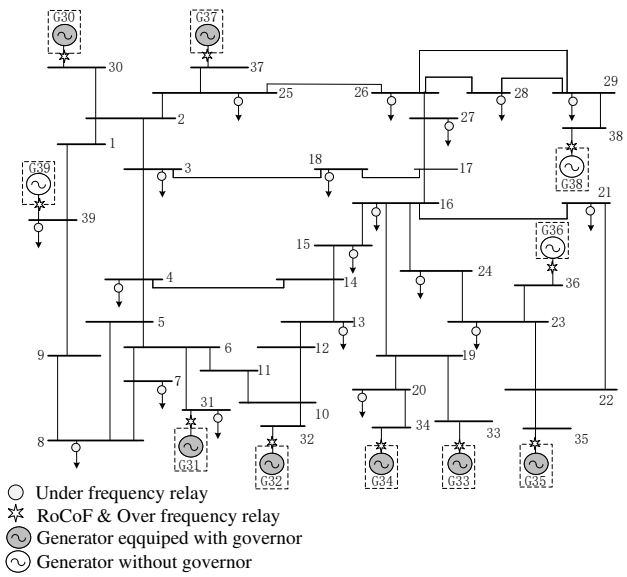


Fig. 4. IEEE 39 bus system.

The OFDIA is implemented in Julia for Mathematical Programming (JuMP), which is a domain-specific modeling language for mathematical optimization [44] and is solved using Gurobi [45].

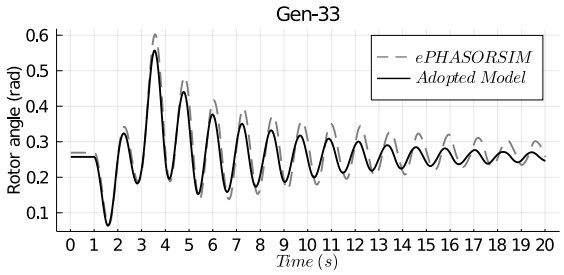
B. Model Validation

In this section, we aim to validate the modeling accuracy of the power system dynamics adopted in this paper. To this end, we need to make sure that the dynamic behavior of the test system is only due to the power system modeling represented in (7) through (15). Therefore, we put all the load measurement attack values in (17) equal to zero i. e., $\widetilde{P}_i^l[k] = 0, \quad \forall i \in \mathcal{A}, \forall k \in \mathcal{C}$, and disable constraints (18) through (26). Thereafter, we run (17) for a load disturbance of 500 MW (25 MW at each load bus). This disturbance is 8.13% of the total load 6,150 MW in the system which lasts for 2 s (from t = 1 s to t = 3 s). The generator and governor parameters used in this validation process are given in Table IV.

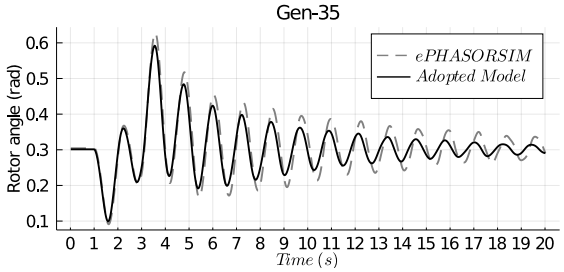
Due to space considerations, we only demonstrate the comparison of the frequency and rotor angle behavior of the generators at buses 33 and 35 obtained in Fig. 5. It can be

TABLE IV
GENERATOR AND GOVERNOR PARAMETERS IN MODEL VALIDATION AND OPTIMALITY VALIDATION STUDIES.

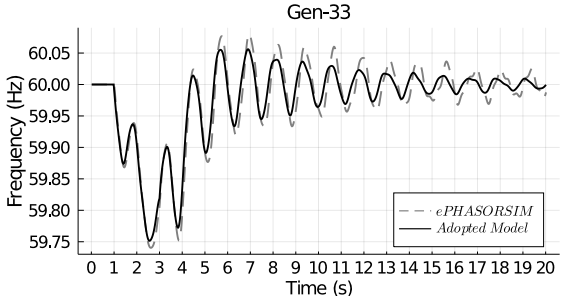
Bus No.	Generator	Governor	
	H(s)	R(p.u.)	T(s)
30	4.20	0.05	0.50
31	3.03	0.05	0.50
32	3.58	0.05	0.50
33	2.86	0.05	0.50
34	2.60	0.05	0.50
35	3.48	0.05	0.50
36	2.64	-	-
37	2.43	-	-
38	3.45	-	-
39	50.00	-	-



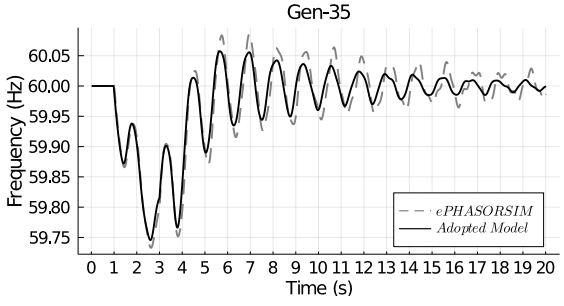
(a)



(b)



(c)



(d)

Fig. 5. Comparison of the adopted model accuracy and the developed test system in ePHASORSIM for rotor angle of a) generator 33, b) generator 35, and frequency behavior of c) generator 33, and d) generator 35.

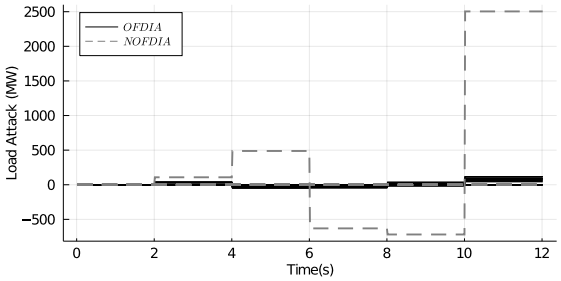
seen that the dynamic responses of the adopted model in this paper are sufficiently able to capture the actual dynamic of the test system developed in ePHASORSIM. Note that the adopted method utilizes the DC power flow to increase the scalability of the optimization model. This is while ePHASORSIM applies AC power flow in modeling the power systems' dynamics. The little-observed discrepancy in the results is due to the difference in utilized power flow methods.

C. Model optimality validation

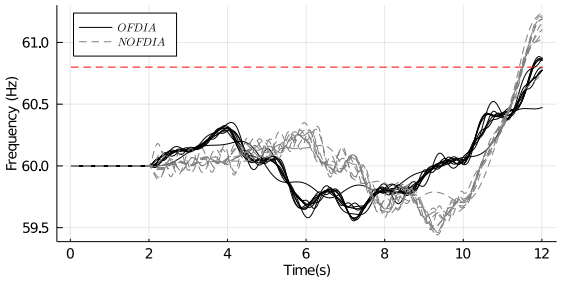
To demonstrate the optimality of the proposed OFDIA, we compare the results of a successful non-optimal FDIA (NOFDIA), which is a random feasible solution, and the proposed OFDIA on load measurements and show their impacts on the frequency behavior of the power system. The information of this study is given in Tables II, III, and IV.

Fig. 6(a) shows the load attack values on all of the load measurements in the test system. For the OFDIA, it can be seen that all the attack values have small magnitudes with small changes in two successive cycles. This is due to the stealthiness constraints (18) to (25) in (17), which keeps the amount of attack within a permissible range. However, from the figure, it's clear that at least one of the NOFDIA attack values has a very large amount with big changes between two successive cycles. Although such an attack can cause protection-relay operations in the power system, it is most likely to be detected by attack detection methods in the control center before causing any issues due to the unstealthy manipulations in measurements. Fig. 6(b) also shows the frequency behavior of the system for these two types of attacks. According to this figure, both OFDIA and NOFDIA can create an over frequency (f >61.8 Hz) in the system within the same timeframe (12 seconds). While the operation of even one of the protection relays in the system is considered a successful attack, the NOFDIA causes an over-frequency in all of the generators, which is due to the non-optimal injections in load measurements. Nevertheless, OFDIA causes only some of the generators to experience over-frequency, which manifests the optimality of the proposed OFDIA method.

We agree that the problem could be formulated as mixed integer linear programming (MILP) to include 'either ROCOF or frequency' related constraints in the problem formulation. The MILP type of model would not scale up for the larger system; hence, we combined the constraints through slack variables that avoid the use of integer variables. However, we have carried out an additional simulation that shows two scenarios: a) with only ROCOF-related constraints ((18)-(19)) b) frequency-related constraints ((20)-(21)), and presented the results in Fig. 7. Figure 7(a) demonstrates the amount of the launched attack on load measurements ($\widetilde{P}^l$) for optimal frequency-targeted (F-OFDIA) and RoCoF-targeted (R-OFDIA) attacks. Activation of different constraints (frequency or RoCoF) in OFDIA results in distinct $\widetilde{P}^l$s, which can be seen in this figure. Fig. 7(b) also demonstrates that the frequency oscillations in F-OFDIA cross the threshold (60.8 Hz) while these oscillations in R-OFDIA stay less than the threshold. This is because the primary focus of R-OFDIA is to find

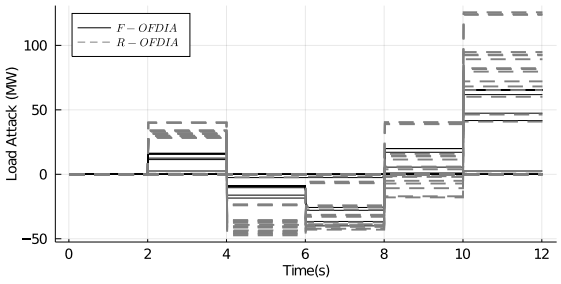


(a)

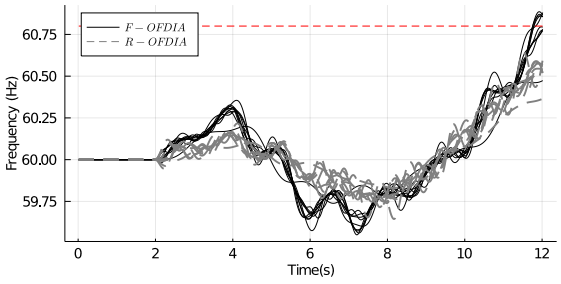


(b)

Fig. 6. Comparison of optimal attack (OFDIA) and non-optimal attack (NOFDIA) a) load measurement attacks b) frequency dynamic.



(a)



(b)

Fig. 7. Comparison of OFDIA with frequency constraints (F-OFDIA) only vs. ROCOF constraints (R-OFDIA) only.

optimal $\widetilde{P}^l$s to cause a RoCoF attack in the system regardless of frequency values and its behavior. A closer look at Fig. 6(b) and Fig. 7(b) shows that frequency oscillations of OFDIA and F-OFDIA are similar. This clarifies that regardless of frequency constraints and RoCoF constraints being activated at the same time or separately, the proposed OFDIA objective function returns optimal attack on load measurements with the possibility of constraint violation.

TABLE V
POWER SYSTEM PARAMETERS USED IN CASE STUDIES.

Case No.	H (s)	R (p.u.)	T (s)	x (%)	Accessible Loads	Accessible Loads Total Size (%)
C1	0.30	0.07	0.50	15.0	[3, 12, 24]	10.39
C2	1.80	0.07	0.50	15.0	[15, 16, 31]	10.71
C3	2.10	0.07	0.50	15.0	[3, 25, 39]	26.83

D. Case Studies

We study three different case studies to show the system's dynamic behavior once the attacker launches OFDIA on $\mathcal{A}$. The power system parameters of these case studies are shown in Table V. In all the case studies, the simulation starts at t = 0 s and stops at the end of each dispatching cycle. If OFDIA is not successful, then it runs for one more cycle. This process continues until a successful OFDIA or the maximum number of dispatching cycles $\overline{C}$ reaches. Table III shows the simulation parameters used in these case studies.

Figures 8, 9, and 10 show the dynamic behavior of $\widetilde{P}_i^l, i \in \mathcal{A}$, $\widehat{P}_i^s, i \in \mathcal{F}$, $\widehat{f}_i, i \in \mathcal{N}$, and $\dot{f}_i, i \in \mathcal{G}$ for the case studies where different attacks exist. The attack is launched at t = 2 s in all the case studies. Before applying the attack, we have $\widetilde{P}^l$ = 0 p.u., $\widehat{P}^s$ at the initial values, $\omega = \omega_o$ and $\dot{\omega}^r$ = 0 Hz/s. The values of $\widetilde{P}^l$ and $\widehat{P}^s$ remain constant within one dispatching cycle. Another attack, if needed, can be launched at the beginning of the following dispatching cycles. The control center receives the attacked load measurements from the power system and simultaneously sends $\widehat{P}^s$ to the governors. As it can be seen, these values create some fluctuations in the frequency (Figures 8(c), 9(c), 10(c)) that consequently makes $\dot{\omega}^r$ fluctuate as well (Figures 8(d), 9(d), 10(d)). Below, we discuss these behaviors in detail.

Case Study 1 (C1): In this case, we demonstrate the FDIAs on load measurements, as shown in Fig. 8(a), for which the system undergoes only RoCoF attack. As shown in Fig. 8(d), the RoCoF of all the generator buses crosses the threshold except one. This fact shows that the system with small inertia might experience sharp frequency fluctuations when subject to any load-generation imbalance, even though the frequency remains within the permissible range.

Case Study 2 (C2): In this scenario, due to the OFDIAs on load measurements depicted in Fig. 9(a), we observe only under-frequency attacks in the second case. Here, we change the value of H while the rest of the power system parameters remains the same as C1. It can be seen that an increase in H left no RoCoF attacks in this scenario. However, this increase introduces the under-frequency attack, in which one or more loads get disconnected from the grid.

Case Study 3 (C3): In the third case study, the system experiences both under-frequency and RoCoF attacks (Fig. 10) as it experiences the OFDIAs on load measurements shown in Fig. 10(a). One might expect not to have any RoCoF attack in C3 since we have the largest H compared to C1 and C2. However, the difference in the total accessible load percentage of C3 with C1 and C2 should be noticed. While the number of accessible loads is the same in all the case studies, in C3, we have access to the largest load of the system (bus 39). This

accessibility gives an attacker the opportunity to launch an FDIA on the system resulting in more variety of FRO. Hence, we can premise that securing the meters of large loads can make the system less vulnerable to FDIAs.

VI. Evaluation

In this section, we perform a comprehensive study of the impact of power system parameters on the vulnerability of power grids against FDIAs. In particular, we discuss the impact of power system parameters H, R, T, and x on t^a and P.

A. Methodology

Load distribution is usually variable across the power system. This makes a randomly chosen load set often not a good representative of the accessible loads. For example, let's consider a system with four load buses, and these buses have loads [1 2 80 100] MW. We want to select a set of two loads that are accessible to the attacker. It is obvious that if the chosen set includes [1 2] MW, t^a can be significantly different from the case we select [80 100] MW as the accessible loads. Larger accessible loads give the chance to the attacker to inject larger false data into the measurements without being detected by the bad data detection algorithms in the control center. Larger false data can cause faster fluctuations in the system leading to a faster FRO attack. Therefore, since we do not know anything about the load distribution across the power system, we consider a random sets of accessible loads for each value of x and run the algorithm to make sure the results of t^a are accurate. Thus, in order to increase the accuracy of the evaluation, in each case study, we randomly pick a = 30 different accessible load sets ($\mathcal{A}$) and consider t^a as the average time of successful attacks of these 30 random load sets. For instance, given the total number of loads which is 19 for the 39 bus test system, if x = 15%, 3 (19× 15% = 2.85 ≈ 3) of the loads are randomly selected as one accessible load set $\mathcal{A}$, and this process is repeated for 30 times to find 30 different accessible load sets. The distribution of the total accessible load normalized with the total load in the system is shown in Fig. 11 for different x.

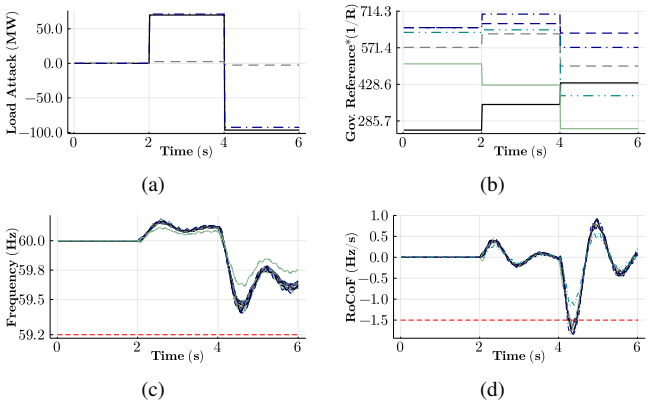


Fig. 8. Dynamic behavior of the system for case study C1 where only RoCoF attack occurs within C = 3 a) attack values on load measurements ($\widehat{P}^l$) b) changes in the governor reference set-points ($\widehat{P}^s$) c) frequency behavior d) RoCoF behavior.

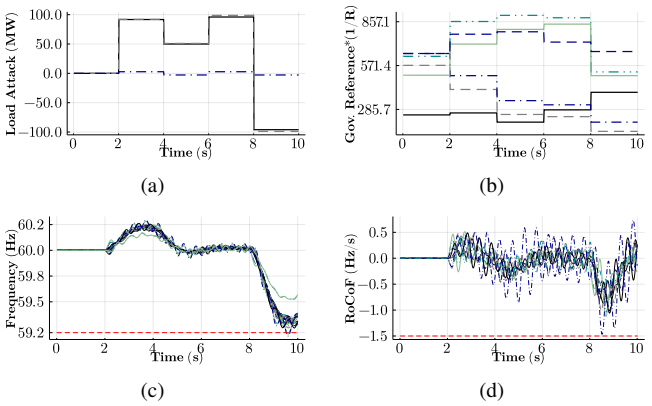


Fig. 9. Dynamic behavior of the system for case study C2 where only under-frequency attack occurs within C = 5 a) attack values on load measurements ($\widehat{P}^l$) b) changes in the governor reference set-points ($\widehat{P}^s$) c) frequency behavior d) RoCoF behavior.

To find t^a, we run the OFDIA shown in Fig. 3 for a times sequentially, each sequence for one of the accessible load sets. If there is any successful attack among all the sequences, t^a is considered as the average of the time for these successful attacks, and the simulation stops afterward. Otherwise, i.e., there is no successful attack among all the sequences, and no

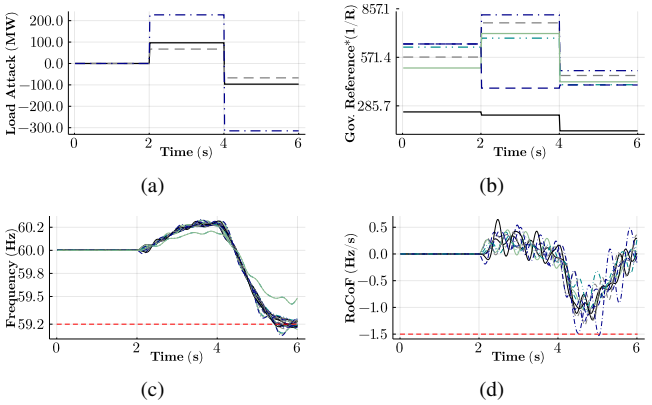


Fig. 10. Dynamic behavior of the system for case study C3 where RoCoF and under-frequency attacks happen within C = 3 a) attack values on load measurements ($\widehat{P}^l$) b) changes in the governor reference set-points ($\widehat{P}^s$) c) frequency behavior d) RoCoF behavior.

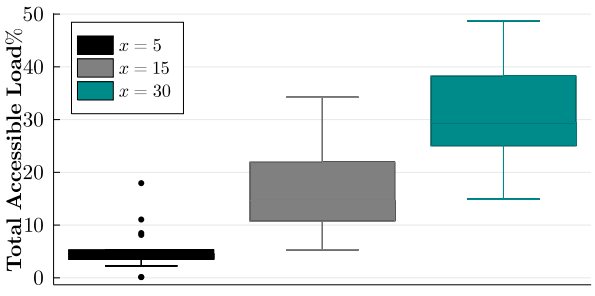


Fig. 11. Distribution of the total accessible load sets normalized with the total grid's load for different accessibilities (x) while a = 30.

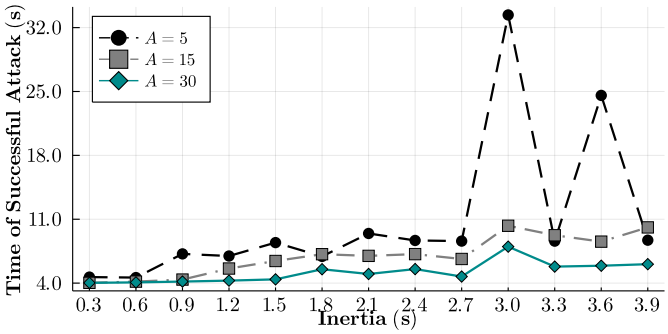


Fig. 12. Power grids inertia (H) vs. t^a for different accessibility (x).

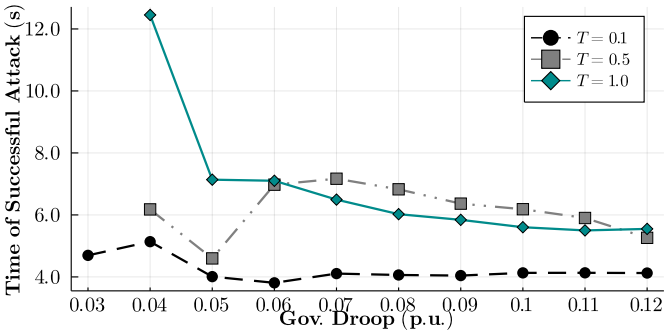


Fig. 14. Governor's droop (R) vs. t^a for different governor time constant (T).

value is considered for t^a.

B. Evaluation results

In this section, we discuss the simulation results of the presented methodology.

Impacts of power system parameters on average time minimally required for a successful attack: Fig. 12 shows the relation between H and t^a. By ignoring the two outlier points H = 3 s and 3.6 s, there can be seen an upward trend line between H and t^a for different values of x. Moreover, for all values of x, t^a is constant at the beginning, then starts rising in different values of H. These rising points are H = 0.6, 0.9, 1.5 s for x = 5, 15, 30%, respectively. It can be seen that the rising point increases when x increases.

Moreover, for a fixed value of H in Fig. 12, a decrease in x causes t^a to become larger. This clarifies that by decreasing the number of accessible loads to the attacker, launching a successful attack takes longer to take place.

The relation between t^a and R for different values of H is demonstrated in Fig. 13. There can be seen different start points for the curves in this figure. This is due to the fact that there is no successful attack for the values before the start points. For example, there is no successful attack when R = 0.03 p.u. and H = 0.3 s. Therefore, there is no point in the graph for this case. Besides, there are three points in this figure which are worth mentioning. The first point is that by increasing H, the start point shifts to the right, although not continuously. This can be interpreted as a decrease in P while H increases even though this is not always valid. The second point is that there is always a peak value for t^a on each of the curves. Although there is not a clear pattern when this peak shifts to the right and left, it always increases when H goes up. The third point is that in all the curves t^a starts declining after the peak value. To have a more frequency-stable power system against FDIAs, these points need to be considered when designing the governor parameters. Fig. 13 also shows an increase in t^a for an increase in power grids' inertia. This phenomenon has a direct relationship with the frequency robustness of power grids – the higher the generators' inertia, the more robust the frequency of power grids. This relationship specifies that in power grids with higher inertia, more time is needed for the attacker to achieve a frequency oscillation and RoCoF violating the allowed thresholds.

Fig. 14 presents the behavior of t^a versus R for different values of T. The first point observable in this figure is that all the curves start from $R \geq 0.03$ p.u. meaning that there is no successful attack while $R < 0.03$ p.u.. This suggests that for $R < 0.03$ p.u., the system is secure against FDIAs, regardless of how much T is. Another point is that there is a maximum value for t^a in each curve. For example, for T = 0.50 s this maximum t^a emerges at R = 0.07 p.u. while this happens at R = 0.04 p.u. for T = 1.00 s. However, there can not be seen any specific relation between these values and variation of R. Therefore, it is best to consider $R < 0.03$ p.u. to eliminate P in this test system. Otherwise, the maximum t^a needs to be explored for each value of T.

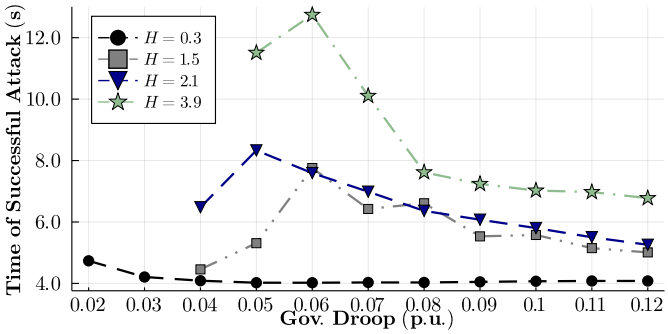


Fig. 13. Governor's droop (R) vs. t^a for different vales of inertia (H).

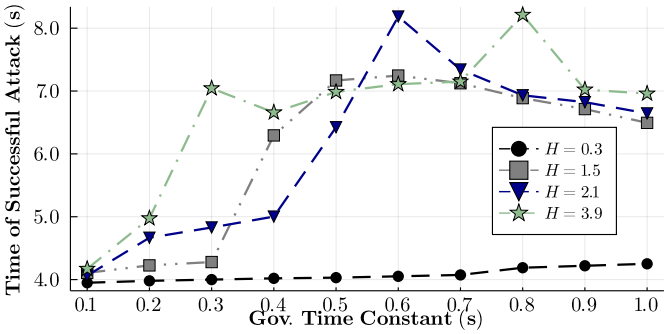


Fig. 15. Governor's time constant (T) vs. t^a inertia (H).

Fig. 15 represents the relation between t^a, T and H. At first glance, what can be seen from this figure is that when T increases, t^a also increases, although not continuously. This means that if studying the system behavior in detail for different values of T is not possible, then consideration of large values for T compared to small values has better results in securing the system against attacks. For instance, when H = 2.1 s, t^a has a greater value for T = 1 s than T = 0.1 s. However, another point seen in the figure is the existence of a peak value for t^a in the curves. For example, when H = 0.3 s, the peak arises at T = 1 s while for H = 1.8 s this occurs at T = 0.6 s. However, these peak values do not show a completely predictable pattern for variation of T. In other words, in order to make the system as secure as possible, the maximum value of t^a needs to be explored for the system.

Impacts of power system parameters on attack success possibility: As mentioned before, in each case study, we consider 30 different accessible load sets and implement the proposed formal modeling to find successful attacks. This is why some of these case studies do not return any successful attack. In this subsection, we discuss this attack success possibility (P) in Figures 16 and 17. The first point observable in Fig. 16 is that for a small value of inertia (H = 0.3 s), P = 100% in almost entire values of R. This fact clearly shows that systems with low inertia lead to frequency instability against FDIAs regardless of the value of R. Another significant observation is that there is an increase in R in all the curves, along with an increase in P. Moreover, for small values of R, there is no successful attack if H is large enough. This fact declares that small values of R are accompanied by a reduction of P and an enhancement of power systems' frequency stability against FDIAs.

Fig. 17 also confirms the results shown in Fig. 16. It can be seen that by increasing R, P grows as well. Moreover, it shows that growth in T can significantly reduce P while R is a small value ($<$ 0.07 s). For higher values of R ($\geq$ 0.07 s), the impact of T on P becomes insignificant as all the curves saturate to 100%.

C. Discussion

In this subsection, we propose some suggestions based on the findings from case studies and evaluation results as preventive measures to mitigate/eliminate the detrimental impacts of FDIA leading to FRO in power systems.

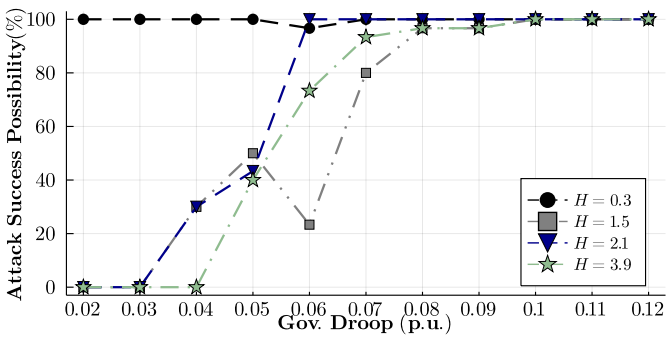


Fig. 16. Impact of governor's droop (R) on attack success possibility (P) for different H.

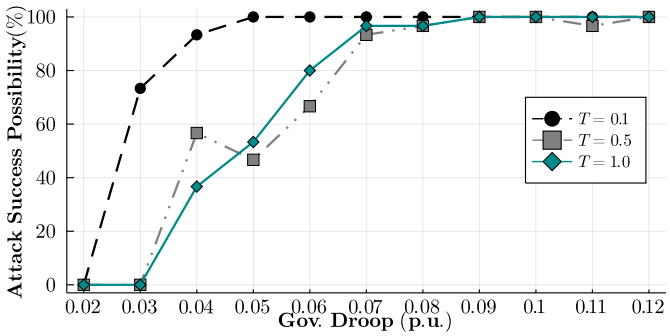


Fig. 17. Impact of governor's time constant (T) on attack success possibility (P) for different H.

Fig. 12 shows that although with an increment in the power system's inertia, there are some fluctuations in the average time of a successful attack; in general, a growing trend in successful attack time can be seen. This is due to the fact that for small values of inertia, the frequency fluctuates more easily so as a successful attack can be launched in a shorter time. Therefore, when the power system's inertia is low, for example, when the penetration of renewable energy resources is high in the system, lowering the number of accessible loads by securing more load meters has a direct impact on the increment of the minimum required time for a successful attack.

In Fig. 13, it can also be seen that the greater the inertia of the power system, the larger the time for a successful attack. As mentioned earlier, When the inertia is small in power systems, frequency tends to fluctuate more easily. This might lead to the triggering of RoCoF relays and the disconnection of the generators from the power system. Therefore, low inertia exposes the power system to more vulnerabilities against FDIAs and shortens the time required for a successful attack. Consideration of different set-points for RoCoF relays can help the power system not experience triggering of all the RoCoF relays at once time and a blackout ultimately. One of the cases in which the power systems' inertia becomes smaller is the integration of renewable energy resources. Renewable energy resources such as photovoltaic and wind turbines normally have zero or negligible inertia. Increasing the penetration of such resources into power systems requires fewer synchronous generators, which are the major source of inertia in power systems. This can significantly affect the frequency stability of power systems against FDIAs. Therefore, consideration of synchronous generators with larger inertia values can help the power systems' frequency stability enhancement against FDIAs. If such generators are not available or are not enough to enhance the power system's frequency stability, securing more load meters can be a doubled solution. Securing load meters reduces the attacker's accessibility to them and makes it take longer to compromise the measurements.

Another approach to improve the power system's stability, based on Fig. 14, is to consider small values of governor droop and large values of the governor's time constant. A power system equipped with such governors will encounter

an increment of time required for a successful attack or even an elimination of the attack success possibility. Figures 16 and 17 also suggest that an increase in the power system's inertia, as well as small values for governors' droop, can significantly lower the possibility of a successful attack in power systems.

VII. Conclusion

This paper targeted the analysis of an OFDIA on load-frequency control in power systems, focusing on the false operation of protection relays, including synchronous generator's over-frequency and RoCoF relays as well as under-frequency load shedding relays. We proposed a sequential optimization-based formal method to optimize the size of the attack leading to a FRO while minimizing the required average time. We implemented the proposed method on the IEEE 39 bus system and designed several case studies to demonstrate the behavior of the power system under FRO attacks. Thereafter, we ran an extensive number of simulations using the proposed method with multiple values of power system parameters such as inertia, governor's time constant, and droop to evaluate the impact of these parameters on the vulnerability of the power systems' frequency stability against FDIAs. Ultimately, we presented a discussion on how to increase the frequency stability of power grids against FRO attacks by choosing the appropriate values of these power system parameters. Our evaluation showed that matters such as increasing the penetration of renewable energy resources in power grids that results in decreasing the power system's inertia can make the power systems' frequency stability more vulnerable to FDIA. In contrast, a combination of large values of governor time constant and small values of droop can raise the required time for a successful attack, making the power systems' frequency more stable against attacks. This paper intends to evaluate the feasibility of FRO of frequency-based protection relays which can affect the power system's frequency security. To this end, we first proposed the OFDIA model to observe the feasibility of such attacks in one-area power grids, which mostly include load measurements. As future work, we would consider multi-area power grids with different sensors, including tie-line sensors.

References

[1] X. Yu and Y. Xue, "Smart grids: A cyber–physical systems perspective," *Proc. IEEE*, vol. 104, no. 5, pp. 1058–1070, 2016.

[2] A. Bose, "Smart transmission grid applications and their supporting infrastructure," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 11–19, 2010.

[3] X. Lu, X. Xiao, L. Xiao, C. Dai, M. Peng, and H. V. Poor, "Reinforcement learning-based microgrid energy trading with a reduced power plant schedule," *IEEE Internet of Things J.*, vol. 6, no. 6, pp. 10 728–10 737, 2019.

[4] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, 2017.

[5] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, 2016.

[6] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Preprints of the First Workshop on Secure Control Sys., CPSWEEK*, vol. 2010. Stockholm, Sweden, 2010.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. and Syst. Secur. (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[8] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *Proc. IECON 37th Annu. Conf. of the IEEE Ind. Electron. Soc.*, 2011, pp. 4490–4494.

[9] "Hackers infiltrated power grids," 2014. [Online]. Available: http://on.recode.net/1FpKP7Y

[10] U. DHS, "Insider threat to utilities," 2011. [Online]. Available: https://info.publicintelligence.net/DHS-InsiderThreat.pdf

[11] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics and Security*, vol. 12, no. 7, pp. 1609–1624, 2017.

[12] "Technical report on the events of 9 August 2019," Sep. 2019. [Online]. Available: https://www.nationalgrideso.com/document/152346/download

[13] P. M. Anderson and A. A. Fouad, *Power System Control and Stability*. John Wiley & Sons, 2008.

[14] M. Grebla, J. R. A. K. Yellajosula, and H. K. Høidalen, "Adaptive frequency estimation method for ROCOF islanding detection relay," *IEEE Trans. Power Delivery*, vol. 35, no. 4, pp. 1867–1875, 2020.

[15] Y. Tofis, S. Timotheou, and E. Kyriakides, "Minimal load shedding using the swing equation," *IEEE Trans. Power Syst.*, vol. 32, no. 3, 2017.

[16] M. Jafari, M. H. Shahriar, M. A. Rahman, and S. Paudyal, "False relay operation attacks in power systems with high renewables," in *Proc. IEEE Power Energy Soc. General Meeting*, 2021, pp. 01–05.

[17] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014.

[18] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *Proc. IEEE Power Energy Soc. General Meeting*. IEEE, 2010, pp. 1–6.

[19] A. Ashok, P. Wang, M. Brown, and M. Govindarasu, "Experimental evaluation of cyber attacks on automatic generation control using a CPS security testbed," in *Proc. IEEE Power Energy Soc. General Meeting*, 2015, pp. 1–5.

[20] H. E. Brown and C. L. DeMarco, "Risk of cyber-physical attack via load with emulated inertia control," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5854–5866, 2017.

[21] J. Chen, G. Liang, Z. Cai, C. Hu, Y. Xu, F. Luo, and J. Zhao, "Impact analysis of false data injection attacks on power system static security assessment," *J. of Modern Power Sys. and Clean Energy*, vol. 4, no. 3, pp. 496–505, 2016.

[22] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, "Resonance attacks on load frequency control of smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4490–4502, 2018.

[23] S. Bhowmik, K. Tomsovic, and A. Bose, "Communication models for third party load frequency control," *IEEE Trans. Power Syst.*, vol. 19, no. 1, pp. 543–548, 2004.

[24] K. Tomsovic, D. E. Bakken, V. Venkatasubramanian, and A. Bose, "Designing the next generation of real-time control, communication, and computations for large power systems," *Proc. IEEE*, vol. 93, no. 5, pp. 965–979, 2005.

[25] Y. Li, R. Huang, and L. Ma, "False data injection attack and defense method on load frequency control," *IEEE Internet of Things J.*, vol. 8, no. 4, pp. 2910–2919, 2021.

[26] S. d. Roy and S. Debbarma, "Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid," *IEEE Sys. J.*, vol. 14, no. 2, pp. 2023–2031, 2020.

[27] M. Khalaf, A. Youssef, and E. El-Saadany, "Joint detection and mitigation of false data injection attacks in AGC systems," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4985–4995, 2019.

[28] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad, K. K. Yen, and A. I. Sarwat, "Resilient control design for load frequency control system under false data injection attacks," *IEEE Trans. Ind. Electron.*, vol. 67, no. 9, pp. 7951–7962, 2020.

[29] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 1513–1523, 2018.

[30] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, 2015.

[31] K. Pan, E. Rakhshani, and P. Palensky, "False data injection attacks on hybrid AC/HVDC interconnected systems with virtual inertia—vulnerability, impact and detection," *IEEE Access*, vol. 8, pp. 141 932–141 945, 2020.

[32] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, "Attack detection and identification for automatic generation control systems," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4760–4774, 2018.

[33] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Trans. Industrial Informatics*, vol. 14, no. 5, pp. 1932–1941, 2017.
[34] M. A. Rahman, E. Al-Shaer, and R. G. Kavasseri, "A formal model for verifying the impact of stealthy attacks on optimal power flow in power grids," in *Proc. ACM/IEEE Int. Conf. on Cyber-Phys. Sys. (ICCPS)*, 2014, pp. 175–186.
[35] M. Jafari, M. A. Rahman, and S. Paudyal, "False data injection attack against power system small-signal stability," in *Proc. IEEE Power Energy Soc. General Meeting*, 2021, pp. 1–5.
[36] S. Prasad, "Counteractive control against cyber-attack uncertainties on frequency regulation in the power system," *IET Cyber-Phys. Sys.: Theory & Applications*, vol. 5, no. 4, pp. 394–408, 2020.
[37] R. Tan, H. H. Nguyen, E. Y. Foo, X. Dong, D. K. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Optimal false data injection attack against automatic generation control in power grids," in *Proc. ACM/IEEE 7th Int. Conf. on Cyber-Phys. Sys. (ICCPS)*, 2016, pp. 1–10.
[38] P. Kundur, *Power System Stability*. CRC Press New York, NY, USA, 2007, vol. 10.
[39] B. P. Zeigler, A. Muzy, and E. Kofman, *Theory of Modeling and Simulation: Discrete Event & Iterative Sys. Computational Foundations*. Academic press, 2018.
[40] I. C. Report, "Dynamic models for steam and hydro turbines in power system studies," *IEEE Trans. Power App. and Sys.*, vol. PAS-92, no. 6, pp. 1904–1915, 1973.
[41] M. R. Alam, M. T. A. Begum, and K. M. Muttaqi, "Assessing the performance of ROCOF relay for anti-islanding protection of distributed generation under subcritical region of power imbalance," *IEEE Trans. Industry Applications*, vol. 55, no. 5, pp. 5395–5405, 2019.
[42] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2016.
[43] M. A. Rahman, E. Al-Shaer, and R. G. Kavasseri, "Security threat analytics and countermeasure synthesis for power system state estimation," in *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pp. 156–167.
[44] I. Dunning, J. Huchette, and M. Lubin, "JuMP: A modeling language for mathematical optimization," *SIAM Review*, vol. 59, no. 2, 2017.
[45] Gurobi Optimization, LLC, "Gurobi optimizer reference manual," 2022. [Online]. Available: https://www.gurobi.com

Mohamadsaleh Jafari (M'18) received his B.E. degree from Shahrood University of Technology, Iran, in 2010, and his M.Sc. degree from the Amirkabir University of Technology, Iran, in 2013 in Electrical Engineering. He obtained his second M.Sc. and a Ph.D. degree in Electrical Engineering from Florida International University, Miami, FL, USA, in 2020 and 2021, respectively. Jafari recently joined California Independent System Operator (CAISO) as an Operations Engineer. His research interests include power grid modeling, dynamic studies, renewable energy, optimization, and cyber security in power systems.

Mohammad Ashiqur Rahman (M'11, SM'21) is an Associate Professor in the Department of Electrical and Computer Engineering at Florida International University, USA. Earlier, he was an Assistant Professor in the Department of Computer Science at Tennessee Tech University. He obtained a Ph.D. degree in computing and information systems from the University of North Carolina at Charlotte in 2015. Rahman's research covers a wide area of computer networks, including computer and information security in both cyber and cyber-physical systems. His research interest includes formal security analysis, risk assessment and security hardening, secure and dependable resource management, and distributed computing.

Sumit Paudyal (M'12, SM'23) received the B.E. degree from Tribhuvan University, Nepal, in 2003, the M.Sc. degree from the University of Saskatchewan, Saskatoon, Canada, in 2008, and the Ph.D. degree from the University of Waterloo, Waterloo, Canada, in 2012, all in electrical engineering. He was a faculty member at Michigan Technological University, Houghton, MI, USA, from 2012 to 2019. Since 2019, he has been an Associate Professor in the Department of Electrical and Computer Engineering at Florida International University, Miami, FL, USA. His research interests include distribution grid modeling, dynamic studies, and optimization techniques in power systems.