A Bi-Level Differential Game-Based Load Frequency Control With Cyber-Physical Security

Saptarshi Ghosh, *Member, IEEE*, and Charalambos Konstantinou, *Senior Member, IEEE*

***Abstract*—Load frequency control (LFC) is used in power systems to prevent frequency fluctuations caused by load disturbances and maintain power supply reliability. LFC utilizes communication channels to generate control signals, thus it is potentially vulnerable to cyber-attacks and faults. This work considers a cyber-physical model for LFC in which the adversary compromises the resources of the cyber layer to inject a stealthy false data injection attack (FDIA) vector. The FDIA injects the best-effort stealthy error into the data collected by the LFC, corrupting the control center's calculations and leading to incorrect control signals. To effectively manage this complex decision-making scenario, a game theory-based framework is established to analyze the interaction between the controller and the attacker. Based on the model, an FDIA defense mechanism based on a bi-level differential game is proposed. The experiments conducted on a three-region interconnected power system based on the IEEE 39-bus system demonstrate that the proposed strategy can effectively maintain the stability of the frequency and inter-regional power deviation within acceptable limits, even in the presence of FDIAs.**

***Index Terms*—Load frequency control, cyber-physical modeling, game theory, false data injection attacks.**

I. Introduction

LOAD frequency control (LFC) is used in power systems to maintain the balance between generation and load. LFC uses feedback control loops based on the deviation of the frequency from its nominal value to control the generated output. The design of LFC is a trade-off between stability and dynamic response, with the aim of ensuring a quick response to changes in demand while also maintaining system stability [1]. The objective of LFC is to ensure zero steady-state error for frequency deviations and minimize unscheduled tie-line power flows between neighbouring control areas. This is achieved through effectively following changes in load demands and disturbances, resulting in limited overshoot and rapid stabilization of frequency and tie-line power deviations. The maximum deviation for LFC depends on the system's characteristics and requirements, such as size, complexity, load demand patterns, available generation capacity, and interconnections. Typically, it is limited to a small range around the nominal frequency, like 49.5-50.5 Hz for a 50 Hz nominal frequency.

LFC typically uses communication signals to transmit information (between the various control centers, generation units, and loads in the system) such as the deviation of the frequency from its nominal value, the power generation output, and the load demand. These signals can be transmitted using various technologies such SCADA systems. As a result, LFC signals can be vulnerable to various cyber-attacks, such as deception attacks and denial-of-service (DoS) attacks. In deception attack or false data injection attacks (FDIAs), the attacker injects data, which can then result in incorrect control actions and potentially cause significant system problems [2], [3]. In the case of LFC, FDIAs can result in incorrect frequency control actions and potentially lead to power system instability or blackouts [4]. The effect of DoS attacks on the LFC has been studied in [5]. Although the work in [5] exploits the cyber layer vulnerabilities by considering the effect of frequency and duration of DoS attacks on the LFC, more potent attacks can be designed by exploiting the vulnerabilities of the physical layer. In this work, both the cyber and physical layers are exploited by the attacker to design the attack vector with the aim of causing maximum damage to the physical layer without getting detected.

LFC of a multiple control area power system consists of multiple decision-makers. Consequently, the coupling among the controllers of these control areas are governed by different decision-makers. This introduces complications in the construction of control strategies, besides the evolution dynamics serving as the dynamical constraints. Meanwhile, power systems operate in the presence of disturbances [6]. Disturbances caused by the load variation from their forecasted value have been considered in [7]. However, unlike the existing literature, the effect of the disturbances has been taken into consideration during the design procedure of control and attack strategies.

In the existing literature, the two main attack objectives concerning LFC target the frequency and tie-line interchange power measurements. In [8], the authors modeled the interaction between the attacker and the defender, considering a time-independent attack on the tie-line power measurements.

Manuscript received 6 July 2023; revised 25 November 2023 and 16 March 2024; accepted 27 April 2024. Date of publication 3 May 2024; date of current version 23 August 2024. Paper no. TSG-01020-2023. *(Corresponding author: Charalambos Konstantinou.)*

Saptarshi Ghosh was with the Computer, Electrical and Mathematical Sciences and Engineering Division, King Abdullah University of Science and Technology, Thuwal 23955, Saudi Arabia. He is now with the Department of Electrical and Electronics Engineering, Rajiv Gandhi Institute of Petroleum Technology Jais, Amethi 229304, India (e-mail: sghosh@rgipt.ac.in).

Charalambos Konstantinou is with the Computer, Electrical and Mathematical Sciences and Engineering Division, King Abdullah University of Science and Technology, Thuwal 23955, Saudi Arabia (e-mail: charalambos.konstantinou@kaust.edu.sa).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2024.3396623.

Digital Object Identifier 10.1109/TSG.2024.3396623

© 2024 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License.
For more information, see https://creativecommons.org/licenses/by/4.0/

The work in [8] concluded that frequency stability is more vulnerable to cyber-attacks compared to power imbalances, as falsification of frequency measurements can be easily detected through comparisons with normal readings. Hence, only cyber-attacks on tie-line interchange measurements by an attacker are considered. The LFC commands are also vulnerable to FDIA [9], [10] while they are distributed to the generating units over the cyber layer, with the aim of reducing power imbalances and ensuring frequency stability. In [9], the authors examined a two-area power system and evaluated its performance in the scenario where an adversary has gained unauthorized access to the automatic generation control (AGC) signal of one of the two areas and he/she optimizes his/her plan for the worst attack pattern. The attacker interrupts the correct control signals and injects false data to steer the system to unstable frequency deviation values. The work aimed to identify the worst attack pattern by evaluating its potential effect on the two-area system. An optimal controller that offers useful feedback gain is the linear–quadratic–Gaussian (LQG) control [11]. LQG controller has the ability to minimize the cost when it is used for frequency stabilization. It can provide stable performance under system noise and uncertainty. The authors in [10] analyzed an infinite horizon LQG system, in which the control inputs transmitted over cyber links are vulnerable to manipulation and FDIAs. On the contrary, in [12], the authors investigated the LQG control problem under jamming attacks on the signals from the controller to the plants, i.e., measurement data. A linear quadratic regulator (LQR) is similar to LQG, but the performance of the former deviates in the presence of system noise [13]. This drawback of LQR problems is addressed in [14], [15] using risk-aware estimation and control. In addition to system noises, the works in [10] and [12] concentrated on devising control mechanisms under worst-case FDIA. Therefore, it is evident from the aforementioned research that most of the attention has been given to the secure estimation and control problem of LFC in the physical layer, either from the defender's or attacker's perspective. On the other hand, there is literature like [16], which proposes a dynamic modeling framework for a closed-loop system that is capable of intrusion detection in the cyber layer. The authors of [17] have investigated the issue of stable operation of a cyber-physical system under multiple DoS attackers from the perspective of both the attacker and the controller. In the cyber layer, multiple DoS attackers cooperate with each other to compromise an optimal number of measurements, while the controller and the attacker compete with each other in the physical layer. However, the interaction between the attacker and the defender in the cyber layer is static in nature. In practice, the attack on the cyber layer is a dynamic process [16]. To the best of the knowledge of the authors, the effect of the dynamics of intrusion, infection, and recovery of the cyber layer nodes has not been considered when investigating FDIAs on the LFC.

Due to its overwhelming advantage in the analysis of the interaction among multiple decision-makers involved in the decision-making process, game theory has gained more and more attention in the existing literature on LFC. Several game theory models, namely Stackelberg [18], evolutionary [19], stochastic [20], and Markov game [21] models, have been used in literature to ensure robust LFC. The authors in [22], [23] have used zero-sum differential game model to design robust optimal control schemes under stochastic uncertainty. These works have mainly considered uncertainties due to load forecasting errors. In previous studies, various differential game models, namely cooperative [24], and non-cooperative [22], [23], [25], [26], have been applied for LFC. In non-cooperative differential games, the control signals are generated locally in each control area. Hence, non-cooperative differential games are more suitable than cooperative differential games for systems that are vulnerable to FDIA on control signals. It is evident from the existing literature that the effect of an FDIA on the equilibrium solution of differential game-based LFC is still an open problem. Further, none of the aforementioned works considered the effect of the cyber layer. The issue of security breaches in the cyber layer and its effect on the physical process is addressed in [17], [27] using game-based analysis. However, the cyber game and the physical game in the aforementioned works are played in different time scales. Although the cyber and physical layer resources are closely related, their treatment in the aforementioned works is different. It is important to note that both the attacker and the defender face resource limitations in both cyber and physical layers, as the defender has to protect against malicious actions while the attacker has to conserve energy. Therefore, there is a need to solve this problem in a comprehensive framework that involves both the defender and the adversary. The dynamic nature of launching FDIAs on the LFC by compromising the resources in the cyber layer is still an open problem.

This article addresses the research gaps highlighted above by considering a bi-level differential game between an attacker targeting LFC and a defender. The payoff of the attacker and defender considers the cost due to deviation of the state variables, implementation of control signals, and cumulative expected predictive variance. The aim of the defender/attacker is to minimize/maximize the aforementioned cost. In order to launch FDIA on the LFC, the attacker needs to gain access to the cyber layer nodes that are collecting and transmitting the measurements. The interaction between the attacker and the defender in the cyber layer is also modeled as a differential game. This constitutes an interconnected bi-level differential game framework that models the effect of the cyber layer vulnerabilities on the LFC. The novel contributions of this work are as follows:

(1) By modeling the LFC system as a cyber-physical system, a novel FDIA model is proposed that considers both the characteristics of the LFC system and the vulnerabilities of the cyber layer used for transmitting measurements. The closed-form expression for the cyber layer vulnerabilities derived in this work reveals the exact dependence of the cyber layer resource allocation on the dynamic control strategies of the physical layer.

(2) A bi-level non-cooperative differential game is proposed to solve the interaction model between the controller and the attacker in both the cyber and physical layers. By locally generating the control signals, the proposed

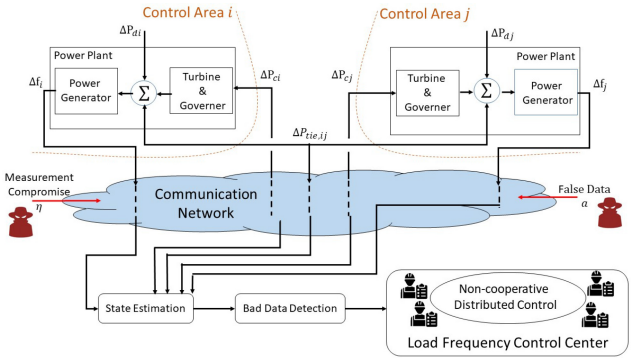


Fig. 1. Illustration of the two-area load frequency control (LFC) system and the compromise of its measurements.

game-based approach reduces the risk of FDIA on control signals. In the physical game, the robust feedback Nash equilibrium is constructed by considering the probability of successful FDIA and load forecasting errors simultaneously.

(3) The design of a bi-level differential game-based LFC for a power system whose evolution is controlled by chance-constrained FDIA is solved, and its performance is evaluated for the first time in this work. The quadratic equivalent of the chance constraint for FDIA, derived in Lemma 2, reveals a novel method of designing attacks with limited system information that can cause maximum damage to differential game-based LFC in terms of the control cost.

The rest of the paper is as follows. Section II presents the system and threat model of the examined problem. Section III introduces the bi-level game framework followed by the solution approach. In Section IV, results are presented, and Section V concludes the work.

II. System and Threat Model

In a multi-area power system, there are typically k control areas, denoted as CA_i, where $i = 1, \ldots, k$ and $k \in \mathbb{Z}^+$, and each area has $m \in \mathbb{Z}^+$ generators. The stability of the system frequency is crucial and primarily dependent on maintaining a balance between the load and the active power output of the generators. To mitigate any imbalance, the active power output of generators must be adjusted in real-time to align with the load. Failure to do so will cause a change in generator speed, leading to a change in the system frequency, which can impact the frequency of not only the current area but also its interconnected areas. In this regard, in such an interconnected system, generators are supported with LFC.[1] A simplified two-area system with LFC is presented in Fig. 1.

LFC objective is to maintain frequency stability within each control area and regulate the power exchange between areas. The LFC of area i is characterized by the frequency measurement of generator j in area i, denoted as $f_{i,j}$, where $j = 1, \ldots, m$, and the interchange of power of tie-line s, $P_{tie,is}$. In a multi-area LFC scheme, all the generators in each control area are represented as an equivalent generation unit whose frequency measurement is denoted by f_i. The aim of LFC is achieved by incorporating the area control error (ACE) collected from distributed sensors into the frequency feedback loop. ACE is a linear combination of the frequency deviation of a given control area i (CA_i), Δf_i, and the deviation of tie-line power, $\Delta P_{tie,ij}$, between that area and other $\forall j \neq i$:

$$\mathrm{ACE}_i = \beta_i \Delta f_i + \sum_{j=1, j\neq i}^{k} \Delta P_{tie,ij} \tag{1}$$

where ΔP_{tie} is the deviation of tie-line power and β_i is frequency bias factor. The requested deviation of the generator output of CA_i, ΔP_{ci}, is obtained from a PI controller with ACE_i as input. The control command to CA_i, u_i, is the request to adjust the speed, obtained by differentiating ΔP_{ci}.

The data transmission rate measured by grid metering devices, such as phasor measurement units (PMUs) is usually $30 - 120$ samples per second. Thus, a discrete system state space response model is utilized to represent the system state space. The state vector is considered as follows:

$$\mathbf{x}(t) = \Bigg[\underbrace{\Delta f_i(t), \Delta P_{gi}(t), \Delta X_{gi}(t), \int ACE_i,}_{CA_i}$$
$$\underbrace{\Delta f_j(t), \Delta P_{gj}(t), \Delta X_{gj}(t), \int ACE_j,}_{CA_j} \underbrace{\Delta P_{tie,ij}(t)}_{\text{Tie-line}} \Bigg]^T \tag{2}$$

The control signal sent by the LFC center to the CA_i to change the generator output is denoted by $u_i(t)$. The perturbations of loads and intermittent energy output of CA_i obtained by forecasting are denoted as ΔP_{di}. The control signals and the perturbations are compactly represented as:

$$\mathbf{u}(t) = \left[u_i(t), u_j(t)\right]^T, \Delta \mathbf{P}_d(t) = \left[\Delta P_{di}(t), \Delta P_{dj}(t)\right]^T \tag{3}$$

The output signal is:

$$\mathbf{y}(t) = \left[ACE_i, \int ACE_i, ACE_j, \int ACE_j\right]^T \tag{4}$$

In this work, we consider that false data can be injected in the frequency and power measurements[2] by compromising the meters in the cyber layer that aggregates the sensor data [2]. Consequently the erroneous Δf_i, Δf_j, and $\Delta P_{tie,ij}$ results in the attack vector $\mathbf{a}(t)$. In [28], the designed attack considers two sets of measurements, one that can be compromised and another that cannot. The division of the measurements into the above sets is predetermined. In [29], the authors considered a random model for the DoS attacks with a constraint on its duration. However, the DoS attack in the cyber layer is independent of the physical layer parameters. This work addresses resource allocation in the cyber layer, considering

[1]Generators are also equipped with an automatic voltage regulator (AVR). The time constant of AVR is faster than LFC, allowing for rapid transient damping. Thus, LFC and AVR control loops can be analyzed independently.

[2]Unlike [10], FDIA is not considered on the control signals since they can be generated locally in differential game based LFC.

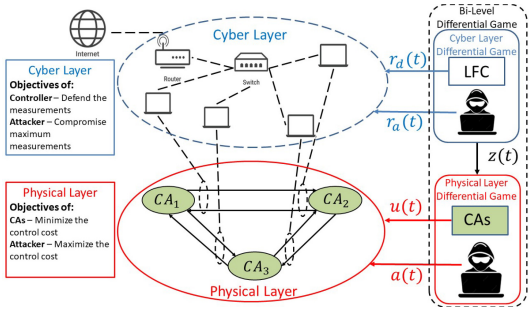


Fig. 2. Structure of the problem formulation.

its effect on the LFC. Fig. 2 denotes the dependence between the cyber and physical layer nodes considered in this work. $\eta_m(t)$ denotes whether $y_m(t)$ is corrupted or not:

$$\eta_m(t) = \begin{cases} 1, & y_m(t) \text{ is compromised} \\ 0, & y_m(t) \text{ is not compromised} \end{cases} \tag{5}$$

For the considered system:

$$\boldsymbol{\eta}(t) = \text{diag}\{[\eta_1(t), \ldots, \eta_m(t), \ldots, \eta_{2k}(t)]\}, \tag{6}$$

where diag$\{[x]\}$ denotes a matrix with $[x]$ as the diagonal elements. Based on the individual values of $\eta_m(t)$, the j^{th} instance of $\boldsymbol{\eta}(t)$ is denoted as $\boldsymbol{\eta}_j(t)$. Consequently, the attacker has two choices: m measurements carry the real data $y_m(t)$ or compromised data $y_{ma}(t)$:

$$y_m(t) = \begin{cases} y_m(t) = \mathbf{C}_m\mathbf{x}(t), & \eta_m(t) = 0 \\ y_{ma}(t) = \mathbf{C}_m\mathbf{x}(t) + \mathbf{a}_m(t), & \eta_m(t) = 1 \end{cases} \tag{7}$$

where $\mathbf{C}_m$ denotes the m^{th} row of:

$$\mathbf{C} = \begin{bmatrix} \mathbf{C}_i & \mathbf{0} & \mathbf{C}_{i0} \\ \mathbf{0} & \mathbf{C}_j & \mathbf{C}_{j0} \end{bmatrix}, \mathbf{C}_i = \begin{bmatrix} -\beta_i & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \mathbf{C}_{i0} = \begin{bmatrix} (-1)^i \\ 0 \end{bmatrix} \tag{8}$$

The compromise, FDIA, and detection of these meters in the cyber layer from such malicious actions are considered periodic activities. The set of cyber layer resources available for accomplishing the above activities is denoted as R_a for the attacker, and R_d for the defender. The resources can be financial, communication bandwidth, computational power and memory, etc. [30], [31]. Such resources are continuous and limited for both [31], [32]. Hence, the attacker and the defender must distribute their resources across a limited number of measurements $M \in \mathbb{R}$ simultaneously. Let this be denoted as $r_d = (r_{d1}, \ldots, r_{dM})$ and $r_a = (r_{a1}, \ldots, r_{aM})$. It is obvious that the probability of a successful attack or defence, depends on the allocated resources in the cyber layer.

The first step in recovering the compromised nodes is detecting the FDIA. The LFC scheme raises the alarm if deviations of the states are beyond predetermined threshold values. In this regard, the residual vector of CA_i after implementing the FDIA at time $t+1$ is calculated as:

$$\begin{aligned} \mathbf{r}_a(t+1) &= \mathbf{y}_a(t+1) - \boldsymbol{\eta}_j(t+1)\mathbf{C}\mathbf{x}_a(t+1) \\ &= \mathbf{y}(t+1) + \mathbf{a}(t+1) - \boldsymbol{\eta}_j(t+1) \\ &\quad \times \mathbf{C}(\mathbf{A}\mathbf{x}(t) + \mathbf{B}\mathbf{u}(t) + \mathbf{E}\Delta\mathbf{P}_d(t) + \mathbf{H}) \\ &= \mathbf{r}(t+1) + \mathbf{a}(t+1) - \boldsymbol{\eta}_j(t+1)\mathbf{C}\mathbf{H} \end{aligned} \tag{9}$$

In case the Euclidean norm of the residual vector in (9) satisfies $||\mathbf{r}_a(t)||_2 > \tau$, the data is considered under attack; otherwise the data is normal. For the attack vector to be stealthy, the vector should satisfy the equation $\mathbf{a} = \boldsymbol{\eta}\mathbf{C}\mathbf{H}\boldsymbol{c}$ following the DC power flow model, where $\mathbf{H}$ is a measurement Jacobian matrix and $\boldsymbol{c}$ denotes the error introduced by the attacker. In literature, works such as [28], consider a fixed $\mathbf{H}$ to design the attack vector. In this paper, we design the attack vector $\mathbf{a}$ in the physical layer based on a probabilistic $\mathbf{H}$ obtained from the cyber layer game between the attacker and the defender.

The dynamics of the proposed LFC can be compactly represented as:

$$\text{Process: } \dot{\mathbf{x}}(t) = \mathbf{A}\mathbf{x}(t) + \mathbf{B}\mathbf{u}(t) + \mathbf{E}\Delta\mathbf{P}_d(t) \tag{10}$$

$$\text{Output: } \mathbf{y}_a(t) = \mathbf{C}\mathbf{x}(t) + \boldsymbol{\eta}_j(t)\mathbf{a}(t) = \mathbf{y}(t) + \boldsymbol{\eta}_j(t)\mathbf{a}(t) \tag{11}$$

$$\text{Anomaly Detector: } \mathbf{r}_{a,i}(t) = \mathbf{y}_{i,a}(t) - \boldsymbol{\eta}_j(t)\mathbf{C}\mathbf{x}_{i,a}(t) \tag{12}$$

$$\text{Initial condition: } \dot{\mathbf{x}}(0) = \mathbf{x}_0 \tag{13}$$

where $\mathbf{y}_a$ and $\mathbf{y}$, as well as $\mathbf{r}_a$ and $\mathbf{r}$, represent the measurements and residue with and without attack, respectively.

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{ii} & \mathbf{0} & \mathbf{A}_{i0} \\ \mathbf{0} & \mathbf{A}_{jj} & \mathbf{A}_{j0} \\ \mathbf{A}_{0i} & \mathbf{A}_{0j} & \mathbf{0} \end{bmatrix}, \mathbf{B} = \begin{bmatrix} \mathbf{B}_i & \mathbf{0} \\ \mathbf{0} & \mathbf{B}_j \\ 0 & 0 \end{bmatrix}, \mathbf{E} = \begin{bmatrix} \mathbf{E}_i & \mathbf{0} \\ \mathbf{0} & \mathbf{E}_j \\ 0 & 0 \end{bmatrix} \tag{14}$$

$$\mathbf{A}_{ii} = \begin{bmatrix} -\frac{D_i}{M_i} & \frac{1}{M_i} & 0 & 0 \\ 0 & -\frac{1}{T_{ti}} & \frac{1}{T_{ti}} & 0 \\ -\frac{1}{T_{gi}\sigma_i} & 0 & -\frac{1}{T_{gi}} & 0 \\ -\beta_i & 0 & 0 & 0 \end{bmatrix}, \mathbf{A}_{i0} = \begin{bmatrix} \frac{(-1)^i}{M_i} \\ 0 \\ 0 \\ (-1)^i \end{bmatrix}, \mathbf{A}_{0i} = \begin{bmatrix} X_{tie}^{-1} \\ 0 \\ 0 \\ 0 \end{bmatrix}^T$$

$$\mathbf{B}_i = \begin{bmatrix} 0 & 0 & \frac{1}{T_{gi}} & 0 \end{bmatrix}, \mathbf{E}_i = \begin{bmatrix} \frac{1}{M_i} & 0 & 0 & 0 \end{bmatrix}$$

The definitions of D_i, M_i, T_{ti}, T_{gi}, σ_i, and X_{tie} can be found in [1]. In differential game-based control schemes, solving the equilibrium solution generates the control command to each CA_i. Linear quadratic differential games (LQDGs)-based LFC of interconnected power systems has been considered using the non-cooperative game approach in [26]. In [24], the authors used a cooperative game approach to find LQDG. The CAs interact among themselves based on the considered game model. In this work, non-cooperative differential game-based LFC is considered since enforcing the solution of the cooperative game requires the CAs to follow assigned control commands even when the loads or the energy outputs deviate from the forecasted values. The attacker can also cause output deviation using FDIA.

In this work, the attacker decides the $\mathbf{a}(t)$ such that the cost incurred by the CAs, J_i, can be maximized while avoiding detection. To minimize the attack costs, the attacker prioritizes state variables with fewer non-zero elements in Eq. (10). To achieve this, the attacker uses a two-stage plan. First, the attacker targets the sensors by compromising the security solution of the defender. Due to resource constraints, attackers can only compromise a limited number of meters in the cyber layer. Next, using the compromised sensors, the attacker manipulates the sensor data through an FDIA to increase the state error in LFC.

Remark 1: The final aim of the attacker is to inject false data in the measurements with the aim of maximizing the control cost of the controller. However, to insert the false data, the attacker needs to have access to the network over which the

measurement data is being transmitted. Hence, the attacker must gain access to the cyber layer resources before injecting false data. This is the reason physical layer decisions come after the network layer.

III. Bi-Level Differential Game Framework

An overview of the problem formulated in this section is summarized in Fig. 2. It can be observed from the figure that the measurements of the CAs are collected by the sensors and exchanged over the network. The controller and the attacker interact in the cyber layer to allocate the available resources to secure and attack the measurements of the CAs, respectively. The objective of the controller/attacker is to secure/compromise the measurements. This interaction is modeled as a non-cooperative differential game (highlighted in Fig. 2 with a blue outline) that results in an equilibrium rate at which the cyber layer nodes are successfully compromised/defended. Next, using the cyber layer resources, the measurements of the CAs are transmitted in the presence of an attacker to estimate the state of the power system and generate control signals. The attacker injects false data into the measurements using the compromised cyber layer nodes while remaining undetected. The objective of the CAs is to generate control signals to minimize the deviations of the state variables from their desired set points while minimizing the cost of implementing control signals. On the contrary, the attacker aims to maximize the deviations of the state variables. This interaction between the CAs and the attacker in the physical layer is modeled as a non-cooperative differential game (highlighted using a red outline in Fig. 2). The non-cooperative differential game-based decision-making in the cyber and the physical layers are interconnected by the probability that the cyber layer nodes are compromised, resulting in the proposed bi-level differential game model as depicted using the black dotted line in Fig. 2.

A. Controller Design Using LQDG

The cost incurred by the LFC for the deviations of the state variables from their desired set values and implementing control signals in a multiple control area power system is denoted by J_i. FDIAs on the measurements and errors in load forecasting can trigger deviations of the state variables. The mean cost incurred by the i^{th} CA is given as:

$$\mathbb{E}\{J_i\} = \frac{1}{2}\mathbb{E}\left\{\sum_{t=0}^{T-1}\left(\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t)+\mathbf{u}^T(t)\mathbf{R}_i\mathbf{u}(t)\right)+\mathbf{y}^T(T)\mathbf{Q}_i\mathbf{y}(T)\right\} \tag{15}$$

where $\mathbf{Q}_i$ is a positive definite weight matrix that determines the penalty associated with the deviation in ACE_i and $\int ACE_i$ which in turn depends on frequency and tie-line power deviations. The control costs of CA_i is represented by a positive definite weight matrix $\mathbf{R}_i$. CA_i specifies the functioning of its LFC by setting $\mathbf{Q}_i$ and R_i. Further, it can be noted from (15) that the cost incurred by CA_i depends on the control signals (u_{-i}) and control cost (R_{-i}) of the other CAs. The cumulative expected predictive variance of the state cost, i.e., $\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t)$, is used as the risk measure.

$$\mathrm{Var}\{\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t)\} = \mathbb{E}\left\{\sum_{t=1}^{T}\left[\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t)-\mathbb{E}\left(\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t)|\mathcal{F}_{t-1}\right)\right]^2\right\} \tag{16}$$

where the σ-algebra generated by all the observations till $t-1$ is denoted by $\mathcal{F}_{t-1}$. The predictive variance in (16) incorporates information about the tail and skewness of the penalty. (16) enables the LFC controller of the CAs to take higher order statistics of the disturbance into account, mitigating the effect of inadequately designed FDIA and rare though large noise values. Further, the constraint (9) on the design of the attack vector act as *path constraint*, i.e., the constraint applies at intermediate points or over the whole path. The path constraint in (9) is also a global constraint that applies to all the CAs that are finding their control signals by solving the optimization problem in (17)-(20). Due to the uncertainty associated with the attack-defence process and the process noise, the performance metric is considered to minimize both *expected cost* and the *risk*.

This work aims to obtain $u_i(t)$, $\forall i \in K$, that minimizes the operating cost of the respective control areas for an optimized $\mathbf{a}(t)$ that maximizes the operating cost. The attacker aims to increase the cost of the CAs by remaining undetected by designing attacks that satisfy the residual in (9) below the threshold of τ. The operating cost can be increased by maximizing the payoff function in (15) and (16) by choosing an appropriate attack $\mathbf{a}(t)$. Hence, the following optimization problem is to be solved by CA_i:

$$\min_{u_i}\max_{\mathbf{a}}\ \mathbb{E}\{J_i\}+\kappa_i\mathrm{Var}\{\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t)\} \tag{17}$$

$$s.t.\ \dot{\mathbf{x}}(t)=\mathbf{A}\mathbf{x}(t)+\mathbf{B}\mathbf{u}(t)+\mathbf{E}\Delta\mathbf{P}_d(t) \tag{18}$$

$$\mathbf{y}(t)=\mathbf{C}\mathbf{x}(t)+\mathbf{a}(t) \tag{19}$$

$$Prob\left\{\left\|\mathbf{r}(t)+\mathbf{a}(t)-\boldsymbol{\eta}_j(t)\mathbf{C}\mathbf{H}\right\|_2\le\tau\right\}\ge 1-\epsilon. \tag{20}$$

The expectation operation in (17), (18), and (20) is over $\boldsymbol{\eta}$, $\Delta\mathbf{P}_d$. $0\le\kappa_i\le 1$ denotes the trade-off between the risk and the average loss. Parameter $\kappa_i\in\mathbb{R}$ shows the player's attention to risk. Note that if $\kappa_i=0$, it is understood as CA_i is risk neutral. If $\kappa_i>0$, then CA_i is risk loving, and if $\kappa_i<0$, then CA_i is risk averse. Next, for a risk-averse CA, we find the quadratic representation of predictive variance of the state cost in (17).

Lemma 1: The equivalent representation of the risk measure in (17) as a quadratic function is:

$$\mathrm{Var}\{\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t)\} = \mathbb{E}\{4\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{C}\mathbf{E}\mathbf{W}\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\mathbf{y}(t) +4\mathbf{y}^T(t)\mathbf{Q}_iM_3\}+m_4-4Tr\{\mathbf{W}\mathbf{Q}_i\mathbf{C}\mathbf{E}\mathbf{W}\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\}. \tag{21}$$

The proof of Lemma 1 is discussed in Appendix. For the stationary operation of the proposed LFC, the residual and the attack vector should fall outside of the constraint set $||\mathbf{r}(t)+\mathbf{a}(t)-\boldsymbol{\eta}_j(t)\mathbf{C}\mathbf{H}||_2\le\tau$ with a probability level of at most $\epsilon\in(0,1)$. The chance constraint in (20) is a function of $\boldsymbol{\eta}$ whose distribution will be discussed in the next subsection. (21) can be modified as $\sum_{j=1}^{S}\Pr(\boldsymbol{\eta}_j)\chi_j\ge\epsilon$ where χ_j denotes a characteristic functions which equals 1 if $||\mathbf{r}(t)+\mathbf{a}(t)-$

$\boldsymbol{\eta}_i\mathbf{CH}||_2 \leq \tau$ and 0 otherwise. Thereby introducing an artificial binary variable $\zeta \in \{0,1\}^S$ to deal with χ_js makes (17)-(20) a mixed-integer non-linear optimization problem. The difficulty of solving such problems is addressed by relaxing the $\zeta_j \in \{0,1\}$ into $\zeta_j \in [0,1]$. Hence the equivalent representation of (20) is given in the following lemma.

Lemma 2: The resulting equivalent representation of the chance constraint in (20) is denoted as:

$$\Big(\big\|\mathbf{y}(t) - \mathbf{C}\mathbf{x}(t) + \mathbf{a}(t) - \boldsymbol{\eta}_j(t)\mathbf{CH}\big\|_2^2 - \tau^2\Big)\zeta_j \leq 0, \quad (22)$$

$$0 \leq \zeta_j \leq 1, \forall j = 1, \ldots, S, \quad (23)$$

$$\sum_{j=1}^{S} \zeta_j p\big(\boldsymbol{\eta}_j\big) \geq 1 - \epsilon. \quad (24)$$

Lemma 1 and 2 are critical because they show that the risk and chance constraints can be represented as a quadratic function of the state, control inputs, and attack vector. The optimization problem in (17)-(20) can be solved by considering the variational Lagrangian in the following lemma.

Lemma 3: The objective function (17), constraints in (18)-(20) are the functions of the state variables, outputs, control, and attack inputs. The compact representation of the resulting variational Lagrange function for CA_i is denoted as:

$$\begin{aligned}
&\mathcal{L}(\mathbf{y}(t), \mathbf{u}(t), \mathbf{a}(t), \{\mu_i\}, \xi)\\
&= \mathbb{E}\left\{ g_T(\mathbf{y}(T), \mathbf{u}(T), \mathbf{a}(T), \{\mu_i\}) + \sum_{t=0}^{T-1} g_t(\mathbf{y}(t), \mathbf{u}(t), \mathbf{a}(t), \{\mu_i\}) \right\}\\
&+g_\mu(\{\mu_i\}) + g(\xi), \quad (25)\\
&\text{where } g_T(\mathbf{y}(T), \mathbf{u}(T), \mathbf{a}(T), \{\mu_i\}) \triangleq \mathbf{y}(T)\mathbf{Q}_i\mathbf{y}(T) +\\
&+\kappa_i 4\mathbf{y}^T(T)\mathbf{Q}_i\mathbf{CEWE}^T\mathbf{C}^T\mathbf{Q}_i\mathbf{y}(T) + \kappa_i 4\mathbf{y}^T(T)\mathbf{Q}_i M_3\\
&+\mu_i\big(\mathbf{r}^T(T)\mathbf{a}(T) + \mathbf{a}^T(T)\mathbf{r}(T) + \mathbf{a}^T(T)\mathbf{a}(T) - \boldsymbol{\eta}_i\mathbf{a}^T(T)\mathbf{CH}\\
&\quad -\boldsymbol{\eta}_i\mathbf{H}^T\mathbf{C}^T\mathbf{a}(t)\big), \quad (26)\\
&g_t(\mathbf{y}(t), \mathbf{u}(t), \mathbf{a}(t), \{\mu_i\}) \triangleq \mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t) + \mathbf{u}^T(t)\mathbf{R}_i\mathbf{u}(t)\\
&+\kappa_i 4\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{CEWE}^T\mathbf{C}^T\mathbf{Q}_i\mathbf{y}(t) + \kappa_i 4\mathbf{y}^T(t)\mathbf{Q}_i M_3\\
&+\mu_i\big(\mathbf{r}^T(t)\mathbf{a}(t) + \mathbf{a}^T(t)\mathbf{r}(t) + \mathbf{a}^T(t)\mathbf{a}(t) - \boldsymbol{\eta}_i\mathbf{a}^T(t)\mathbf{CH}\\
&-\boldsymbol{\eta}_i\mathbf{H}^T\mathbf{C}^T\mathbf{a}(t)\big), \quad (27)\\
&g_\mu(\{\mu_i\}) \triangleq \mathbb{E}\Big\{\boldsymbol{\mu}_i\big(\mathbf{r}^T(t)\mathbf{r}(t) - \boldsymbol{\eta}_i\mathbf{r}^T(t)\mathbf{CH} - \boldsymbol{\eta}_i\mathbf{H}^T\mathbf{C}^T\mathbf{r}(t)\\
&\qquad +\boldsymbol{\eta}_i^2\mathbf{H}^T\mathbf{C}^T\mathbf{CH}\big)\Big\}, \quad (28)\\
&g(\xi) \triangleq \kappa_i\big(m_4 - 4Tr\big\{\mathbf{WQ}_i\mathbf{CEWE}^T\mathbf{C}^T\mathbf{Q}_i\big\}\big)\\
&\qquad +\xi\left(\sum_{j=1}^{S}\zeta_j \mathrm{Pr}(\boldsymbol{\eta}_j) - (1-\epsilon)\right). \quad (29)
\end{aligned}$$

It is evident from (27) that the stage cost matrix $\mathbf{Q}_i + 4\kappa_i\mathbf{Q}_i\mathbf{CEWE}^T\mathbf{C}^T\mathbf{Q}_i$ is inflated in our case, instead of the original $\mathbf{Q}_i$. The derived stage cost suggests that the control gain becomes more stringent in directions that are simultaneously more costly and prone to noise denoted by the covariance $\mathbf{W}$. The state variables are also determined by the control signal and attack vector, which are yet to be derived. Further, the attacks that result in large residuals cause more damage to the *CA*s in terms of cost. However, these attacks are restricted by the attack detection probability and the defence measures. Consequently, duality theory can be applied. The dual function is defined as:

$$\begin{aligned}
D(\{\mu_i\}, \xi) = \inf_{\mathbf{u}} \sup_{\mathbf{a}} \{&g_T(\mathbf{u}(T), \mathbf{a}(T), \{\mu_i\})\\
&+g_t(\mathbf{u}(t), \mathbf{a}(t), \{\mu_i\}) + g_\mu(\{\mu_i\}) + g(\xi)\big\}. \quad (30)
\end{aligned}$$

Theorem 1: Consider the Lagrange function in (25) with (18) and (19) as the constraints. Utilizing Bellman's principle of optimality, we obtain the coupled first-order conditions (94) and (95) that are satisfied by the solution. The solution to the dual problem of the optimal control problem in the presence of error and the attacker is found to be:

$$\begin{aligned}
&\mathcal{L}^*(\mathbf{y}(t), \{\mu_i\}, \xi)\\
&= \mathbf{y}^T(t)P(t)\mathbf{y}(t) + \mathbf{y}^T(t)L(t) + M(t)\mathbf{y}(t) + N(t), \quad (31)\\
&\textit{where } \mathbf{P}(t) = \big(\mathbf{A}^T\mathbf{C}^T + \mathbf{K}_u^T(t)\mathbf{B}^T\mathbf{C}^T + \mathbf{K}_a^T(t)\big)\mathbf{P}(t+1)\\
&\quad (\mathbf{CA} + \mathbf{CBK}_u(t) + \mathbf{K}_a(t)) \quad (32)\\
&\mathbf{L}(t) = \big(\mathbf{A}^T\mathbf{C}^T + \mathbf{K}_u^T(t)\mathbf{B}^T\mathbf{C}^T + \mathbf{K}_a^T(t)\big)\mathbf{P}(t+1)\\
&\quad \big(\mathbf{CB}(\mathbf{l}_u + \mathbf{k}_u) + \mathbf{CE}\bar{\Delta}\bar{\mathbf{P}}_d + (\mathbf{l}_a + \mathbf{k}_a)\big)\\
&\quad +\big(\mathbf{K}_u^T(t)\mathbf{B}^T\mathbf{C}^T + \mathbf{K}_a^T(t) + \mathbf{A}^T\mathbf{C}^T\big)\mathbf{L}(t+1) \quad (33)\\
&\mathbf{M}(t) = \big(\big(\mathbf{l}_u^T + \mathbf{k}_u^T\big)\mathbf{B}^T\mathbf{C}^T + \bar{\Delta}\bar{\mathbf{P}}_d\mathbf{E}^T\mathbf{C}^T + \big(\mathbf{l}_a^T + \mathbf{k}_a^T\big)\big)\\
&\quad \mathbf{P}(t+1)(\mathbf{CA} + \mathbf{CBK}_u(t) + \mathbf{K}_a(t))\\
&\quad +\mathbf{M}(t+1)(\mathbf{CA} + \mathbf{CBK}_u(t) + \mathbf{K}_a(t)) \quad (34)\\
&\mathbf{N}(t) = \Big(\big(\mathbf{l}_u^T + \mathbf{k}_u^T\big)\mathbf{B}^T\mathbf{C}^T + \bar{\Delta}\bar{\mathbf{P}}_d^T\mathbf{E}^T\mathbf{C}^T + \big(\mathbf{l}_a^T + \mathbf{k}_a^T\big)\Big)\mathbf{P}(t+1)\\
&\quad \big(\mathbf{CB}(\mathbf{l}_u + \mathbf{k}_u) + \mathbf{CE}\bar{\Delta}\bar{\mathbf{P}}_d + (\mathbf{l}_a + \mathbf{k}_a)\big)\\
&\quad +\Big(\big(\mathbf{l}_u^T + \mathbf{k}_u^T\big)\mathbf{B}^T\mathbf{C}^T + \bar{\Delta}\bar{\mathbf{P}}_d^T\mathbf{E}^T\mathbf{C}^T + \big(\mathbf{l}_a^T + \mathbf{k}_a^T\big)\Big)\mathbf{L}(t+1)\\
&\quad +\mathbf{M}(t+1)\big(\mathbf{CB}(\mathbf{l}_u + \mathbf{k}_u) + \mathbf{CE}\bar{\Delta}\bar{\mathbf{P}}_d + (\mathbf{l}_a + \mathbf{k}_a)\big)\\
&\quad +\mathbf{N}(t+1) \quad (35)
\end{aligned}$$

Thereby, solving the conditions mentioned above, the optimal solution in linear feedback form can be written as:

$$\begin{aligned}
\mathbf{u}^*(\{\mu_i\}, \xi) &= -\mathbf{K}_u(t)\mathbf{x}(t) + \mathbf{l}_u + \mathbf{k}_u \quad (36)\\
\mathbf{a}^*(\{\mu_i\}, \xi) &= -\mathbf{K}_a(t)\mathbf{x}(t) + \mathbf{l}_a + \mathbf{k}_a \quad (37)\\
\text{where } \mathbf{T}_1^i(t+1) &= \big(\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\mathbf{CB} + \mathbf{R}_i\big)^{-1} \quad (38)\\
\mathbf{T}_2^i &= \mathbf{Q}_i + 4\kappa_i\mathbf{Q}_i\mathbf{CEWE}^T\mathbf{C}^T\mathbf{Q}_i \quad (39)\\
\mathbf{T}_5^i &= -4\kappa_i\mathbf{Q}_i\mathbf{M}_3 - \sum_i \mu_i\big(\mathbf{r}(t) - \boldsymbol{\eta}_i(t)\mathbf{CH}\mathrm{Pr}(\boldsymbol{\eta}_i)\big) \quad (40)
\end{aligned}$$

The outline of the proof of Theorem 1 is discussed in Appendix. The optimal controller and the attack vector in (36)

$$\mathbf{T}_3^i(t+1) = \mathbf{T}_1^i(t+1)\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\left(-\mathbf{P}(t+1)\mathbf{CB}\mathbf{T}_1^i(t+1)\mathbf{B}^T\mathbf{C}^T + \mathbf{P}(t+1) + \mathbf{T}_2^i + \sum_i \mu_i\right)^{-1} \quad (41)$$

and (37) are affine with respect to the state. The state-feedback terms in (36) and (37) account for the internal dynamics of the physical system (39), the state of the cyber layer nodes (40) and the interaction among the *CA*s (38). The optimal primal solution to the solution of dual problem is:

$$\mathcal{L}\big(\mathbf{y}(t),\{\mu_i^*\},\xi^*\big)=\sup_{\{\mu_i\},\xi}\mathcal{L}(\mathbf{y}(t),\{\mu_i\},\xi) \tag{49}$$

where the sufficient optimality conditions are given as follows.

Lemma 4: Consider the control and attack policy $\mathbf{u}^*(\{\mu_i\},\xi)$, $\mathbf{a}^*(\{\mu_i\},\xi)$, $\mu_i>0,\forall i$, $\xi>0$ as defined in (36) and (37). Then the following statements are true:

1) The control cost in (17) is increasing with $\mu_i\geq 0,\forall i$, and $\xi\leq 0$ while (22) is decreasing and (24) is increasing.
2) The optimal Lagrange multipliers can be defined as:

$$\mu_i^*=\inf\Big\{\mu_i\geq 0:\big(\|\mathbf{y}^*(t)-\mathbf{C}\mathbf{x}^*(t)+\mathbf{a}^*(t)-\boldsymbol{\eta}_j(t)\mathbf{C}\mathbf{H}\|_2^2-\tau^2\big)\zeta_j\Big\},\quad\forall i, \tag{50}$$

$$\xi^*=\inf\left\{\xi\leq 0:\sum_{j=1}^{S}\zeta_j^*\Pr(\boldsymbol{\eta}_j)\geq 1-\epsilon\right\}. \tag{51}$$

3) The control and attack policy in (36) and (37) are optimal for the primal problem in (17)-(20) when μ_i^* is finite.

The outline of the proof of Lemma 4 is discussed in the Appendix. The stability of the proposed differential game based is discussed in the following lemma.

Lemma 5: Let us consider the optimal control signal $\mathbf{u}^*(\{\mu_i\},\xi)$, derived in (36), for a given $\mu_i\geq 0,\xi\geq 0$. $P(t)$ converges exponentially to the unique stabilizing solution of the following algebraic Riccati equation as $T\to\infty$:

$$\mathbf{P}=\big(\mathbf{A}^T\mathbf{C}^T+\mathbf{K}_u^T\mathbf{B}^T\mathbf{C}^T+\mathbf{K}_a^T\big)\mathbf{P}(\mathbf{C}\mathbf{A}+\mathbf{C}\mathbf{B}\mathbf{K}_u+\mathbf{K}_a) \tag{52}$$

Consequently, the following conditions, (54)–(64), as shown at the bottom of the page, are true for every $t\geq 0$ as $T\to\infty$. The conditions in (54)-(64) converge exponentially fast, and the closed-loop matrix $(\mathbf{C}\mathbf{A}+\mathbf{C}\mathbf{B}\mathbf{K}_u(t)+\mathbf{K}_a(t))$ is stable.

The outline of the proof for Lemma 5 is given in Appendix.

Remark 2: The mean cost incurred by the controller satisfies the following property when Nash equilibrium-based control

$$\mathbf{T}_4^i(t+1)=\left(-\mathbf{P}(t+1)\mathbf{C}\mathbf{B}\mathbf{T}_1^i(t+1)\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)+\mathbf{P}(t+1)+\mathbf{T}_2^i+\sum_i\mu_i\right)^{-1} \tag{42}$$

$$\mathbf{K}_u(t)=-\big[\mathbf{T}_3^i(t+1)\big(-\mathbf{P}(t+1)\mathbf{C}\mathbf{A}-\mathbf{T}_2^i\mathbf{C}+\mathbf{P}(t+1)\mathbf{C}\mathbf{B}\mathbf{T}_1^i(t+1)\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\mathbf{C}\mathbf{A}\big)-\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\mathbf{C}\mathbf{A}\big] \tag{43}$$

$$\mathbf{l}_u=\big[-\mathbf{T}_3^i(t+1)\big(-\mathbf{P}(t+1)\mathbf{C}\mathbf{E}+\mathbf{P}(t+1)\mathbf{C}\mathbf{B}\mathbf{T}_1^i(t+1)\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\mathbf{C}\mathbf{E}\big)-\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\mathbf{C}\mathbf{E}\big]\bar{\Delta}\mathbf{P}_d \tag{44}$$

$$\mathbf{k}_u=\big[-\mathbf{T}_3^i(t+1)\big(-\mathbf{I}+\mathbf{P}(t+1)\mathbf{C}\mathbf{B}\mathbf{T}_1^i(t+1)\mathbf{B}^T\mathbf{C}^T\big)\mathbf{L}(t+1)-\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\mathbf{T}_5^i\big] \tag{45}$$

$$\mathbf{K}_a(t+1)=\mathbf{T}_4^i(t+1)\big(-\mathbf{P}(t+1)\mathbf{C}\mathbf{A}-\mathbf{T}_2^i\mathbf{C}+\mathbf{P}(t+1)\mathbf{C}\mathbf{B}\mathbf{T}_1^i(t+1)\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\mathbf{C}\mathbf{A}\big) \tag{46}$$

$$\mathbf{l}_a=\mathbf{T}_4^i(t+1)\big(-\mathbf{P}(t+1)\mathbf{C}\mathbf{E}+\mathbf{P}(t+1)\mathbf{C}\mathbf{B}\mathbf{T}_1^i(t+1)\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\mathbf{C}\mathbf{E}\big) \tag{47}$$

$$\mathbf{k}_a=\mathbf{T}_4^i(t+1)\big[\big(-\mathbf{I}+\mathbf{P}(t+1)\mathbf{C}\mathbf{B}\mathbf{T}_1^i(t+1)\mathbf{B}^T\mathbf{C}^T\big)\mathbf{L}(t+1)+\mathbf{T}_5^i\big] \tag{48}$$

$$\mathbf{L}(t)\to\mathbf{L}=\big(\mathbf{I}-\big(\mathbf{K}_u^T(t)\mathbf{B}^T\mathbf{C}^T+\mathbf{K}_a^T(t)+\mathbf{A}^T\mathbf{C}^T\big)\big)^{-1}\big(\mathbf{A}^T\mathbf{C}^T+\mathbf{K}_u^T(t)\mathbf{B}^T\mathbf{C}^T+\mathbf{K}_a^T(t)\big)\mathbf{P}\big(\mathbf{C}\mathbf{B}(\mathbf{l}_u+\mathbf{k}_u)+\mathbf{C}\mathbf{E}\bar{\Delta}\mathbf{P}_d+(\mathbf{l}_a+\mathbf{k}_a)\big) \tag{53}$$

$$\mathbf{M}(t)\to\mathbf{M}=\big(\big(\mathbf{l}_u^T+\mathbf{k}_u^T\big)\mathbf{B}^T\mathbf{C}^T+\bar{\Delta}\mathbf{P}_d\mathbf{E}^T\mathbf{C}^T+\big(\mathbf{l}_a^T+\mathbf{k}_a^T\big)\big)\mathbf{P}(\mathbf{C}\mathbf{A}+\mathbf{C}\mathbf{B}\mathbf{K}_u(t)+\mathbf{K}_a(t))(\mathbf{I}-(\mathbf{C}\mathbf{A}+\mathbf{C}\mathbf{B}\mathbf{K}_u(t)+\mathbf{K}_a(t)))^{-1} \tag{54}$$

$$\mathbf{T}_3^i=\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\mathbf{P}\left(-\mathbf{P}\mathbf{C}\mathbf{B}\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T+\mathbf{P}+\mathbf{T}_2^i+\sum_i\mu_i\right)^{-1} \tag{55}$$

$$\mathbf{T}_4^i=\left(-\mathbf{P}\mathbf{C}\mathbf{B}\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\mathbf{P}+\mathbf{P}+\mathbf{T}_2^i+\sum_i\mu_i\right)^{-1} \tag{56}$$

$$\mathbf{K}_u(t)\to\mathbf{K}_u=-\big[\mathbf{T}_3^i\big(-\mathbf{P}\mathbf{C}\mathbf{A}-\mathbf{T}_2^i\mathbf{C}+\mathbf{P}\mathbf{C}\mathbf{B}\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\mathbf{P}\mathbf{C}\mathbf{A}\big)-\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\mathbf{P}\mathbf{C}\mathbf{A}\big] \tag{57}$$

$$\mathbf{l}_u=\big[-\mathbf{T}_3^i\big(-\mathbf{P}\mathbf{C}\mathbf{E}+\mathbf{P}\mathbf{C}\mathbf{B}\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\mathbf{P}\mathbf{C}\mathbf{E}\big)-\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\mathbf{P}\mathbf{C}\mathbf{E}\big]\bar{\Delta}\mathbf{P}_d \tag{58}$$

$$\mathbf{k}_u=\big[-\mathbf{T}_3^i\big(-\mathbf{I}+\mathbf{P}\mathbf{C}\mathbf{B}\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\big)\mathbf{L}-\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\mathbf{P}\mathbf{T}_5^i\big] \tag{59}$$

$$\mathbf{K}_a(t)\to\mathbf{K}_a=\mathbf{T}_4^i\big(-\mathbf{P}\mathbf{C}\mathbf{A}-\mathbf{T}_2^i\mathbf{C}+\mathbf{P}\mathbf{C}\mathbf{B}\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\mathbf{P}\mathbf{C}\mathbf{A}\big) \tag{60}$$

$$\mathbf{l}_a=\mathbf{T}_4^i\big(-\mathbf{P}\mathbf{C}\mathbf{E}+\mathbf{P}\mathbf{C}\mathbf{B}\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\mathbf{P}\mathbf{C}\mathbf{E}\big) \tag{61}$$

$$\mathbf{k}_a=\mathbf{T}_4^i\big[\big(-\mathbf{I}+\mathbf{P}\mathbf{C}\mathbf{B}\mathbf{T}_1^i\mathbf{B}^T\mathbf{C}^T\big)\mathbf{L}+\mathbf{T}_5^i\big] \tag{62}$$

$$\mathbf{T}_1^i=\big(\mathbf{B}^T\mathbf{C}^T\mathbf{P}\mathbf{C}\mathbf{B}+\mathbf{R}_i\big)^{-1} \tag{63}$$

$$\mathbf{T}_5^i=-4\kappa_i\mathbf{Q}_i\mathbf{M}_3-\sum_i\mu_i\big(\mathbf{r}-\boldsymbol{\eta}_i\mathbf{C}\mathbf{H}\Pr(\boldsymbol{\eta}_i)\big) \tag{64}$$

and attack strategies are followed:

$$\mathbb{E}\{J_i(\mathbf{y}^*(t), \mathbf{u}_i^*(t), \mathbf{u}_{-i}^*(t)\mathbf{a}^*(t))\} + \kappa_i \mathrm{Var}\{\mathbf{y}^{*T}(t)\mathbf{Q}_i\mathbf{y}^*(t)\}$$
$$\leq \mathbb{E}\{J_i(\mathbf{y}(t), \mathbf{u}_i(t), \mathbf{u}_{-i}^*(t)\mathbf{a}^*(t))\} + \kappa_i \mathrm{Var}\{\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t)\}$$

$\forall i = 1, \ldots, k$. The above equation denotes that the attacker/defender cannot maximize/minimize the cost by unilaterally deviating from the Nash equilibrium solution. Hence, Nash equilibrium provides the optimal solution in competitive situations. The control signals based on Nash equilibrium consist of a set of feedback gains K_u. These gains are not related to the initial state $y(t_0)$ and the forecasted value of $\Delta P_d(t)$ but are determined only by the physical structure of the LFC system, which explains that the Nash equilibrium-based control signal is strongly time consistent. As a result, for a given attack strategy, the CAs would not violate the control signals generated locally, even if the loads deviate from the forecasted values.

Remark 3: The attack vector in linear feedback form (37), which brings the most increase in the expected cost corresponding to the Nash equilibrium control strategies (36), is the worst case that the i^{th} *CA* may face. However, in most scenarios, CA_i may incur accost lesser than the worst-case scenario. Due to the different levels of risk sensitivity defined by $\mathbf{Q}_i$, the worst-case attack vectors are calculated by each player before calculating their control strategies. Consequently, the actual attack calculated by each *CA* following (37) will differ for each of the *CA*s. Further, during the evolution of system states, the actual attack vector perturbing the dynamics will not be the same as any worst-case attack vectors (37), which lessens the expected cost of all the *CA*s.

B. Design of the Game Model in the Cyber Layer

The control input and the attack vector, derived in (36) and (37), are due to the application of linear static feedback. For $\mathbf{K}_l$, $l = \{u, a\}$ derived in (36) and (37), an entry $K_l^{i,j} \neq 0$, denotes that the i^{th} control and the attack input is related to the j^{th} state variable. Further, it is evident that the $u_i(t)$ and $a_i(t)$ for CA_i may be dependent on the state variables of the other *CA*s. The state variables are estimated from the outputs delivered over the cyber infrastructure. Hence, before proceeding further, $\mathbf{K}_l$ is reorganized so that the states and the control and attack inputs are organized according to their physical locations. The resulting matrix is $\mathbf{K}_l^* \in \mathbb{R}^{n\times n}$, in which each block $\mathbf{K}_l^{ij}$ represents feedback of the states of CA_i to the control inputs of CA_j, with $i = j$ corresponding to local feedback and $i \neq j$ represents control and attack inputs are dependent on data from the cyber layer. As there are k *CA*s, each CA_i controls n_i nodes in the physical system.

$$\text{Control Area } k \implies \{\Delta f_k, \Delta P_{tie,kj}\}$$

Based on these partitions, the LFC dynamics can be rewritten:

$$\dot{\mathbf{x}}_i(t) = \sum_{r=1}^{k} \mathbf{A}_{ir}\mathbf{x}_r(t) + \sum_{r=1}^{k} \mathbf{B}_{ir}\mathbf{u}_r(t) + \mathbf{E}_i\Delta\mathbf{P}_d(t) \quad (65)$$

$$\text{where } [\mathbf{u}_1(t)\ldots\mathbf{u}_k(t)]^T = -\left[\mathbf{K}_u^1 \ldots \mathbf{K}_u^k\right]^T \mathbf{x}(t) + l_u + k_u \quad (66)$$

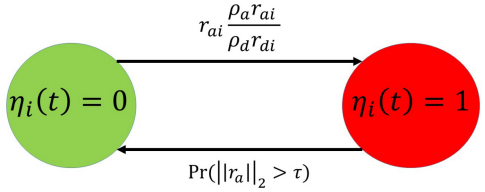


Fig. 3. State evolution model between normal and compromised nodes.

$$[\mathbf{a}_1(t)\ldots\mathbf{a}_k(t)]^T = -\left[\mathbf{K}_a^1 \ldots \mathbf{K}_a^k\right]^T \mathbf{x}(t) + l_a + k_a \quad (67)$$

$\mathbf{u}_i^*(t)$ and $\mathbf{a}_i^*(t)$ in (66) and (67) denote the relationship between the control signal and FDIA for the CA_i and the measurements from various nodes. Let $z_i(t)$ be the probability that node i is compromised. The relation between the probability of i^{th} measurement $\Pr(\eta_i(t))$ and probability of j^{th} node $z_j(t)$ is given as:

$$\Pr(\eta_i(t)) = 1 - \prod_{j=1}^{4k+1} \left(1 - z_j(t)\right)$$

The attacker's objective is to increase the economic value of the attack by attacking the optimal set of measurements in the network using the compromised nodes. The defender will aim to reduce the economic value of the attack by defending the optimal set of measurements. Let us consider that the controller uses r_{di} resources out of $|R_d|$ for defending measurement i. The controller also incurs a cost for deploying r_{di} resources. Considering that the attacker uses r_{ai} resources out of $|R_a|$ for measurement i, the cost of compromising the measurements in the network is defined as r_{ai}. Let ρ_a be the probability that the attacker chooses to compromise a measurement, i.e., $r_{ai} > 0$, where $0 \leq \rho_a \leq 1$. Similarly, ρ_d denotes the probability with which the defender chooses to defend the measurements, i.e., $r_{di} > 0$, where $0 \leq \rho_d \leq 1$.

The transition of a measurement from a normal mode ($\eta_i(t) = 0$) to compromised mode ($\eta_i(t) = 1$) at a rate of $r_{ai}\frac{\rho_a r_{ai}}{\rho_d r_{di}}$, where $\frac{r_{ai}}{r_{di}}$ denotes *attack/defense strength* and $\frac{\rho_a}{\rho_d}$ denotes the *attack/defence probability*. The rate of a measurement becoming compromised increases with $\rho_a r_{ai}$ and decreases with $\rho_d r_{di}$. If the measurement is successfully compromised, the controller can recover the measurement only if the attack is detected. Hence, the compromised measurement becomes secure at a rate of $\Pr(||r_a||_2 > \tau)$, which denotes the *detection probability*. This is presented graphically in Fig. 3. Thereby, from the basic understanding of differential dynamic systems [33], the evolution of the state of measurement i over time can be denoted by the following differential equation:

$$\dot{z}_i(t) = r_{ai}(\frac{\rho_a r_{ai}}{\rho_d r_{di}})(1 - z_i(t)) - \Pr(||r_a||_2 < \tau)z_i(t) \quad (68)$$

Based on the above definitions, the payoff matrices of the attacker and defender are given in Table I, using the reasoning:

- In the case both the attacker and the defender allocate a non-zero amount of resources with probability, the node is successfully defended ($\eta_i(t) = 0$) with probability $z_i(t)$. The probability of successful compromise ($\eta_i(t) = 1$) is $1 - z_i(t)$. Further, the attacker and the defender also incur the cost of using the resources.

TABLE I
PAYOFF MATRIX OF THE ATTACKER AND DEFENDER DUE TO i^{th} MEASUREMENT

Defender/Attacker's Utility	**Defend** ($r_{di} > 0$)	**Not Defend** ($r_{di} = 0$)
Attack ($r_{ai} > 0$)	$U_{ai}(t) = z_i(t)J_i^* + (1 - z_i(t))J_i^{a*} - r_{ai}(t)$ $U_{di}(t) = -z_i(t)J_i^* - (1 - z_i(t))J_i^{a*} - r_{di}(t)$	$U_{ai}(t) = J_i^{a*} - r_{ai}(t)$ $U_{di}(t) = -J_i^{a*}$
Not Attack ($r_{ai} = 0$)	$U_{ai}(t) = J_i^*$ $U_{di}(t) = -J_i^* - r_{di}(t)$	$U_{ai}(t) = J_i^*$ $U_{di}(t) = -J_i^*$

- In case the attacker attacks a node ($r_{ai} > 0$) that is not defended ($r_{di} = 0$), the error is introduced in the system with absolute probability. The cost of using resources is only incurred by the attacker.
- In case the defender defends a node ($r_{di} > 0$) that is not attacked ($r_{ai} = 0$), the error is not introduced in the system. The cost of using resources is only incurred by the defender.

Based on the utilities of the players shown in Tables I, the average payoff functions for defending and attacking measurement i at time t are derived as:

$$\bar{U}_{di}(t) = \rho_d\big(\rho_a\big(-z_i(t)J_i^* - (1 - z_i(t))J_i^{a*} - r_{di}(t)\big) + (1 - \rho_a)\big(-J_i^* - r_{di}(t)\big)\big) + (1 - \rho_d)\big(\rho_a\big(-J_i^{a*}\big) + (1 - \rho_a)\big(-J_i^*\big)\big) \tag{69}$$

$$\bar{U}_{ai}(t) = \rho_a\big(\rho_d\big(z_i(t)J_i^* + (1 - z_i(t))J_i^{a*} - r_{ai}(t)\big) + (1 - \rho_d)\big(J_i^{a*} - r_{ai}(t)\big)\big) + (1 - \rho_a)\big(\rho_d\big(J_i^*\big) + (1 - \rho_d)\big(J_i^*\big)\big) \tag{70}$$

If played repeatedly over time, the overall utility of the attacker and defender is obtained by aggregating the utility functions mentioned above over time. The optimization problem for the network controller is to minimize the net cost incurred by the interconnected power system, whereas the attacker aims to maximize the cost. Hence, the optimization problem of the network controller and the attacker is:

$$\min_{r_{di}(t)} \sum_{t=1}^{T} \bar{U}_{di}(t), \;\; s.t. \;(36), (68), \& \sum_{i=1}^{k} r_{di}(t) = |R_d|. \tag{71}$$

$$\min_{r_{ai}(t)} \sum_{t=1}^{T} \bar{U}_{ai}(t), \;\; s.t. \;(37), (68), \& \sum_{i=1}^{k} r_{ai}(t) = |R_a|. \tag{72}$$

Theorem 2: Considering the optimal control by *CA*s in the physical layer, the Hamiltonian function of (71) and (72) can be expressed as:

$$H_q(t) = \bar{U}_{qi}(t) + \mu_q\left(\sum_i r_{qi}(t) - |R_q|\right) + \sum_i \Lambda_{qi}(t)\dot{z}_i(t) + \sum_i \Lambda_i(t)\dot{x}_i(t) \tag{73}$$

where $q = \{d, a\}$. A set of controls $\{r_{di}^*(t), r_{ai}^*(t)\}$ constitutes an equilibrium to the problem in (71) and (72), and $z_i^*(t)$ is the corresponding state trajectory:

$$r_{di}^*(t) = \arg\max_{r_{di}(t)} H_d(t) = \sqrt{\frac{\Lambda_{di}(t) r_{ai}^2 \rho_a (1 - z_i(t))}{\rho_d(-\rho_d(1 - \rho_a) + \mu_d)}} \tag{74}$$

$$r_{ai}^*(t) = \arg\max_{r_{ai}(t)} H_a(t) = \frac{(\rho_a(1 - \rho_d) - \mu_a) r_{di} \rho_d}{2\Lambda_{ai}(t)\rho_a(1 - z_i(t))} \tag{75}$$

Based on (74) and (75), the optimal cyber layer attack/defence resource allocation by the attacker/defender can be obtained in the form of $\Lambda_{ai}(t)/\Lambda_{di}(t)$. For each *CA* and attacker equilibrium strategy, the evolution of the co-state is given as:

$$\dot{\Lambda}_{ai}(t) = \rho_a\rho_d\big(J_i^* - J_i^{a*}\big) - \Lambda_{ai}(t)\left(\frac{\rho_a r_{ai}^2}{\rho_d r_{di}} + \Pr(||r_a||_2 < \tau)\right) - \Lambda_i(t)\big(\mathbf{T}_1^i \mathbf{B}^T \mathbf{C}^T \mathbf{P}(t+1)\mu_i\eta_i\mathbf{CH}\big) \tag{76}$$

$$\dot{\Lambda}_{di}(t) = \rho_d\rho_a\big(-J_i^* + J_i^{a*}\big) - \Lambda_{di}(t)\left(\frac{\rho_a r_{ai}^2}{\rho_d r_{di}} + \Pr(||r_a||_2 < \tau)\right) - \Lambda_i(t)\big(\mathbf{T}_1^i \mathbf{B}^T \mathbf{C}^T \mathbf{P}(t+1)\mu_i\eta_i\mathbf{CH}\big) \tag{77}$$

The evolution of the co-sate of the dynamics in the physical layer is found to be:

$$\dot{\Lambda}_i(t) = -\left(\sum_{r=1}^{k} \mathbf{A}_{ir} - \sum_{r=1}^{k} \mathbf{B}_{ir}\mathbf{K}_u(t)\right) \tag{78}$$

which is dependent on the deviations of the state parameters after applying the control actions in presence of FDIA. The closed-form expression of the Lagrange multipliers corresponding to (71) and (72) are:

$$\mu_d = \frac{1}{\rho_d |R_d|^2}\left(\sum_{i=1}^{k} \Lambda_{di}(t) r_{ai}^2(t)\rho_a(1 - z_i(t))\right) - \rho_d(1 - \rho_a) \tag{79}$$

$$\mu_a = \rho_a(1 - \rho_d) - \frac{|R_a|}{\sum_{i=1}^{k}\left(\frac{r_{di}(t)\rho_d}{2\Lambda_{ai}(t)\rho_a(1 - z_i(t))}\right)} \tag{80}$$

It is evident from (76) and (77) that the evolution of the co-states of the cyber layer dynamics is dependent on the actual value of the co-state of the dynamics in the physical layer. The optimal resource allocation by the defender (74) increases with increasing co-state value. This means that as the rate at which the control cost changes with the node infection rate, increases, the defender allocates more cyber layer resources to minimize the fluctuations. The optimal resource allocation by the attacker (75) decreases with increasing co-state value. This means that as the rate at which the control cost changes with the node infection rate decreases, the attacker allocates more cyber layer resources to maximize the fluctuations.

Remark 4: In practice, ρ_a is decided by the attacker, which will be unknown to the controller. Similarly, ρ_d will be unknown to the attacker. However, the probability distribution of these unknown parameters can be estimated by observing the parameters while interacting repeatedly over time. In this

situation, the solution of the proposed game formulation can be derived by considering the average payoffs as:

$$\bar{U}_{di}(t) = \int_0^1 \rho_d\big(\rho_a\big(-z_i(t)J_i^* - (1-z_i(t))J_i^{a*} - r_{di}(t)\big) + (1-\rho_a)\big(-J_i^* - r_{di}(t)\big)\big) + (1-\rho_d)\big(\rho_a\big(-J_i^{a*}\big) + (1-\rho_a)\big(-J_i^*\big)\big)\mathrm{d}\rho_a$$

$$\bar{U}_{ai}(t) = \int_0^1 \rho_a\big(\rho_d\big(z_i(t)J_i^* + (1-z_i(t))J_i^{a*} - r_{ai}(t)\big) + (1-\rho_d)\big(J_i^{a*} - r_{ai}(t)\big)\big) + (1-\rho_a)\big(\rho_d\big(J_i^*\big) + (1-\rho_d)\big(J_i^*\big)\big)\mathrm{d}\rho_d$$

instead of (69) and (70), respectively. The approach to finding the solution will be the same as discussed in Section III-B.

Remark 5 (Scalability): For $\alpha > 1$, we define $F_d(\alpha, r_{ai}) \triangleq \alpha r_{di}^*(r_{ai}) - r_{di}^*(\alpha r_{ai})$. Then the proof of scalability is equivalent to proving that $F_d(\alpha, r_{ai}) > 0$ for any $\alpha > 1$. First, it is obvious that $F_d(1, r_{ai}) = 0$. Thus the sufficient condition for $F_d(\alpha, r_{ai}) > 0$ is that $F_d(\alpha, r_{ai})$ is an increasing function of α, i.e., $\frac{\partial F_d(\alpha, r_{ai})}{\partial \alpha} > 0$. To proceed further, the first-order and second-order partial derivatives of $F_d(\alpha, r_{ai})$ w.r.t. α are obtained as:

$$\frac{\partial F_d(\alpha, r_{ai})}{\partial \alpha} = \sqrt{\frac{\Lambda_{di}(t) r_{ai}^2 \rho_a (1-z_i(t))}{\rho_d(-\rho_d(1-\rho_a)+\mu_d)}} - \frac{1}{\alpha^3} \times \frac{\sqrt{\Lambda_{di}(t) r_{ai}^2 \rho_a (1-z_i(t))}\Big(\sum_{j\neq i} \Lambda_{dj}(t) r_{aj}^2 \rho_a (1-z_j(t))\Big)}{\Big(\Lambda_{di}(t) r_{ai}^2 \rho_a (1-z_i(t)) + \frac{1}{\alpha^2}\sum_{j\neq i} \Lambda_{dj}(t) r_{aj}^2 \rho_a (1-z_j(t))\Big)^{\frac{3}{2}}} \tag{81}$$

$$\frac{\partial^2 F_d(\alpha, r_{ai})}{\partial \alpha^2} = \frac{3\sqrt{\Lambda_{di}(t) r_{ai}^2 \rho_a (1-z_i(t))}}{\alpha^4} \times \frac{\big(\Lambda_{di}(t) r_{ai}^2 \rho_a (1-z_i(t))\big)\Big(\sum_{j\neq i} \Lambda_{dj}(t) r_{aj}^2 \rho_a (1-z_j(t))\Big)}{\Big(\Lambda_{di}(t) r_{ai}^2 \rho_a (1-z_i(t)) + \frac{1}{\alpha^2}\sum_{j\neq i} \Lambda_{dj}(t) r_{aj}^2 \rho_a (1-z_j(t))\Big)^{\frac{5}{2}}} \tag{82}$$

Since $\frac{\partial^2 F_d(\alpha, r_{ai})}{\partial \alpha^2}$ is always greater than 0, which indicates that $\frac{\partial F_d(\alpha, r_{ai})}{\partial \alpha}$ is increasing in α. A similar conclusion can be drawn by following the above-mentioned steps for the (75). Hence, once the solution in (74) and (75) is found, the equilibrium when any increment in the amount of available resources can be obtained without increased complexity.

IV. Simulations and Results

This section investigates the performance of the networked LFC of a 39-bus power system through unreliable cyber layer resources in the presence of attackers. The IEEE 39-bus test power system, also known as the 39-bus New England system, consists of 39 buses, 29 lines, 46 branches of which 12 transformers, and 10 generating units. The total load is 6150MW, and the total generating capacity is 7300 MVA. The generators are equipped with excitation and power system stabilizer units. Among the 39 buses, one is the slack bus (Bus 31), nine are voltage-controlled buses (Bus 39, Bus 32, Bus 33, Bus 34, Bus 35, Bus 36, Bus 37, Bus 38 and Bus 30) and the rest are load buses. This test system has been chosen because the same system is believed to mimic the properties of a typical power system closely and it has been widely used by previous researchers for various purposes. The power system is split up into control areas such that the generators in each control area will share the maximum amount of load change in that control area's load bus. Based on these criteria, the division of control area 1 is optimal since a load change in the bus in CA_1 is mostly met by the generators in CA_1. For instance, over 75% of the 1% load change applied to any of the buses 25, 26, and 27, of CA_1 are met by the generators of CA_1. However, the separation between CAs 2 and 3 is modified from the existing works such that there is significant tie-line power flow between the control areas when the load at the bus changes. For instance, 29%, 22%, and 25% of a change of 1% load at bus 8 placed in the CA 3 are met by the generators in bus 31, 32, and 30, respectively. Increased power flow on the tie-lines will enable the study of the worst effect of FDIAs, as non-zero tie-line power measurement will increase the probability of successfully injecting stealthy false data. On the other hand, 75% of the energy demand is met by the generators of CA_2 when 1% load change happens in any of the loads in buses 3, 4, 15, 16, 18, 20-24, 31. To present the problem addressed in this paper, the dynamic model of the LFC for a system with three *CA*s is considered (Fig. 4) where the state variables, control signals and process errors are obtained by modifying the definitions in (2), (3), and (4) for a three *CA* system.

The linear model of the three *CA* system is obtained by modifying the definitions in (8) and (14):

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_1 & \mathbf{0} & \mathbf{0} & \mathbf{A}_{10} \\ \mathbf{0} & \mathbf{A}_2 & \mathbf{0} & \mathbf{A}_{20} \\ \mathbf{0} & \mathbf{0} & \mathbf{A}_3 & \mathbf{A}_{30} \\ \mathbf{A}_{01} & \mathbf{A}_{02} & \mathbf{A}_{03} & \mathbf{0} \end{bmatrix}, \mathbf{B} = \begin{bmatrix} \mathbf{B}_1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{B}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{B}_3 \\ 0 & 0 & 0 \end{bmatrix},$$

$$\mathbf{E} = \begin{bmatrix} \mathbf{E}_1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{E}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{E}_3 \\ 0 & 0 & 0 \end{bmatrix} \mathbf{C} = \begin{bmatrix} \mathbf{C}_1 & \mathbf{0} & \mathbf{0} & \mathbf{C}_{10} \\ \mathbf{0} & \mathbf{C}_2 & \mathbf{0} & \mathbf{C}_{20} \\ \mathbf{0} & \mathbf{0} & \mathbf{C}_3 & \mathbf{C}_{30} \end{bmatrix}$$

where $M_i = 1.67$, $D_i = 0.083$, $T_{ti} = 0.30$, $T_{gi} = 0.08$, $\sigma_i = 2.4$, $\beta_i = 0.5$, and $X_{tie} = 3.93$. The tie-line power deviation between the three *CA*s are defined as:

$$\Delta P_{tie,12} = \Delta P_{2,3} + \Delta P_{27,17}$$
$$\Delta P_{tie,23} = \Delta P_{5,8} + \Delta P_{7,8}$$
$$\Delta P_{tie,13} = \Delta P_{2,1}$$

The three-area power system simulation experiment in this article is carried out on MATLAB 2022a. The aim of the controller is to minimize the change in frequency and tie line flows due to disturbances and FDIA to near-zero values by generating control signals to adjust the generation to match the load demand.

A. Cyber Layer Differential Game

The objective of the controller is to allocate the available cyber layer resources to protect the measurements from FDIAs. Here, the total resources available with the controller and the attacker are denoted as $|R_d|$ and $|R_a|$, whereas the resources allocated by them for the i^{th} measurement are represented as r_{di} and r_{ai}. The effect of cyber layer resource allocation on the corresponding physical layer measurements is studied in Figs. 5 and 6. For ease of presentation, an FDIA is considered only on the tie-line power measurements for

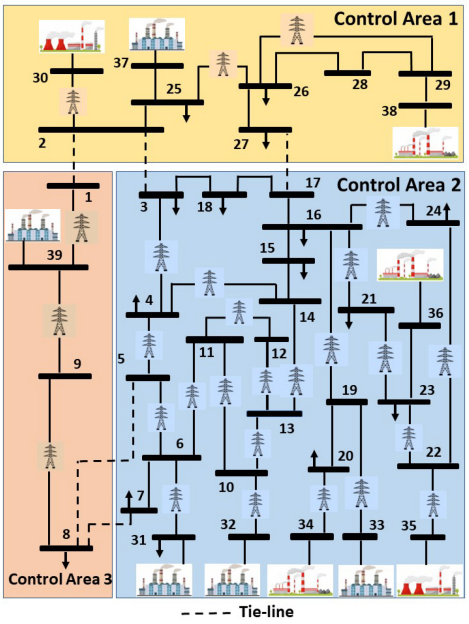


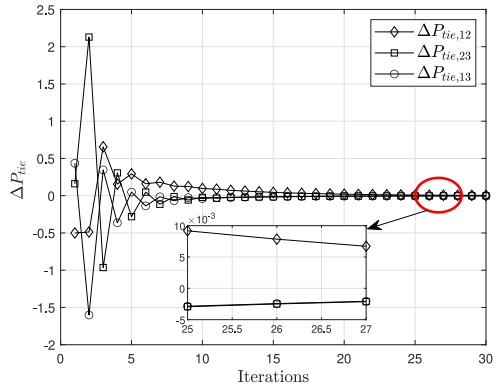
Fig. 4. Single-line diagram of the IEEE 39-bus test system.

preparing this result. It is evident from Fig. 5(a) and 6(a) that the deviation of the $\Delta P_{tie,12}$ is 0.007 when the probability of allocating cyber layer resources to defend the corresponding measurement is 0.25. As the probability of allocating cyber resources to defend the measurement is 0.5, the $\Delta P_{tie,12}$ deviation becomes 0.005 in Figs. 5(b) and 6(b). Finally, the deviation of the $\Delta P_{tie,12}$ becomes 0.0009 in Figs. 5(c) when the probability of allocated cyber layer resources to defend the corresponding measurement is 0.6 (evident from Fig. 6(c)). This observation is intuitive as allocating more resources to defend the cyber layer will reduce the effect of the FDIAs.

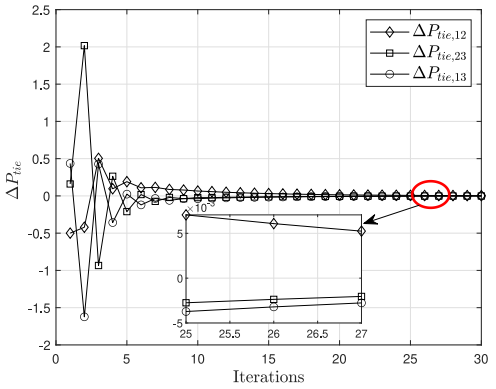
B. Differential Game Based LFC

For the LFC, the weight matrices in the cost functions of the three control areas are considered as time-invariant matrices having $Q_1(1,1) = Q_1(10,10) = Q_1(12,12) = Q_2(1,4) = Q_3(7,7) = Q_3(11,11) = Q_3(12,12) = 1$. Control cost penalty matrices have $R(1,1) = 5$, $R(2,2) = 10$, and $R(3,3) = 5$. The values of all other elements in the above matrices are zero. The aversions to the process error for the three *CA*s shown in Fig. 4 are considered to be $W_1 = 1.3$, $W_2 = 1.5$, and $W_3 = 1.2$. The time horizon T is set as 100. The noise and the node compromise rate used in simulating the Nash equilibrium, derived in (36), are illustrated in Fig. 7.

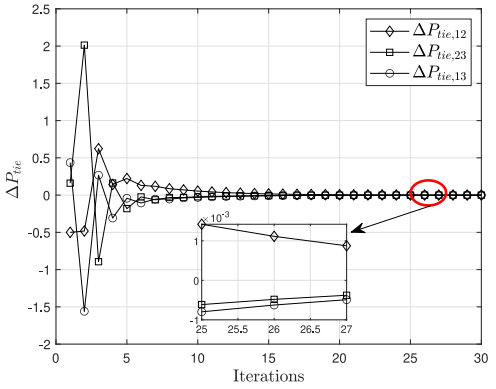
A coordinated FDIA is implemented on the LFC of CA_1 at $t = 1s$. The frequency deviation, tie-line power deviation, and ACE signal of the system after FDIA, targeting the frequency and tie-line power is launched, are shown in Fig. 8(a). The deviation of the ACE signal for the CA_1 (as shown in Fig. 8(a)) proves it is erroneous, causing the CA_1's frequency and tie-line power to further deviate from the set value. The deviation will spread to affect other interconnected *CA*s. The deviations of the frequency and tie-line power and the ACE signals of CA_2 and CA_3 after implementing FDIA on the LFC system of CA_1 are also shown in Fig. 8(a). It can be concluded that, if left



(a)



(b)



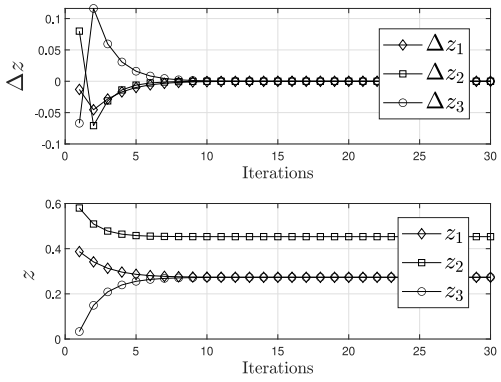
(c)

Fig. 5. Variation of ΔP_{tie} for the following allocations cyber layer resources (a) $\frac{r_{d1}}{r_{a1}} = 0.4$, $\frac{r_{d2}}{r_{a2}} = 0.3$, $\frac{r_{d3}}{r_{a3}} = 0.3$, (b) $\frac{r_{d1}}{r_{a1}} = 0.6$, $\frac{r_{d2}}{r_{a2}} = 0.3$, $\frac{r_{d3}}{r_{a3}} = 0.1$, (c) $\frac{r_{d1}}{r_{a1}} = 0.7$, $\frac{r_{d2}}{r_{a2}} = 0.2$, $\frac{r_{d3}}{r_{a3}} = 0.1$.

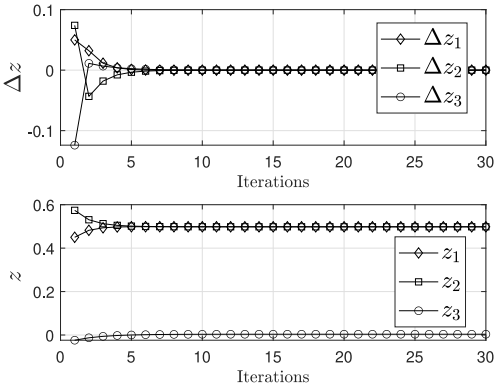
unattended, the power system will be in an unstable state due to the FDIA attack on CA_1. Next, the effect of the proposed control and defence mechanism will be analyzed.

We compare the proposed cyber layer differential game approach with the following scenarios:

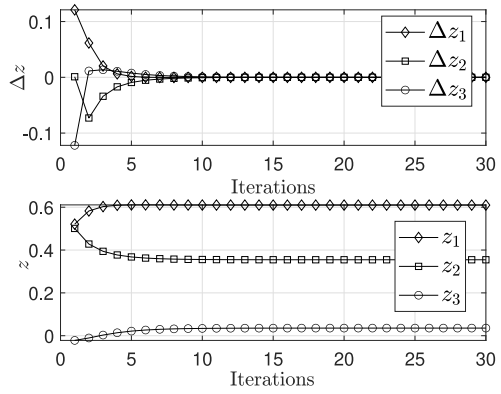
- *Scenario 1:* Attacker and grid operator allocate cyber layer resources according to (72) and (71).
- *Scenario 2:* Grid operator allocates cyber layer resources according to (71); Attacker allocates resources uniformly, i.e., $r_{ai}(t) = |R_a|/k$.



(a)



(b)



(c)

Fig. 6. Variation of Δz and z for the following allocations cyber layer resources (a) $\frac{r_{d1}}{r_{a1}} = 0.4$, $\frac{r_{d2}}{r_{a2}} = 0.3$, $\frac{r_{d3}}{r_{a3}} = 0.3$, (b) $\frac{r_{d1}}{r_{a1}} = 0.6$, $\frac{r_{d2}}{r_{a2}} = 0.3$, $\frac{r_{d3}}{r_{a3}} = 0.1$, (c) $\frac{r_{d1}}{r_{a1}} = 0.7$, $\frac{r_{d2}}{r_{a2}} = 0.2$, $\frac{r_{d3}}{r_{a3}} = 0.1$.

- *Scenario 3:* Attacker allocates cyber layer resources according to (72); Grid operator allocates resources uniformly, i.e., $r_{di}(t) = |R_d|/k$.
- *Scenario 4:* Grid operator and attacker uniformly allocate their cyber layer resources, i.e., $r_{di}(t) = |R_d|/k$ and $r_{ai}(t) = |R_a|/k$, respectively.

In Scenario 1, the accumulative costs incurred by the CA_1, CA_2, and CA_3 are $J_1 = 2.13$, $J_2 = 3.74$, and $J_3 = 2.03$, respectively. The expected costs in Scenarios 2, 3, and 4 are (2.98, 3.83, 2.67), (3.24, 3.24, 2.42), and (2.54, 3.34, 2.87),

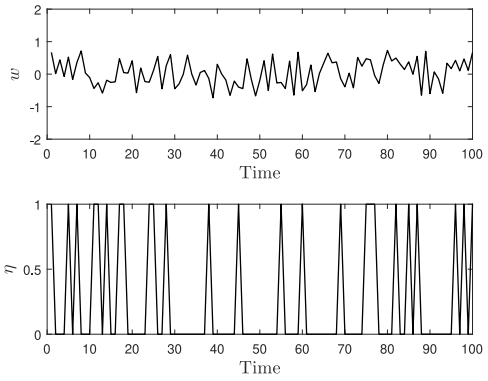
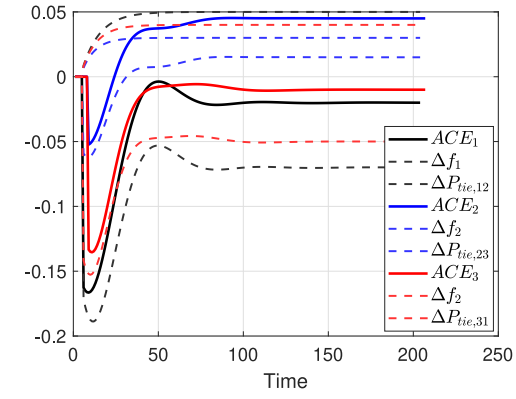


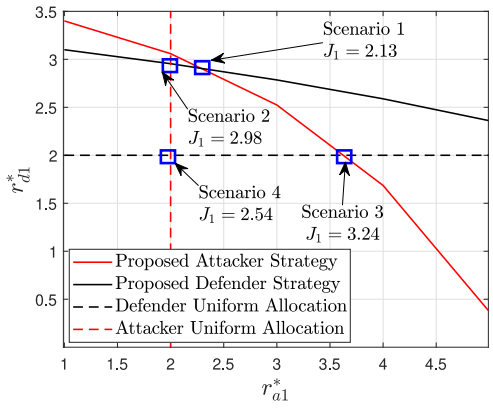
Fig. 7. Noise and node compromise rate Vs. time.

respectively. These costs are depicted in Fig. 8(b) as the intersection point of the strategies of the attacker and the defender. For Scenario 1, the plots of strategies are obtained from (71) and (72). To find the actual reason for the improvement in the cost, the deviations of the ACE signals are plotted in Fig. 8(c). The difference between the accumulative cost of each player for Scenario 1 and the other scenarios, shows that the basic concept of Nash equilibrium brings an extra decrease in cost. Nash equilibrium states that the unilateral deviation of the attack and the control in Scenarios 2 and 3 from the saddle point, given in (94) and (95), results in the cost margin provided by the Nash equilibrium strategies adopted by the *CA*s. Further, the cost incurred in Scenario 1 can be optimized for ρ_a and ρ_d. The optimal cost value is 1.068 from the plot in Fig. 9(a). The tie-line power measurement, with and without FDIA, is listed in Table II. The attacker injects false data in the tie-line data, leading to a generation load imbalance in the system. The deviation in the power flow due to false data is the least in Scenario 1 because the attacker and the defender are competing against each other to maximize their objectives. The deviation in the power flow data is maximum for Scenario 3 when the attacker causes maximum damage by optimally allocating resources according to (72), whereas the defender uniformly allocates its resources. Following Scenario 2, the controller incurs more cost in comparison to Scenarios 1 and 4, whereas the incurred cost is less than Scenario 3.

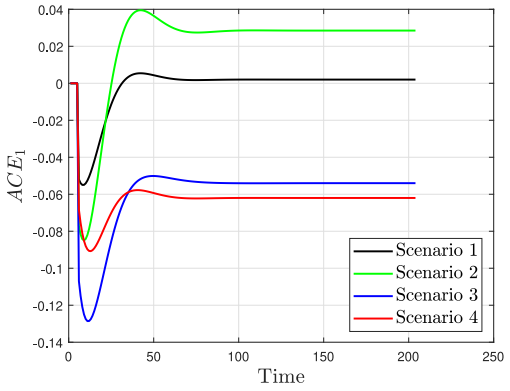
Next, we compare the performance of the proposed non-cooperative game-based differential control with PI controller and a centralized controller. The optimum values of PI controller parameters are unknown. The initial values of these parameters are chosen randomly and are then tuned using an optimization algorithm. We have chosen the integral time absolute error (ITAE) as the objective function that is minimized by the genetic algorithm (GA). The centralized controller generates the control signals by solving an optimization problem where the objective function is the aggregate of (17), $\forall i = 1, \ldots, k$. Constraints have also been modified accordingly. It is evident from the plot in Fig. 10 that the deviation of the tie-line power is maximum for the PI controller. The proposed LQDG controller performs better than the PI controller as both load disturbance and worst-case attack vector are considered at the same time for the generation control of the CAs. The root mean square error (RMSE) of both controllers



(a)

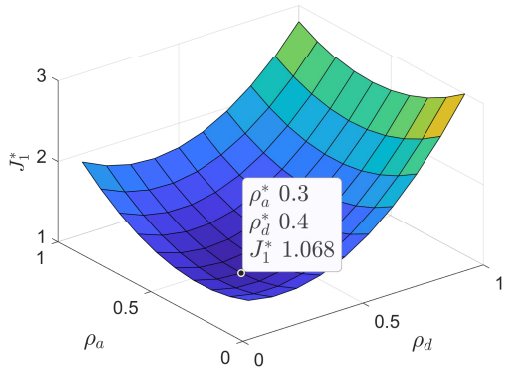


(b)

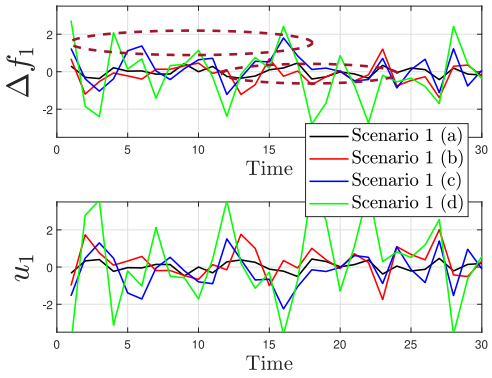


(c)

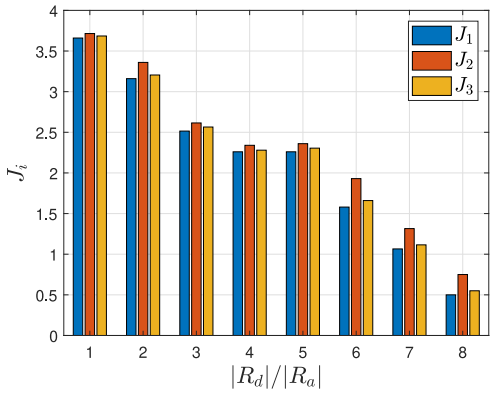
Fig. 8. (a) State variables after the attack, (b) Comparison of the 4 scenarios in terms of J_1, (c) Comparison of the 4 scenarios in terms of ACE_1.



(a)



(b)



(c)

Fig. 9. (a) Optimal cost J_1^* for varying ρ_a and ρ_d, (b) Variation of state variable and control signal for scenarios 1(a), 1(b), 1(c), and 1(d), (c) Variation of cost J_i for varying $\frac{R_d}{R_a}$.

related to the setpoints reveals that there is around 8.77% improvement using the LQDG controller in the tie-line power deviation while there is an improvement of 18.09% in terms of frequency deviation. The maximum frequency and tie-line power deviation of the proposed LQDG controller are also smaller than the PI controller by 4.7% and 6.6%, respectively. The control of deviations in the state variables is hard for the PI controller since the load disturbance is not included in the structure of the PI controller. The PI controller only reacts to the load disturbance after it causes deviations in the referenced frequency and tie-line power measurements. Although the proposed controller performs better than the PI controller, the deviation in tie-line power is 3.1% more than the centralized controller. The difference in the performance of the proposed and the centralized scheme is due to the concept called *Price of Anarchy* [34]. Following the proposed LQDG-based LFC, the generation of each CA is controlled to mitigate the deviations of that CA. On the contrary, the centralized differential game-based controller controls the generation of all the CAs to minimize the deviation of the state variables of the CAs, leading to more efficient control. The RMSE of

TABLE II
ACTUAL AND MODIFIED TIE-LINE FLOWS

Tie-Line	True $\Delta P_{tie,ij}$	False $\Delta P_{tie,ij}$			
		Scenario 1	Scenario 2	Scenario 3	Scenario 4
2-3	81.78	-216.98	88.12	-136.43	30.48
27-17	-310.75	81.74	-374.8	72.87	-142.3
5-8	212.63	140.6	53.2	-130.2	-20.4
7-8	-162.87	-501.63	-132.1	176.74	56.7
2-1	-185.88	145.37	-34.1	-213.4	-321.5

TABLE III
COMPARISON OF VARIOUS PARAMETERS FOR THE PROPOSED, CENTRALIZED, AND PI CONTROLLERS

Parameters	Scenario 1 with η^*		
	Proposed	Centralized	PI Controller
J_1	1.623	1.583	1.834
J_2	0.723	0.586	0.943
J_3	0.63	0.42	0.754
$\text{Var}\{\mathbf{y}^T(t)\mathbf{Q}_1\mathbf{y}(t)\}$	1.35	0.62	1.85
$\text{Var}\{\mathbf{y}^T(t)\mathbf{Q}_2\mathbf{y}(t)\}$	1.32	1.25	1.78
$\text{Var}\{\mathbf{y}^T(t)\mathbf{Q}_3\mathbf{y}(t)\}$	1.30	0.82	1.69
$Prob\{\|\|\mathbf{r}(t)+\mathbf{a}(t)-\boldsymbol{\eta}(t)\mathbf{CH}\|\|_2 \le \tau\}$	0.88	0.82	0.76

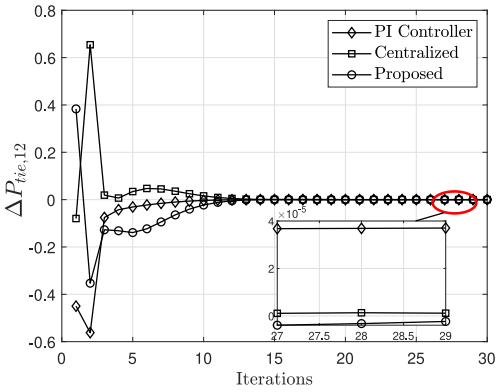


Fig. 10. Tie-line power deviation for the proposed, centralized, and PI controllers.

the centralized controller shows an improvement of 2.43% in comparison to the proposed LQDG controller in tie-line power, while there is an improvement of 7.38% in terms of frequency deviation. The maximum frequency and tie-line power deviation of the centralized controller are also smaller than the proposed LQDG-based controller by 5.57% and 3.21%, respectively. However, the advantage of the proposed scheme over the centralized scheme is its immunity against FDIA on the control signals since they are generated locally at each *CA*. Further, the exact values of some of the important parameters of the considered system are listed in Table III, for the proposed, centralized, and PI controllers. It is evident from the table that both the proposed and the centralized schemes perform better than the PI controller. Following the centralized scheme, the control cost and variance cost are minimum for CA_3 and CA_2, respectively. However, the control cost and variance cost are more evenly distributed among the *CA*s in the proposed scheme. This is due to the competitive interaction among the *CA*s in a non-cooperative framework. For the same reason, the detection probability of the centralized scheme is better than the proposed scheme.

Fig. 8(b) shows that the cyber layer differential game approach outperforms the other scenarios. Next, we compare the following scenarios for the physical layer LFC: (1a) *Proposed LQR in (17)-(20)*, (1b) *Proposed LQR without (20)*, (1c) *Proposed LQR without risk* ($\kappa_i = 0$) *with (20)* and (1d) *Conventional LQR without risk* ($\kappa_i = 0$) *and (20)*. In (1a), CA_1 minimizes the tie-line power and frequency deviations following the proposed differential game-based control. As per the game formulation, the actions of CA_1 also affect the tie-line power in CA_2 and CA_3. Further, the control signal of CA_1 impels the variation in CA_2 and CA_3, which hinders CA_2 and CA_3 from keeping the frequency and other tie-line powers at the desired setpoint. Thus, the strategy of CA_2 and CA_3, as well as the attack and the inevitable disturbance perturbing the LFC system, should be considered when CA_1 constructs its control strategy and vice versa. This coupled construction of control and attack strategies is handled by Theorem 1 from a non-cooperative differential game-theoretic perspective. The control actions of the *CA*s corresponding to the Nash equilibrium are illustrated in Fig. 9(b). With the control and attack strategies obtained, the state trajectory of the closed-loop system is shown in Fig. 9(b). Scenarios (1a), (1b), and (1c) are compared based on the two regions highlighted in 9(b). It is evident that the peak deviations are more prominent for scenarios (1c) and (1d) due to the absence of risk measures. Although the peak deviations are not prominent for (1b), deviations are consistently more than (1a) due to the absence of attack detection. Hence, the control cost for (1a), (1b), (1c), and (1d) are 3.12, 8.3, 9.4, and 11.2, respectively. The minimum control cost for the proposed technique reinforces its efficacy.

The equilibrium values of z_i derived for different values of $|R_d|/|R_a|$ are listed in Table IV. z_i values for other scenarios are also listed in Table IV. For each resource budget ratio $|R_d|/|R_a|$, the bi-level differential game among the *CA*s and the attacker is solved according to the proposed solution in (36)–(37). The resulting measurement compromise rates z_i^*

TABLE IV
NODE COMPROMISE RATE VS. THE RATIO OF CYBER LAYER RESOURCES AVAILABLE TO DEFENDER AND ATTACKER

$\lvert R_d\rvert/\lvert R_a\rvert$	**0.75**	**0.95**	**1.15**	**1.30**
z^* (**Scenario 1**)	0.54	0.623	0.68	0.703
z^* (**Scenario 2**)	0.47	0.58	0.72	0.68
z^* (**Scenario 3**)	0.32	0.42	0.63	0.61
z^* (**Scenario 4**)	0.63	0.53	0.74	0.74

under different resource budgets for the attacker and defender in the cyber-layer are listed in Table IV. It can be deduced that the increase in the cyber layer resource budget decreases the measurement compromise rate, leading to the rise of FDIA detection probability and improved performance in the physical layer.

The effect of the stochastic nature of $\boldsymbol{\Delta P_d}$ is studied by simulating the bi-level differential game 30 times for various combinations of cyber layer resource budgets of the attacker and the controller. The mean of the resulting costs (15) of each *CA* is calculated and plotted in Fig. 9(c). The controlling costs of all the *CA*s decrease with the increase of the $|R_d|/|R_a|$, which in turn reflects the improvement of the control performance in the physical layer caused by the reduced capabilities of the attacker in the cyber layer. Further, the worst performance of CA_2 in terms cost is due to the fact that r_{d23}/r_{a23} and r_{d2}/r_{a2} are the least among all the *CA*s.

To test the effectiveness of the proposed controller under random changes in load perturbation, a random varying step load perturbation is considered in CA_1 as seen in Fig. 11(a). Simulating the IEEE 39-bus power system with the load perturbation shown in Fig. 11(a) results in the frequency deviations of CA_1 as shown in Fig. 11(b). The results in Fig. 11(b) confirm that the frequency deviation of the CA_1 is within acceptable limits, thus satisfying the robustness of the proposed controller under the random change in load disturbances. A sensitivity analysis of the proposed bi-level LQDG is also conducted, where ΔP_{d1}, generated for different values of variance W_1, are employed in the power system to investigate the stability of the proposed framework. It can be observed from Fig. 11(b) that although both the maximum deviation and the convergence time increase as the variance increases, the proposed method is still able to control the frequency deviation. The reason for this behavior has been identified in (27), where the control gain becomes more stringent in directions that are prone to noise variance.

Next, we investigate the importance of the design of chance constraint in (20) by plotting J_i with varying τ and ϵ in Fig. 12. As ϵ increases, the constraint on the design of the attack vector becomes more stringent. Consequently, the false data introduced by the attacker is reduced, resulting in a decrease of J_i. On the other hand, as τ increases, the attack vector space increases, thereby increasing the control cost for the *CA*s.

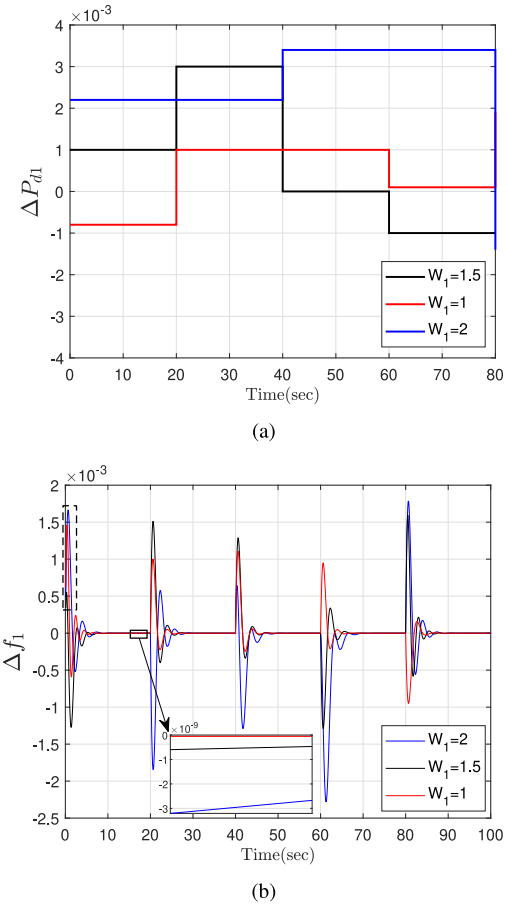


Fig. 11. (a) Load disturbance with varying variance, (b) Effect of load disturbance on the frequency deviation of CA_1.

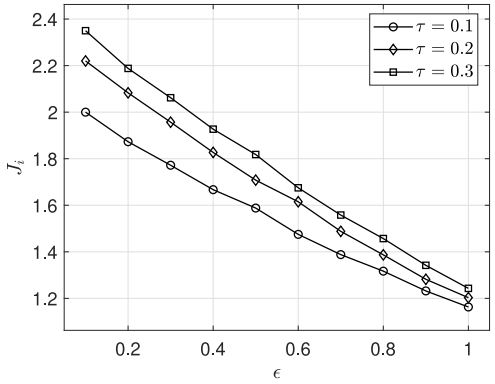


Fig. 12. Control cost J_i vs. ϵ for varying τ values.

V. CONCLUSION

This paper has established a novel bi-level differential game-theoretic framework of LFC, considering the decision-making of an attacker and controller in both the cyber and physical layers. In the cyber layer game, the status of the cyber layer nodes has been designed using a state-space model, where the transition between the states depends on the allocation of resources. Thereby, the resource allocation among multiple nodes by the attacker and the controller has been investigated from the viewpoint of a non-cooperative game. In the physical layer, the resource allocation of the attacker and the controller is investigated subject to some practical constraints from the viewpoint of minimizing the cost of controlling a power system when the attacker designs an attack with

minimum detection probability. We have finally illustrated the effectiveness of the proposed control architecture through simulations of a three-control area IEEE 39 bus system. The proposed comprehensive bi-level game framework shows improvements in minimizing the average and peak deviations of the state variables compared to standalone differential game-based LFC. The proposed game framework performs better than the conventional PI controller and closely follows the performance of a centralized controller. The differential game model proposed in this paper can be used to mimic a scenario where the first player (the controller) attempts to minimize the cost in the event that his opponent (attacker) engages in the worst possible conduct (targeted unknown disturbances). Control problems, such as the safe landing of aircraft in the presence of wind shear [35] and an autonomous convoy of vehicles with tampered location data [36], can be addressed using the algorithm developed in this work. The analysis presented in this work is limited by the fact that LQDG based LFC problem is solved considering the attacker takes optimal decisions representing the worst case for the controller. Further, this work does not explicitly model the spread of infections of the cyber layer nodes and their influences on attackers' and controllers' decisions, which will be addressed in our future work. Additionally, in future, we will investigate the performance of a cooperative game-based differential game framework under FDIAs and implement the theoretical findings in a real-time simulation environment.

APPENDIX

Proof (Lemma 1): Let $\Delta(t) \triangleq \mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t) - \mathbb{E}\{\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t)|\mathcal{F}_{t-1}\}$ be the prediction error of the stage penalty at time t given $\mathcal{F}_{t-1}$. Next, the closed form representation is derived for the expected predictive variance $\mathbb{E}\{\Delta^2(t)\}$. The output $\mathbf{y}(t)$ of the LFC depends on states $\mathbf{x}(t)$, input $\mathbf{u}(t)$, attack vector $\mathbf{a}(t)$, and past noises $\Delta\mathbf{P_d}(t)$. Let us define:

$$\hat{\mathbf{y}}(t) \triangleq \mathbb{E}\{\mathbf{y}(t)|\mathcal{F}_{t-1}\} = \mathbf{C}\big(\mathbf{A}\mathbf{x}(t-1) + \mathbf{B}\mathbf{u}(t-1) + \mathbf{E}\Delta\bar{\mathbf{P}}_d\big) + \mathbf{a}(t) \tag{83}$$

$$\delta(t) \triangleq \Delta\mathbf{P}_d(t) - \Delta\bar{\mathbf{P}}_d \tag{84}$$

where $\mathbb{E}\{\Delta\mathbf{P}_d(t)\} = \Delta\bar{\mathbf{P}}_d$. Replacing $\mathbf{y}(t)$ with $\hat{\mathbf{y}}(t) + \mathbf{C}\mathbf{E}\delta(t)$:

$$\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t) = \hat{\mathbf{y}}^T(t)\mathbf{Q}_i\hat{\mathbf{y}}(t) + 2\hat{\mathbf{y}}^T(t)\mathbf{Q}_i\mathbf{C}\mathbf{E}\delta(t) + \delta^T(t)\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\mathbf{C}\mathbf{E}\delta(t) \tag{85}$$

The expectation of $\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t)$ conditioned on $\mathcal{F}_{t-1}$ is

$$\mathbb{E}\big\{\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t)|\mathcal{F}_{t-1}\big\} = \hat{\mathbf{y}}^T(t)\mathbf{Q}_i\hat{\mathbf{y}}(t) + Tr\big\{\mathbf{W}\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\mathbf{C}\mathbf{E}\big\} \tag{86}$$

where $\mathbf{W} = \mathbb{E}\{(\Delta\mathbf{P}_d(t) - \Delta\bar{\mathbf{P}}_d(t))(\Delta\mathbf{P}_d(t) - \Delta\bar{\mathbf{P}}_d(t))^T\}$. Then, finding the difference between the above quantities and taking its square:

$$\mathbb{E}\Big\{\Delta^2(t)|\mathcal{F}_{t-1}\Big\} = m_4 + 4\hat{\mathbf{y}}^T(t)\mathbf{Q}_i\mathbf{C}\mathbf{E}\mathbf{W}\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\hat{\mathbf{y}}(t) + 4\hat{\mathbf{y}}^T(t)\mathbf{Q}_iM_3 \tag{87}$$

where $m_4 \triangleq \mathbb{E}\Big\{\big(\delta^T(t)\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\mathbf{C}\mathbf{E}\delta(t) - Tr\big\{\mathbf{W}\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\mathbf{C}\mathbf{E}\big\}\big)^2\Big\}$

$M_3 \triangleq \mathbb{E}\big\{\mathbf{C}\mathbf{E}\delta(t)\big(\delta^T(t)\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\mathbf{C}\mathbf{E}\delta(t)\big)\big\}$

Repeating the expectation operation gives:

$$\mathbb{E}\Big\{\Delta^2(t)\Big\} = m_4 + \mathbb{E}\big\{4\hat{\mathbf{y}}^T(t)\mathbf{Q}_i\mathbf{C}\mathbf{E}\mathbf{W}\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\hat{\mathbf{y}}(t) + 4\hat{\mathbf{y}}^T(t)\mathbf{Q}_iM_3\big\} \tag{88}$$

By orthogonality property of $\hat{\mathbf{y}}(t)$, $\delta(t)$ and since $\mathbb{E}\{\delta(t)\} = 0$ and $\mathbb{E}\{\delta^T(t)\delta(t)\} = \mathbf{W}$, we get:

$$\mathbb{E}\Big\{\Delta^2(t)\Big\} = \mathbb{E}\big\{4\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{C}\mathbf{E}\mathbf{W}\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\mathbf{y}(t) + 4\mathbf{y}^T(t)\mathbf{Q}_iM_3\big\} + m_4 - 4Tr\big\{\mathbf{W}\mathbf{Q}_i\mathbf{C}\mathbf{E}\mathbf{W}\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\big\} \tag{89}$$

Proof (Lemma 3): The Lagrangian of the optimization problem in (17)-20) is formulated and consequently expanded as:

$$\begin{aligned}
&\mathcal{L}(\mathbf{y}(t), \mathbf{u}(t), \mathbf{a}(t), \{\mu_i\}, \xi)\\
&= \mathbb{E}\left\{\frac{1}{2}\sum_{t=0}^{T-1}\big(\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t) + \mathbf{u}^T(t)\mathbf{R}_i\mathbf{u}(t)\big) + \mathbf{y}^T(T)\mathbf{Q}_i\mathbf{y}(T)\right\}\\
&+\kappa_i\Bigg(\mathbb{E}\Bigg\{\sum_{t=1}^{T}\big(4\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{C}\mathbf{E}\mathbf{W}\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\mathbf{y}(t) + 4\mathbf{y}^T(t)\mathbf{Q}_iM_3\big)\\
&\qquad + m_4 - 4Tr\big\{\mathbf{W}\mathbf{Q}_i\mathbf{C}\mathbf{E}\mathbf{W}\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\big\}\Bigg\}\Bigg)\\
&+\mu_{ijp}(\boldsymbol{\eta}_i)\mathbb{E}\Big\{\big\|\mathbf{y}(t) - \mathbf{C}\mathbf{x}(t) + \mathbf{a}(t) - \boldsymbol{\eta}_i\mathbf{C}\mathbf{H}\big\|_2^2 - \tau^2\Big\} \qquad (90)\\
&= \mathbb{E}\left\{\frac{1}{2}\sum_{t=0}^{T-1}\big(\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{y}(t) + \mathbf{u}^T(t)\mathbf{R}_i\mathbf{u}(t)\big) + \mathbf{y}^T(T)\mathbf{Q}_i\mathbf{y}(T)\right\}\\
&+\kappa_i\big(\mathbb{E}\big\{4\mathbf{y}^T(t)\mathbf{Q}_i\mathbf{C}\mathbf{E}\mathbf{W}\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\mathbf{y}(t) + 4\mathbf{y}^T(t)\mathbf{Q}_iM_3\big\} + m_4\\
&\qquad -4Tr\big\{\mathbf{W}\mathbf{Q}_i\mathbf{C}\mathbf{E}\mathbf{W}\mathbf{E}^T\mathbf{C}^T\mathbf{Q}_i\big\}\big)\\
&+\mathbb{E}\Big\{\boldsymbol{\mu}_i\Big(\mathbf{r}^T(t)\mathbf{r}(t) + \mathbf{r}^T(t)\mathbf{a}(t)\\
&\qquad -\boldsymbol{\eta}_i\mathbf{r}^T(t)\mathbf{C}\mathbf{H} + \mathbf{a}^T(t)\mathbf{r}(t) + \mathbf{a}^T(t)\mathbf{a}(t) - \boldsymbol{\eta}_i\mathbf{a}^T(t)\mathbf{C}\mathbf{H}\\
&\qquad -\boldsymbol{\eta}_i\mathbf{H}^T\mathbf{C}^T\mathbf{r}(t) - \boldsymbol{\eta}_i\mathbf{H}^T\mathbf{C}^T\mathbf{a}(t) + \boldsymbol{\eta}_i^2\mathbf{H}^T\mathbf{C}^T\mathbf{C}\mathbf{H}\Big)\Big\} \qquad (91)
\end{aligned}$$

Rearranging the terms in (90), we get the compact Lagrangian representation in (25). ■

Proof (Theorem 1): The proof is carried out by applying the technique of mathematical induction.

1. The value of the Lagrange function at stage $t = T$ can be determined from the standard definition as:

$$\mathcal{L}^*(\mathbf{y}(T), \{\mu_i\}, \xi) = \mathbf{y}^T(T)\mathbf{Q}(T)\mathbf{y}(T) \tag{92}$$

which satisfies the condition $\mathbf{P}(T) = \mathbf{Q}(T)$.

2. Stage $t = 0, \ldots, T-1$. Function value at stage $t+1$ is:

$$\mathcal{L}^*(\mathbf{y}(t), \{\mu_i\}, \xi) = \inf_{\mathbf{u}(t)}\sup_{\mathbf{a}(t)}\mathbb{E}\big\{g_t(\mathbf{u}(t), \mathbf{a}(t), \{\mu_i\}) + g_\mu(\{\mu_i\}) + \mathcal{L}^*_{t+1}(\mathbf{y}(t+1), \{\mu_i\})|\mathcal{F}_t\big\} \tag{93}$$

Thereby, Bellman's principle of optimality is applied to get the optimal actions at stage t. Hence, $\mathbf{u}^*(t)$ and $\mathbf{a}^*(t)$

is derived according to the following coupled first-order conditions:

$$\begin{aligned}&\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\mathbf{CA}\mathbf{x}(t)+\left(\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\mathbf{CB}+\mathbf{R}_i\right)\mathbf{u}(t)\\&+\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\mathbf{CE}\bar{\Delta}\mathbf{P}_d+\mathbf{B}^T\mathbf{C}^T\mathbf{P}(t+1)\mathbf{a}(t+1)\\&+\mathbf{B}^T\mathbf{C}^T\mathbf{L}(t+1)=0.\end{aligned}\tag{94}$$

$$\begin{aligned}&\left(\mathbf{P}(t+1)\mathbf{CA}+\mathbf{Q}_i\mathbf{C}+4\kappa_i\mathbf{Q}_i\mathbf{CEWE}^T\mathbf{C}^T\mathbf{Q}_iC\right)\mathbf{x}(t)\\&+\mathbf{P}(t+1)\mathbf{a}(t+1)+\left(Q_i+4\kappa_i\mathbf{Q}_i\mathbf{CEWE}^T\mathbf{C}^T\mathbf{Q}_i\right)\mathbf{a}(t)\\&\mathbf{P}(t+1)\mathbf{CBu}(t)+\mathbf{P}(t+1)\mathbf{CE}\bar{\Delta}\mathbf{P}_d+\mathbf{L}(t+1)+4\kappa_i\mathbf{Q}_i\mathbf{M}_3\\&+\sum_i\mu_i\left(\mathbf{r}(t)+\mathbf{a}(t)-\boldsymbol{\eta}_i(t)\mathbf{CH}\Pr(\boldsymbol{\eta}_i)\right)=0\end{aligned}\tag{95}$$

Proof (Theorem 2): The candidate optimal strategies of the attacker and the defender can be found using Pontryagin's maximum principle-based necessary condition. In this regard, the Hamiltonian of the attacker and defender is (73). Performing maximization/minimization on (73) yields (74) and (75). For $\{r_{di}^*\}$ and $\{r_{ai}^*\}$ to be the equilibrium strategies of the cyber-layer game and $\{z_i^*\}$ to be the corresponding state trajectory, there should exist the co-state functions in (76), (77), and (78) using:

$$\dot{\Lambda}_{ai}(t)=-\frac{\partial H_a(t)}{\partial z_i},\ \dot{\Lambda}_{di}(t)=-\frac{\partial H_d(t)}{\partial z_i},\ \&\ \dot{\Lambda}_i(t)=-\frac{\partial H_q(t)}{\partial x_i}.$$

Proof (Lemma 4): Let us denote $C(\{\mu_i\},\xi)=(||\mathbf{y}^*(\{\mu_i\},\xi)-\mathbf{Cx}^*(\{\mu_i\},\xi)+\mathbf{a}^*(\{\mu_i\},\xi)-\boldsymbol{\eta}_j(t)\mathbf{CH}||_2^2-\tau^2)\zeta_j$. To prove part 1) in Lemma 4, we consider $\mu_i'>\mu_i>0$. From definitions of the optimal solution of the dual problem, we can conclude that $(\mu_i'-\mu_i)\{C(\{\mu_i\},\xi)-C(\mu_i',\{\mu_{-i}\},\xi)\}\geq 0$, which shows that $C(\{\mu_i\},\xi)>C(\mu_i',\{\mu_{-i}\},\xi)$. To prove (50) of Lemma 4, it is sufficient to show that for $\mu_i^*>0$, $C(\mu_i^*,\{\mu_{-i}\},\xi)=0$. From (36) and (37), it is evident that $C(\{\mu_i\},\xi)$ is continuous function of $\{\mu_i\}$ and ξ. Now if we assume that $C(\{\mu_i\},\xi)<0$, then by continuity $0<\bar{\mu}_i<\mu_i^*$ such that $C(\bar{\mu}_i,\{\mu_{-i}\},\xi)$, which contradicts (50). Let $E(\mathbf{u},\mathbf{a})=J(\mathbf{u},\mathbf{a})+Var(y^T(\mathbf{u},\mathbf{a})Qy(\mathbf{u},\mathbf{a}))$. Suppose there are $\mathbf{u}^\dagger$,$\mathbf{a}^\dagger$ such that $C(\mathbf{u}^\dagger,\mathbf{a}^\dagger)$. For every $\mu_i\geq 0$, we find $D(\{\mu_i\},\xi)-\mu_iC(\mathbf{u}^\dagger,\mathbf{a}^\dagger)\leq E(\mathbf{u}^\dagger,\mathbf{a}^\dagger)\leq\infty$. Next suppose that for every $\mu_i>0$, $C(\mathbf{u}^*,\mathbf{a}^*)\geq 0$. Since $E(\mathbf{u}^*,\mathbf{a}^*)$ is increasing $E(\mathbf{u}^\dagger,\mathbf{a}^\dagger)\geq 0$ which contradicts $E(\mathbf{u}^\dagger,\mathbf{a}^\dagger)<\infty$.

Proof (Lemma 5): The pair $(\mathbf{CA},\mathbf{T}_2^{i\,1/2})$ is detectable as $\mathbf{T}_2^i\succeq\mathbf{Q_i}$ and $(\mathbf{CA},\mathbf{Q_i}^{1/2})$ is detectable. Following the standard theory of LQR controller, the exponential convergence of $\mathbf{P}(t)$, $\mathbf{K}_u(t)$, and $\mathbf{K}_a(t)$ to $\mathbf{P}$, $\mathbf{K}_u$, and $\mathbf{K}_a$, respectively, and the stability of $(\mathbf{CA}+\mathbf{CBK}_u(t)+\mathbf{K}_a(t))$ are ensured due to the fact that $(\mathbf{CA},\mathbf{CB})$ can be stabilized, $(\mathbf{CA},\mathbf{T}_2^{i\,1/2})$ is detectable and $\mathbf{R}_i\succ 0$. Similar steps can be used to demonstrate the convergence of the remaining terms.

REFERENCES

[1] R. D. Christie and A. Bose, "Load frequency control issues in power system operations after deregulation," *IEEE Trans. Power Syst.*, vol. 11, no. 3, pp. 1191–1200, Aug. 1996.

[2] C. Konstantinou and M. Maniatakos, "A case study on implementing false data injection attacks against nonlinear state estimation," in *Proc. 2nd ACM Workshop Cyber-Phys. Syst. Security Privacy*, 2016, pp. 81–92.

[3] A. Intriago, F. Liberati, N. D. Hatziargyriou, and C. Konstantinou, "Residual-based detection of attacks in cyber-physical inverter-based microgrids," *IEEE Trans. Power Syst.*, vol. 39, no. 2, pp. 4020–4038, Mar. 2024.

[4] A. D. Syrmakesis, H. H. Alhelou, and N. D. Hatziargyriou, "Novel SMO-based detection and isolation of false data injection attacks against frequency control systems," *IEEE Trans. Power Syst.*, vol. 39, no. 1, pp. 1434–1446, Jan. 2024.

[5] X. Bu, W. Yu, Y. Yin, and Z. Hou, "Event-triggered data-driven control for nonlinear systems under frequency-duration-constrained DoS attacks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1449–1460, 2023.

[6] N. Vafamand, M. M. Arefi, M. H. Asemani, and T. Dragičević, "Decentralized robust disturbance-observer based LFC of interconnected systems," *IEEE Trans. Ind. Electron.*, vol. 69, no. 5, pp. 4814–4823, May 2022.

[7] Y. Zheng et al., "Power system load frequency active disturbance rejection control via reinforcement learning-based memetic particle swarm optimization," *IEEE Access*, vol. 9, pp. 116194–116206, 2021.

[8] W. Bi, C. Chen, and K. Zhang, "Optimal strategy of attack-defense interaction over load frequency control considering incomplete information," *IEEE Access*, vol. 7, pp. 75342–75349, 2019.

[9] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "A robust policy for automatic generation control cyber attack in two area power network," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, 2010, pp. 5973–5978.

[10] R. Zhang and P. Venkitasubramaniam, "False data injection and detection in LQG systems: A game theoretic approach," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 1, pp. 338–348, Mar. 2020.

[11] 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. 42160–42179, 2023.

[12] A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, 2010, pp. 1096–1101.

[13] C. Lin, B. Hu, C. Shao, W. Li, C. Li, and K. Xie, "Delay-dependent optimal load frequency control for sampling systems with demand response," *IEEE Trans. Power Syst.*, vol. 37, no. 6, pp. 4310–4324, Nov. 2022.

[14] P. Tooranjipour, B. Kiumarsi, and H. Modares, "Risk-aware safe optimal control of uncertain linear systems," in *Proc. 58th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, 2022, pp. 1–5.

[15] N. Koumpis, A. Tsiamis, and D. Kalogerias, "State-output risk-constrained quadratic control of partially observed linear systems," in *Proc. IEEE 61st Conf. Decis. Control (CDC)*, 2022, pp. 188–195.

[16] A. W. Al-Dabbagh, Y. Li, and T. Chen, "An intrusion detection system for cyber attacks in wireless networked control systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 8, pp. 1049–1053, Aug. 2018.

[17] A.-Y. Lu and G.-H. Yang, "Stability analysis for cyber-physical systems under denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 51, no. 11, pp. 5304–5313, Nov. 2021.

[18] Z. Ming, H. Zhang, Y. Li, and Y. Liang, "Mixed H_2/H_∞ control for nonlinear closed-loop Stackelberg games with application to power systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 21, no. 1, pp. 69–77, Jan. 2024.

[19] Z. Zhang, J. Hu, J. Lu, J. Cao, and F. E. Alsaadi, "Preventing false data injection attacks in LFC system via the attack-detection evolutionary game model and KF algorithm," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 6, pp. 4349–4362, Nov./Dec. 2022.

[20] A. Gupta, C. Langbort, and T. Başar, "Dynamic games with asymmetric information and resource constrained players with applications to security of cyberphysical systems," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 71–81, Mar. 2017.

[21] Y. Ma, Z. Hu, and Y. Song, "A reinforcement learning based coordinated but differentiated load frequency control method with heterogeneous frequency regulation resources," *IEEE Trans. Power Syst.*, vol. 39, no. 1, pp. 2239–2250, Jan. 2024.

[22] C. Mu, K. Wang, and C. Sun, "Learning control supported by dynamic event communication applying to industrial systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2325–2335, Apr. 2021.

[23] X. Tong, D. Ma, R. Wang, X. Xie, and H. Zhang, "Dynamic event-triggered-based integral reinforcement learning algorithm for frequency control of microgrid with stochastic uncertainty," *IEEE Trans. Consum. Electron.*, vol. 69, no. 3, pp. 321–330, Aug. 2023.

[24] C. Mu, K. Wang, Z. Ni, and C. Sun, "Cooperative differential game-based optimal control and its application to power systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5169–5179, Aug. 2020.

[25] P. Srikantha and D. Kundur, "A DER attack-mitigation differential game for smart grid security analysis," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1476–1485, May 2016.

[26] H. Chen, R. Ye, and R. Lu, "Differential games based load frequency control of interconnected power system," in *Proc. IEEE PES Asia-Pac. Power Energy Eng. Conf. (APPEEC)*, 2013, pp. 1–5.

[27] Y. Li, D. Shi, and T. Chen, "False data injection attacks on networked control systems: A Stackelberg game analysis," *IEEE Trans. Autom. Control*, vol. 63, no. 10, pp. 3503–3509, Oct. 2018.

[28] X. He, X. Liu, and P. Li, "Coordinated false data injection attacks in AGC system and its countermeasure," *IEEE Access*, vol. 8, pp. 194640–194651, 2020.

[29] S. Hu, X. Ge, Y. Li, X. Chen, X. Xie, and D. Yue, "Resilient load frequency control of multi-area power systems under DoS attacks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 936–947, 2023.

[30] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29775–29818, 2021.

[31] A. Ferdowsi, W. Saad, and N. B. Mandayam, "Colonel blotto game for sensor protection in interdependent critical infrastructure," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2857–2874, Feb. 2021.

[32] F. Fotiadis, A. Kanellopoulos, and K. G. Vamvoudakis, "Constrained differential games for secure decision-making against stealthy attacks," in *Proc. Am. Control Conf. (ACC)*, 2020, pp. 4658–4663.

[33] H. K. Khalil, *Nonlinear Systems*. London, U.K.: Pearson Educ., 2002.

[34] X. Qin, B. Li, and L. Ying, "Efficient distributed threshold-based offloading for large-scale mobile cloud computing," *IEEE/ACM Trans. Netw.*, vol. 31, no. 1, pp. 308–321, Feb. 2023.

[35] M. Yue, H. Zheng, H. Cui, and Z. Wu, "GAN-LSTM-based ADS-B attack detection in the context of air traffic control," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12651–12665, Jul. 2023.

[36] S. Iqbal, P. Ball, M. H. Kamarudin, and A. Bradley, "Simulating malicious attacks on VANETs for connected and autonomous vehicle cybersecurity: A machine learning dataset," in *Proc. 13th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, 2022, pp. 332–337.