Optimal False Data Injection Attacks Against Power System Frequency Stability

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

***Abstract*—The automatic generation control (AGC) is one of the core control systems in power grids that regulate frequency within the permissible range. However, its dependence on communication makes it highly vulnerable to cyber-attacks. An arbitrary false data injection attack (FDIA) on AGC frequency and tie-line flow measurements will likely be detectable by bad data detection methods; however, if an attack can be launched optimally, it often becomes stealthy. In this regard, we develop a framework of optimal FDIAs (OFDIAs) to demonstrate the feasibility of such attacks in the power system frequency control loop. We propose a linearized formulation of discretized power systems' dynamics in an optimization framework to model OFDIAs that compromise the AGC system by corrupting tie-line flow and generators' frequency measurements. Using the proposed formal modeling, we study the effects of two types of FDIAs, continuous and time-limited, on the frequency behavior in power grids. The results demonstrate that continuous OFDIAs can lead to severe consequences on a power grid's performance, such as frequency instability. In contrast, the time-limited FDIAs can cause the frequency to fluctuate beyond the acceptable range, which may lead to the triggering of the frequency-based protection relays.**

***Index Terms*—False data injection attack, automatic generation control, frequency stability, dynamic modeling, optimization.**

I. Nomenclature

Sets and Indices

$(\tilde{\cdot})$	Attack value.
$\dfrac{d(.)}{dt}$	Rate of change of a parameter.
$\mathcal{A}$	Set of generators participating in AGC.
$\mathcal{A}_z$	Set of generators of area z participating in AGC.
$\mathcal{B}$	Set of areas of the power system.
i,j,z	Indices.
k	Discrete step.
$\mathcal{C}$	Set of discrete steps of AGC cycles $\{\frac{W}{h},\frac{2W}{h},...,\frac{CW}{h}\}$.
$\mathcal{G}$	Set of generators.
$\mathcal{L}_z$	Set of tie-lines connected to area z.
$\mathcal{N}$	Set of buses.
$\mathcal{O}$	Set of generators equipped with the governor.
$\mathcal{T}$	Set of discrete steps in the optimization horizon $\{1,2,...,\frac{CW}{h}\}$.

Parameters and Variables

α	Weighting factors.
δ	Generator's rotor angle.
ω	Angular frequency.
ω_o	Nominal angular frequency.
ε^{ω}	The slack term for frequency attack.
$\overline{\varepsilon}^f$	Slack term for over-frequency.
ε^{tie}	Slack term for attack on tie-lines' power flow deviations.
$\Delta\omega$	Angular frequency deviation.
τ^{ω}	Bad data detection threshold for frequency changes in two successive discrete steps.
τ^{a}	Bad data detection threshold for ACE changes in two successive discrete steps.
$\overline{\tau}^f$	Over-frequency threshold.
τ^{tie}	Bad data detection threshold for tie-line power deviations from the scheduled values in two successive discrete steps.
ΔP^{tie}	Tie-line power flow deviation from the scheduled value.
h	Discretization time-step size.
ACE	Area control error of individual generator.
$\overline{ACE}$	Upper limit of individual generator area control error.
$\underline{ACE}$	Lower limit of individual generator area control error.
$B_{i,j}$	Imaginary part of line admittance between bus i and bus j.
C	AGC cycles.
f_o	Nominal frequency.
H	Inertia constant of synchronous generator.
K^D	Load damping factor.
K^I	Integral gain of AGC controller.
n	Number of discretized steps in modeling.
P^g	Generator's active power output.
$\overline{P}^g$	The upper limit of generator active power.
$\underline{P}^g$	Lower limit of generator active power.
P^m	Mechanical input power of generator.
$\overline{P}^m$	The upper limit of generator mechanical power.
$\underline{P}^m$	Lower limit of generator mechanical power.
P^r	Governor's reference set-point.
P^s	Governor's steady-state reference set-point.
R	Governors' speed droop.
S^b	Base apparent power in MVA.
T	Governors' time constant.
W	Time interval between two successive AGC cycles.

II. Introduction

SMART grids are increasingly employing measurement and communication technologies that bring several benefits to

This work is supported in part by National Science Foundation grant ECCS 2001732, CNS 1929183, and FIU Graduate School Dissertation Year Fellowship (DYF). Authors are with Florida International University, Miami, FL, USA. Emails: mjafa006@fiu.edu, marahman@fiu.edu, spaudyal@fiu.edu.

the system operations [1]. However, this technology enrichment opens up new challenges, such as cyber-attacks, which make the power grids vulnerable. Among various types of cyber-attacks, false data injection attacks (FDIAs) have been widely examined for power systems [2] due to real-world FDIA incidents. One of such attacks is FDIA on distribution grids in Ukraine in 2015 which left around 200 thousand customers with no electricity for several hours [3]. Apart from that, there have been some real attack incidents in recent years such as the Stuxnet [4] and Dragonfly [5] that needed strong knowledgeable attackers who have access to the real-time data in the control centers to be successful. Injecting false control signals, the Stuxnet worm attacked nuclear centrifuges and manipulated the system states. Although these attacks did not target power systems, such attacks with such a level of access to data can be easily launched on power systems as well. Generally speaking, there is evidence manifesting that the danger of insider attackers is serious [3]. Besides, some of the existing literature such as [6] showed that it is possible for the adversaries to stealthily learn the impact of the attack, based on sensor data and some of the power system constants that are either publicly available or can be achieved, for instance, via social engineering against employees in the control center of the grid. Therefore, we aimed at studying FDIAs while the attacker has full knowledge of the victim's power system.

An FDIA in power grids entails manipulating the data (measurements or control signals) transmitted between the control center and the field devices or distributed controllers. Here, an attacker infuses some wrong data into measurements/control signals to mislead the control center/distributed controllers' actions [7]. It is crucial to ensure that the received measurements/control signals are sound and accurate. Hence, some bad data detection algorithms are considered in control centers to classify the received data as normal or outlier [8]. The traditional bad data detection algorithms work based on the residuals between estimated and observed measurements. When the residual is not within the permissible range, the data is categorized as bad data [9]. A stealthy FDIA can bypass the control center's bad data detection process and mislead the operator to take a wrong control action, compromising the operation of the smart grids [10], [11].

The grid frequency in power systems needs to be continuously monitored and maintained. Any major fluctuations of the frequency need to be corrected in order to keep it within the permissible range (e.g., between 59.3 and 60 Hz.); otherwise, it can lead to serious consequences including blackouts. For example, there was a blackout in England and Wales in 2019 caused by a frequency decline that left about one million people with no electricity [12]. The primary frequency response in power systems, which includes automatic decentralized control action of the active power output of generators, immediately determines the grid frequency following any disturbances in power systems. However, it is the automatic generation control (AGC) system that maintains the frequency around the nominal value, although in a slower time scale in comparison to the primary frequency response.

Following any frequency oscillations in a power system, AGC adjusts the reference set-points of the governors equipped on the generators (communicating the control signal from the control center) to bring the frequency back within the permissible range. Therefore, AGC is dependent on the communication and measurements where FDIAs may affect the frequency stability of power systems [13]. As an example of how FDIA on AGC can impact the power systems' performance, let's assume an attacker injecting false data into tie-lines active power frequency measurements to mislead the control center of a generation shortage. These faulty measurements make the control center incorrectly estimate the area control error (ACE) and update the governors' reference setpoints. ACE is the criteria used to update governors' reference setpoints. Any non-zero ACE represents a load-generation imbalance in the area that needs to be addressed by updating the governors' setpoints within the control area. According to the new adjustment, the governor changes the mechanical input power of the generators, and consequently, the load-generation balance is not maintained. This imbalance causes fluctuations in the power system's frequency dynamics, which might lead to frequency instability.

The impact of FDIAs on AGC has been studied by various researchers [14]–[16], considering different types of attacks, such as random noises, signal scaling, surges, and ramps. In a similar study [17], the impacts of some predefined templates of FDIAs (such as constant and random packet delays) are investigated. In [18], the authors confirm that FDIAs may lead to grid frequency deviations which can eventually trigger load shedding relays. Similarly, impacts of FDIAs on rate-of-change-of-frequency (RoCoF) relays are studied in [19]. FDIAs on local controllers of inertia-emulating loads and their impacts on power systems' frequency are evaluated in [20]. It is shown that the resulting oscillations in the system due to the instability might cause the RoCoF relays to operate and disconnect some of the generators from the grid. Despite the abovementioned papers that only consider a single attack model, [21] investigates a coordinated combination of FDIAs on AGC. However, the FDIA model considered in these works [14]–[21] are based on arbitrary or preset attack values. An arbitrary FDIA can be successful, however, due to its low probability, it will take a substantial amount of time to satisfy the stealthiness criteria [22], [23]; thus, such attacks are impractical in the real world.

Optimal FDIAs (OFDIAs), although not focused on AGC, have also been explored in literature as they, if stealthy, can defeat the control center's defense mechanism [24], [25]. The authors of [26], [27] assess OFDIAs which leads to transmission line outages. In [28], the authors present an optimization framework to investigate the vulnerability and impact of FDIAs on AC/HVDC (high-voltage DC) load frequency control. The authors in [29] target studying a hybrid stealthy attack on AGC as an optimization problem to disrupt the normal operation of AGC. However, this work intends to find the optimal multiplier in launching a combination of two types of pre-selected attacks, under- and negative- compensation, through an optimization process. Restricting the optimization method to some pre-selected types of attacks might lead to an inaccurately-designed optimization problem that can impact the optimal output results. Similarly, the authors of [6] model an optimal attack consisting of a series of FDIAs on AGC within a short time. Although there is some similarity between the focus of this paper and our current work, there are two major differences including the utilized method in power system modeling whereas this paper uses Laplace-domain modeling of power system and applies a multi-step sequential for loop in finding the optimal attack. This simplification and application of sequential algorithms reduce the accuracy of the proposed OFDIA.

To overcome the problems discussed earlier, this paper makes contributions as follows:

- Pre-selected attacks have been widely used in the literature [14]–[21]. However, in this paper, we propose a linear and scalable optimization-based formal modeling to find the OFDIA while minimizing the magnitude of the attack on the frequency of generators participating in AGC and the tie-lines active power deviation. To simulate the worst-case scenario, we assume that the attacker has access to all (not a limited number) tie-lines' measurements. This assumption makes the attack even more stealthy as the attacker does not need to compromise a limited set of measurements with a larger magnitude of manipulation.
- Unlike most papers in the literature that uses a Laplace-domain model of power systems and simplifies a multi-machine area with a single-machine area in the state-space format ([6], [21]), this work presents the detailed time-domain dynamic of multi-machine multi-area power systems. This makes the study of the impact of the obtained attacks more accurate and closer to the real world.
- Thereafter, leveraging the proposed formal modeling, we analyze and present a comprehensive study of the impact of OFDIA on the dynamic behavior of the IEEE 39-bus system for different scenarios of the attacker's time-flexibility in launching the attack.

The rest of this paper is organized as follows. In Section III, we present background on the frequency control in power systems. In Section IV, we discuss preliminaries needed to model FDIAs on grid measurements. In Section V, we propose the formal model of OFDIA on the frequency stability of power systems. The numerical studies are presented and discussed in Section VI. Some comments are given in Section VII on detection and mitigation methods. Ultimately, we conclude the paper in Section VIII.

III. Frequency Control in Power Grids

The frequency control in power systems is based on maintaining the load-generation balance. If a power imbalance is not corrected in a timely manner, it might trigger protection relays (e.g., over/under-frequency) to operate or may lead to worse consequences including instability of the power grids. To prevent such adverse impacts, there are two major frequency control actions in power systems. i.e., the primary frequency control and the secondary frequency control (also called AGC) [30]. Fig. 1 shows the load-frequency control in a typical 2-area power system including synchronous generators, governors, measurement devices, and frequency-based protection relays. These two areas are connected together through a tie-line. As shown in Fig. 1, the frequency deviation of synchronous generators is fed back to governors that perform the primary frequency control. In case of any frequency deviations, the speed-droop characteristic of governors adjusts the output power of synchronous generators [31] to ensure load-generation balance. Though the primary frequency control ensures power balance and steady frequency, it can lead to frequency deviation from the nominal value. On secondary frequency control, the frequency measurements along with tie-lines power flows are used by the control center in the AGC process. The control center calculates the ACE signals at a regular interval (e.g., 2-4 s) and sends them to selected governors in each area to adjust their reference set-points dynamically [32]. As a result, the frequency in each area and the power flow in tie-lines remain at their scheduled values.

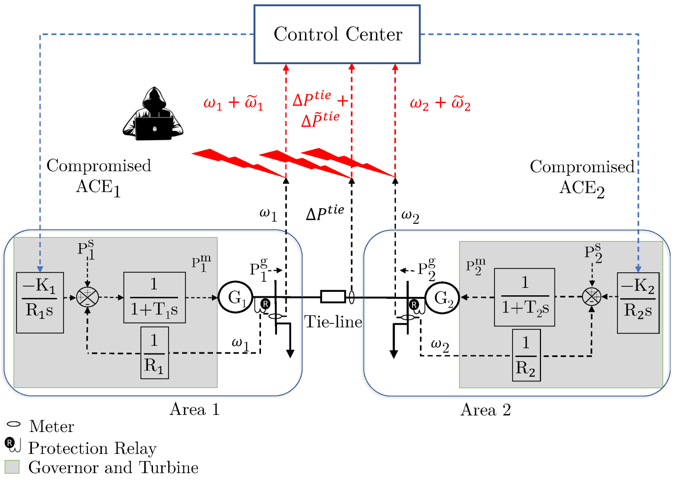


Fig. 1. Load-frequency control in a typical 2-area power system in presence of FDIA on the frequency of AGC generators and tie-lines' power deviation.

A. Primary Frequency Response

The frequency behavior of multi-machine power system can be expressed using the Swing equation as [30],

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

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

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 [33],

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

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

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

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

B. Area Control

AGC is a secondary control system to adjust the governors' reference set-points in order to maintain the frequency at the nominal value as well as keep the power exchange of each area at its scheduled value. Based on the measured values of the grid frequency deviation and the power exchange divination from their nominal values, as shown in Fig. 1, ACE signal for each generator is derived as follows [16],

$$ACE_i = \beta_i \Delta\omega_i + \sum_{j \in \mathcal{A}_z} \Delta P^{tie}_j, \quad \forall z \in \mathcal{B}, \forall i \in \mathcal{A}_z, \tag{5}$$

$$\beta_i = \frac{1}{R_i} + K^D_i, \;\; \forall z \in \mathcal{B}, \, \forall i \in \mathcal{A}_z, \tag{6}$$

The control center may run the DC power flow (4) based on measurements and obtain steady-state reference set-points as,

$$P^s_i = P^g_i, \quad \forall i \in \mathcal{O}. \tag{7}$$

Therefore, the total reference set-point of the governor's can be written as,

$$P^r_i = P^s_i - \int K^I_i ACE_i, \quad \forall i \in \mathcal{A}, \tag{8}$$

IV. Preliminaries

FDIA model is developed considering the dynamics of the power grid and actions of the control center in case of any compromised measurements as shown in Fig. 1. Consider that $\Delta\widetilde{P}^{tie}_i, \forall z \in \mathcal{B}, \forall i \in \mathcal{A}_z$, and $\widetilde{\omega}_i, \forall i \in \mathcal{A}$ denote the magnitude of the injected false data into the tie-lines' power deviation and AGC-participating buses frequency measurements, respectively. The compromised measurements utilized by the control center in generation of ACEs are $\Delta P^{tie}_i + \Delta\widetilde{P}^{tie}_i, \forall z \in \mathcal{B}, \forall i \in \mathcal{A}_z$, and $\omega_i + \widetilde{\omega}_i, \forall i \in \mathcal{A}$. Therefore, the outcome of the AGC algorithm, which is calculated based on compromised measurements, is compromised ACEs for the governors. When these compromised ACEs are sent to the governors, a load-generation imbalance will take place in the system that leads to frequency violation or even instability. Hence, the control center unknowingly participates in the attacker's plan to launch an attack on the load-frequency control in power grids.

A. Attack on Measurements

In order to launch the attack, we assume that the attacker targets two set of measurements, i.e., frequency of generators participating in AGC and the tie-lines' active power deviation from the scheduled value. These attack on these measurements can be modeled as following,

$$\omega_i[k] = \begin{cases} 0 & \forall\, i \notin \mathcal{A}, \forall\, k \in \mathcal{T}, \\ \widetilde{\omega}_i[k] & \forall\, i \in \mathcal{A}, \forall\, k \in \mathcal{T}, \end{cases} \tag{9}$$

$$\Delta P^{tie}_i[k] = \begin{cases} 0 & \forall\, i \notin \mathcal{A}, \forall\, k \in \mathcal{T}, \\ \Delta\widetilde{P}^{tie}_i[k] & \forall\, z \in \mathcal{B}, \forall\, i \in \mathcal{A}_z, \\ & \forall\, k \in \mathcal{T}, \end{cases} \tag{10}$$

B. Discretized Power Grid Frequency Dynamics

In this paper, we would like to model the dynamic behavior of power systems in an optimization framework. To model this dynamic behavior, we consider the continuous format of equations that represent the major components (synchronous generators and governors) of power systems in the dynamic analysis of power systems. In order to be able to observe the changes in synchronous generators' rotor angles and assess the frequency stability of power systems, we used the DC power flow that gives us the new values of rotor angles for any changes in power systems such as generators' active power output or the loads. However, all of the equations discussed in Section III are in a continuous format, which is not implementable in the optimization framework. To overcome this issue, we discretize these equations using the Backward Euler method [34] so that we can utilize them in the optimization framework. The discretized version of the continuous dynamic model can be modeled as,

$$ACE_i[k] = (\frac{1}{R_i} + K^D_i)(\Delta\omega_i[k] + \Delta\widetilde{\omega}_i[k]) + \tag{11}$$

$$\sum_{j \in \mathcal{A}_z} (\Delta P^{tie}_j + \Delta\widetilde{P}^{tie}_j), \quad \forall i \in \mathcal{A}_z, \, \forall z \in \mathcal{B}, \, \forall k \in \mathcal{T},$$

$$P^r_i[k+1] = P^r_i[k] - K^I_i h\, ACE_i[j] + P^s_i[k+1], \tag{12}$$

$$\forall i \in \mathcal{A}, \, \forall k \in \mathcal{T}, \, \forall j \in \mathcal{C},$$

$$P^m_i[k+1] = P^m_i[k] + \frac{h}{R_i T_i}\Big(P^r_i[k+1] -$$

$$\Delta\omega_i[k+1] - R_i P^m_i[k+1]\Big), \quad \forall i \in \mathcal{A}, \, \forall k \in \mathcal{T}, \tag{13}$$

$$\delta_i[k+1] = \delta_i[k] + h\,\Delta\omega_i[k+1], \, \forall i \in \mathcal{N}, \, \forall k \in \mathcal{T}, \tag{14}$$

$$\omega_i[k+1] = \omega_i[k] + \frac{h}{2H_i}\Big(P^m_i[k+1] - P^g_i[k+1] -$$

$$K^D_i\,\Delta\omega_i[k+1]\Big), \forall i \in \mathcal{G}, \, \forall k \in \mathcal{T}, \tag{15}$$

$$P^g_i[k] - P^l_i[k] = \sum_{j \in \mathcal{N}} B_{i,j}\,(\delta_i[k] - \delta_j[k]),$$

$$\forall i \in \mathcal{N}, \, \forall k \in \mathcal{T}, \tag{16}$$

Here, (11) and (12) model the ACE signals coming from the control center to governors and the reference set-point adjustment based on this signal, respectively. Equation (13) models the behavior of mechanical input power to the generator. Equations (14) and (15) represent the synchronous generators rotor angle and frequency dynamics, respectively. The DC power flow is represented by equation (16).

V. Optimal False Data Injection Attack

The proposed OFDIA in this paper is based on access to system parameters and limited real-time data (tie-line measurements only). System parameters include various factors or settings concerning generators, governors, and transmission lines, which are constant and need to be obtained once. The attacker can achieve these parameters through different processes such as insider. The other type of data used in OFDIA is real-time data that includes frequency and active power measurements of tie-lines. Hence, to launch a successful attack, the attacker needs access to a few real-time measurements (tie-line measurements only, not all the measurements). For instance, to attack the test bus system studied in this paper, there are only five tie-lines (Fig. 2). Thus, the attacker needs to know only the frequency and active power measurements of these five lines. Attacking the frequency of AGC-participating generators ($\widetilde{\omega}$) and the tie-line active power deviations ($\Delta \widetilde{P}^{tie}$) might lead to an over-frequency incident (the actual system state) or instability in power systems. The injection of $\widetilde{\omega}$ and $\Delta \widetilde{P}^{tie}$ into the measurements causes an error in calculation of ACE in (11) by the control center. By sending these ACEs from the control center to governors (see Fig. 1), the governors' reference set-points start to vary in (12), causing some fluctuations in the mechanical input power of generators in (13). This fluctuation of the mechanical input power leads to changes in rotors' speed, and consequently, rotors' angle in (13) and (14). Ultimately, the active power outputs of the generators vary due to the rotor angle oscillations in (16). In this paper, we consider that the estimated and observed measurements are similar, i.e., the residual value is always zero. This helps us capture the scenario where the attacker is able to manipulate the measurement and bypass the BDD algorithm with zero residual value of estimated and observed measurements. However, there are some thresholds, defined and explained in (22) through (30), that if not satisfied, the BDD algorithm marks the measurements as abnormal. Therefore, the thresholds are considered as constraints while modeling the attack as an optimization problem. Moreover, as mentioned before, we assume that the attacker is capable of launching the attack on any measurements in such a way that the residual of estimated and observed values is zero. This is regardless of whether these measurements are tie-line power measurements or any other measurements needed in launching a successful attack. However, since the focus of this paper is the frequency stability of power systems, given that AGC/LFC has a direct impact on power systems frequency, we consider the tie-line power measurements as ones that the attacker is interested in manipulating.

Based on this, we develop OFDIA model that minimizes the amount of the frequency attack values ($\widetilde{\omega}$) and the tie-line active power deviations ($\Delta \widetilde{P}^{tie}$) subject to the constraints (12)-(16) and (18)-(30). We formulate the OFDIA as follows to make the problem linear programming in nature that yields a tractable formulation,

OFDIA:

$$\textbf{Min} \;\; \alpha_1 \sum_{\substack{k\in\mathcal{C}\\ i\in\mathcal{A}}} \varepsilon_i^{\omega}[k] + \alpha_2 \sum_{\substack{k\in\mathcal{C}\\ i\in\mathcal{B}}} \varepsilon_i^{tie}[k] + \alpha_3 \sum_{\substack{k\in\mathcal{T}\\ i\in\mathcal{G}}} \overline{\varepsilon}_i^{f}[k] \tag{17}$$

$$\textbf{S. t.:} \;\; \text{Constraints } (12)-(16),$$

$$\varepsilon_i^{\omega}[k] \geq 0, \quad \forall i \in \mathcal{A}, \forall k \in \mathcal{T}, \tag{18}$$

$$\overline{\varepsilon}_i^{f}[k] \geq 0, \quad \forall i \in \mathcal{G}, \forall k \in \mathcal{T}, \tag{19}$$

$$\varepsilon_i^{tie}[k] \geq 0, \quad \forall i \in \mathcal{B}, \forall k \in \mathcal{T}, \tag{20}$$

$$\omega_i[k] + \overline{\varepsilon}_i^{f}[k] \geq \overline{\tau}^{f}, \quad \forall i \in \mathcal{A}, \forall k \in \mathcal{T}, \tag{21}$$

$$\varepsilon_i^{\omega}[k] \geq \widetilde{\omega}_i[k] - \widetilde{\omega}_i[k+1], \quad \forall i \in \mathcal{A}, k \in \mathcal{C}, \tag{22}$$

$$\varepsilon_i^{\omega}[k] \geq \widetilde{\omega}_i[k+1] - \widetilde{\omega}_i[k], \quad \forall i \in \mathcal{A}, k \in \mathcal{C}, \tag{23}$$

$$\varepsilon_i^{tie}[k] \geq \Delta \widetilde{P}_i^{tie}[k+1] - \Delta \widetilde{P}_i^{tie}[k], \quad \forall i \in \mathcal{B}, k \in \mathcal{C}, \tag{24}$$

$$\varepsilon_i^{tie}[k] \geq \Delta \widetilde{P}_i^{tie}[k] - \Delta \widetilde{P}_i^{tie}[k+1], \quad \forall i \in \mathcal{B}, k \in \mathcal{C}, \tag{25}$$

$$\underline{P}_i^{m} \leq P_i^{m}[k] \leq \overline{P}_i^{m}, \quad \forall i \in \mathcal{O}, \forall k \in \mathcal{T}, \tag{26}$$

$$\underline{ACE}_i \leq ACE_i[k] \leq \overline{ACE}_i, \quad \forall i \in \mathcal{G}, \forall k \in \mathcal{T}, \tag{27}$$

$$-\tau^{a} \leq ACE_i[k+1] - ACE_i[k] \leq \tau^{a}, \quad \forall i \in \mathcal{A}, \forall k \in \mathcal{C}, \tag{28}$$

$$-\tau^{\omega} \leq (\omega_i[k+1] + \widetilde{\omega}_i[k+1]) - (\omega_i[k] + \widetilde{\omega}_i[k]) \leq \tau^{\omega}, \quad \forall i \in \mathcal{A}, \forall k \in \mathcal{C}, \tag{29}$$

$$-\tau^{tie} \leq (\Delta P_i^{tie}[k+1] + \Delta \widetilde{P}_i^{tie}[k+1]) - (\Delta P_i^{tie}[k] + \Delta \widetilde{P}_i^{tie}[k]) \leq \tau^{tie}, \quad \forall i \in \mathcal{A}, \forall k \in \mathcal{C}, \tag{30}$$

The developed OFDIA model (17) attempts to minimize the amount of the attack to be launched (the first two terms), along with minimizing the time of the violation of the fluctuations from the over-frequency thresholds that these attacks impose on the power system's frequency (the latter). The first two terms $\sum_{\substack{k\in\mathcal{C}\\ i\in\mathcal{A}}} \varepsilon_i^{\omega}[k]$ and $\sum_{\substack{k\in\mathcal{C}\\ i\in\mathcal{B}}} \varepsilon_i^{tie}[k]$ minimize the variation of the attack on the frequency of the buses participating in AGC and the tie-lines' active power deviation within two consecutive AGC cycles, respectively. Note that in this paper we intend to consider the worst-case scenario, that is, the attacker has access to all the tie-lines' measurements, and does not need to attack a limited number of measurements. Hence, we do not study the minimization of the number of attackable measurements. However, to reduce the possibility of the attack getting detected by the BDD algorithm, the attacker needs to launch an attack with the minimum amount. Thus, in this paper, we aim at minimizing the amount of attacks to minimize the possibility of attack detection. On the other hand, the attacker needs to launch an attack in the shortest time to reduce the remaining time for the control center in taking any possible remedial actions. To this end, the term $\sum_{\substack{k\in\mathcal{T}\\ i\in\mathcal{G}}} \overline{\varepsilon}_i^{f}[k]$ in (17) minimizes the sum of the frequency violations from the threshold. This term combined with the other terms minimizes the time period in which the frequencies of the attacked buses violate the permissible upper limit. To have a better understanding of how the third term participates in minimizing the attack time, one should notice that in order to optimize the objective function, the solver needs to minimize all of the first, second, and third terms in (17). All of these terms, including the third term, are a summation of positive values (refer to (18), (19), and (20)). Therefore, the solver needs to minimize each of these values to be able to minimize (17). The minimum possible value for each of these slack terms is zero. More specifically, talking about the third term, the solver will create the over-frequency in the system as quickly as possible so that there is no more need for these slack terms to possess non-zero values (refer to (21)). In other words, the over-frequency occurs in the minimum number of steps or in minimum amount of time in the system. Here, constraints (18), (19), and (20) ensure that the slack terms are positive. Constraint (21) implements the attack on the frequency of AGC-participating buses. In this paper, we assumed that all the generators are equipped with over-frequency protection relays only. This over-frequency protection is modeled as a threshold in OFDIA (see (21)). By adding this constraint to OFDIA, the solver tries to find an attack to trigger the over-frequency protection relays to disconnect associated generators. Constraints (22) and (23) together determine whether an increase or decrease in the frequency attack value would bring the minimum attack value change between two successive AGC cycles. Similarly, constraints (24) and (25) together specify if an increase or decrease in $\Delta\widetilde{P}^{tie}$ constitutes the minimum attack value change between two consecutive AGC cycles. Constraint (26) implements the input mechanical power limit. Constraints (27), (28), (29), and (30) ensure the attack stealthiness in OFDIA. Constraint (27) keeps the ACE to be within the permissible range defined, which is not detectable by bad data detection algorithms. Constraint (28) make sure that the difference between two consecutive AGC cycles does not cross the upper and lower bounds. Similarly, constraints (29) and (30) ensure that the difference between two consecutive values of the AGC-participating generator frequencies and the tie-lines' active power deviation seen by the control center is within the threshold set by the bad data detection algorithms. This paper considers attacking the power system based on its dynamic frequency behavior. Contrary to the steady-state frequency of power systems, the frequency during dynamics can vary in different locations even though this variation is within a small range. Taking advantage of this small difference in the power systems' dynamic frequency, the attacker launches a stealthy attack on the frequency measurement of tie-lines by injecting a small amount of false data which is not detectable by the control center (refer to (22), (23), and (29)). We will study the impact of two different attack types utilizing the developed OFDIA: continuous-attack and time-limited attack. The continuous-attack is defined as an attack in which the attacker does not have any time restriction in launching the attack. On the contrary, the time-limited attack is a type of attack with a limited launch time.

VI. Numerical Studies

A. Test System

We use the IEEE 39-bus system [29] shown in Fig. 2 as the test system to carry numerical simulation. The system is divided into three areas connected together through tie-lines and includes 10 synchronous generators with total generation capacity of 10,000 MVA and $K_i^D = 0\ \forall i \in \mathcal{G}$, and a total load of 6,150 MW. For simplicity, we assume that the loads in the grid remain constant throughout the optimization horizon. Nevertheless, the proposed formal model is able to capture the load fluctuations as well. All the generators are protected with over-frequency relays. The generators connected to buses 30 through 35 and bus 39 are equipped with governors participating in the AGC process. The generators at buses 36, 37, and 38 do not have any governors, and their mechanical input power is considered constant. We implemented the OFDIA model in JuMP [35] and solved using Gurobi [36]. We also implemented a power system dynamic model in ePHASORSIM to verify dynamics from OFDIA and the impact of the OFDIA on the frequency response. The test system parameters and the simulation parameters are provided in Table I and Table II, respectively.

B. Model Validation

Before studying the impact of FDIAs, we need to validate the accuracy of the power system dynamics modeling adopted in this paper. To do so, we disable all the attack constraints in (17) i.e., $\widetilde{\omega}_i[k] = 0\ \forall i \in \mathcal{A}, \forall k \in \mathcal{T}$, $\Delta\widetilde{P}_i^{tie}[k] = 0\ \forall z \in \mathcal{B}, \forall i \in \mathcal{A}_z, \forall k \in \mathcal{T}$, and (21). This is to ensure that the dynamic behavior is only due to the power system modeling represented in (12) to (16), and none of the attack-related constraints contribute to the results. Thereafter, we apply a load disturbance to the test system and compare the dynamics with the dynamic behavior of the test system from ePHASORSIM to check the proximity of the results. The discretization time-step used in this validation process is 0.016 s (1/60 Hz). The load disturbance considered is a load increase of 800 MW (40 MW at each load bus which is equivalent to 13% of the total load) for 3 s (starting at t = 1 s and terminating at t = 4 s) on top of the existing load of 6,150 MW in the system.

Due to space limitations, we only show the rotor angle and frequency behavior of the generators installed at buses 33 and 35 obtained from the adopted dynamic model and ePHASORSIM in Fig. 3. Further information can be found in [37]. It can be seen that the dynamic responses are very close. Note that the power flow method used in the adopted

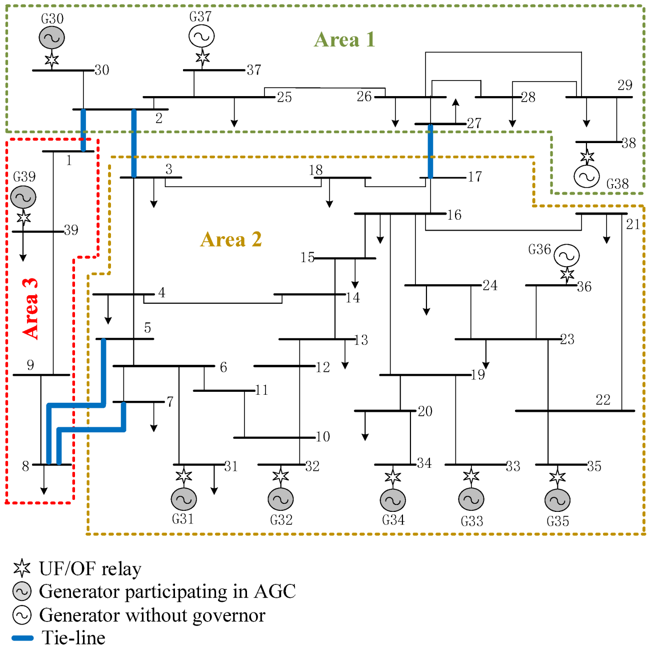


Fig. 2. IEEE 39-bus power system with three control areas [29].

method in this paper is DC. The main motivation to use the DC power flow is to keep the resulting optimization model linear in nature so that it is applicable to larger power systems as well. This is while ePHASORSIM uses AC power flow in modeling the power systems' dynamics. This difference in the utilized power flow methods causes the little discrepancy observed in the results.

C. Case Studies

We implemented two different forms of attacks, i.e., continuous attack and time-limited attack on frequencies and the tie-lines power deviations in each area of the power system. In the continuous attack, it is assumed that the attacker is capable of launching the attack throughout the optimization horizon, and in the time-limited attack, the attacker can launch the attack for only a limited number of AGC cycles. Each AGC cycle is 2 s. In both case studies, the simulation starts at $t = 0$ s and continues its normal operation (unattacked measurements) for one AGC cycle. Then, the attack begins at the beginning of the second AGC cycle. We would like to demonstrate the power system behavior before and after the attack. Our proposed model can capture the details regardless of the time of the attack incident. Therefore, we assumed that the attack starts at the first AGC cycle so that we could present the system's behavior shortly for one cycle before the attack started. In the time-limited attack scenario, this attack stops (i.e., $\widetilde{\omega} = 0$, and $\Delta\widetilde{P}^{tie} = 0$) after four AGC cycles, while in the continuous-attack scenario, the attack lasts for the entire optimization horizon (i.e., 10 AGC cycles).

*1) **Continuous Attack:*** In this case study, we demonstrate the scenario in which the system undergoes a continuous attack on the frequency and tie-line power measurements.

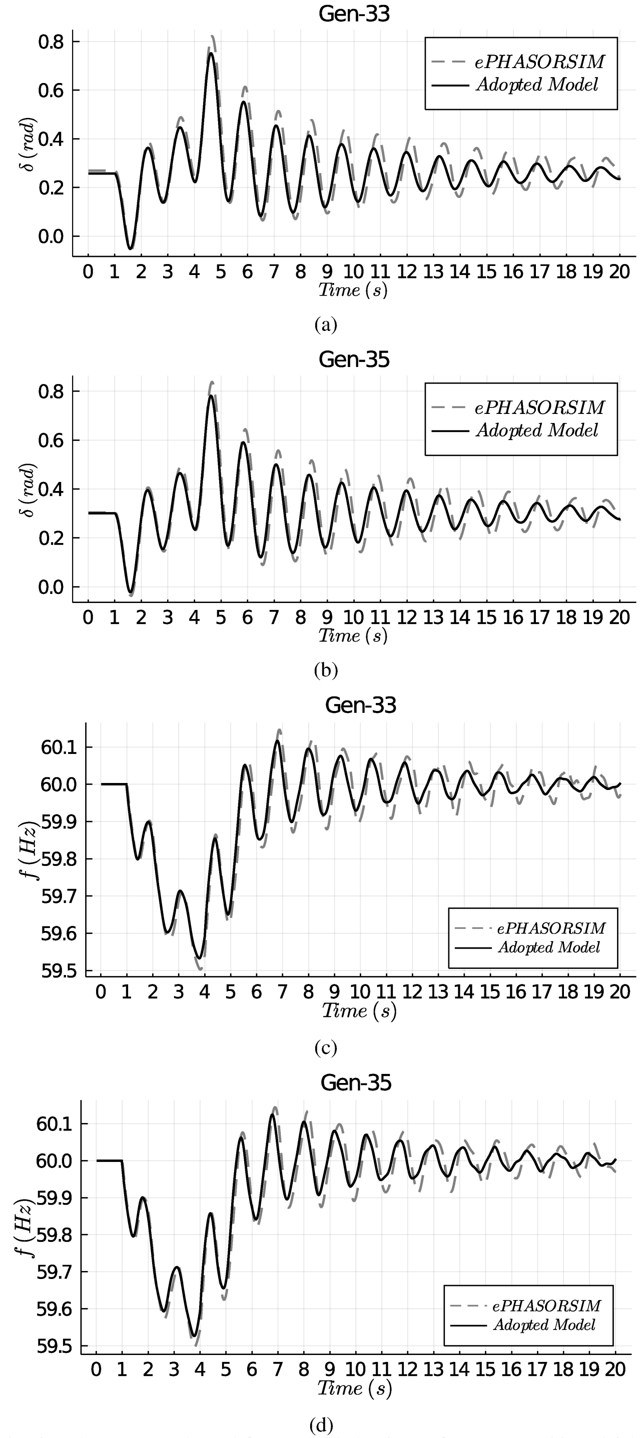
Fig. 4 shows the OFDIA solutions for the attack values on the frequency of the generators equipped with AGC. The proposed method suggests a zero attack value on the frequency measurements of the generators 30 and 39 in Area 1 and Area 3 while the attack values on the frequency of the generators 31 to 35 in Area 3 are identical. Fig. 5 shows the total attack values on the tie-line measurements. Note that these values are the sum of all the tie-lines connected to an area. For instance, Area 1, on one hand, is connected to Area 2 through the tie-lines between buses 2 and 3, and the tie-lines between buses 17 and 27. On the other hand, it is connected to Area 3 through the tie-line between buses 1 and 2 (see Fig. 2). Therefore, the attack value of Area 1's tie-lines shown in Fig. 5 is the sum

TABLE I
GENERATORS AND GOVERNORS PARAMETERS

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	0.05	0.50

TABLE II
SIMULATION AND MODELING PARAMETERS

Parameter	Value	Parameter	Value
f_o (Hz)	60.00	$\overline{\tau}^f$ (p.u.)	1.80
h (s)	1/60	$\overline{P}^m$ (p.u.)	1.10
W (s)	2.00	$\underline{P}^m$ (p.u.)	0.00
S^b (MVA)	100.00	$\overline{ACE}$ (p.u.)	-0.05
τ^{tie} (p.u.)	1.00	$\underline{ACE}$ (p.u.)	0.05
τ^a (p.u.)	0.03	C	10.00



(d)

Fig. 3. The rotor angle and frequency behaviour of generators 33 and 35 for the adopted modeling and the simulation.

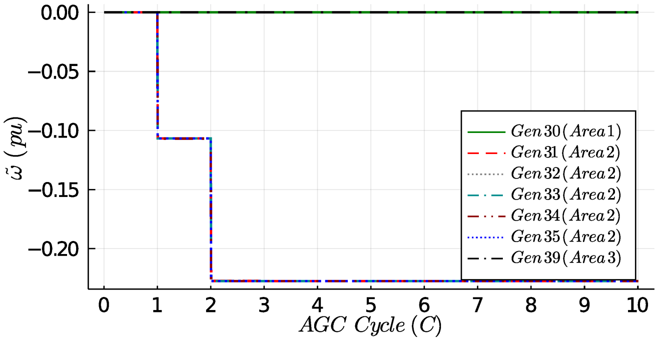


Fig. 4. Continuous-attack on frequency measurements used in AGC based on the OFDIA.

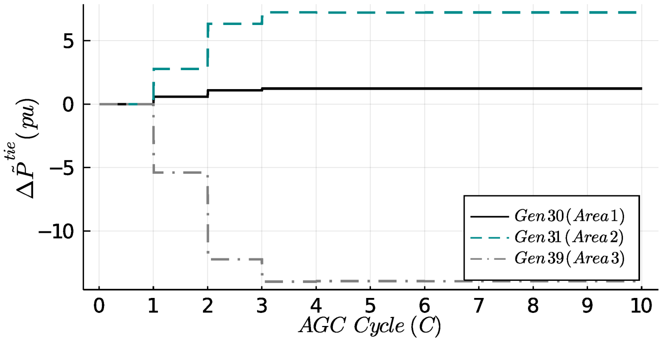


Fig. 5. Sum of the tie-lines continuous-attack values obtained from OFDIA for each of the three areas.

of all these tie-lines attack values.

The attack values shown in Fig. 4, and Fig. 5 cause some variations in ACEs. These ACE variations are demonstrated in Fig. 6. It can be seen that before the attack begins, ACE is 0. This is due to the fact that the power system is working at its nominal frequency in all areas; hence, there is no need to adjust ACEs. However, by launching the continuous-attack scenario, ACEs start to vary.

In order to observe the impacts of the continuous-attack FDIA on the dynamics of the power system, we use the ACEs shown in Fig. 6 as an input to the dynamic model built-in ePHASORSIM. Fig. 7 demonstrates the governors' reference set-points (P^r) impacted by the continuous-attack scenario in which all P^r values are continuously growing. This behavior can be explained by looking at (11) where the ACEs are the arguments of the integrator term. Since ACEs in Fig. 6 are not zero, therefore, the integrator term, and subsequently P^r, continue to grow with time. Mechanical input power to the generators have are shown in Fig. 8. Since Generators 36, 37, and 38 are not equipped with governors, therefore, their mechanical input powers are always constant. Any fluctuations in the mechanical power outputs can lead to an oscillation in the rotor speed and frequency as well. Fig. 9 shows the frequency dynamics of the generators. As can be seen, the frequency of all the generators is ever increasing while they all overlap. This clearly shows that launching a continuous-attack OFDIA makes the system unstable.

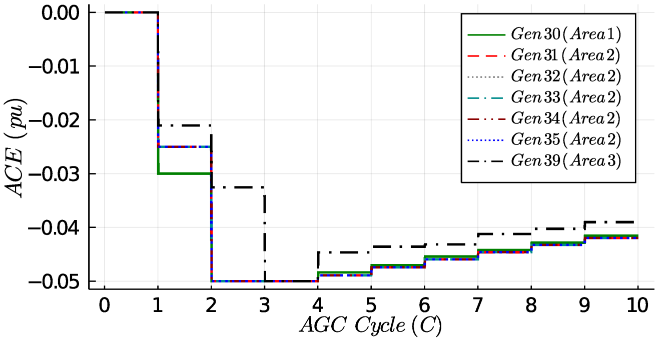


Fig. 6. Automatic error control (ACE) signal variations resulting from the 'continuous-attack' OFDIA.

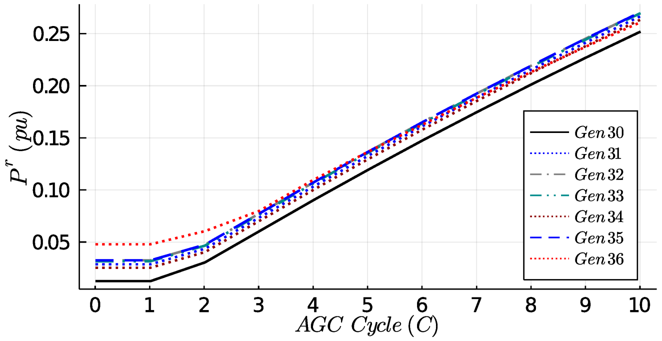


Fig. 7. The governors reference set-points (P^r) in continuous-attack scenario.

The rotor angles behavior of the generators is demonstrated in Fig. 10. Before t = 2 s (the attack launch time), there is no fluctuation in the rotor angles as the generators are running in a steady state, and after the attack, the rotor angles start to oscillate. Note that the curves seen in this figure are the relative rotor angles with respect to the slack generator's rotor angle, i.e., $\delta_i - \delta_{39},\ \forall i \in \mathcal{G}$. The active power output of the generators is shown in Fig. 11. As shown, the slack generator's active power output decreases after the attack incident in the system and stays at negative values.

*2) **Time-Limited Attack:*** We also studied the time-limited attack scenario in which the attacker has only a limited number of AGC cycles (3 cycles in this case study) to launch the attack. Thereafter, similar to Section VI-C1, we present the

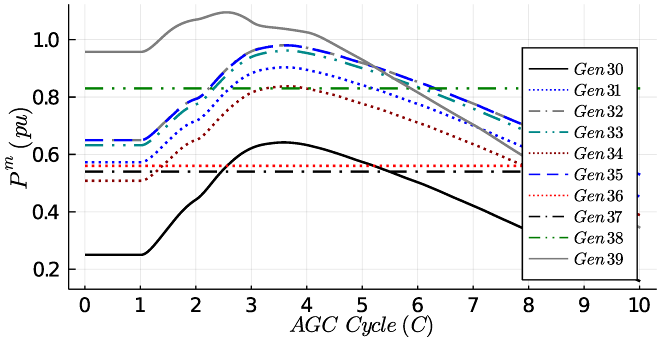


Fig. 8. The generators mechanical input power variations due to the continuous-attack OFDIA.

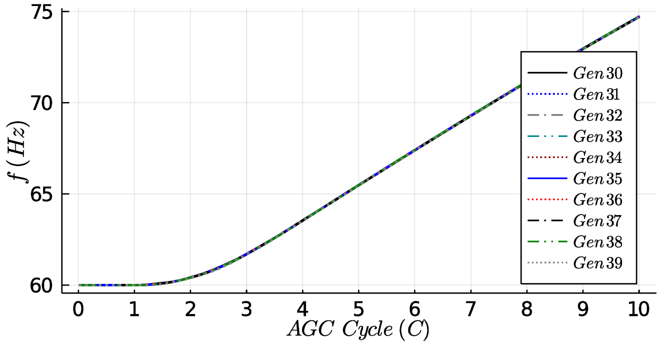


Fig. 9. Frequency behavior of the generators caused by implementation of the continuous-attack OFDIA.

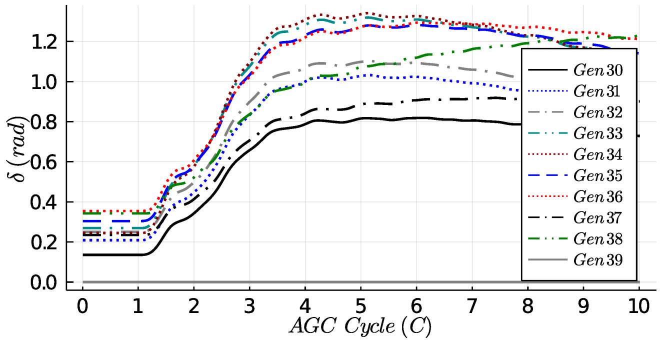


Fig. 10. The generator rotor angles dynamics for the continuous attack using OFDIA.

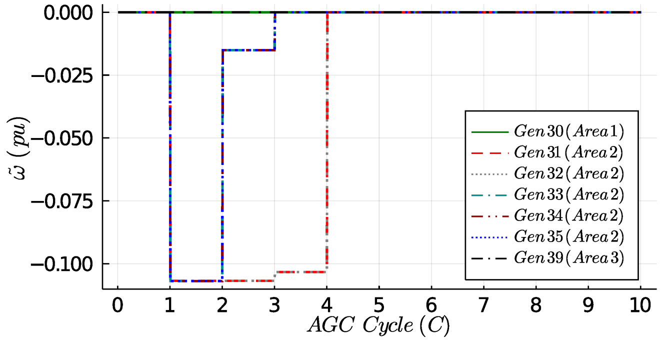


Fig. 12. Interrupted-attack values on the frequency of the generators participating in AGC in each of the three areas.

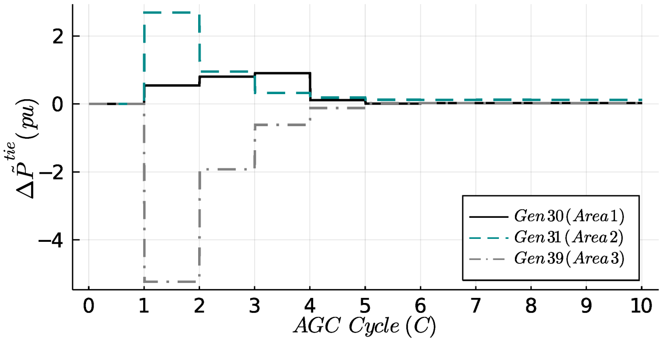


Fig. 13. Sum of the tie-lines time-limited attack values for each of the three areas.

dynamic behavior of the power system for this attack scenario as well. Fig. 12 and Fig. 13 show the OFDIA solutions for the attack values $\widetilde{\omega}$ and $\Delta\widetilde{P}^{tie}$. As expected, the attack values for the AGC cycles out of the attack period are zero. This is while the proposed OFDIA returns non-zero attack values for the generators in Area 2, and zero-attack values for the frequency of the generators in Areas 1 and 3. The influence of these attack values can be seen on ACEs in Fig. 14. It is apparent that ACEs approach zero shortly after the attack stops at the fourth AGC cycle. However, since there are fluctuations in the frequency and tie-line powers, these values do not return to zero abruptly. The impact of such behavior of ACEs on P^r can be observed in Fig. 15. Unlike the reference set-points in Fig. 7 that increasingly grow up due to the non-zero ACE values, P^r values, in this attack scenario, have limited growth and tend to approach their initial values after a while. The impact of the limited increase in P^r values appears in the generators' mechanical power behavior as well. As it is evident in Fig. 16 that the mechanical power of the generators, except for the ones with no governors, tends to settle to the steady-state value after the attack is removed from the system.

Fig. 17 shows the frequency response. It is clear from the figure that the generators' frequencies do not tend to become unstable. This behavior is in contrast to that of f in the continuous-attack OFDIA where it was continuously growing (see Fig. 9). However, the generators' frequencies

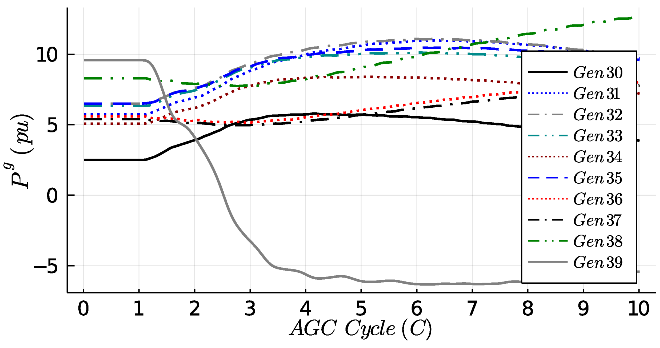


Fig. 11. The generators active power output changes caused by the continuous-attack.

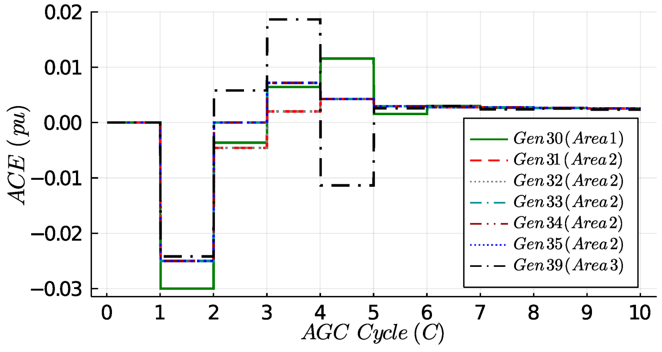


Fig. 14. Automatic error control (ACE) signal variations resulting from the time-limited OFDIA.

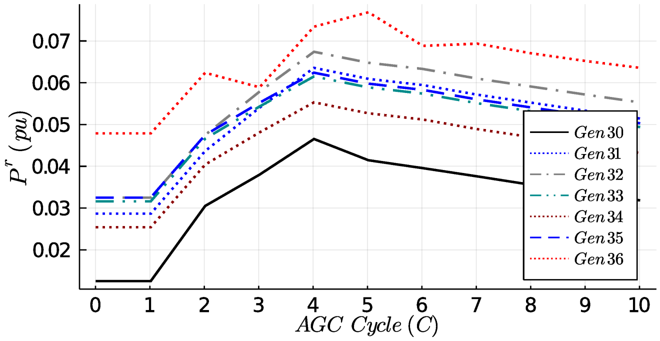


Fig. 15. The governors reference set-points (P^r).

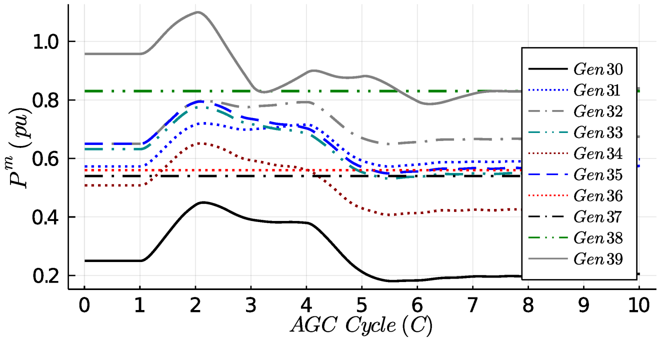


Fig. 16. The generators mechanical input power variations due to the time-limited attack in OFDIA.

in the time-limited OFDIA attack exceeded the given over-frequency threshold in this study (1.8 p.u.) which triggers the over-frequency protection of the generators and leads to false unintentional tripping of generators.

The relative rotor angle dynamics of the generators and the active power output of the generators are shown in Fig. 18 and Fig. 19, respectively. Some oscillations are observed in the response that tends to disappear after the attack is removed at $t = 8\,\text{s}$.

In summary, we implemented two different attack scenarios, continuous attack and time-limited attack, with the same simulation parameters as given in Table II but with different attack launch periods. In the continuous attack, the attacker does not have any time limit in launching the attack while in the time-limited attack, the attacker needs to stop the attack in a specified period of time (3 AGC cycles in this study). The root cause of the differences between the power system's dynamics in these two scenarios comes from the difference in the corresponding ACEs (see Fig. 6, and Fig. 14) sent by the control center. In the continuous-attack scenario, since the attack is not stopped throughout the simulation, ACE values continue to deviate from zero. As mentioned before, any nonzero value of ACE causes some fluctuations in the power system dynamics. Therefore, longer periods of nonzero values of ACEs may create more serious consequences in power systems such as frequency instability (see Fig. 9). This is while in the time-limited attack scenario, the nonzero values of ACE disappear faster as the attack is time-limited after a limited period of time. Hence, the attack consequences are less serious such as over-frequency protection relay operations (see Fig. 17) in comparison to the frequency instability in the continuous-attack scenario. Therefore, it is vital to have detection mechanisms in power systems that can quickly detect the presence of FDIAs on frequency control of power grids.

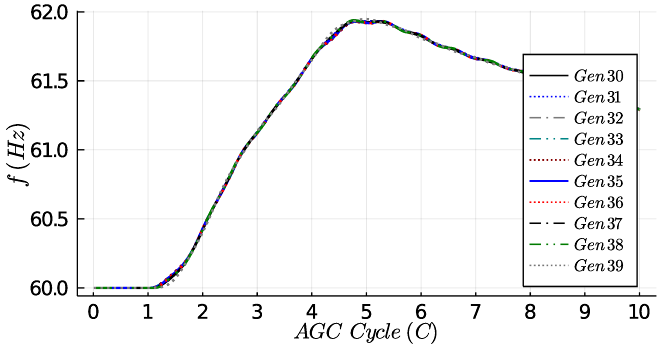


Fig. 17. Frequency behavior of the generator buses resulting from the implementation of the time-limited attack in OFDIA.

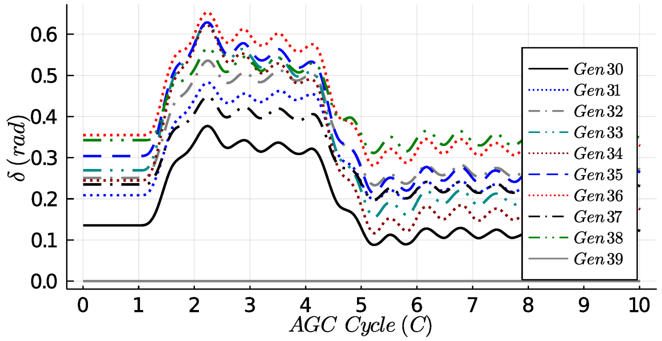


Fig. 18. The generator rotor angles dynamics relative to the slack generator rotor angle after implementing the time-limited OFDIA.

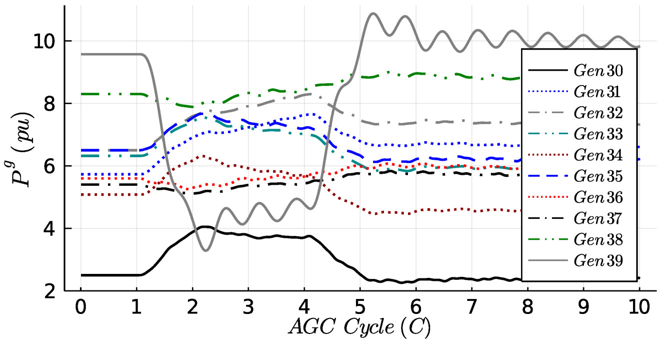


Fig. 19. The generators active power outputs changes caused by the time-limited OFDIA.

VII. Comments on Detection and Mitigation Methods

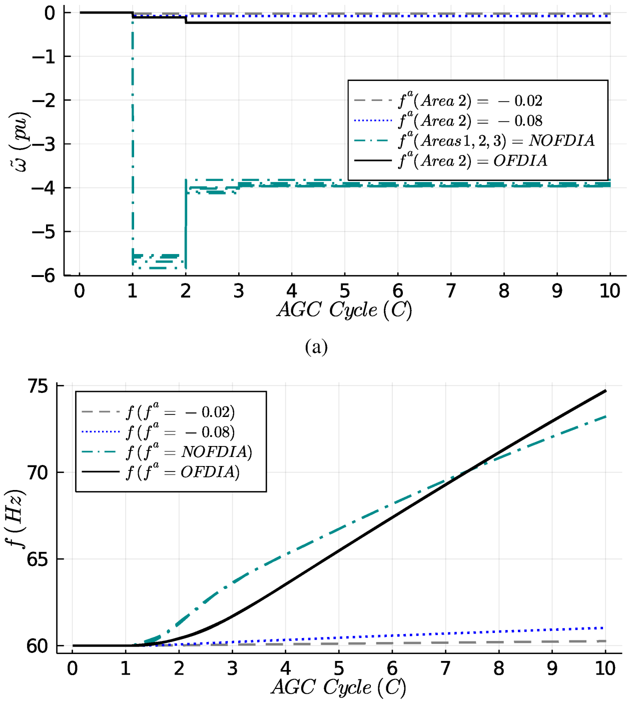
Detection and mitigation of OFDIA should complement the proposed work of OFDIA; however, as the scope of this work is only on the modeling of OFDIA, we provide some perspectives on how OFDIA can be detected and mitigated. A detection and defense mechanism for FDIAs against AGC is proposed in [38] by utilizing generative adversarial networks.

The authors in [39] introduce a semi-supervised learning approach for anomaly detection in the AGC loop is introduced. In [40], the authors identify and mitigate FDIAs on AGC utilizing forecasted data of ACE. Considering FDIAs as an unknown input and estimating their values, the authors in [41], [42] try to compensate the impacts of FDIAs on AGC. Kalman filter and artificial neural network are simultaneously used in [43] to propose a control mechanism for the detection and mitigation of FDIAs. An online framework to detect cyber attacks on AGC is proposed in [44] based on dynamic watermarking. The authors in [45] develop a mitigation method to thwart destabilizing time-delay switch attacks on control lines in power systems by adding a time-delay estimator to controllers. However, the FDIA model considered in these works [38], [40], [41], [43] is based on arbitrary or preset attack values. Such random attacks often cannot create a harmful impact on the system or may take so long or require a large amount of data manipulation to be successful which makes such attacks impractical from the attackers' point of view [22]. Sophisticated adversaries can launch OFDIAs to create maximum damage while being stealthy, as shown in this paper. In the following, we will compare some arbitrary and random attack impacts with the proposed OFDIA impacts on power systems to make this statement clear.

To demonstrate the optimality of the proposed OFDIA, we study two pre-selected continuous arbitrary attacks and a non-optimal FDIA (NOFDIA) and compare their impacts with the OFDIA attack found in Section VI-C1 on the test system frequency behavior. For the simplicity, in pre-selected attacks and NOFDIA, we assume that there are no attacks on tie-lines' active power ($\Delta\widetilde{P}_i^{tie}[k] = 0\ \forall z \in \mathcal{B}, \forall i \in \mathcal{A}_z, \forall k \in \mathcal{T}$). Moreover, we choose two values of -0.02 and -0.08 as the attack on the frequency of the generators in Area 1 which have smaller magnitudes than the OFDIA-found attacks magnitudes (-0.11 and -0.22). For Area 1 and 3 in the pre-selected attacks, we consider that the attacks on the frequency of the generators are zero as these values are equal to zero in the OFDIA-found attack as well. In other words, for the pre-selected attacks, we have $\widetilde{\omega}_i[k] = 0\ \forall i \in \{1, 3\},\ \forall k \in \mathcal{T}$. This is while there are no limitations on the frequency attacks in Areas 1, 2, and 3 for the NOFDIA. These attack scenarios can be seen in Fig. 20(a).

The frequency behavior of these attacks is demonstrated in Fig. 20(b). It can be seen that the pre-selected attacks are not able to cause any over-frequency ($f > 61.8$ Hz) or instability in the system. This shows that the attacker might not be able to launch a successful attack by arbitrarily attacking the measurements. Apart from that, taking a look at the random attack manifest that there could be some random attacks that are successful in causing an over-frequency/instability in the system. However, a comparison of the magnitude of this successful scenario of random attack with the OFDIA-found attack clarifies that a random attack can have a very large magnitude which might make it detectable by BDD algorithms in the control center. Therefore, such attacks might not be of interest to attackers in the real world.

Considering this fact, it is obvious that assuming pre-selected or random attacks might not be always efficient in the performance evaluation of detection and mitigation methods. In order to have a reliable detection and mitigation method, we recommend evaluating the performance of detection methods with an optimal attack as proposed in this paper. If a detection method can detect an OFDIA that bypasses all the BDD algorithm constraints with minimum magnitude, it can definitely detect any FDIAs with larger magnitudes.



(a)

(b)

Fig. 20. Comparison of pre-selected attacks, random attacks and OFDIA impacts on the test system's frequency: a) attack on tie-lines' frequency ($\widetilde{\omega}$) b) frequency dynamics of all of the generators.

VIII. Conclusion

In this paper, we studied OFDIA on AGC in multi-area power systems. We introduced an optimization-based formal model minimizing the magnitude of attacks on the generators' frequencies participating in AGC and tie-lines active power deviations from their scheduled values. Before studying the impact of OFDIAs, we implemented the proposed method on the IEEE 39-bus 3-area system and compared the rotor angle and frequency of the generators with the results from ePHASORSIM. We showed that the adopted model is sufficiently accurate in capturing the dynamic of power systems. Thereafter, we demonstrated the power system dynamics, including governors' reference set-points and generators' mechanical power input, active power output, frequency, and rotor angle under two different attack scenarios, continuous attack and time-limited attack. Ultimately, we discussed the impact of the attack period on the severity of the consequences in power systems. The results manifested that continuous attacks may have severe effects, such as frequency instability on power systems, while time-limited attacks can create less severe consequences, such as over-frequency relay operations of the generators. Moreover, we compared the performance of some pre-selected and random attacks with the proposed OFDIA and showed that these types of attacks might not be proper in performance validation of detection and mitigation methods due to their not optimal amounts. Consideration of the proposed OFDIA helps improve the detection and mitigation methods' accuracy. In future work, we will show the model's scalability in a large-scale power grid and evaluate the impact of other types of attacks like time delay on power systems' frequency stability. In addition, we will develop detection and mitigation methods capable of detecting and reducing the impact of the proposed OFDIA in this paper.

References

[1] A. R. Metke and R. L. Ekl, "Smart grid security technology," in *Proc. Innov. Smart Grid Technol. Conf. (ISGT)*. IEEE, 2010, pp. 1–7.

[2] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, 2013.

[3] 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.

[4] 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.

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

[6] 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.

[7] M. Ahmed and A.-S. K. Pathan, "False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure," *Complex Adaptive Sys. Modeling*, vol. 8, pp. 1–14, 2020.

[8] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.

[9] A. Zakerian, A. Maleki, Y. Mohammadnian, and T. Amraee, "Bad data detection in state estimation using decision tree technique," in *Proc. Iranian Conf. on Electrical Engineering (ICEE)*, 2017, pp. 1037–1042.

[10] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel and Distributed Sys.*, vol. 25, no. 3, pp. 717–729, 2013.

[11] M. A. Rahman, E. Al-Shaer, and R. Kavasseri, "Security threat analytics and countermeasure synthesis for state estimation in smart power grids," in *Proc. 44th IEEE/IFIP Int. Conf. on Dependable Sys. and Netw. (DSN)*, Jun 2014.

[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] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[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] X. He, X. Liu, and P. Li, "Coordinated false data injection attacks in AGC system and its countermeasure," *IEEE Access*, vol. 8, pp. 194 640–194 651, 2020.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] P. Kundur, *Power System Stability*. CRC Press New York, NY, USA, 2007, vol. 10.

[31] M. Rahmani and N. Sadati, "Two-level optimal load-frequency control for multi-area power systems," *Int. J. of Electrical Power & Energy Sys.*, vol. 53, pp. 540–547, 2013.

[32] R. Shankar, S. Pradhan, K. Chatterjee, and R. Mandal, "A comprehensive state of the art literature survey on LFC mechanism for power system," *Renewable and Sustain. Energy Reviews*, vol. 76, pp. 1185–1207, 2017.

[33] 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.

[34] B. P. Zeigler, A. Muzy, and E. Kofman, *Theory of Modeling and Simulation: Discrete Event & Iterative Sys. Computational Foundations*. Academic press, 2018.

[35] I. Dunning, J. Huchette, and M. Lubin, "JuMP: A modeling language for mathematical optimization," *SIAM Review*, vol. 59, no. 2, pp. 295–320, 2017.

[36] Gurobi Optimization, LLC, "Gurobi optimizer reference Manual," 2022. [Online]. Available: https://www.gurobi.com

[37] M. Jafari, M. A. Rahman, and S. Paudyal, "Optimal improvement of post-disturbance dynamic response in power grids," in *Proc. IEEE Industry Applications Soc. Annu. Meeting*, October 2022, [Accepted].

[38] 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.

[39] S. D. Roy and S. Debbarma, "A novel OC-SVM based ensemble learning framework for attack detection in AGC loop of power systems," *Electric Power Syst. Research*, vol. 202, p. 107625, 2022.

[40] 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.

[41] 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.

[42] A. Ameli, A. Hooshyar, A. H. Yazdavar, E. F. El-Saadany, and A. Youssef, "Attack detection for load frequency control systems using stochastic unknown input estimators," *IEEE Trans. Inf. Forensics and Security*, vol. 13, no. 10, pp. 2575–2590, 2018.

[43] 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.

[44] T. Huang, B. Satchidanandan, P. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6816–6827, 2018.

[45] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, "Preventing time-delay switch attack on load frequency control in distributed power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 1176–1185, 2015.

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 (SM'21) is an Assistant 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 the PhD degree in computing and information systems from the University of North Carolina at Charlotte in 2015. Rahman's research area covers a wide area of computer networks that includes 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) 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 is 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.