Online Recursive Detection and Adaptive Fuzzy Mitigation of Cyber-Physical Attacks Targeting Topology of IMG: An LFC Case Study

Author(s): Abazari, Ahmadreza; Soleymani, Mohammad Mahdi; Zadsar, Masoud; Ghafouri, Mohsen; Assi, Chadi; Shafie-Khah, Miadreza

Title: Online Recursive Detection and Adaptive Fuzzy Mitigation of Cyber-Physical Attacks Targeting Topology of IMG: An LFC Case Study

Year: 2023

Version: Accepted manuscript

Please cite the original version:

Abazari, A., Soleymani, M. M., Zadsar, M., Ghafouri, M., Assi, C. & Shafie-Khah, M. (2023). Online Recursive Detection and Adaptive Fuzzy Mitigation of Cyber-Physical Attacks Targeting Topology of IMG: An LFC Case Study. *IEEE Transactions on Smart Grid*. https://doi.org/10.1109/TSG.2023.3304537

Online Recursive Detection and Adaptive Fuzzy Mitigation of Cyber-Physical Attacks Targeting Topology of IMG: An LFC Case Study

Ahmadreza Abazari, *Member, IEEE*, Mohammad Mahdi Soleymani, *Member, IEEE*, Masoud Zadsar, Mohsen Ghafouri, *Member, IEEE*, Chadi Assi, *Fellow, IEEE*, and Miadreza Shafie-khah, *Senior Member, IEEE*

***Abstract*—Due to the low inertia of inverter-based islanded microgrids (IMGs), these systems require a delicate and accurate load frequency control (LFC) scheme. The deployment of such a control scheme, which preserves the balance between the load and generation, needs a cyber layer on top of the physical system that makes IMGs an appealing target for a variety of cyber-physical attacks (CPAs). Among these CPAs, there is a family of malicious CPAs whose aim is to compromise the LFC scheme by changing the topology of IMG and its parameters. On this basis, an online system identification method is developed to estimate the parameters of IMG using the recursive least square forgetting factor (RLS-FF) approach. Then, based on the estimated parameters, an anomaly-based intrusion detection system (IDS) is developed to identify CPAs and distinguish them from the uncertainties in the normal operation of IMG. Following anomaly detection, a mitigation scheme is proposed to regulate the IMG's frequency using an adaptive interval type-2 fuzzy logic controller (IT2FLC). The proposed IT2FLC uses different types of distributed energy resources (DERs)—i.e., tidal power plants and solar panels which are, respectively, equipped with inertia emulation and droop-based controllers—to improve the frequency excursion resulting from CPAs. The simulation results verify the performance of the developed detection and mitigation schemes, particularly when the RLS-FF parameters, i.e., forgetting factor, covariance matrix, and reset parameter, are obtained through the grey wolf optimization (GWO) algorithm. Furthermore, the designed mitigation scheme is corroborated by comparing its performance with several well-known attack-resilient control frameworks in LFC studies, e.g., linear quadratic regulator (LQR) and H_∞, using real-time simulations.**

***Keywords*—Islanded Microgrid, Cyber-Physical Attacks, Recursive Least Square with Forgetting Factor, Online System Identification, Interval Type-2 Fuzzy Logic Controller.**

NOMENCLATURE

Abbreviation:

IMG	Islanded microgrid
LFC	Load frequency control
CPAs	Cyber physical attacks
RLS-FF	Recursive least square forgetting factor
IDS	Intrusion detection system
DERs	Distributed energy resources
IT2FLC	Interval type-2 fuzzy logic controller
T1FLC	Type-1 fuzzy logic controller
LQR	Linear quadratic regulator
IED	Intelligent electronic device
GWO	Grey wolf optimization
ICTs	Information and communication technologies
ANN	Artificial neural network
TPPs	Tidal power plants
PV	Photovoltaic
LS	Least Square
SGs	Synchronous generators
CBs	Circuit breakers
CFMD	Central frequency measurement device
RESs	Renewable energy sources
GTs	Gas turbines
IAE	Integral absolute error
ISE	Integral square error
SNR	Signal noise ratio
SM	Security margin
MFs	Membership functions

Parameters and Variables:

R_{eq}, H_{eq}	Equivalent droop speed governor, and equivalent inertia constant
T_{f_Mea}, D_{eq}	Time constant of central frequency measurement device (CFMD), and equivalent damping coefficient
T_{M-tpp}, T_{M-pv}	Time constant of tidal power plant (TPP), and PV frequency measurement device (FMD)
Δf, $\Delta f^{'}$	Real and measured frequency deviation
$\Delta P_{g1}...\Delta P_{gn}$	Governor valve positions for n synchronous generators
$\Delta P_{mt1}...\Delta P_{mtn}$	Changes in output power for n synchronous generators
ΔP_C	Supplementary control action
T_{ti}, T_{gi}	Turbine time constant, and governor time constant
$\gamma_1...\gamma_n$	Participation factors of gas turbines in LFC studies
P_{MPPT}^{TPP}	Maximum mechanical output power from tidal stream
P_{MPPT}^{PV}	Maximum output power extracted from solar energy
$\Delta f_{PV}^{'}$, ΔP_{inv}	Measured frequency by FMD, and PV inverter power
$\Delta f_{tpp}^{'}$, $\Delta f'_{wf}$	Measured frequency, and filtered frequency obtained from a washout filter
$\Delta\omega_r$, ΔP_ω	Rotor speed variation, and output proportional-integral (PI) speed controller
β	Pitch angle (degree)
ΔV_{ss}	Tidal stream speed

ΔP_{out_PV}	Output power of PV solar arrays
ΔP_{out_tpp}	Output power of tidal power plant (TPP)
T_{inv}, T_{id_PV}	Time constant of PV inverter, and interconnection device
T_{wf}, M_{tpp}	Time constant of washout filter, and mechanical inertia of rotational masses in TPP
K_{pf}, K_{df}	Extra damping and extra inertia of TPP
$\theta(k)$	Parameter vector at time index k
$\hat{\theta}(k)$	Estimated parameter vector at time index k
$b_p \dots a_q$	Elements of parameter vector $\hat{\theta}(k)$
$e(k)$	Error signal at time index k
$\Delta f(k)$	Frequency of IMG at time index k
$\Delta \hat{f}(k)$	Estimated frequency of IMG at time index k
$u(k)$	Control input signal from LFC controller
J_M	Loss function at time index k
$\phi(k)$	Regression vector at time index k
$L(k)$	Gain matrix of RLS-FF estimation method at time index k
$P(k)$	Covariance matrix at time index k
λ	Forgetting factor
λ_0	Initial value of forgetting factor
$P_0 = \sigma_0 I$	Initial value of covariance matrix $P(k=0)$
I	Identity matrix for system identification process
σ_0	Coefficient for initialization process of estimation
θ_0	Initial value of system parameter
Cov	Reset factor (0 or 1)
T_s	Sampling time
t_0	Initial tracking time
t_s	Average estimation time
$r_s(k)$	Residual signal for alarm activation
χ	Predetermined threshold for each IMG parameter
S_0, S_1	Indicator for normal operation of the IMG, and occurrence of attack
K_1, K_2	Input scaling factor of fuzzy logic controller
$\alpha^{'}, \beta^{'}$	Output scaling factors of type-2 fuzzy controller
s	The number of fuzzy rules
$Rules\{1, \dots s\}$	Fuzzy rules from number 1 to s
$\tilde{A}_{s1},\ \tilde{A}_{s2}$	Type-2 membership functions (MFs) for input-1 and input-2 signals
$W_1 \dots W_s$	A set of consequent parameters of type-2 MFs
r_1, r_2	Input signals of fuzzy logic controller after scaling
u_f	Output signal of type-2 fuzzy logic controller
$\overline{\mu}$, $\underline{\mu}$	Upper and lower bounds of type-2 MFs
$\overline{f}^l, \underline{f}^l$	Upper and lower firing strength of rule-s
α^*, β^*	Optimal values of output scaling factors
$V(t)$	Lyapunov function
ψ	A vector of all fuzzy rules
$\varepsilon(t)$	Output error signal
$J = \partial y / \partial u$	Jacobian Matrix
κ_1, κ_2	Coefficients of derivative of output scaling factors

*Other parameters/variables are defined in the paper's content.

I. Introduction

RECENTLY, the deployment of information and communication technologies (ICTs) in various applications of smart grids, e.g., wide-area monitoring and control systems [1], protection devices [2], and smart meters [3], has witnessed a surge of interest. In smart grids, islanded microgrids (IMGs) are among the most vulnerable systems to cyber-physical attacks (CPAs) due to their inherent specifications, i.e., wide use of distributed energy resources (DERs) with low inertia and huge dependency on intelligent electronic devices (IEDs) for protection and control purposes [4]. One of the main purposes of CPAs is to compromise specific functionalities in IMGs that can cause disruption in their normal operations [5]. Load frequency control (LFC), which plays a significant role in keeping the frequency of an IMG in the acceptable ranges and providing high-quality electricity energy for consumers, can be maliciously exploited by such attacks [6]. Targeting this extremely delicate scheme can lead to frequency instability in IMGs, and consequently total curtailment of its loads. As a result, the development of effective online detection and adaptive mitigation schemes to combat cyber attacks against this control scheme during different operating points of the IMG is of paramount importance [7].

A wide range of publications has recently addressed different detection methods, which can report failures and attacks on LFC models. Detection approaches generally are categorized into learning-based and model-based methods [8]. Learning-based approaches use machine learning algorithms, e.g., support vector machine [9], multi-layer perceptual classification [10], and artificial neural network (ANN) [11], to detect attacks on LFC systems. The major drawbacks of these techniques are the need for abundant data for training them, and their dependence on the operating point of the system.

In model-based methods, however, an observer is often designed using the mathematical model of the system to estimate state variables under normal conditions. As a result, an attack can be detected when there is a meaningful difference between the measured and the estimated states. In [12], the authors used the Kalman filter to estimate state variables of the LFC scheme and detect the attack; however, the accuracy of this static estimation can be affected by the selected threshold used to distinguish anomaly. Other well-established model-based approaches in the literature include the parametric feedback linearization using a static estimation process [13], graphical-based methods [14], chi-square detector [15], matrix separation approach [16], nonlinear observer-based methods [17], and non-stationary signal processing approach of Hilbert-Huang transform [18]. Despite the advantages of mentioned approaches for CPAs detection, e.g., real-time detection and low computational burden, they are often designed for a single time slot, i.e., operation point, not a wide range of system operation [19], [20]. Moreover, the mentioned approaches neglect the uncertainties in the operation of IMG, e.g., varying parameters, topology change owing to load disturbances, intermittent nature of RESs, and operation in islanded and grid-connected modes [21]. Additionally, the performance of these techniques depends on the accuracy of the system's mathematical model and parameters [22], [23]. In summary, the dependence on the operating point of the system, and the accuracy of the system's mathematical model are drawbacks of learning-based and model-based methods, respectively.

On the other hand, many research works have recently addressed mitigation methods of attacks targeting control or

Table I. COMPARISON WITH THE LITERATURE

	[6], [27]	[29], [30]	[8], [12], [19], [20]	[31], [32]	**Our Proposed Method**
Considering external disturbances	✓				✓
Considering parametric uncertainties		✓		✓	✓
No dependence to operating point					✓
Adaptive mitigation for different time slots					✓
Attack detection mechanism	✓	✓	✓	✓	✓
RESs participation during CPAs mitigation		✓			✓

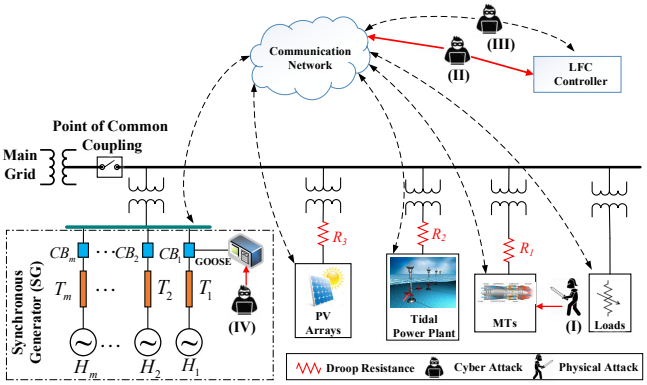


Figure 1. The diagram of cyber-physical attacks (CPAs) on the IMG.

measurement channels of LFC systems. In [24], a new virtual inertia control strategy in IMGs is introduced to alleviate the impact of the attack. Additionally, researchers in [25]–[27] deploy approaches to estimate attack vectors with the aim of removing false data from feedback control loops. These methods ignore a part of the dynamic model of systems and lead to large error signals and low performance. In this regard, the above-mentioned mitigation approaches are not suitable for the LFC model of IMGs when IMGs require high-speed performance in case of uncertainty and critical changes in system operation. Moreover, recent studies on the mitigation of attacks on LFC models cannot represent a delicate approach to alleviate the destructive impacts of attacks resulting in a change of IMG topology [28], [29].

Inspired by the above discussions, in this paper, a framework for the detection and mitigation of CPAs, which target the LFC model of IMGs, has been proposed. First, the IMG is modeled accurately, and tidal power plants (TPPs) and solar panels are used in the LFC scheme to improve the frequency excursion stems from the CPAs. Then, in the detection part of the developed framework, a well-tuned online system identification technique—which is based on the RLS-FF method—estimates the parameters of IMGs. The performance of the RLS-FF is improved by the GWO algorithm and compared with the least square (LS) method. Next, using the estimated parameters, an online anomaly-based intrusion detection system (IDS) is proposed to find CPAs in the IMG. Since the developed system identification provides the real-time parameters of the IMG, an adaptive interval type-2 fuzzy logic controller (IT2FLC) is used to mitigate CPAs that target the topology of IMG by updating control input signals. The effectiveness of the proposed framework is evaluated using real-time simulations. The contributions of this paper are:

1) Analyzing the security of the IMG in the presence of attacks targeting the topology of IMG, and investigating the potential use of DERs, i.e., TPPs and solar panels, for improving the resultant frequency deviation;
2) Developing an online anomaly-based IDS based on the RLS-FF as a well-tuned system identification approach to (i) update IMG's state matrix (A) for the adaptive control scheme and (ii) detect the impacts of attacks targeting the topology of the IMG;
3) Designing an adaptive fuzzy control mechanism along with the developed system identification technique to mitigate the impacts of CPAs that target the topology of the IMG leading to instability. The proposed framework is implemented in a real-time simulator (RTS) and its performance is compared with recent attack-resilient LFC schemes, e.g., the LQR and H_∞ control frameworks, to demonstrate its superior performance.

Generally speaking, many previous papers have focused on the behaviours of state variables and used model-based or alternatively utilized learning-based approaches to identify the type of cyber attacks which manipulate only measurement and control channels [19]–[21]. The suggested detection and mitigation methods in these works depend heavily on operating points and they are designed for a single time slot. On this basis, they cannot be practically deployed for a wide range of system operations during external uncertainties. However, in this paper, a family of malicious CPAs is introduced, whose aim is to compromise the topology of IMGs, leading to changes in the system's parameters. From this perspective, online detection and adaptive mitigation must be proposed to combat such attacks during different operating points of IMGs. To show the difference between our work and existing studies, a summarized comparison has been made in Table I. Compared to the authors' previous work [33], this manuscript fills a number of important research gaps. In [33], for the first time, a family of malicious attacks—which aim to compromise the topology of the IMG and change its parameters—were studied. It has been shown that these attacks, which change the operating point of the system, have more detrimental impacts on the system stability compared to previously-studied ones, which manipulate control commands or sensory networks. However, no mitigation mechanism was developed there to counter the attacks for different operating points [33]. Moreover, the detection mechanism proposed in [33] was only a simple proof of concept, and thus it was neither realistic nor verified using real-time simulations. Finally, the behavior of DERs following CPAs and their impact on possible countermeasures were not studied there.

The rest of the paper is organized as follows. Section II explains the physical and cyber attacks on different components of IMG. Section III represents the system modeling and LFC model of IMG. Section IV describes the online system identification and detection strategies. In the following, section V discusses adaptive mitigation for detrimental impacts of CPAs and the stability proof. Section VI depicts real-time simulation results, the impacts of concurrent CPAs on IMG' stability, and the scalability of the proposed techniques. The conclusion is drawn in Section VII.

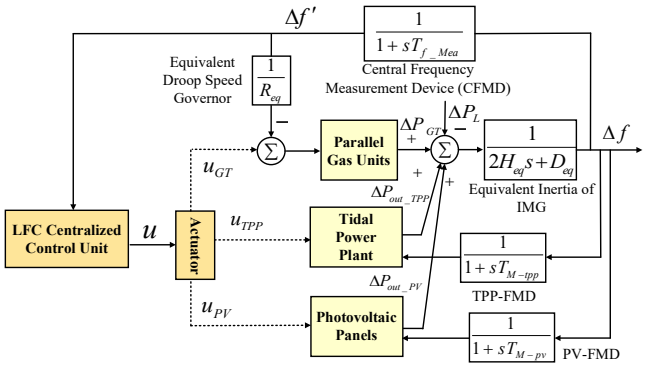


Figure 2. Load frequency control model of the IMG for CPAs studies.

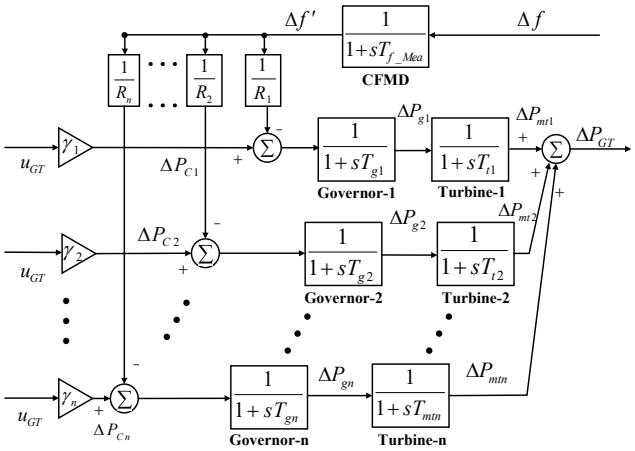


Figure 3. Dynamic model of parallel gas turbine systems

II. Threat Model

As building blocks of smart grids, IMGs can provide reliable energy production for residential/industrial customers and generate clean energy. These improvements require the deployment of extensive cyber systems and IEDs on top of the physical layers, that result in the vulnerability of IMGs to CPAs, e.g., attacks that target LFC schemes. Several examples of CPAs against the topology of LFC models, whose aims are to maliciously target the frequency stability, are demonstrated in Fig. 1, i.e., (i) Attack I: physically attack IMG generation units and eliminate them from the IMG, (ii) Attack II: compromise the communication network or LFC controller and disconnect RESs by sending false commands, (iii) Attack III: delay the measurement of the frequency response in LFC schemes, and (iv) Attack IV: target the intelligent electronic devices (IEDs) by sending trip commands to circuit breakers and disconnect their corresponding components from the IMG. These threats can be categorized into two different groups, namely, cyber and physical attacks as follows:

A. Physical Attacks

The considered threat model in this type of attack is described as follows: (i) **Attack Objective:** The aim of adversarial actions is to cause an outage of equipment, e.g., gas turbine, and create a mismatch between load demand and generation (i.e., frequency stability condition) that can cause a complete outage of loads in the IMG; (ii) **Attacker's Actions:** The adversary physically intrudes into IMG and disconnect a piece of equipment by launching deliberate physical damage; (iii) **Attacker's Knowledge:** The attacker's knowledge includes the topology of IMG and the location of DERs. The adversaries wait for the critical moment of operation, e.g., when MG supplies load variations, and then launch their attack; and (iv) **Attack Formulation:** The attack results in an outage of several droop-based generation units, i.e., units 1 to n_{out}. To fix the frequency, in normal operation, these units measure frequency and adjust their generation based on a droop gain, $R_i, \forall i \in \{1, \ldots, n\}$, where n is the number of droop-based generation units. However, under attack conditions and with the outage of units 1 to n_{out}, the equivalent droop speed governor, expressed in (1), changes and the ability of IMG to control the frequency will decrease [34]:

$$1 \Big/ R_{eq} = \sum\nolimits_{i=n_{out}}^{n} 1/R_i \tag{1}$$

B. Cyber Attacks

The cyber attacks considered in this threat model are divided into two groups, i.e., cyber attack $\mathcal{A}$ and $\mathcal{B}$. Cyber attack $\mathcal{A}$ targets the synchronous generators (SGs) aiming to disconnect them and impact the frequency stability of the LFC scheme. The cyber attack $\mathcal{B}$ focuses on adding delays to the measurements devices and feedback control loops of the LFC model with the aim of destabilizing the IMG:

1) Cyber attack $\mathcal{A}$: In attack $\mathcal{A}$, adversaries compromise the LFC controller, communication infrastructure, or IEDs associated with SGs with the aim of disconnecting them from the IMG's energy production planning. The threat model for this attack includes: (i) **Attack Objective:** The aim of adversaries is to disconnect SGs, reduce the inertia of the IMG, and create a frequency instability issue that can result in the shutdown of the IMG; (ii) **Attacker's Actions:** Attackers are entities who can inject false data into the communication links, compromised LFC controller or forward generic object-oriented substation events (GOOSE) messages based on IEC-61850 with the aim of tripping circuit breakers (CBs) associated with SGs [35]; (iii) **Attacker's Knowledge:** The adversaries have knowledge about the communication infrastructure, the protocols used to transmit the data, or the protective IEDs to craft a fake trip command; and (iv) **Attack Formulation:** The attackers aim at opening CBs of one or several SGs, i.e., units 1 to m_{out} and change the equivalent inertia constant as expressed in (2). In normal operation, having high values for H_{eq} guarantees lower variations of the frequency following any change in generation or load. However, during the mentioned attack, this value reduces and IMG can be exposed to large frequency excursions [34]:

$$H_{eq} = \sum\nolimits_{j=m_{out}}^{m} H_j$$

2) Cyber attack $\mathcal{B}$: In this attack, adversaries delay the data packets to disrupt the operation of the IMG [36]. The considered threat model includes several assumptions as follows: (i) **Attack Objective:** The main objective of adversaries is to delay the feedback loop of the LFC scheme, destabilize the frequency response, and create a complete load disconnection in the IMG; (ii) **Attacker's Actions:** Attackers penetrate into the communication infrastructure

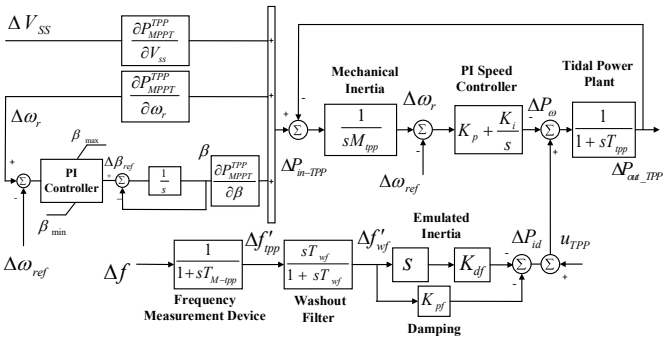


Figure 4. Load frequency control model of tidal power plant (TPP).

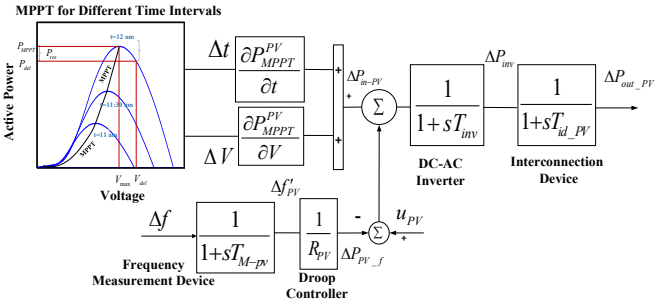


Figure 5. load frequency control model of photovoltaic panels.

of frequency measurement devices (FMDs) to prevent the LFC from receiving timely feedback signals; (iii) **Attacker's Knowledge:** The attackers should have sufficient knowledge about the communication infrastructure and protocols as well as the structure of CFMDs, and (iv) **Attack Formulation:** The adversaries adds predefined delay to the readings of the central frequency measurement device (CFMD) and consequently to the dynamic model of IMG. As a result, the dynamic model of the CFMD can be defined as follows [37]:

$$\dot{\Delta f}^{'} = \frac{1}{T_{f\_Mea}}(\Delta f - \Delta f^{'}) \tag{3}$$

where Δf and $\Delta f^{'}$ are, respectively, the real and measured frequency deviation, and T_{f_Mea} is the time constant obtained from the delay model.

III. The System Model

To have an efficient identification system for the estimation of IMG parameters and detection and mitigation of the described CPAs, the first step is to obtain the detailed LFC model of the IMG based on Fig. 2. In this layout, the IMG deploys the LFC centralized control unit which can improve the stability of the IMG by updating the control input signals of RESs, e.g., parallel gas turbines and synchronous generations, tidal power plants, and PV arrays. The linearized state-space representation of this system can be represented as:

$$\begin{cases} \dot{x}(t) = A_m x(t) + B_m u(t) + E_m w(t) \\ y(t) = C_m x(t) + D_m u(t) \end{cases} \tag{4}$$

where the vectors $x(t)$, $u(t)$, and $y(t)$ are, respectively, states, control input, and output vectors of the system. Moreover, $w(t)$ represents all disturbances and power fluctuations related to RESs. In the following, the DERs of the IMG, which play an important role in the LFC model, are studied in detail.

A. Gas Turbine System Model

The low-order model for the turbine–governor dynamics in the frequency analysis is illustrated in Fig. 3. In this figure, $T_{g1}, \ldots, T_{gn}$ are governor time constants, and $T_{t1}, \ldots, T_{tn}$ are referred to as turbine time constants. Furthermore, ΔP_g, ΔP_{mt}, and ΔP_C denote the variation of governor valve position, change in the output power of the gas turbine, and supplementary control action, respectively. $\gamma_1, \gamma_2, ..., \gamma_n$ are also defined as participation factors of gas turbines [34].

B. Tidal Power Plants Model

The LFC model of the tidal power plant is illustrated in Fig. 4. Based on this model, the integration of emulated inertia and damping coefficients are suggested to simulate virtual inertial and droop control schemes for frequency studies that is shown by the following equation:

$$\Delta P_{id} = -K_{pf}(\Delta f) - K_{df}(\frac{\partial(\Delta f)}{\partial t}) \tag{5}$$

To follow the reference tidal stream speed during transient situations, a proportional-integral (PI) speed controller is defined in this model as follows:

$$\Delta P_{\omega} = K_p\,(\Delta\omega_r - \Delta\omega_{ref}) + K_i \int (\Delta\omega_r - \Delta\omega_{ref})dt \tag{6}$$

The input active power of the proposed TPP is obtained from the maximum power point tracking (MPPT) method and depends on three components, i.e., $\partial P^{TPP}_{MPPT}/\partial\beta$, $\partial P^{TPP}_{MPPT}/\partial\omega$, and $\partial P^{TPP}_{MPPT}/\partial V_{ss}$ [38]:

$$\Delta P_{in\_TPP} = \Delta\beta\frac{\partial P^{TPP}_{MPPT}}{\partial\beta} + \Delta\omega_r\frac{\partial P^{TPP}_{MPPT}}{\partial\omega_r} + \Delta V_{ss}\frac{\partial P^{TPP}_{MPPT}}{\partial\Delta V_{ss}} \tag{7}$$

In this LFC model, $\Delta\omega_r$, β, and ΔV_{ss} denotes rotor speed deviation, pitch angle, and tidal stream speed, respectively. A high-pass washout filter is also used to remove the impacts of the high-frequency noise in the LFC studies. Furthermore, M_{tpp} and T_{tpp} are defined as the mechanical inertia of rotational masses and the time constant of TPP, respectively.

C. Photovoltaic Panels Model

The LFC model of photovoltaic panels in the under-study IMG has been illustrated in Fig. 5. Active power, which can be generated by the PV array, is defined based on the MPPT method as follows [39]:

$$\Delta P_{in-PV} = \frac{\partial P^{PV}_{MPPT}}{\partial V}\Delta V + \frac{\partial P^{PV}_{MPPT}}{\partial t}\Delta t \tag{8}$$

where two mentioned items, i.e., $\partial P^{PV}_{MPPT}/\partial V$ and $\partial P^{PV}_{MPPT}/\partial t$, can be calculated and explained in more detail in [39]. In this model, the DC-AC converter, interconnection devices, and frequency measurement device is represented by the first-order model. Droop-based model is also considered to control active power in case of LFC studies.

D. State-Space Model

The first step in obtaining the state-space representation is to define appropriate state variables based on the proposed models in section II-(A,B,C). In this regard, a set of governor valve positions ($x_g = [\,\Delta P_{g1} \quad ... \quad \Delta P_{gn}\,]$) and changes in output power ($x_{mt} = [\,\Delta P_{mt1} \quad ... \quad \Delta P_{mtn}\,]$) is defined to be independent state variables for GT systems. Moreover, state variables related to PV arrays consist of $\Delta f^{'}_{PV}$, ΔP_{inv} and ΔP_{out_PV}, which are referred to the measured frequency by FMD, the power of inverter, and the output power of PV panels, respectively. The state variables related to TPP are $\Delta f'_{tpp}$, $\Delta f'_{wf}$, $\Delta\omega_r$, ΔP_ω, and ΔP_{out_tpp}, which denote the measured frequency, filtered frequency obtained from the washout filter, the rotor speed variation, the output PI controller with the aim of tracking transient behaviours, and the output power of TPPs, respectively. All state variables can be summarized in $x(t)$ vector:

$$x(t) = [\; x_g \quad x_{mt} \quad \Delta f' \quad \Delta f'_{PV} \quad \Delta P_{inv} \quad \Delta P_{out\_PV} \; ... \\ \Delta f'_{tpp} \quad \Delta f'_{wf} \quad \Delta\omega_r \quad \Delta P_\omega \quad \Delta P_{out\_tpp} \quad \Delta f \;]^T \tag{9}$$

The LFC centralized control unit must update control signals and forward new commands to RESs during CPAs using the control input vector:

$$u(t) = [\, u_{GT} \quad u_{PV} \quad u_{TPP}\,]^T \tag{10}$$

To study the impacts of time-varying disturbances and weather changes on the performance of the IMG during CPAs, a disturbance vector $w(t)$ is also defined. This vector includes changes in solar irradiation ΔP_{in-PV}, tidal power fluctuation ΔP_{in-TPP}, and a multi-step variation of load demand ΔP_L:

$$w(t) = [\, \Delta P_{in-PV} \quad \Delta P_{in-TPP} \quad \Delta P_L\,]^T \tag{11}$$

Since CPAs introduced in the threat model, can manipulate the topologies of the IMG, finding nominal components of the state matrix, i.e. A_m is a critical issue. Since the dimension of the under-study state matrix is relatively large, this paper divides it into several sub-sections as follows:

$$A_m = \begin{bmatrix} A_{11} & A_{12} & A_{13} & A_{14} \\ A_{21} & A_{22} & A_{23} & A_{24} \\ A_{31} & A_{32} & A_{33} & A_{34} \\ A_{41} & A_{42} & A_{43} & A_{44} \end{bmatrix} \tag{12}$$

where the first row of this matrix, i.e. $A_{11}, A_{12}, A_{13}, A_{14}$ is related to gas turbine systems used in the IMG that includes system parameters as follows:

$$A_{11} = A_{GT}, A_{12} = 0_{(2n+1)\times 3}, A_{13} = 0_{(2n+1)\times 5}, ... \\ A_{14} = [\, 0_{1\times 2n} \quad 1/T_{f\_Mea}\,]^T \tag{13}$$

$$A_{GT} = \begin{bmatrix} \eta_{11} & \eta_{12} & \eta_{13} \\ \eta_{21} & \eta_{22} & \eta_{23} \\ \eta_{31} & \eta_{32} & \eta_{33} \end{bmatrix} \tag{14}$$

where A_{GT} is one of the elements of matrix A_m that consist of information of parallel GTs including droop speed gain R_i, turbine time constant T_{ti}, and governor time constant T_{gi}:

$$\eta_{11} = diag[\; -1/T_{g1} \quad ... \quad -1/T_{gn} \;], \eta_{12} = 0_{n\times n}, ... \\ \eta_{13} = [\; -1/T_{g1}R_1 \quad -1/T_{g2}R_2 \quad ... \quad -1/T_{gn}R_n \;]^T \tag{15}$$

$$\eta_{21} = diag[\; 1/T_{t1} \quad ... \quad 1/T_{tn} \;], \eta_{22} = -\eta_{21}, \eta_{23} = 0_{n\times 1} \tag{16}$$

$$\eta_{31} = \eta_{32} = 0_{1\times n}, \eta_{33} = [-1/T_{f\_Mea}] \tag{17}$$

The second row of the state matrix is the interaction between PV arrays and other sections of the IMG. $A_{22} = A_{PV}$ is a PV element that describes the dynamic model of solar panels. T_{M-pv}, T_{inv}, and T_{id_PV} are the time constant of PV-FMD, inverter, and interconnection device, respectively:

$$A_{21} = 0_{3\times(2n+1)}, A_{22} = A_{PV}, A_{23} = 0_{3\times 5}, ... \\ A_{24} = [\, 1/T_{M-pv} \quad 0 \quad 0\,]^T \tag{18}$$

$$A_{PV} = \begin{bmatrix} -1/T_{M-pv} & 0 & 0 \\ -1/R_{PV}T_{inv} & -1/T_{inv} & 0 \\ 0 & 1/T_{id\_PV} & -1/T_{id\_PV} \end{bmatrix} \tag{19}$$

The third row of the state matrix is allocated to the TPP and interaction with other energy sources. Similar to the previous description, $A_{33} = A_{TPP}$ is a sub-section that represents the parameters of the TPP. T_{M-tpp}, T_{wf}, M_{tpp}, and T_{tpp} are the time constant of TPP-FMD, the time constant of washout filter, mechanical inertia of rotational masses, and time constant of TPP unit, respectively. Moreover, K_{pf} and K_{df} are referred to as the extra damping and the extra inertia of TPPs:

$$A_{31} = 0_{5\times(2n+1)}, A_{32} = 0_{5\times 3}, A_{33} = A_{TPP}, ... \\ A_{34} = [\, 1/T_{M-tpp} \quad 1/T_{M-tpp} \quad 0 \quad 0 \quad -K_{df}/T_{ttp}T_{M-tpp}\,]^T \tag{20}$$

$$A_{TPP} = \begin{bmatrix} \frac{-1}{T_{M-tpp}} & 0 & 0 & 0 & 0 \\ \frac{-1}{T_{M-tpp}} & \frac{-1}{T_{wf}} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{-1}{M_{tpp}} \\ 0 & 0 & K_i & 0 & \frac{-K_p}{M_{tpp}} \\ \frac{K_{df}}{T_{M-tpp}T_{tpp}} & \frac{(K_{df}-K_{pf}T_{wf})}{T_{wf}T_{tpp}} & 0 & \frac{-1}{T_{tpp}} & \frac{-1}{T_{tpp}} \end{bmatrix} \tag{21}$$

Finally, the fourth row of A_m is considered to depict the equivalent inertia (H_{eq}) of the IMG and equivalent load damping coefficient (D_{eq}):

$$A_{41} = [\; 0_{1\times n} \quad [\; 1/2H_{eq} \quad ... \quad 1/2H_{eq} \;]_{1\times n} \quad 0 \;], ... \\ A_{42} = [\; 0 \quad 0 \quad 1/2H_{eq} \;], ... \\ A_{43} = [\; 0 \quad 0 \quad 0 \quad 0 \quad 1/2H_{eq} \;], A_{44} = -D_{eq}/2H_{eq} \tag{22}$$

The control input matrix (B_m) includes three elements, i.e., B_{11}, B_{21}, and B_{31}, for GTs, PV, and TPP, respectively, as well as a zero element B_{41}, which can be expressed as follows:

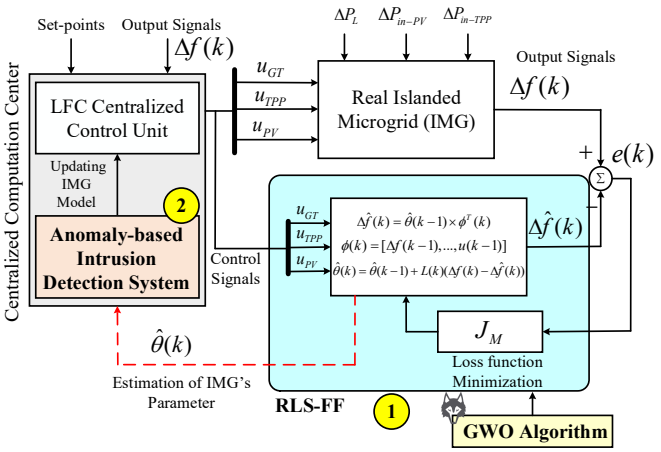


Figure 6. Collaboration between online system identification and adaptive mitigation schemes.

$$B_m = [\ B_{11} \quad B_{21} \quad B_{31} \quad B_{41}\ ]^T \tag{23}$$

$$B_{11} = B_{GT}, B_{21} = B_{PV}, B_{31} = B_{TPP}, B_{41} = 0_{1\times 3} \tag{24}$$

$$B_{GT} = \begin{bmatrix} [\ \gamma_1/T_{g1} \quad \gamma_2/T_{g2} \quad \dots \quad \gamma_n/T_{gn}\ ] & 0_{1\times(n+1)} \\ 0_{2\times n} & 0_{2\times(n+1)} \end{bmatrix}^T \tag{25}$$

$$B_{PV} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1/T_{inv} & 0 \\ 0 & 0 & 0 \end{bmatrix} B_{TPP} = \begin{bmatrix} 0_{4\times 3} \\ [0 \quad 0 \quad 1/T_{tpp}] \end{bmatrix} \tag{26}$$

Moreover, the disturbance matrix (E_m), which provides coefficients for load changes, TPP fluctuation, and variation in solar radiation, is represented by four elements as follows:

$$E_m = [\ E_{11} \quad E_{21} \quad E_{31} \quad E_{41}\ ]^T \tag{27}$$

$$\begin{gathered} E_{11} = 0_{(2n+1)\times 3}, E_{21} = E_{PV}, E_{31} = E_{TPP}, \dots \\ E_{41} = [0 \quad 0 \quad 1/2H_{eq}] \end{gathered} \tag{28}$$

$$E_{PV} = \begin{bmatrix} 0 & 0 & 0 \\ 1/T_{inv} & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad E_{TPP} = \begin{bmatrix} 0_{2\times 3} \\ [0 \quad 1/M_{tpp} \quad 0] \\ [0 \quad K_p/M_{tpp} \quad 0] \\ 0_{1\times 3} \end{bmatrix} \tag{29}$$

Eventually, the output matrix (C_m) and the feed-forward matrix (D_m) is defined as:

$$C_m = [0_{1\times(2n+9)} \quad 1], \quad D_m = 0_{1\times 3} \tag{30}$$

IV. Detection Strategy

The overall layout of the online detection and mitigation has been illustrated in Fig. 6. The detection scheme consists of two different steps. First, the RLS-FF approach is developed for the online estimation of the parameters of the IMG. To improve the performance of the RLS-FF method in the estimation of the IMG's parameter, the GWO algorithm is also implemented offline by optimizing the amount of the forgetting factor, the covariance matrix, and the reset parameter of the RLS-FF approach (Step 1 in Fig. 6). Collaboration between the RLS-FF and GWO algorithm can be defined as online system identification. Then, the estimation of the parameters of the IMG is sent to the anomaly-based IDS and compared with the nominal values of the system's parameters to identify the attack on the different components of the IMG (Step 2 in Fig. the LFC centralized controller unit updates control input signals at each time index based on the estimated parameters of the IMG and keeps the frequency response in the permissible range during different CPAs.

A. Background to Recursive Least Square Method with Forgetting Factor

During the normal operation of IMGs, the system's state matrix $A(k)$ at time index k remains generally constant. However, there are the attacks proposed in the threat model (Section II) that target the topology of the IMG, i.e., elements of the matrix $A(k)$, leading to the frequency deviation. To follow the changes of $A(k)$, the RLS-FF is customized to estimate elements of the state matrix of the IMG. Compared to the frequent least square (LS) methods [40], the RLS-FF can provide an online accurate estimation of system parameters to update control input signals. Based on the proposed scheme in Fig. 6, the control input signals, i.e., $u_{GT}(k), u_{TPP}(k)$, and $u_{PV}(k)$, are consequently updated, and then used to calculate parameters of the IMG. Additionally, to study the impacts of external disturbances, three terms, i.e., ΔP_L, ΔP_{in-TPP}, and ΔP_{in-PV}, are added to the IMG. At each time index k, the transfer function of the system is firstly calculated by the following equation [41]:

$$\frac{\Delta f(k)}{u(k)} = \frac{b_1 z^{-1} + b_2 z^{-2} + \dots + b_p z^{-p}}{1 + a_1 z^{-1} + a_2 z^{-2} + \dots + a_q z^{-q}} \tag{31}$$

where $\Delta f(k)$ and $u(k)$ are defined as the IMG output and control input signals at time index k, respectively. The $b_1, b_2, \dots b_p, a_1, a_2, \dots a_q$ are referred to as elements of the system parameters vector. Additionally, p and q are real numbers and z is a forward shift operator in z-domain transformation. Equation 31 is rewritten in the form of a matrix according to two following expressions:

$$\Delta f(k) + \sum_{i=1}^{q} a_i \Delta f(k-i) = \sum_{j=1}^{p} b_i u(k-j) \tag{32}$$

$$\Delta f(k) = \theta(k) \times \phi^T(k) \tag{33}$$

where $\theta(k) = [-a_1, ..., -a_q, b_1, ..., b_p]$ is the nominal parameter vector at time index k, and $\phi^T(k)$ is defined as the transpose of the regression vector:

$$\phi(k) = [\Delta f(k-1), ..., \Delta f(k-q), u(k-1), ..., u(k-p)] \tag{34}$$

This regression vector is computed by the use of measured control inputs and outputs of IMG. Since the main aim of the proposed RLS-FF method is to estimate IMG parameters, it is more efficient to have a recursively updated estimation. As a result, an error signal $(e(k) = \Delta f(k) - \Delta\hat{f}(k))$, which measures the difference between estimated and true values of the output signal at time index k, is updated consecutively to converge estimation of IMG's parameters to their true values using the minimization of the loss-function (J_M) as follows:

$$J_M = \sum_{\tau=1}^{k} \lambda^{k-\tau} e^2(\tau) \tag{35}$$

where λ is a forgetting factor that improves the speed of convergence, and $e(\tau)$ is the error signal. This loss function ignores the old measurements exponentially. In this regard, an observation related to t old samples has a λ^t times weighted compared to recent observations. Minimization of J_M results in a gain matrix, i.e., $L(k)$, that can update the estimation of parameters vector $(\hat{\theta}(k))$, as follows:

$$\hat{\theta}(k) = \hat{\theta}(k-1) + L(k)(\Delta f(k) - \Delta\hat{f}(k)) \tag{36}$$

The value of $L(k)$ at time index (k) can be updated based on the following statement:

$$L(k) = \phi(k) \times \frac{P(k-1)}{\lambda + \phi^T(k)P(k-1)\phi(k)} \tag{37}$$

where $P(k)$ and $P(k-1)$ are defined as the covariance matrix of the estimated parameters at time indexes k and $k-1$, respectively. This matrix can be recursively obtained as:

$$P(k) = \frac{P(k-1)}{\lambda}[I - L(k)\phi^T(k)] \tag{38}$$

To calculate the $P(k)$ matrix, the gain matrix $L(k)$ is firstly updated at each time index using 37. The performance of the RLS-FF method during the estimation of IMG parameters is related to initial values of (i) system parameters (θ_0), (ii) the covariance matrix (P_0), and (iii) the forgetting factor (λ_0) that can be optimally obtained using the GWO algorithm.

B. Grey Wolf Optimization Algorithm

Since the initialization of the RLS-FF parameters can dramatically impact the convergence speed and accuracy of the proposed detection method, this paper utilizes the grey wolf optimization (GWO) algorithm due to its superior convergence speed and acceptable performance in unknown research space [42]. The evaluation criteria as objective function and optimization variables need to be first defined for the GWO algorithm: (i) the ability to follow initial values of IMG parameters by an initial tracking time (t_0), (ii) the capability to estimate system parameters during a proposed time interval by average estimation time (t_s), (iii) presenting a measure of method performance by integrating the absolute error over a fixed interval, i.e. the integral absolute error (IAE), and (iv) proposing another measure by integrating the square of the error over a fixed interval, i.e., the integral square error (ISE). By deployment of the GWO algorithm, initial values of the forgetting factor (λ_0) and the covariance matrix are tuned offline. Given $P_0 = \sigma_0 I$ as the standard form of the initial covariance matrix, σ_0 is used in the initialization process in this paper. Furthermore, a reset parameter Cov is defined to update the initial value of the covariance matrix after specific iterations in the case of an online estimation process. If Cov is equal to 1, it means that this matrix is returned to its initial value, whereas if Cov is 0, no return to the initial value is considered. Therefore, in the offline process, the variable vector of the optimization algorithm can consider an agent with three-dimension including the initial values of λ_0, σ_0, and Cov and obtain optimal values.

Algorithm 1: System Identification for Estimation of IMG's Parameters

Inputs: Input signal vector $u(t)$ and output signal vector (Δf) ;
Output: Estimation of IMG's parameter vector,$\hat{\theta}(k)$, at time index k ;
1) Initialize: P_0, λ_0, Cov and θ_0 by GWO algorithm;
2) Initialize: θ_0 by Operator;
3) Select: Sampling time (T_s);
4) Measure: Initial values of input and output signals $(\Delta f(k), u(k))$;
5) Calculate: Regression vector $(\phi^T(k))$;
6) Calculate: $\Delta\hat{f}(k) = \hat{\theta}(k-1) \times \phi^T(k)$;
7) Calculate: Error signal: $e(k) = \Delta f(k) - \Delta\hat{f}(k)$;
8) Minimize: J_M loss function;
9) Obtain: Gain matrix $L(k)$;
10) Estimate: IMG's parameters vector:
$\hat{\theta}(k) = \hat{\theta}(k-1) + L(k)(\Delta f(k) - \Delta\hat{f}(k))$;
11) Update: Covariance matrix $P(k)$;
for *k=1:1: [Time Interval]/ T_s* **do**
  Update $e(k) = \Delta f(k) - \Delta\hat{f}(k)$;
  Update $L(k)$;
  Calculate $\hat{\theta}(k) = \hat{\theta}(k-1) + L(k)(\Delta f(k) - \Delta\hat{f}(k))$;
  Update $P(k)$;
  Save estimation of IMG parameters $(\hat{\theta}(k))$ in the Centralized Computation Center;
end

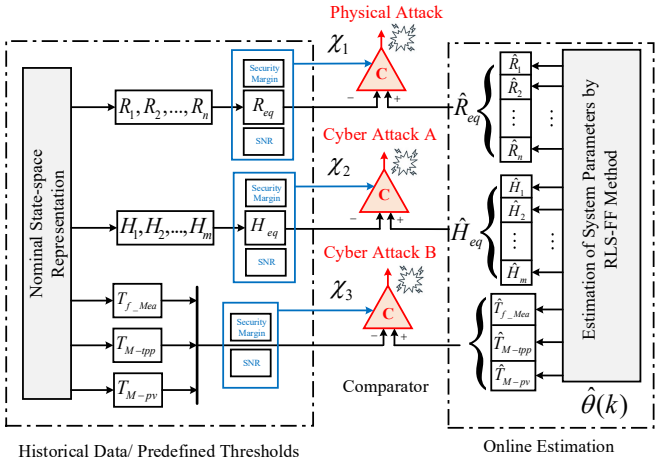


Figure 7. Anomaly-based intrusion detection system (IDS) in centralized computation center.

Algorithm 2: Anolmaly-based Intrusion Detection System

Inputs: Estimation of parameter vector $\hat{\theta}(k)$;
Output: S_0 or S_1 as indicator for attack detection ;
Location of IDS: At centralized computation center;

while *Measure input and output signals* **do**
  Define different thresholds: $\{\chi_1, \chi_2, ...\chi_n\}$ based on SM (%) and SNR (dB) for each IMG's parameter ;
  Calculate $r_{s1}(k) = \hat{R}_{eq} - R_{eq}$;
  Calculate $r_{s2}(k) = \hat{H}_{eq} - H_{eq}$;
  Calculate $r_{s3}(k) = \hat{T}_{f\_Mea} - T_{f\_Mea}$;
  if $r_s(k) > \chi$ **then**
    Attack detection and alarm activation $\Rightarrow S_1$;
    if $r_s(k) \leq \chi$ **then**
      Display normal operation and no attack $\Rightarrow S_0$;
    end
  end
end

The design parameters of the GWO algorithm, i.e., the minimum and maximum values of λ_0 and σ_0, are considered to be 0.4, 1×10^3, 1, and 1×10^{30}, respectively. The value of Cov. is a binary number. i.e., 0 or 1, and the number of iterations is 1000. The number of search agents for this problem is 200.

C. Online Anomaly-based Intrusion Detection System (IDS)

The recursive method and offline optimization process are under the umbrella of the online estimation of the IMG parameters, which can be carried out by using the pseudo-code of Algorithm 1. Fig. 7 illustrates the platform of the proposed anomaly-based intrusion detection system (IDS), which is installed in the centralized computation center of the IMG. First, acceptable ranges for the parameters of IMG, which may be targeted based on the threat model, must be defined in the strict sense. In this regard, during normal operation of the IMG, a noise is modeled as independent, white, and Gaussian, with a signal-to-noise ratio (SNR) based on dB for system parameters. Moreover, a security margin (SM) is also added to these system parameters to model parametric uncertainties in the IMG operation. Any deviation from the assumed acceptable ranges can be introduced as suspicious activity, which could trigger system alarms. For instance, to detect the occurrence of the physical attack on the equivalent droop speed governor of gas turbines (R_{eq}),

Table II. THE FUZZY RULE BASE USED FOR UPPER AND LOWER MEMBERSHIP FUNCTIONS

Δf \ $\Delta f/\Delta t$	LN	MN	SN	ZO	SP	MP	LP
LN	LP	LP	LP	MP	MP	SP	ZO
MN	LP	MP	MP	MP	SP	ZO	SN
SN	LP	MP	SP	SP	ZO	SN	MN
ZO	MP	MP	SP	ZO	SN	MN	MN
SP	MP	SP	ZO	SN	SN	MN	LN
MP	SP	ZO	SN	MN	MN	MN	LN
LP	ZO	SN	MN	MN	LN	LN	LN

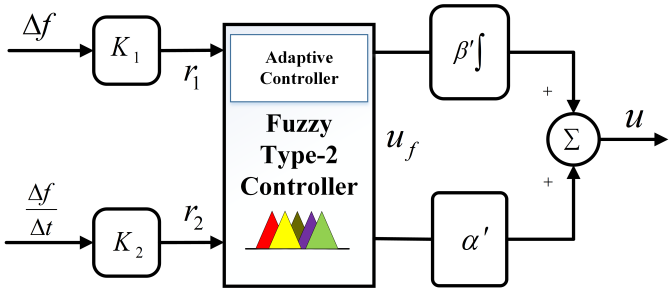


Figure 8. Layout of proposed interval type-2 fuzzy logic controller.

a conventional detector is proposed. One detector, which can take advantage of a residual signal, can be calculated as:

$$r_s(k) = |\hat{R}_{eq}(k) - R_{eq}(k)| \tag{39}$$

where $\hat{R}_{eq}(k)$ is defined as the online estimation of equivalent droop of governor at time index k, and $R_{eq}(k)$ is referred to as the nominal value of this parameter. A comparator identifies the occurrence of an attack by comparison of $r_s(k)$ with a predetermined threshold (χ), which is a function of a predefined security margin and noise. The main rule of this detector in the centralized computation center is defined as:

$$\begin{cases} if: r_s(k) \le \chi(SM, SNR) \Rightarrow S_0 \\ if: r_s(k) > \chi(SM, SNR) \Rightarrow S_1 \end{cases} \tag{40}$$

where the indicator S_0 depicts the normal operation of the IMG and the indicator S_1 informs operators about the occurrence of an attack that disturbs the physical performance of the speed governor. The performance of this anomaly-based IDS with the help of the proposed system identification is summarized in Algorithm 2. After each estimation of parameters, the centralized computation center is notified of this new estimation and updates its control input vectors.

V. MITIGATION STRATEGY

A. Designing Interval Fuzzy Logic Controller

In this section, an adaptive framework is developed to mitigate the detrimental impacts of CPAs introduced in the threat model. Moreover, a comparison between recent techniques, like type-1 fuzzy logic controller, Linear Quadratic Regulator (LQR) [6], [29], and H_∞ resilient control scheme [31], [32] is carried out. Based on the proposed scheme of IT2FLC in Fig. 8, a fuzzifier section is deployed to map input signals, i.e., Δf and $\Delta f/\Delta t$. The output signal (u_f) of this controller is able to keep an optimum balance between generation and demand. Additionally, in this IMG, the Mamdani-type inference system is developed and 7-segments triangular shapes, i.e. LN (Large negative), MN (medium negative), SN (small negative), ZO (Zero), SP (small positive), MP (medium positive), and LP (large positive) are allocated to both lower and upper membership functions (MFs). A set of rules that consist of 49 fuzzy maps the input signals to the output signal which has been presented in Table II.

B. Stability Proof of Proposed Controller

In the proposed IT2FLC, patterns of rules are represented based on the following statement [43]:

$Rules\{1, 2, ...s\}$: IF r_1 is $\tilde{A}_{s1}$ and r_2 is $\tilde{A}_{s2}$, THEN $u_f = W$. where $\tilde{A}_{s1}$ is the type-II MFs for the first input signal (Δf) and $\tilde{A}_{s2}$ for the second input signal $(\Delta f/\Delta t)$. Furthermore, $W = [W_1 \quad W_2 \quad ... \quad W_s]$ is defined as a set of consequent parameters related to type-2 MFs which are depicted through centroid representation method. To show the IMG stability, the output of this controller can be summarized as follows:

$$u_f = \sum_{l=1}^{l=s} W_l(\overline{f}^l + \underline{f}^l) \Big/ \sum_{l=1}^{l=s} (\overline{f}^l + \underline{f}^l) = W^T\psi \tag{41}$$

In 41, $\overline{f}^l = \overline{\mu}^{s1}(r_1) \cap \overline{\mu}^{s2}(r_2)$ and $\underline{f}^l = \underline{\mu}^{s1}(r_1) \cap \underline{\mu}^{s2}(r_2)$ are referred to as lower and upper firing strength of rule-s that is an intersection of the first input r_1 and second input r_2 of the controller. In this equation, $\overline{\mu}$ and $\underline{\mu}$ are also defined as the lower and upper bounds of MFs, respectively. To summarise all fuzzy rules, the vector ψ is defined as well. In the under-study IMG, the main aim is to mitigate the frequency deviation during changes in the IMG's topology. On this basis, an adaptive mechanism is added to the IT2FLC that can improve the performance of the closed-loop stability of the IMG. To prove the stability of this controller in the platform of the IMG, a Lyapunov function can be defined as follows:

$$V(t) = \frac{1}{2}[\varepsilon^2 + \frac{1}{\kappa_1}(\alpha^* - \alpha')^2 + \frac{1}{\kappa_2}(\beta^* - \beta')^2] \tag{42}$$

where $\varepsilon(t) = y_0(t) - y(t) = \Delta f_0 - \Delta f$, and α' and β' are output scaling factors. Besides, α^* and β^* are defined as the optimal values of α' and β', respectively. Adaptation laws for mentioned parameters and the set of consequent parameters are defined:

$$\dot{\alpha}'(t) = \kappa_1\varepsilon J\dot{u}_f, \dot{\beta}'(t) = \kappa_2\varepsilon J u_f, \dot{W}(t) = -a_0 W + \psi/\|\psi\|^2 \varepsilon J u_f \tag{43}$$

where $J = \partial y/\partial u$ is an approximation of the Jacobean matrix which can be calculated to obtain the sensitivity of the under-study IMG based on adaptation laws [44]. The Lyapunov function can be differentiated as follows:

$$\dot{V}(t) = \varepsilon\dot{\varepsilon} - \frac{1}{\kappa_1}(\alpha^* - \alpha')\dot{\alpha}'(t) - \frac{1}{\kappa_2}(\beta^* - \beta')\dot{\beta}'(t) \tag{44}$$

$$\dot{\varepsilon} = \frac{\partial\varepsilon}{\partial t} = \frac{\partial\varepsilon}{\partial y}\frac{\partial y}{\partial u}\left(\frac{\partial u}{\partial u_f}\frac{\partial u_f}{\partial t} + \frac{\partial u}{\partial(\int u_f dt)}\frac{\partial(\int u_f dt)}{\partial t}\right) = -J(\alpha'\dot{u}_f + \beta' u_f) \tag{45}$$

If 45 is substituted into the time derivative of the Lyapunov function, we will have:

$$\dot{V}(t) = -\varepsilon J(\alpha'\dot{u}_f + \beta' u_f) - \frac{1}{\kappa_1}(\alpha^* - \alpha')\dot{\alpha}'(t) - \frac{1}{\kappa_2}(\beta^* - \beta')\dot{\beta}'(t) \tag{46}$$

With the aim of two adaptation laws in

$$\dot{V}(t) = -\varepsilon J(\alpha^*\dot{u}_f + \beta^* u_f) \tag{47}$$

According to the adaptive mechanism, the consequent parameters of MFs are adjustable; consequently, the derivative of output of the IT2FLC (u_f) can be estimated as:

$$\dot{u}_f \approx \dot{W}^T\psi \tag{48}$$

By taking into account 47 and 48, we have:

$$\dot{V}(t) = -\varepsilon J(\alpha^*\dot{W}^T\psi + \beta^* W^T\psi) \tag{49}$$

In 43, $a_0 = \beta^*/\alpha^*$ is firstly assumed, and then, the last adaptation law is replaced in 49. The final equation is obtained which shows the stability of this closed-loop IMG system:

Table III. NOMINAL VALUES OF IMG'S PARAMETERS

Parameter	Value	Parameter	Value
D_{eq}	0.015	K_i	0.15
H_{eq}	0.1667	K_{df}	0.2
R_{eq}	0.565	K_{pf}	2
T_{f_Mea}	0.02	T_{wf}	6
T_{gi}	0.4	T_{M-tpp}	0.02
T_{ti}	0.08	T_{id_PV}	0.004
$\gamma_1 \dots \gamma_5$	1	T_{inv}	0.04
T_{tpp}	0.2	R_{PV}	0.25
M_{tpp}	0.3878	T_{M-pv}	0.022
K_p	1.5	Δf_0	60

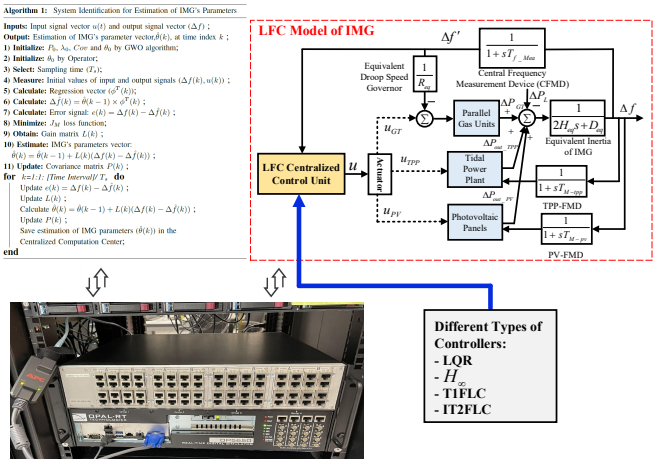


Figure 9. Real-time experimental setup of IMG and the proposed RLS-FF system identification and well-known attack-resilient LFC frameworks.

$$\dot{V}(t) = -\varepsilon^2 J^2 < 0 \tag{50}$$

To show how this IT2FLC works in the case of proposed CPAs in the threat model, Algorithm 3 is developed.

Algorithm 3: Adaptive Fussy Type-2 Mitigation Startegy

Input: Estimated parameter vector, $\hat{\theta}(k)$, at time index k ;
Output: Control input signals u_{GT}, u_{TPP}, and u_{PV} at time index k ;
1) **Save:** $\hat{\theta}(k)$ in centralized computation center ;
2) **Update:** Parameters of IMG, $\{R_{eq}$, H_{eq}, T_{f_Mea} and ...$\}$;
3) **Define:** 7-segment triangle MFs and 49 fuzzy rules based on Table II;
4) **Recieve:** Δf and $(\Delta f/\Delta t)$ at each time index k ;
5) **Start:** Adaptive fuzzy control mechanism;
for $k = 1 : 1 :$ *[time interval]*$/ T_s$ **do**
  Initiate: $\{K_1, K_2, \alpha', \beta'\}$ based on Lyapunov function $V(t)$;
  Calculate: $\varepsilon(t) = \Delta f_0 - \Delta f$;
  Update: Patterns of 7-Triangles MFs ;
  Minimize: $\varepsilon(t)$ based on 7-Triangle MFs ;
  Update: u_{GT}, u_{TPP}, and u_{PV} at time index k.
end

VI. RESULTS AND DISCUSSION

This section evaluates the collaboration between the proposed system identification and adaptive mitigation schemes under different attack scenarios by real-time simulations, whose framework is shown in Fig. 9. This framework consists of OPAL-RT-5650 as a real-time simulator (RTS) with the aim of simulating components of the IMG, system identification methods to estimate the IMG parameters, and the proposed adaptive control mechanism to update control input signals for RESs. The time step for this framework is set to 0.05 s. To build up this framework, first, the IMG model is implemented

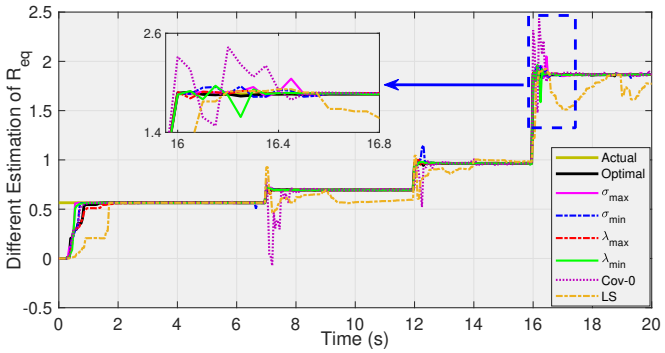


Figure 10. Online estimation of equivalent droop speed governor (R_{eq}).

Table IV. EVALUATION OF PROPOSED ESTIMATION METHOD FOR R_{eq}.

λ_0	σ_0	Cov	t_0	t_s	IAE	ISE
0.6911	1.75×10^{8}	1	1.35	0.3	2.3×10^{-2}	1.79×10^{-4}
1.0	1.75×10^{8}	1	1.9	0.3	3.6×10^{-2}	8.13×10^{-4}
0.4	1.75×10^{8}	1	0.75	0.3	5.2×10^{-2}	5.09×10^{-3}
0.6911	1.0×10^{30}	1	0.55	1.36	5.7×10^{-2}	2.58×10^{-3}
0.6911	1.0×10^{3}	1	0.75	1.2	6.3×10^{-2}	4.78×10^{-3}
0.6911	1.75×10^{8}	0	0.95	N.A.	5.0×10^{-1}	1.82×10^{-1}

in RT-LAB software, and several subsystems, including computation and graphical user interface (GUI), are allocated to different cores of the RTS. These subsystems are converted to **C** program and loaded on this equipment. Finally, the proposed system identification and adaptive mitigation strategies are simulated in the RTS, and results are shown.The numeral parameters of the IMG are represented in Table IV [45]. Additionally, the IMG consists of five GT units with the droop coefficient value of $R_1 = 2$ pu.s, $R_2 = 3$ pu.s, $R_3 = 3.5$ pu.s, $R_4 = 2.5$ pu.s, and $R_5 = 4$ pu.s, respectively. In line with the threat model elaborated in Section II, three attack scenarios are introduced as follows:

Scenario I (physical attack on GTs): The attacker consecutively targets GTs considering a stealthy manner that induces the outage of R_2, R_4, and R_1 at $t = 7s$, $t = 12s$, and $t = 16s$, respectively.

Scenario II (cyber attack $\mathcal{A}$, attack on the circuit breaker (CB) of synchronous generators (SGs)): In this scenario, the attacker compromises the CB of SGs consecutively and changes the equivalent inertia constant of the IMG at $t = 6s$, $t = 9s$, and $t = 16s$ in a stealthy manner to create oscillatory frequency response leading to severe damage to residential and industrial loads and the early aging of electric machines.

Scenario III (cyber attack $\mathcal{B}$, time delay on CFMD): The attacker targets the CFMD and increases the related time constant (T_{f_Mea}) from its nominal value during three steps at $t = 5s$, $t = 11s$, and $t = 17s$.

A. Performance of Proposed System Identification

Before discussing anomaly-based IDS, the superiority of the RLS-FF approach is investigated. In Scenario I, a physical attack is launched to manipulate gas turbine generators, leading to variations in the equivalent droop speed governor (R_{eq}) used in the physical layer of the IMG. Considering initial values of $R_1 \dots R_5$, the equivalent droop speed governor is calculated by 1 as $R_{eq} = 0.565$. Based on the threat model, attackers can target GTs by the outage of R_2 at $t = 7s$, R_4 at $t = 12s$, and R_1 at $t = 16s$, respectively. Fig. 10 shows the variation of this parameter, which has changed from 0.565 to 1.866 during 3 steps. During such an attack on the IMG, the main aim of the RLS-FF approach is to estimate this variation and provide enough information for LFC centralized control unit to stabilize the IMG after any changes in IMG's topology. To improve the performance of the estimation process, the selection of λ_0, σ_0,

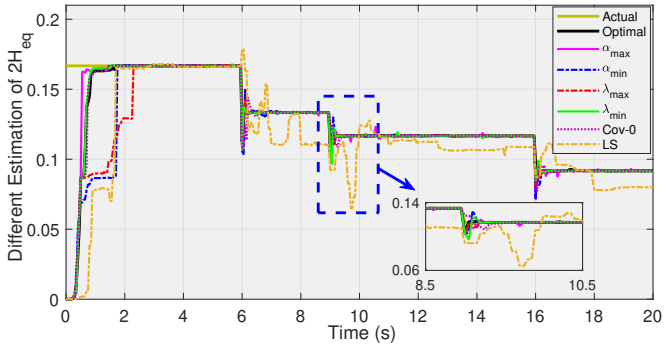


Figure 11. Online estimation of equivalent inertia constant (H_{eq}).

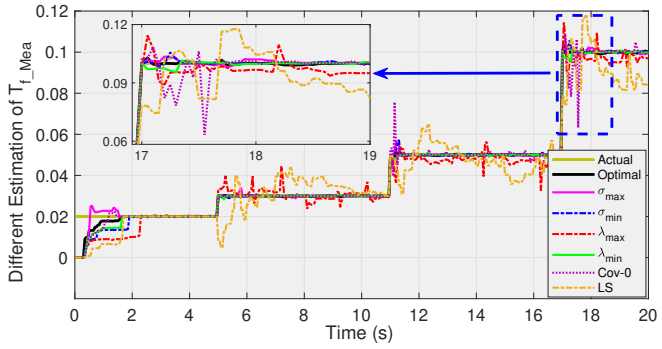
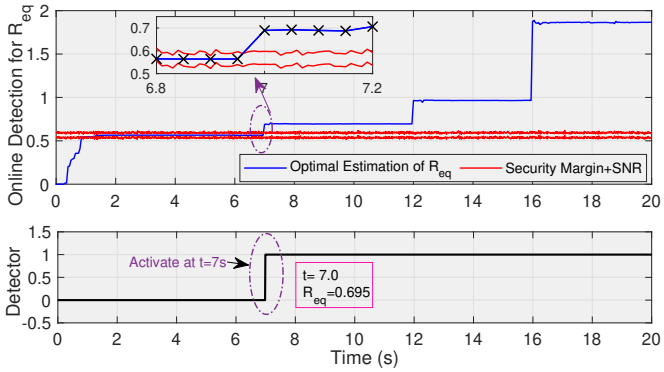
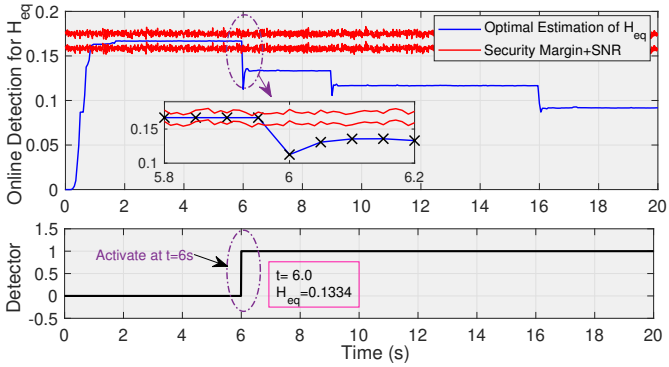


Figure 12. Online estimation of time constant for CFMD (T_{f_Mea}).

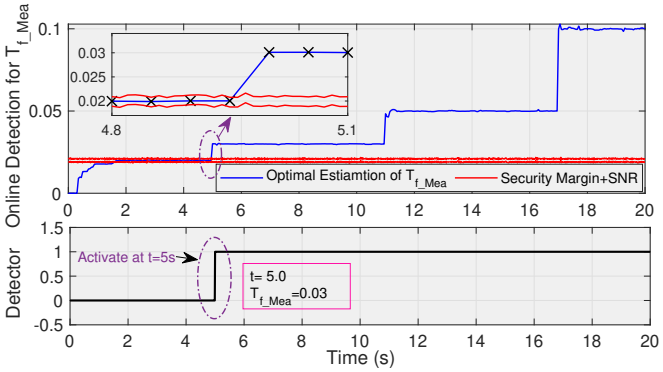
and Cov is carried out by the GWO. The impacts of different values of λ_0, σ_0, and Cov on the estimation of R_{eq} have been illustrated in Fig. 10. The results of the least square (LS) method, which is known as a non-recursive identification approach [40], have been also shown. It is clear that the recursive feature yields more acceptable performance in the estimation of R_{eq}. In brief, collected results are listed as six modes for each system parameter in Table IV. According to these results, different estimations of R_{eq} are acquired by selecting the minimum, maximum, or optimal values of λ_0, σ_0, and Cov in the recursive method. However, to have the best estimation performance, optimal values of λ_0, σ_0, and Cov are suggested to be 0.6916, 1.75×10^8, and 1, respectively, through the GWO algorithm. In the optimal mode of estimation, IAE and ISE have less amount of error compared to the other 5 modes. In the optimal mode, the initial tracking time (t_0) and the average estimation time (t_s) for R_{eq} are $1.35s$ and $0.3s$, respectively. Moreover, the average estimation time cannot be obtained for one mode during the estimation of R_{eq} in the case of $Cov = 0$. The main reason is that the RLS-FF method is not able to follow the variation of this parameter due to improper selection of the Cov parameter that is depicted as not applicable $(N.A.)$ in Table IV. Before launching the attack of Scenario II, the nominal value of H_{eq} is first considered to be 0.1667 under normal operations of the IMG. In Scenario II, it is assumed that the attack must be stealthy and the attacker starts manipulating the CBs of SGs one after another, removing them and reducing the equivalent inertia constant to 0.1334 at $t = 6s$. Afterward, the attacker targets several CBs at $t = 9s$ and $t = 16$ which leads to a reduction of this value to 0.1167 and 0.0917 during 2 steps, respectively. The variation of H_{eq} and the performance of the RLS-FF approach in estimating this variable is illustrated in Fig. 11. In scenario III, the attacker increases the nominal value of this time constant from 0.02 to 0.03 at $t = 5s$. Then, this time constant will rise to 0.05 at $t = 11s$, and the last change occurs at $t = 17s$ during this period as shown in Fig. 12. Real-time simulations show that the RLS-FF method can estimate changes of T_{f_Mea} accurately compared to the LS method.



(a)



(b)



(c)

Figure 13. Online anomaly-based intrusion detection system for (a) physical attack on (R_{eq}), (b) cyber attack on equivalent inertia constant (H_{eq}), (c) cyber attack on the time constant of CFMD (T_{f_Mea}).

B. Online Detection

To evaluate the performance of the proposed anomaly-based IDS, the physical attack in Scenario I is first implemented. Based on Fig. 13-(a), the estimated value of $R_{eq}(k)$ is compared to a predefined threshold (χ_1). This (χ_1) is a function of two items: (i) a $\pm 5\%$ security margin for the nominal value of $R_{eq}(k)$ and (ii) $25dB$ SNR that is added to the nominal value of $(R_{eq}(k))$. Any deviation more than the permissible range can trigger the comparator leading to anomaly notification in the IMG. This online detector is able to trigger the alarm at $t = 7s$ when the first estimated sample of $R_{eq}(k)$ goes over the predefined limits shown by two parallel lines and reaches 0.695. To assess the effectiveness of the proposed online detection for attack $\mathcal{A}$ proposed in Scenario II, a comparison is carried out between the estimated value of the IMG equivalent

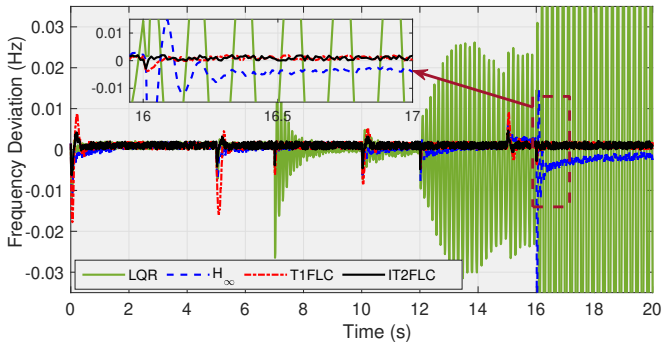


Figure 14. Frequency response of the IMG in case of the physical attack on (R_{eq}) in scenario I.

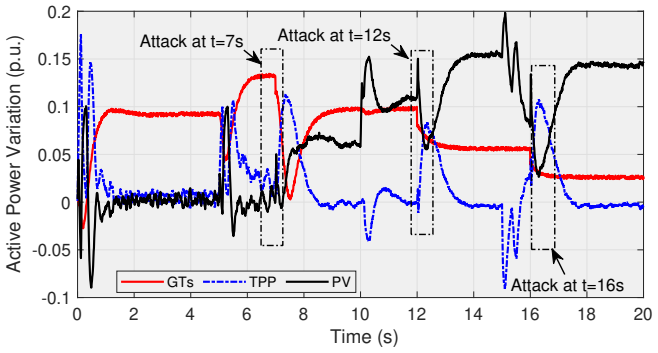


Figure 15. Active power changes for three different energy resources in case of the IT2FLC.

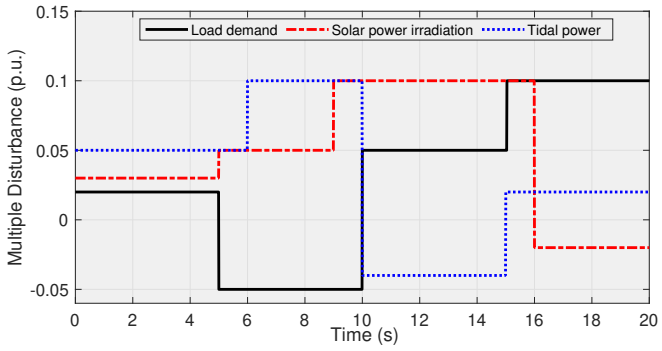


Figure 16. Multiple disturbances consist of step load changes, solar irradiation, and tidal power fluctuation.

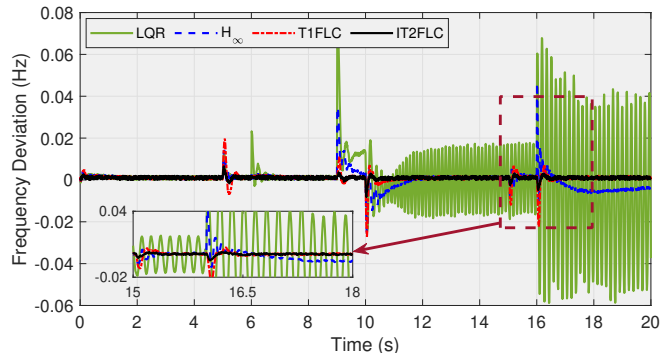


Figure 17. Frequency response of IMG in case of the cyber attack on circuit breakers of SGs in scenario II.

inertia constant $\hat{H}_{eq}(k)$, obtained from the RLS-FF approach, and a predefined threshold (χ_2) similar to the previous part. As Fig. 13-(b) illustrates, the online detector can identify this attack when the first estimated sample of $H_{eq}(k)$ exceeds permissible ranges at $t = 6s$ and decreases from its nominal value, i.e., 0.1667 to 0.13314. In Scenario III, one threshold based on $\pm 5\%$ security margin and $25dB$ SNR is also defined to detect a delay attack on the time constant of the CFMD $(\hat{T}_{f\_Mea}(k))$. According to Fig. 13-(c), under normal conditions, changes of this time constant remain almost constant between two parallel lines which are defined based on a threshold (χ_3). After the occurrence of a delay attack on T_{f_Mea} and changes in this system parameter from its nominal value, the detector can inform about a delay attack on the CFMD of the IMG.

C. Adaptive Mitigation with the help of System Identification

The frequency response is a significant benchmark of system stability that should be continuously monitored and controlled to avoid unacceptable deviations. Based on the threat model, adversaries can manipulate the operation of generation units, corresponding IEDs such as CBs, and frequency measurement devices with the aim of compromising the topology of the IMG. To validate the superiority of the proposed type-2 fuzzy control scheme in the mitigation phase, three different types of control frameworks, i.e., adaptive type-1 fuzzy, linear quadratic regulator (LQR), and H_∞ resilient controllers, are also deployed and their performance are compared together based on three scenarios:

1) Physical Attack on Gas Turbine Systems: In Scenario I, it is assumed that the attackers have enough knowledge about the location of GTs and wait for a critical moment of operation, i.e., load disturbances at $t = 5s, 10s$, and $15s$, to launch their physical attack. Under this attack, the (R_{eq}) changes at $t = 7s$, $12s$, and $16s$ that leads to oscillations in the frequency response. To meet the frequency control objectives, the IT2FLC is implemented and its performance is compared with other controllers. The frequency response of the IMG during a multi-snapshot of the IMG operating points in case of the physical attack at $t = 7s, 12s$, and $16s$ and changes in loads at $t = 5s, 10s$, and $15s$ is illustrated in Fig. 14. It can be clearly observed that the collaboration between the adaptive IT2FLC and online system identification yields a satisfactory performance compared to the T1FLC, LQR, and H_∞ controllers. Since the design of the LQR is dependent on the operating point, after occurring attack targeting the IMG topology at $t = 12s$, the IMG starts to move toward instability. Moreover, since a specific amount of parametric uncertainties can be defined for H_∞ controller to have a resilient performance, this controller cannot yield a satisfactory performance after the attack at $t = 16s$; however, IT2FLC resolves this challenge by collaboration with online system identification. According to the participation of RESs shown in Fig. 15, GTs cannot participate in the LFC scheme at $t = 7s$, $12s$, and $16s$ and their power generation decreases gradually. However, other energy sources, i.e., TPP and PV, provide adequate active power to prevent frequency collapse and stabilize the IMG after this attack.

2) Cyber Attack on CBs of Synchronous Generators: In Scenario II, a reduction in the equivalent inertia constant of the IMG—induced by the manipulation of CBs—can upshot oscillations in the frequency response leading to system instability. To show the performance of the proposed control framework in case of weather changes, the IMG is also exploited under multi-step loads at $t = 5s, 10s$, and $15s$, solar irradiation changes, and tidal power fluctuation whose related patterns are illustrated in Fig. 16. The performance of mentioned controllers in the mitigation of the frequency deviation during the attack on H_{eq} at $t = 6s, 9s, 16s$, and external disturbances is depicted in Fig. 17. It can be observed that the LQR controller is not able to mitigate the frequency instability, so after a decrease in H_{eq} at $t = 9s$, this response starts to fluctuate leading to the IMG instability. Moreover, H_∞ controller after a

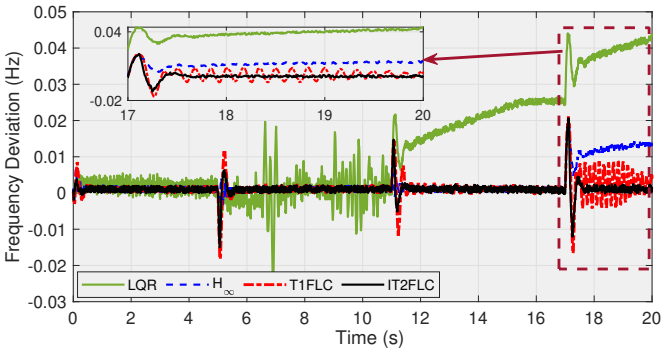


Figure 18. Frequency response of IMG in case of the cyber attack on central FMD in scenario III.

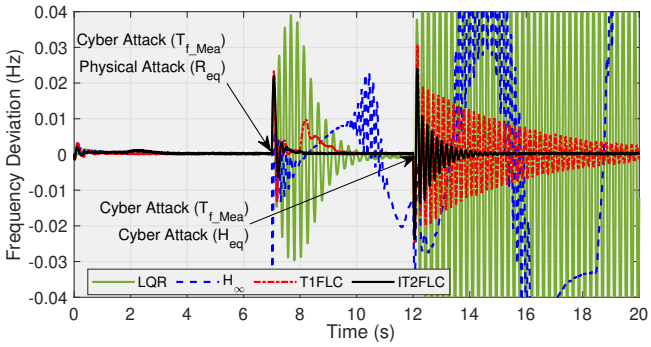


Figure 19. Inter-dependent impacts of different concurrent CPAs on the stability of IMG

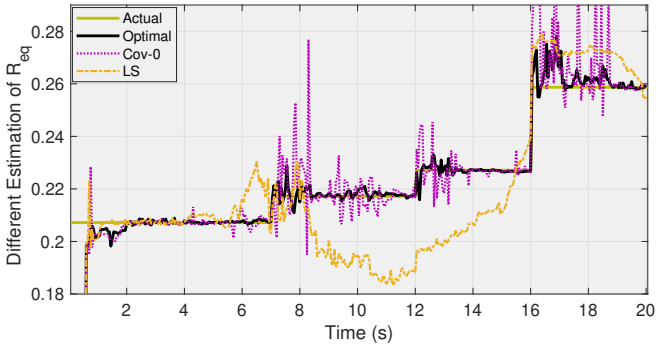


Figure 20. Online estimation of R_{eq} for an IMG equipped with 15 gas turbines to show the scalability of the proposed detection method

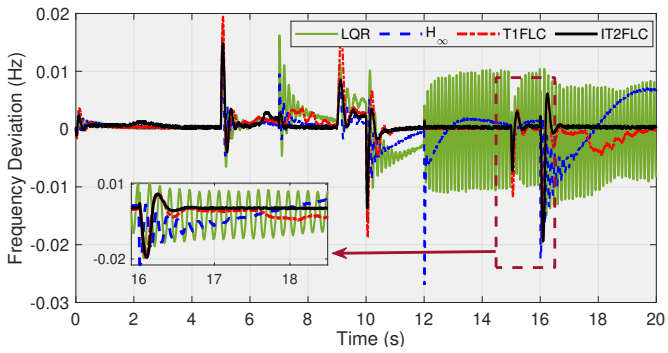


Figure 21. Frequency response of the IMG for a large-scale physical attack on R_{eq}

decrease in H_{eq} at $t = 16s$, cannot stabilize the IMG and has a noticeable steady-state error.

3) Cyber Attack on Frequency Measurement Devices: In Scenario III, the time delay on the time constant of central FMD (T_{f_Mea}) can disrupt the normal operation of the IMG leading to the oscillatory frequency response. Furthermore, predefined patterns for multiple disturbances, i.e., load demands at different times, solar irradiation changes, and tidal power fluctuation, are also assumed during this attack. To illustrate the superiority of the proposed adaptive IT2FLC along with online system identification, its performance is compared to other controllers in Fig. 18. As can be seen, the LQR controller can not provide satisfactory performance and the frequency response starts to oscillate leading to the IMG instability at $t = 5s$. Moreover, the H_∞ can not provide a stable frequency response during different operating points, and at $t = 17s$, the IMG moves toward the instability area.

D. Multiple CPAs and Scalability

In this section, the impacts of simultaneous physical and cyber attacks are investigated on the stability of the IMG. Then, the performance of the proposed mitigation technique is compared with mentioned state-of-the-art attack-resilient control frameworks in LFC studies. These considered multiple CPAs are applied to the IMG as follows:

- A Cyber attack on the central frequency measurement device (T_{f_Mea}) as well as a physical attack on GTs (R_{eq}) are launched at $t = 7s$ based on the proposed threat model. In other words, the nominal value of T_{f_Mea} increases from 0.02 to 0.03 at $t = 7s$, and attackers also target GTs in the physical layer of the IMG through the outage of $R_2 = 3pu.s$, at the same time.
- Attackers manipulate the equivalent inertia constant of the IMG (H_{eq}) and decrease it from 0.1667 to 0.1167 at $t = 12s$. At the same time, they compromise the time constant of the CFMD (T_{f_Mea}) and increase its value from 0.03 to 0.1.

According to the results shown in Fig. 19, the LQR and H_∞ controllers cannot handle simultaneous cyber and physical attacks effectively and they fail in the initial moments resulting in IMG instability. However, the proposed IT2FLC is able to alleviate the impacts of multiple cyber and physical attacks.

To illustrate the scalability of the suggested detection and mitigation techniques, the under-study IMG is first equipped with 15 parallel GTs with droop coefficient values of $R_1 = 2$ pu.s; $R_2 = 3$ pu.s; $R_3 = 3.5$ pu.s; $R_4 = 2.5$ pu.s; $R_5 = 4$ pu.s; $R_6 = 2.5$ pu.s; $R_7 = 3.5$ pu.s; $R_8 = 4.5$ pu.s; $R_9 = 3$ pu.s; $R_{10} = 5$ pu.s; $R_{11} = 2.3$ pu.s; $R_{12} = 3.5$ pu.s; $R_{13} = 2.8$ pu.s; $R_{14} = 3.4$ pu.s; and $R_{15} = 4.1$ pu.s. Afterward, a physical attack is launched to manipulate several GTs that can cause variations in the R_{eq}. Based on the proposed threat model in Section II-A, adversaries result in the outage of R_8 at $t = 7s$, R_{10} at $t = 12s$, and $(R_{14} + R_{15})$ at $t = 16s$, respectively. Fig. 20 illustrates the changes in R_{eq}, which increase from 0.207 to 0.259 during three steps. In case of such a physical attack, the RLS-FF approach estimates an accurate value of R_{eq} and provides its updated value for the LFC centralized control with the aim of keeping the IMG's stability after any changes in IMG's topology. Moreover, the performance of mentioned controllers in the mitigation of the frequency deviation during the cyber attack on R_{eq} at $t = 6s, 9s, 16s$, and load disturbances at $t = 5s, 10s, 15s$ has been depicted in Fig. 21. It can be seen that the collaboration between the IT2FLC and online system identification delivers an acceptable performance compared to the T1FLC, LQR, and H_∞ controllers. Furthermore, to show the scalability of detection and mitigation techniques in the presence of renewable energies in the IMG, it is supposed that adversaries can add delay to the reading of the frequency measurement device of PV arrays based on the suggested threat model in Section II-B. Real-time simulations in

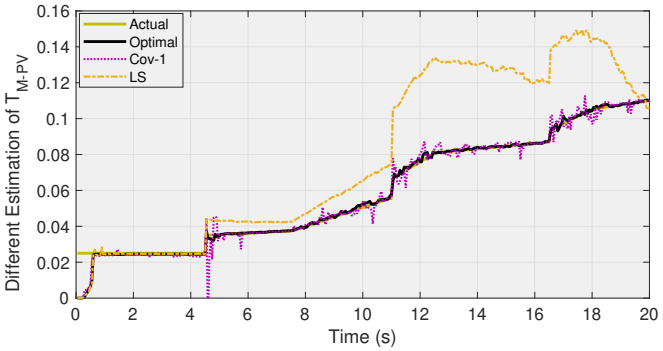


Figure 22. Online Estimation of time constant of PV-FMD (T_{M-pv})

Fig. 22 illustrate that the RLS-FF method can estimate changes in (T_{M-pv}) more accurately compared to the non-recursive (LS) and non-optimal RLS-FF methods.

VII. Conclusion

The cyber-dependent structure of IMGs and their sensitivity to changes in topology make them an appealing target for a variety of CPAs. In this paper, a new family of physical and cyber attacks on components of IMG was studied. To detect the mentioned attacks, the state-space representation of the IMG was first estimated by the RLS-FF technique and then, anomaly-based detection (IDS) was developed to identify CPAs and distinguish them from existing uncertainties in the normal operation of the IMG. Then, an adaptive fuzzy mechanism, which was able to manage both changes in IMG topology and a high level of uncertainties, was introduced to mitigate the detrimental impacts of CPAs. Real-time simulations in the RTS showed that (i) the developed estimation method can estimate IMG parameters and deliver a satisfactory online anomaly-based intrusion detection system (IDS) and (ii) interval type-2 fuzzy logic controller (IT2FLC) with the help of tidal power plant and photovoltaic panels can better mitigate CPAs compared to recent attack-resilient LFC schemes, e.g., linear quadratic regulator (LQR) and H_∞ controllers. In other words, the LQR depended heavily on the operating point and could not yield an acceptable performance in the case of CPAs that targeted the IMG topology. Moreover, the H_∞ controller was also resilient against limited parametric uncertainties and the IMG started to move toward the instability area using the developed H_∞ controller.

References

[1] A. S. Musleh, H. M. Khalid, S. M. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in wamcs applications," *IEEE Syst J.*, vol. 13, no. 1, pp. 710–719, 2019.

[2] H. M. Khalid and J. C.-H. Peng, "A bayesian algorithm to enhance the resilience of wams applications against cyber attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026–2037, 2016.

[3] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-based methods for cyber attacks detection in iot systems: A survey on methods, analysis, and future prospects," *Electronics*, vol. 11, no. 9, p. 1502, 2022.

[4] H. M. Khalid, F. Flitti, M. S. Mahmoud, M. M. Hamdan, S. Muyeen, and Z. Y. Dong, "Wide area monitoring system operations in modern power grids: A median regression function-based state estimation approach towards cyber attacks," *Sustainable Energy, Grids and Networks*, vol. 34, no. 101009, 2023.

[5] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, 2016.

[6] M. R. Khalghani, J. Solanki, S. K. Solanki, M. H. Khooban, and A. Sargolzaei, "Resilient frequency control design for microgrids under false data injection," *IEEE Trans. Ind. Electron.*, vol. 68, no. 3, pp. 2151–2162, 2021.

[7] M. S. Mahmoud, H. M. Khalid, and M. M. Hamdan, *Cyberphysical infrastructures in power systems*. Elsevier, 2021.

[8] M. R. G. Raman and A. P. Mathur, "A hybrid physics-based data-driven framework for anomaly detection in industrial control systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, pp. 1–12, 2021.

[9] M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine-learning-based technique for false data injection attacks detection in industrial iot," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8462–8471, 2020.

[10] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Trans. Ind. Informat.*, vol. 14, no. 5, pp. 1932–1941, 2017.

[11] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "False data injection cyber-attacks mitigation in parallel dc/dc converters based on artificial neural networks," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 68, no. 2, pp. 717–721, 2021.

[12] F. Akbarian, A. Ramezani, M.-T. Hamidi-Beheshti, and V. Haghighat, "Advanced algorithm to detect stealthy cyber attacks on automatic generation control in smart grid," *IET Cyber-Physical Systems: Theory Applications*, vol. 5, no. 4, pp. 351–358, 2020.

[13] A. Farraj, E. Hammad, and D. Kundur, "On the impact of cyber attacks on data integrity in storage-based transient stability control," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3322–3333, 2017.

[14] M. Jorjani, H. Seifi, and A. Y. Varjani, "A graph theory-based approach to detect false data injection attacks in power system ac state estimation," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2465–2475, 2021.

[15] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, 2015.

[16] 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.

[17] X. Wang, X. Luo, Y. Zhang, and X. Guan, "Detection and isolation of false data injection attacks in smart grids via nonlinear interval observer," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6498–6512, 2019.

[18] M. Dehghani, M. Ghiasi, T. Niknam, A. Kavousi-Fard, and S. Padmanaban, "False data injection attack detection based on hilbert-huang transform in ac smart islands," *IEEE Access*, vol. 8, pp. 179 002–179 017, 2020.

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

[20] A. Patel and S. Purwar, "Event-triggered detection of cyberattacks on load frequency control," *IET Cyber-Physical Systems: Theory Applications*, vol. 5, no. 3, pp. 263–273, 2020.

[21] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015.

[22] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702–4711, 2017.

[23] T. N. Pham, A. M. T. Oo, and H. Trinh, "Detecting and isolating false data injection attacks on electric vehicles of smart grids using distributed functional observers," *IET Gener. Transm. Distrib.*, vol. 15, no. 4, pp. 762–779, 2021.

[24] A. M. Mohan, N. Meskin, and H. Mehrjerdi, "Lqg-based virtual inertial control of islanded microgrid load frequency control and dos attack vulnerability analysis," *IEEE Access*, vol. 11, pp. 42 160–42 179, 2023.

[25] T. Huang, D. Wu, and M. Ilić, "Cyber-resilient automatic generation control for systems of ac microgrids," *IEEE Trans. Smart Grid*, pp. 1–1, 2023.

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

[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] S. Saha, T. Roy, M. Mahmud, M. Haque, and S. Islam, "Sensor fault and cyber attack resilient operation of dc microgrids," *International Journal of Electrical Power Energy Systems*, vol. 99, pp. 540–554, 2018.

[29] 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. Power Electron.*, vol. 67, no. 9, pp. 7951–7962, 2020.

[30] Y. Zhang, C. Peng, S. Xie, and X. Du, "Deterministic network calculus-based h_∞ load frequency control of multiarea power systems under malicious dos attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1542–1554, 2022.

[31] J. Wang, D. Wang, L. Su, J. H. Park, and H. Shen, "Dynamic event-triggered h_∞ load frequency control for multi-area power systems subject to hybrid cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, pp. 1–12, 2022.

[32] P. Chen, D. Zhang, L. Yu, and H. Yan, "Dynamic event-triggered output feedback control for load frequency control in power systems with multiple cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, pp. 1–13, 2022.

[33] A. Abazari, M. Zadsar, M. Ghafouri, and C. Assi, "Detection of cyber-physical attacks using optimal recursive least square in an islanded microgrid," in *2022 IEEE Power Energy Society General Meeting (PESGM)*, 2022, pp. 1–5.

[34] H. Bevrani, *Robust power system frequency control*. Springer, 2009.

[35] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 235–244, 2013.

[36] 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, 2016.

[37] J. M. Mauricio, A. Marano, A. Gomez-Exposito, and J. L. Martinez Ramos, "Frequency regulation contribution through variable-speed wind energy conversion systems," *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 173–180, 2009.

[38] A. Kumar and G. Shankar, "Quasi-oppositional harmony search algorithm based optimal dynamic load frequency control of a hybrid tidal–diesel power generation system," *IET Gener. Transm. Distrib.*, vol. 12, no. 5, pp. 1099–1108, 2017.

[39] M. Datta and T. Senjyu, "Fuzzy control of distributed pv inverters/energy storage systems/electric vehicles for frequency regulation in a large power system," *IEEE Trans. on Smart Grid*, vol. 4, no. 1, pp. 479–488, 2013.

[40] P. Yu, J. Li, and H. Peng, "A least square method for parameter estimation of rsc sub-codes of turbo codes," *IEEE Commun. Lett.*, vol. 18, no. 4, pp. 644–647, 2014.

[41] E. W. Kamen and J. K. Su, *Introduction to optimal estimation*. Springer Science Business Media, 1999.

[42] A. L. Seyedali Mirjalili, Seyed Mohammad Mirjalili, "Grey wolf optimizer," *Advances in Eng. Software*, vol. 69, pp. 46–61, 2014.

[43] K. Sabahi, M. Tavan, and A. Hajizadeh, "An adaptive type-2 fuzzy pid controller for lfc in ac microgrid," *Soft Comput.*, vol. 25, p. 7423–34, 2021.

[44] H. Bevrani, T. Hiyama, Y. Mitani, K. Tsuji, and M. Teshnehlab, "Load-frequency regulation under a bilateral lfc scheme using flexible neural networks," *Eng. Intelligent Syst.*, vol. 14, no. 2, pp. 109–117, 2006.

[45] H. Bevrani, M. R. Feizi, and S. Ataee, "Robust frequency control in an islanded microgrid: H_∞ and μ -synthesis approaches," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 706–717, 2016.