Cyber-Resilient Automatic Generation Control for Systems of AC Microgrids

Tong Huang, Member, IEEE, Dan Wu, Member, IEEE, and Marija Ilić, Member, IEEE

Abstract—In this paper we propose a co-design of the secondary frequency regulation in systems of AC microgrids and its cyber security solutions. We term the secondary frequency regulator a Micro-Automatic Generation Control (μAGC) for highlighting its same functionality as the AGC in bulk power systems. We identify sensory challenges and cyber threats facing the μAGC. To address the sensory challenges, we introduce a new microgrid model by exploiting the rank-one deficiency property of microgrid dynamics. This model is used to pose an optimal μAGC control problem that is easily implemented, because it does not require fast frequency measurements. An end-to-end cyber security solution to the False Data Injection (FDI) attack detection and mitigation is developed for the proposed μAGC. The front-end barrier of applying off-the-shelf algorithms for cyber attack detection is removed by introducing a data-driven modeling approach. Finally, we propose an observer-based corrective control for an islanded microgrid and a collaborative mitigation scheme in systems of AC microgrids. We demonstrate a collaborative role of systems of microgrids during cyber attacks. The performance of the proposed cyber-resilient μAGC is tested in a system of two networked microgrids.

Index Terms—Cyber security, automatic generation control for microgrids (μAGC), networked microgrids, inverter-based resource (IBR), false data injection (FDI).

I. INTRODUCTION

THE RECENT decade has witnessed several large-scale electricity outages due to low-probability but high-impact events, such as extreme weather. Examples include the 2012 Hurricane Sandy power outage, the 2020 California rotating electricity outage caused by extreme heat wave [1], and the 2021 Texas power crisis resulting from unusually severe winter storms [2]. During these extreme weather-related events, the bulk transmission systems failed to supply sufficient electric energy to distribution systems, causing millions of businesses and homes to lose their electricity supply [1], [2]. One promising solution to enhance resilience of distribution systems to these extreme events is to integrate Distributed Energy Resources (DERs), e.g., solar panels, micro-turbines, and energy storage, to the distribution systems. However, a large-scale deployment of DERs in the distribution systems introduces unprecedented complexity and the need for extensive Distribution Management Systems (DMSs) [3], [4]. To reduce the management complexity, a distribution system with massive DERs can be configured to be a system of microgrids. Neighboring loads, DERs and their grid infrastructure are clustered into an AC or DC, small-scale power system, i.e., a microgrid. One microgrid can either operate autonomously in an islanded mode [5], or connect to its host distribution system in a grid-connected mode [5], or as an interactive network with its neighboring microgrids and form a system of microgrids that does not physically connect to their host distribution system in a hybrid mode. Each microgrid is managed by the Microgrid Management System (μMS). In such a configuration, the management burden of the DMS is significantly reduced, as the DMS only needs to coordinate several μMSs [3], [4], [5], [6].

For an AC microgrid, frequency regulation is an important functional block in the μMS design, especially when the microgrid enters the islanded or hybrid mode. Similar to bulk transmission systems, frequencies at the microgrid can be regulated in a hierarchical manner. The bottom layer of the frequency regulation entails local controllers in DERs, e.g., power controllers of inverter-based resources (IBRs), and governors of small synchronous generators. These local controllers are termed the primary control of microgrids [5], [6]. As the primary control can yield steady-state errors of frequencies from their nominal values after a disturbance, a secondary control layer is needed in microgrids to regain the nominal frequency [7], [8]. Since the secondary frequency regulation in AC microgrids shares a very similar objective with the Automatic Generation Control (AGC) of bulk transmission systems, we term the secondary frequency regulator in microgrids Micro-AGC (μAGC) to highlight its connection with the AGC that has served the bulk power systems for half of a century. This paper focuses on the μAGC design.

There is a large body of literature that addresses the μAGC design. These design schemes can be generally categorized into centralized, distributed, and decentralized control [9]. Centralized μAGC relies on a monopolistic decision-making platform that gathers measurements from the
DERs under control, computes regulation signals, and dispatches these signals to the DERs [10], [11]. \textit{Distributed $\mu$AGC} employs cooperative control policies among neighboring DERs to achieve certain objectives. It can be further classified into three sub-groups: averaging-based methods [7], distributed-consensus-based methods [12], and event-triggering-based methods [13]. In \textit{decentralized $\mu$AGC} design, each DER participating in the $\mu$AGC recovers its own nominal frequency to a nominal value independently. The washout filter is investigated in [14] and shown to be equivalent to a decentralized secondary control. In [15], a decentralized linear–quadratic regulator (LQR) control design is proposed to achieve frequency restoration in an optimal way. Another idea to achieve decentralized frequency regulation is based on state estimation. The estimation-based $\mu$AGC [16] employs the system states estimated locally instead of the true measurements to generate control signals.

However, a system of microgrids equipped with the $\mu$AGC design mentioned above may be still vulnerable to physical disturbances and/or cyber anomalies. Compared with high-voltage transmission systems, a microgrid is more sensitive to physical disturbances, e.g., load/renewable power fluctuations, and IBR connection and re-connection, due to its small scale and the zero/low inertia of its generation units [5], [17]. These disturbances cause large, and fast fluctuations of microgrid frequencies. The frequency changes induced by the disturbances may not be captured in an accurate and timely manner by the frequency sensors (shall be shown in Section II-B). However, almost all the above-mentioned $\mu$AGC design schemes utilize frequency measurements to make decisions. It is assumed that the frequency information can be reported by DERs or it can be accurately measured in a fast manner. In practice, while the frequency information can be produced by the IBR power controller as a digital, internal control command [18], such a digital signal may not be available for a third-party $\mu$AGC,\footnote{By the third-party $\mu$AGC, we mean that the $\mu$AGC service is not designed and implemented by the inverter manufacture.} and it can only be indirectly obtained by external frequency sensors. As a result, the desirable control performance of the $\mu$AGC relying on accurate frequency measurements might not be attained, especially with fast fluctuations from renewable generation and load. Therefore, it is advantageous to develop a $\mu$AGC that does not depend on the frequency information when a microgrid enters the islanded or hybrid operating mode.

Another important consideration for the $\mu$AGC design is the cyber security. While the distributed and decentralized $\mu$AGC schemes reduce the cyber risks of the $\mu$AGC by sparsifying or eliminating long-distance communication links among DERs, these $\mu$AGC schemes may still susceptible to the false data injection (FDI) attack where the sensors can be manipulated to report wrong information to the $\mu$AGC. Many references concern attenuating the influence of the FDI attacks [19]. One category of methods explores state estimation techniques [20], for example, the Kalman filter method [21] and optimization-based state estimation methods [22]. These methods either rely on the accuracy of measurements or heavy computations [23]. To address these challenges, observer-based detection and control methods have been proposed [19], [24]. Recently, the unknown input observer (UIO) has found a broad range of applications in FDI attack detection and cyber-resilient control designs [25], [26] since it can separate the external disturbances from the attack signals, yielding a more sensitive anomaly diagnosis. However, these cyber security solutions are built upon existing $\mu$AGC designs that require accurate frequency information. It is an open-ended question whether these solutions can extend to other control designs that require different information other than frequencies. While some cyber attack solutions [27], [28] are designed for a general model that serves as an abstraction of many engineering systems, e.g., a state-space model, the model that should be used for the purpose of developing cyber solutions heavily depends on the information feeding its controller. For a specific controller, it might not be straightforward to derive a proper model that lends itself to the cyber solution design even for domain experts. Therefore, the development of $\mu$AGC and its cyber solution are interdependent.

To overcome these challenges in this paper we introduce a co-design of $\mu$AGC and its cyber solutions. We identify the sensory challenges and cyber vulnerability facing the $\mu$AGC design. To address the sensory challenges, we introduce a new microgrid modeling approach by exploiting the structure of microgrid dynamics, i.e., the property of rank-one deficiency. Such a modeling approach leads to an optimal $\mu$AGC that is easily implemented, as it does not require fast frequency measurements that can be hard to obtain [29]. An end-to-end cyber security solution to FDI attack detection and mitigation is developed for the proposed $\mu$AGC. The front-end barrier of applying off-the-shelf algorithms for cyber attack detection is removed by introducing a data-driven modeling approach. Besides, we propose an observer-based corrective control for an islanded microgrid and a collaborative mitigation scheme in systems of AC microgrids. Compared with the existing $\mu$AGC design, the contribution of this paper is summarized as follows: 1) The proposed $\mu$AGC can regulate microgrid frequencies in the presence of both load/renewable power fluctuations and FDI cyber attacks; 2) Compared with the $\mu$AGC design that requires internal digital signals of DERs or fast frequency measurements, the proposed $\mu$AGC is more practically implementable, as it only requires real-time real power which can be measured fast and accurately; 3) Compared with the method that is specifically designed for one type of DERs [15], the proposed $\mu$AGC design can address systems of microgrids with heterogeneous DERs; and 4) We demonstrate the role of systems of microgrids in terms of attenuating the influence of cyber attacks.

The rest of this paper is organized as follows: Section II presents the challenges facing the $\mu$AGC design; Section III introduces the new microgrid modeling approach that is used for designing the $\mu$AGC in the presence of fast load/renewable power fluctuations; Section IV demonstrates the cyber security solutions to the proposed $\mu$AGC; and Section V tests the proposed $\mu$AGC and its cyber security solutions.
Fig. 1. A microgrid with N IBRs and M loads and the control scheme of IBRs. The control variables of loops 1 and 2 are voltage and current measurements from the LC filter, and the modulation index, respectively.

II. NEW MODELING FOR μAGC DESIGN

This section starts with describing the dynamics of systems of microgrids in the conventional state space where voltage phase angles and frequencies are used as the state variables. Then we point out the limitations of conventional μAGC design. We derive a new model which lends itself to more robust μAGC with respect to measurement inaccuracies and cyber attacks.

A. Conventional Microgrid Modeling for μAGC Design

We consider a microgrid with N IBRs and M loads. Without loss of generality, the IBRs are connected to the first N nodes, and the loads and the point that networks with the neighboring microgrids locate at nodes N + 1, N + 2, . . ., N + M, as shown in Figure 1. The effect of the neighboring microgrids on the power fluctuations. If we need ωi to converge to ωnom, ωsi should be set to ωs: where ωs = ωnom + mpP Gi.

Define ∆ωi = ωi − ωnom, ∆ωt = ωt − ωnom, ∆P Gi = P Gi − P Gi, and ∆ωsi = ωsi − ωs. Use ∆xi = [∆δi, ∆ωt, ∆ωsi]T as a state vector. Then, Equation (3) becomes

\[ \dot{x}_i = A_i \Delta x_i + B_1 \Delta \omega_s + B_2 \Delta P_G \]

where

\[ A_i = \begin{bmatrix} 0 & 1 \\ 0 & -\omega_{ci} \end{bmatrix}, \quad B_1 = \begin{bmatrix} 0 \\ \omega_{ci} \end{bmatrix}, \quad B_2 = \begin{bmatrix} 0 \\ -mp_i \omega_{ci} \end{bmatrix}. \]

The dynamics for N IBRs can be described by

\[ \Delta \dot{x} = A G \Delta x + B_1 \Delta \omega_s + B_2 \Delta P_G \]

where

\[ \Delta x = [\Delta x_1^T, \ldots, \Delta x_N^T]^T; \quad \Delta \omega_s = [\Delta \omega_{s1}, \ldots, \Delta \omega_{sN}]^T; \]

\[ \Delta P_G = [P_{G1}, \ldots, P_{GN}]^T; \quad A_G = \text{diag}(A_1, \ldots, A_N); \]

\[ B_1 = \text{diag}(B_{11}, \ldots, B_{1N}); \quad B_2 = \text{diag}(B_{21}, \ldots, B_{2N}). \]

2) Network Constraints: For the microgrid under study, its neighboring microgrids that can be networked with can be considered power injection. For simplicity, real power and voltage magnitudes are assumed to be decoupled, i.e., the voltage magnitudes V_i for i ∈ {1, 2, . . ., N + M} are constant. The IBRs and loads are interconnected via microgrid network which introduces algebraic constraints for i ∈ {1, 2, . . ., N + M}:

\[ P_i = V_i^* g_i - \sum_{k=1, k \neq i}^{N+M} V_i^* V_k^* Y_{ik} \cos(\delta_{ik} - \theta_{ik}) = 0 \]

where P_i is the net real injection to node i; g_i denotes the self-conductance of node i; the admittance of the branch from the i-th to the k-th node is Y_{ik}Δθ_{ik}; V_i is the nominal voltage magnitude at node i; and δ_{ik} is the voltage phase angle difference between nodes i and k, i.e., δ_{ik} = δ_i − δ_k. Denote by (P_i^*, Q_i^*, V_i^*, P^{*}_{ij}, Q^{*}_{ij}, V^{*}_{ij}) | i = 1, 2, . . . , N + M the operating condition that satisfies constraints (7). Define the following vectors

\[ \Delta P_i := [\Delta P_{i1}, \ldots, \Delta P_{iN+M}]^T = [\Delta P_{G1}^T, \Delta P_{L1}^T]^T \]

\[ \Delta \delta := [\Delta \delta_1, \ldots, \Delta \delta_{N+M}]^T = [\Delta \delta_G, \Delta \delta_L]^T \]

where \Delta P_{Li} and \Delta \delta_i are the deviations of P_{li} and \delta_i from P_{li} and \delta_i^*, respectively; \Delta P_G = [\Delta P_{G1}, \ldots, \Delta P_{GN}]^T; \Delta P_L = [\Delta P_{N+1}, \ldots, \Delta P_{N+M}]^T; \Delta \delta_i = [\Delta \delta_1, \ldots, \Delta \delta_N]^T; \Delta \delta_L = [\Delta \delta_{N+1}, \ldots, \Delta \delta_{N+M}]^T; \quad \text{and the subscript of} \ "^T" \ \text{of} \ \Delta P_{li} \ \text{stands for} \ "\text{Injection}." \ \text{If} \ \Delta P_{li} \ \text{and} \ \Delta \delta_i \ \text{for all} \ i \ \text{are small, the relationship between} \ \Delta P_{li} \ \text{and} \ \Delta \delta_i \ \text{can be described by} \]

\[ \Delta P_i = H \Delta \delta \]

where the entry h_{i,k} of the i-th row and the k-th column of H R^(N+M) x (N+M) can be obtained via

\[ h_{i,k} = V_i^* V_k^* \cos(\delta_{ik} - \theta_{ik}) \quad \forall k \neq i \]

\[ h_{i,i} = - \sum_{p=1, p \neq i}^{N+M} V_i^* V_p^* \sin(\delta_{ip}^* - \theta_{ip}). \]
Equation (9) is equivalent to

\[
\begin{bmatrix}
\Delta P_G \\
\Delta P_L 
\end{bmatrix} = \begin{bmatrix}
H_{GG} & H_{GL} \\
H_{LG} & H_{LL} 
\end{bmatrix} \begin{bmatrix}
\Delta \delta_G \\
\Delta \delta_L 
\end{bmatrix} 
\] (11)

where \( H_{GG} \in \mathbb{R}^{N \times N} \), \( H_{GL} \in \mathbb{R}^{N \times M} \), \( H_{LG} \in \mathbb{R}^{M \times N} \), and \( H_{LL} \in \mathbb{R}^{M \times M} \). Based on the above equation, \( \Delta P_G \) can be expressed as a function of \( \Delta \delta_G \) and \( \Delta P_L \), i.e.,

\[
\Delta P_G = (H_{GG} - H_{GL}H_{LL}^{-1}H_{LG})\Delta \delta_G + H_{GL}H_{LL}^{-1}\Delta P_L. 
\] (12)

3) System Dynamics: Plugging (12) into (5), we have

\[
\Delta \dot{x} = A\Delta x + B_1 \Delta \omega_i + F \Delta P_L 
\] (13)

where \( A = A_G + B_2(H_{GG} - H_{GL}H_{LL}^{-1}H_{LG})E; \) and \( F = B_2H_{GL}H_{LL}^{-1} \). In the expression of matrix \( A \), matrix \( E = \text{diag}(E_1, \ldots, E_N) \) where \( E_i = [1, 0] \) for \( i = 1, \ldots, N \). It is worth noting that dynamics (13) directly establish the connection between the frequency change \( \Delta \omega_i \) and the load/tie-line flow fluctuations \( \Delta P_L \).

4) Two Common Assumptions for Conventional \( \mu \)AGC Design: The objective of \( \mu \)AGC is to drive the frequency deviations \( \{\Delta \omega_i\}_{i=1}^N \) to zero by tuning the setpoints of IBRs \( \omega_{s,i} \) in the presence of load/renewable power fluctuations \( \Delta P_L \). With such an objective, a centralized \( \mu \)AGC typically tunes the setpoints \( \omega_{s,i} \) of the IBRs under control by measuring the frequency at a critical node. A decentralized/distributed \( \mu \)AGC observes its local frequency and other variables, e.g., local real power \( P_{Gi} \), to tune its local setpoint \( \omega_{s,i} \). Note that these \( \mu \)AGC design schemes are generally built upon at least one of the following two assumptions: 1) An IBR can report its true frequency \( \omega_i \) to its \( \mu \)AGC, or \( \omega_i \) can be measured accurately by external sensors; and 2) The measurements feeding the secondary controllers are authentic. However, it is possible that neither assumption holds in practice. This will be elaborated in the following two subsections.

B. Sensory Challenges of \( \mu \)AGC Design

The frequency \( \omega_i \) is used as an input for many conventional \( \mu \)AGC to tune the setpoint \( \omega_{s,i} \). For a commercial inverter, this variable is an internal, digital control command that might not be accessible for a third-party \( \mu \)AGC. One alternative solution in order to obtain \( \omega_i \) is to measure the frequency of the fundamental component of terminal voltage at the \( i \)-th IBR. However, it is challenging to measure frequency both fast and accurately in practice. Figure 2 shows the sensory challenges when actual frequency changes fast and the frequency is required to be measured fast. In Figure 2, the orange lines represent the true frequency of three-phase sinusoidal waves, while the blue curves shows the frequencies measured by a Simulink Phasor Measurement Unit (PMU) block [30]. In Figure 2(a), the true frequency changes at the 1-st second, the measured frequency converges to the true frequency. The measurement error is acceptable if the PMU reports the frequency at a slow rate, say 10 samples per second (10 Hz). However, large measurement errors may exist from time \( t = 1 \) s to \( t = 1.1 \) s, if frequency is required to be reported every 0.01 seconds (100 Hz). Furthermore, as shown in Figure 2(b), if the frequency keeps fluctuating, the large measurement errors can persist when a high sampling rate, say, 100 Hz, is required.

One obvious question is why a high sampling rate of measurements is necessary for \( \mu \) AGC, compared with the conventional AGC in bulk transmission systems which issues control commands every 2-4 seconds [31], [32]. The reason is that the fast, large frequency fluctuations are more pronounced in small systems like microgrids than in the bulk transmission systems. Similar to the bulk transmission systems, there are volatile loads/renewables that keep perturbing the microgrid, which cause the microgrid frequencies to keep fluctuating. Compared with the transmission systems, the microgrid is more sensitive to these disturbances due to its smaller scale and the low inertia of its DERs [5]. As a result, the microgrid frequencies may have large, fast fluctuations. To regulate the microgrid frequencies to their nominal values, the rate of issuing control commands should be much faster than the rate at which disturbances change. Otherwise, the frequencies may not be regulated. To issue the fast control commands, the fast and accurate measurements are needed. Since the frequency cannot be measured accurately in a fast manner, a conventional \( \mu \)AGC that takes measured frequency as inputs cannot achieve its desirable control performance. This motivates us to design a fast \( \mu \)AGC without using the fast measurements of frequencies. The solution that addresses the sensory challenge is presented in Section III.

C. Cyber Vulnerability of \( \mu \)AGC

A third-party \( \mu \)AGC coordinates IBRs based on sensor measurements. Figure 3 shows the communication architecture of the proposed \( \mu \) AGC where the sensors that measure electrical variables send their measurements to \( \mu \) AGC via a Wide Area Network (WAN) [33]. Various protocols can be applied to the WAN to establish wireless communication between the sensors and \( \mu \) AGC (See [33] for more details of the protocols). FDI attacks can be launched by intruding into the WAN and/or manipulating the sensors. For most wireless communication, license-free ISM (industrial, scientific, and medical) radio band is used [33]. As a result, the bandwidth can be legally accessed by attackers who aim to tamper with the information transmitted through the communication channel [33]. The risks of such a type of attacks can be reduced by latest cryptographic mechanisms [33]. This paper focuses on
the FDI attacks launched via the sensors shown in Figure 3. Such a type of attacks is feasible in real world. For example, [34] has designed and demonstrated a device that can introduce FDI attack on Hall sensors in a non-intrusive manner by changing an external magnetic field. If such cyber attacks occur in the sensors shown in Figure 3, all control commands from the $\mu$AGC can compromise the safety and efficiency of the microgrids. For example, a cyber attacker can blind the $\mu$AGC by launching a replay attack, i.e., the actual measurements $y$ is replaced by a sequence of pre-recorded $y$ [31]. As another example, an adversary may compromise the efficiency of the $\mu$AGC by superposing random noise upon the actual measurements $y$. Such a FDI attack is termed the noise injection attack [31]. A large body of literature presents cyber attack models and objectives in the context of power grids (see [35], [36] and the references therein) and power electronics devices (See [37] and the references therein). A key question is how to design the $\mu$AGC that is resilient to the FDI attacks on the information feeding the $\mu$AGC. Section IV proposes a potential answer to this question.

III. Fast Micro-Automatic Generation Control

This section introduces a new model that exploits the rank-deficiency property of the microgrid dynamics and describes the microgrid behaviors in a new state space. Such a model lends itself to address the sensory challenge in the presence of fast load/renewable power fluctuations. Based on the model in the new space, we introduce a fast $\mu$AGC for a system of microgrids.

A. New State Space Modeling of Microgrid Dynamics

We describe the microgrid dynamics in a new state-space by exploiting the rank-deficiency property of the system matrix $A_i$ in (4). Such a property is used for analyzing bulk transmission systems in our previous work [38], [39]. It is obvious that $A_i$ is rank deficient, i.e., one of eigenvalues of $A_i$ is zero. Denote by $T_i \in \mathbb{R}^{1 \times 2}$ the left eigenvector associated with the zero eigenvalue of matrix $A_i$. By definition, we have $T_iA_i = 0$. One choice of $T_i$ is

$$T_i = [\omega_{kl}, 1]. \quad (14)$$

Define a scalar $z_i$ as follows:

$$z_i := T_i \Delta x_i. \quad (15)$$

Multiplying both sides of (4) by $T_i$, we obtain

$$\dot{z}_i = \omega_{kl} \Delta \omega_{kl} - m_p \omega_{kl} \Delta P_{Gi}. \quad (16)$$

Here, we show that the scalar $z_i$ lends itself to design a fast $\mu$AGC. The reason lies in the following two observations:

- **Observation 1**: $z_i$ reflects the frequency regulation objective: a zero $\dot{z}_i$ implies that $\Delta \omega_{kl}$ tends to zero.
- **Observation 2**: Computing $z_i$ only requires $P_{Gi}$, suggesting that $z_i$ can be obtained in a fast manner.

**Observation 1** results from Equations (4) and (16) that lead to

$$\Delta \dot{\omega}_{kl} = -\omega_{k} \Delta \omega_{kl} + \dot{z}_i. \quad (17)$$

With a zero $\dot{z}_i$, $\Delta \omega_{kl}(t)$ tends to zero, as time $t$ tends to infinity, given any initial condition $\Delta \omega_{kl}(0)$. This is because the scalar system $\Delta \dot{\omega}_{l} = -\omega_{k} \Delta \omega_{kl}$ is asymptotically stable, where $\omega_{k} > 0$. Observation 1 essentially connects the frequency regulation with the scalar $z_i$, and it suggests that the frequency at the $i$-th IBR can be regulated, if the corresponding $\dot{z}_i$ equals 0.

**Observation 2** is obtained by integrating both sides of (16):

$$z_i(t) = \omega_{kl} \int_0^t (\Delta \omega_{kl}(\tau) - m_p \Delta P_{Gi}(\tau)) d\tau + z_i(0) \quad (18)$$

where $\Delta \omega_{kl}$ is the control command produced by the secondary controller; $\Delta P_{Gi}$ can be measured; and the initial condition $z_i(0)$ can be set to zero for engineering implementation.

Essentially, (18) suggests that if the $\mu$AGC makes decisions by observing $z_i$ in the presence of fast load/renewable power fluctuations, measuring fast $\Delta P_{Gi}$ suffices, and it is unnecessary to have fast frequency measurements. A natural question is: Compared with frequency, why can the instantaneous power $\Delta P_{Gi}$ be measured both fast and accurately? In practice, frequency and instantaneous power are computed based on instantaneous voltage and current measurements. The instantaneous voltage (current) can be measured by a voltage (current) transducer. After being filtered by a low-pass filter, the analog signal of the voltage (current) can be digitized by an analog-to-digital circuit [40]. With the digital voltage/current signal, the frequency of the voltage/current can be estimated by various algorithms [41], e.g., phase-locked loops [42], discrete Fourier transform [41], and least-squares techniques [43]. Before these signal processing techniques accurately track the true frequency, there exists a transient process where the frequency estimated does not match the true frequency. The waveform from 1 sec. to 1.15 sec. in Figure 2(a) of the manuscript shows such a transient process. As shown in Figure 2(b), the concern is that when the true frequency changes during the sensor transient process, these signal processing techniques cannot accurately estimate the frequency anymore. However, with the digital voltage and current signals with a high sampling rate (e.g., 30.7 kHz [44]), the instantaneous power can be computed almost instantaneously using an algebraic equation.\footnote{The algebraic equation is the definition of the instantaneous three-phase power $p_{3Ph}$: $p_{3Ph}(t) = v_0(t)c_0(t) + v_1(t)c_1(t) + v_c(t)c_c(t)$ where $\{v_0, v_1, v_c\}$ and $\{c_0, c_1, c_c\}$ are the instantaneous, three-phase voltages and currents, respectively.} The operation of computing the instantaneous power will not incur the transient process that appears when the frequencies are computed. Therefore,
the instantaneous power can be measured accurately, even
when the true power fluctuates fast. The sensory bottleneck
described in Section II-B is overcome by introducing a new
variable $z_i$.

It is worth noting that the modeling approach is applicable
to other types of DERs that possesses the rank-one
deficiency property. This is because this rank deficiency is a
direct consequence of conservation of energy [38], [39].

Our earlier work [45] addresses synchronous machines using
the same modeling approach. Such a modeling approach lends
itself to a μAGC design for microgrids with heterogeneous
energy resources. The μAGC design for such a kind of
microgrids cannot be formulated by some control methods
that are specifically designed for IBRs, such as [15].

B. Optimal Frequency Regulation

This subsection introduces an optimal μAGC that tunes the
IBR setpoints $\Delta P_{Gi}$ by observing the scalars $z_i$. To drive the
frequency deviations to zero, based on Observation 1, one
possible control law is

$$\Delta \omega_k = m_{P_i} \Delta P_{Gi} \quad \forall i = 1, \ldots, N. \quad (19)$$

According to (16), the control law (19) leads to a zero $z_i$. It
follows that $\Delta \omega_k$ tends to zero, based on Observation 1. It is
worth noting that the control law (19) can be implemented in a
decentralized manner, as the setpoint for the $i$-th IBR is
computed only by its local measurement $P_{Gi}$ for $i = 1, 2, \ldots, N$.

However, the decentralized control law (19) might not achieve
high economical efficiency, since different IBRs incurs differ-
ent generation costs. For example, we may expect the cheaper
IBRs to generate more real power in order to regulate the
microgrid frequencies. Therefore, coordination among IBRs is
needed in order to regulate frequencies at the minimal costs.

Such coordination is achieved by formulating the frequency
regulation problem into the following optimal control problem in
the $z_i$ space:

$$\min_{\Delta \omega_k} \frac{1}{2} \int_0^\infty \left[ z(t)^\top Q z(t) + \Delta \omega_k(t)^\top R \Delta \omega_k(t) \right] dt \quad (20)$$

s.t. $\Delta \dot{x}(t) = A \Delta x(t) + B_1 \Delta \omega_k(t)$

where $z = [z_1, \ldots, z_N]^\top$; matrices $Q \in \mathbb{R}^{N \times N}$ and $R \in \mathbb{R}^{N \times N}$
are positive definite. In the frequency regulation problem in
this paper, both matrices $Q$ and $R$ are diagonal. Denote by $q_i$
and $r_i$ the $i$-th diagonal entry of $Q$ and $R$, respectively.

A relatively large $q_i$ suggests relatively higher quality of service
is required by the end users at node $i$. A relatively large $r_i$
suggests a relatively higher generation cost at the $i$-th IBR.

Based on transformation (14), $z$ can be expressed in terms of
states $\Delta x$ in the conventional space

$$z = T \Delta x \quad (21)$$

where $T = \text{diag}(T_1, \ldots, T_N)$. Plugging (21) into the objective
function of the optimization (20) gives the standard
formulation of the LQR problem:

$$\min_{\Delta \omega_k} \frac{1}{2} \int_0^\infty \left[ \Delta x(t)^\top Q \Delta x(t) + \Delta \omega_k(t)^\top R \Delta \omega_k(t) \right] dt \quad (22)$$

s.t. $\Delta \dot{x}(t) = A \Delta x(t) + B_1 \Delta \omega_k(t)$

where $Q' = T^\top QT$. The solution to (22) has the following
form: $\Delta \omega_k = -K' \Delta x$, where $K'$ can be obtained a process
that has been standardized in some software toolboxes, e.g.,
the function $\text{lqr}$ in MATLAB. As discussed earlier, it is more
desirable to feed μAGC the transformed states $z$, rather than
$\Delta x$ which includes the frequency deviation $\Delta \omega_k$ that is hard
to measure at a fast rate. Therefore, the control law is

$$\Delta \omega_k = -Kz. \quad (23)$$

where matrix $K$ is chosen such that $Kz \approx K' \Delta x$, and one
possible choice of $K$ is $K = K'T^\top(TT^\top)^{-1}$ [39]. Note that
the control law (23) tunes $\Delta \omega_k$ by observing $z$ or by measuring
$P_{Gi}$ for $i = 1, 2, \ldots, N$. Such a control law is immune to
the FDI attacks on frequency or phase angle measurements.
However, it is vulnerable to cyber attacks on $P_{Gi}$. The

IV. CYBER ANOMALY DETECTION AND CORRECTION

To compute $z$, the real power $P_{Gi}$ for all IBRs is needed
to be measured and reported to a μAGC. It is possible that a
malicious adversary can compromise the microgrid by launch-
ing the FDI attacks (described in Section II-C) on the $P_{Gi}$. If
this happens, the control command $\Delta \omega_k$ issued by the μAGC
may fail to stabilize or to regulate the frequency, compromis-
ing the microgrid’s safety and the quality of electricity service.

This section introduces an end-to-end scheme that can
enhance the microgrid resilience to cyber attack on the criti-
cal measurements. The key idea of the scheme is to leverage
a computational model that represents the dynamics of the
microgrid, for the purpose of predicting $P_{Gi}$. The main chal-

A. Computational Model for Cyber Attack Mitigation

Without load/renewable power fluctuations, the real power
$\Delta P_G$ used for computing $z$ in (23) can be predicted by $\Delta \omega_k$
according to the following discrete state space model with the
sample time $\Delta t$:

$$\dot{x}[k] = A' \dot{x}[k - 1] + B' \Delta \omega[k - 1] \quad (24a)$$

$$\Delta \dot{P}_G[k] = C' \dot{x}[k] \quad (24b)$$

where $\Delta \dot{P}_G$ is the predicted version of $\Delta P_G[k]$; $\dot{x}[k]$ is an
intermediate variable which can be obtained by using (24a)
recursively if $\dot{x}[0]$ is given; and $A'$, $B'$, and $C'$ are the system,
input, and output matrices.

One challenge of using (24) to predict $\Delta P_G$ is how to obtain the
matrices $A'$, $B'$, and $C'$. We leverage a system identification

The $\text{N4SID}$ technique (i.e., \text{N4SID} [46]) to learn these matrices using
the experimental measurements of $\Delta \omega_k$ and $\Delta P_G$. Implementing
the $\text{N4SID}$ technique requires: 1) input-output data; and 2) the
order of the system (24).
1) Input-Output Data: Define a rectangular function rect(t) as follows

$$\text{rect}(t) = \mathbb{I}_{t \geq 0} - \mathbb{I}_{t - \Delta t' \geq 0}$$

(25)

where $\Delta t' > \Delta t$ denotes the width of the rectangular pulse; and $\mathbb{I}_{t \geq 0}$ is an indicator function, i.e.,

$$\mathbb{I}_{\geq 0} = \begin{cases} 1 & t \geq 0 \\ 0 & t < 0. \end{cases}$$

The input signal $\Delta \omega_k[t]$ for system identification can be sampled from the following continuous function with sampling time $\Delta t$

$$l(t) = \sum_{k=0}^{\lceil t/\Delta t' \rceil} \alpha_k \text{rect}(t - k \Delta t')$$

(26)

where $\lceil \cdot \rceil$ is the ceiling function; the random scalar $\alpha_k$ is uniformly distributed in $[-\beta, \beta]$ whence $\beta$ is a small positive scalar. By feeding the microgrid the designed setpoint sequence $S = \{\Delta \omega_k[k] = 0, 1, \ldots, K_0\}$, the response of $\Delta P_G$ can be measured at sample time $\Delta t$. The input sequence $S$ associated with the $\Delta P_G$'s response is used for implementing the N4SID technique.

2) Order Selection: The optimal system order $d^*$ is obtained by trial and error. Suppose that there is a set $\mathcal{D}$ that collects some candidate system orders, say, $\mathcal{D} := \{1, 2, \ldots, 10\}$. For $d \in \mathcal{D}$, the N4SID technique can return the identified $A'$, $B'$, and $C'$. With these matrices and the input data $O$, $\Delta P_G$’s prediction $\hat{\Delta P}_{Gd}$ can be computed. The performance of the identified system with the order $d$ can be quantified by

$$\eta_d = \frac{1}{K_0 + 1} \sum_{k=0}^{K_0} \|\hat{\Delta P}_{Gd} - \Delta P_G\|_2.$$  

(27)

The optimal order $d^*$ is chosen such that the smallest $\eta_d$ is attained, viz., $\eta^* = \arg \min_{d \in \mathcal{D}} \eta_d$.

B. Cyber Attack Detection

The state-space model (24) can be used in some cyber attack detection algorithms, e.g., the dynamic watermarking approach [27], and the UIO method [25]. As an example, we show how to use the dynamic watermarking approach to detect cyber attacks on $P_{G_i}$.

Figure 4 shows the basic idea of the dynamic watermarking approach. A small, secret watermark signal $\mathbf{e}[k] \in \mathbb{R}^N$ is superposed upon the IBRs’ setpoints $\Delta \omega_k$ at each time step $k$. The watermark signal possesses some known statistics, e.g., $\mathbf{e}[k] \sim \mathcal{N}(0, \Sigma)$ where matrix $\Sigma$ is the covariance matrix of $\mathbf{e}[k]$. The watermark $\mathbf{e}[k]$ impacts the measurement of $\Delta P_G$. As a result, an authentic measurement of $\Delta P_G$ should reflect the statistical properties concerning the watermark $\mathbf{e}[k]$. By subjecting the measurements of $\Delta P_G$ to certain statistical tests, a wide range of cyber attacks on the measurement of $\Delta P_G$ can be detected [27, 31].

The detailed mechanism of the dynamic watermarking approach is elaborated as follows. Denote by $\Delta P_G^\nu$ the measurements of the real power $\Delta P_G$ that are received by the $\mu AGC$. If there are no cyber attacks on $\Delta P_G$, $\Delta P_G^\nu = \Delta P_G$, with the true sequence of $\{\Delta \omega_k[i]\}$ and $\{\mathbf{e}[i]\}$ for $i = 0, 1, \ldots, k - 1$, one can approximately predict $\Delta P_G[k]$ based on

$$\hat{\mathbf{x}}[k] = A'\hat{\mathbf{x}}[k - 1] + B'(\Delta \omega_k[k - 1] + \mathbf{e}[k - 1])$$

(28a)

$$\Delta \hat{P}_G[k] = C'\hat{\mathbf{x}}[k].$$

(28b)

Define

$$\mathbf{v}[k] := \Delta P_G^\nu[k] - \Delta \hat{P}_G[k].$$

(29)

For a microgrid without cyber attack, i.e., $\Delta P_G^\nu[k] = \Delta P_G[k]$, we can obtain a long sequence $\{\Delta P_G^\nu[k], k = 1, \ldots, W\}$ where $W$ is a large integer. The expectation $\mu^\nu_k$ and covariance matrix $\Sigma^\nu_k$ of $\mathbf{v}$ in the microgrid without cyber attack can be approximated by $\hat{\mu}_v^\nu$ and $\hat{\Sigma}_v^\nu$ where

$$\hat{\mu}_v^\nu = \frac{1}{W} \sum_{k=1}^{W} \mathbf{v}[k]$$

(30a)

$$\hat{\Sigma}_v^\nu = \frac{1}{W} \sum_{k=1}^{W} (\mathbf{v}[k] - \hat{\mu}_v^\nu)(\mathbf{v}[k] - \hat{\mu}_v^\nu)^\top.$$  

(30b)

For the microgrid that might be under cyber attacks where $\Delta P_G^\nu[k]$ may not be equal to $\Delta P_G[k]$, denote by $\hat{\mu}_v$ and $\hat{\Sigma}_v$, the estimated expectation and covariance matrix of $\mathbf{v}$, respectively. Let $\mathcal{M}_\rho$ and $\hat{\mathcal{M}}_\rho$ collect $\Delta P_G^\nu$ and its prediction $\Delta \hat{P}_G$ from time $t = (\rho - W + 1)\Delta t$ to $t = \rho \Delta t$, viz.,

$$\mathcal{M}_\rho := \{\Delta P_G^\nu[k], k = \rho - W + 1, \ldots, \rho\}$$

(31a)

$$\hat{\mathcal{M}}_\rho := \{\Delta \hat{P}_G[k], k = \rho - W + 1, \ldots, \rho\}.$$  

(31b)

$\hat{\mu}_v$ and $\hat{\Sigma}_v$ can be estimated from $\mathcal{M}_\rho$ and $\hat{\mathcal{M}}_\rho$ via

$$\hat{\mu}_v = \frac{1}{\rho} \sum_{k=\rho-W+1}^{\rho} \mathbf{v}[k]$$

(32a)

$$\hat{\Sigma}_v = \frac{1}{\rho} \sum_{k=\rho-W+1}^{\rho} (\mathbf{v}[k] - \hat{\mu}_v)(\mathbf{v}[k] - \hat{\mu}_v)^\top.$$  

(32b)

If $\Delta P_G^\nu[k] = \Delta P_G[k]$, $\hat{\mu}_v$ and $\hat{\Sigma}_v$ should be close to $\mu_v^\nu$ and $\Sigma_v^\nu$, respectively, that is,

$$\xi_1 = \|\hat{\mu}_v - \mu_v^\nu\|_2 < \epsilon_1$$

(33a)

$$\xi_2 = \|\hat{\Sigma}_v - \Sigma_v^\nu\| < \epsilon_2$$

(33b)

where $\|\cdot\|_2$ and $\text{tr}()$ are the $L_2$ norm and the trace operator, respectively; and $\epsilon_1$ and $\epsilon_2$ are positive numbers. Violation of either (33a) or (33b) or both suggests cyber attacks, i.e., $\Delta P_G^\nu[k] \neq \Delta P_G^\nu[k]$. The two conditions in (33) can be checked in a moving-window fashion, which is summarized.
Algorithm 1 Watermarking-Based Cyber Attack Detection

1: function \( \mathcal{D}_W(\mathcal{M}_{\rho-1}, \hat{\mathcal{M}}_{\rho-1}, \Delta P_G^{i}[\rho], \Delta \omega_{i}[\rho], e_{i}[\rho], \hat{x}_{i}[\rho-1], A', B', C', \hat{\mu}^{*}, \hat{\Sigma}^{*}, \xi_{1}, \xi_{2}) \)
2: Compute \( \Delta P_G^{i} \) \( \hat{x} \) by (28)
3: \( \mathcal{M}_{\rho} \leftarrow [\Delta P_G^{i}][\rho] \cup \mathcal{M}_{\rho-1} - [\Delta \hat{P}_G^{i}(\rho - W)] \)
4: \( \mathcal{M}_{\rho} \leftarrow [\Delta P_G^{i}][\rho] \cup \mathcal{M}_{\rho-1} - [\Delta P_G^{i}(\rho - W)] \)
5: Compute \( \mu_{i}, \xi_{i} \) using \( \mathcal{M}_{\rho}, \mathcal{M}_{\rho} \) based on (29), (32)
6: Obtain \( \xi_{1} \) and \( \xi_{2} \) according to (33)
7: if \( (\xi_{1} < \xi_{1}) \cap (\xi_{2} < \xi_{2}) \) then
8: \( \hat{\text{flag}} \leftarrow 0 \) \( \Rightarrow \) No attack is detected
9: else
10: \( \hat{\text{flag}} \leftarrow 1 \) \( \Rightarrow \) Attack is detected
11: end if
12: return \( \text{flag}, \mathcal{M}_{\rho}, \hat{\mathcal{M}}_{\rho}, \hat{x}_{\rho} \)
13: end function

Fig. 5. Physical and cyber architecture of two networked microgrids.

in Algorithm 1. Function \( \mathcal{D}_W \) in Algorithm 1 returns a binary result: “\( \hat{\text{flag}} = 0 \)” suggests that a cyber attack is not detected, while “\( \hat{\text{flag}} = 1 \)” suggests that cyber attack is detected.

C. Corrective Control

This subsection addresses how to regulate frequency under cyber attacks on the real power measurements \( \Delta P_G^{i} \) feeding the proposed control law (23). Depending on whether there are microgrids that can be networked with the microgrid under attack, the \( \mu \text{-AGC} \) under cyber attack can select one of the following two schemes to regulate frequencies.

1) Observer-Based Correction Scheme: Once the cyber attack is detected and there is no neighboring microgrid that can be networked with the microgrid under attack, the microgrid attacked can use the observer-based correction scheme to regulate its frequencies. The basic idea of such a scheme is to leverage an observer to predict the real power measurement \( \Delta P_G^{i} \) and to use the prediction \( \Delta P_G^{i} \) to tune the setpoints \( \Delta \omega_{i} \) of IBRs. Specifically, the observer is defined in (24) [47]. The control law in the observer-based correction scheme is

\[
\Delta \omega_{i} = -K\hat{z}_{i}, \ldots, \hat{z}_{N} \]

where \( \hat{z}_{i}(t) = \omega_{si} \int_{0}^{t} (\Delta \omega_{i}(\tau) - m_{pi} \Delta \hat{P}_G^{i}(\tau))d\tau \).

2) Collaborative Correction Scheme: The control law (19) is blind to load/renewable power fluctuations. As a result, the frequencies cannot be regulated at the nominal frequency if \( \Delta P_L \neq 0 \). This issue can be addressed by the collaborative correction scheme presented here. Suppose that there are two islanded microgrids. Each microgrid has its own \( \mu \text{-AGC} \) designed based on the control law (23). Assume that \( \mu \text{-AGC}_1 \) (\( \mu \text{-AGC}_2 \)) is for Microgrid 1 (Microgrid 2). Suppose that microgrid 1 is under cyber attack on its \( \Delta P_G^{i} \) that is used for computing \( z_{i} \). Once the cyber attack is detected at Microgrid 1 by some cyber attack detection algorithms, e.g., the dynamic watermarking approach, \( \mu \text{-AGC}_1 \) will be disabled, and Microgrid 1 can be networked with Microgrid 2 by closing the tie line between Microgrids 1 and 2. As will be shown in Section V, \( \mu \text{-AGC}_2 \) can regulate the frequencies at all nodes of both Microgrids 1 and 2, while \( \mu \text{-AGC}_2 \) makes decisions only based on the local measurements at Microgrid 2.

The overall procedure described throughout Sections III and IV is summarized in Algorithm 2 where set \( \mathcal{I}_{\rho - 1} \) collects the input for the function \( \mathcal{D}_W \) in Algorithm 1, i.e.,

\[
\mathcal{I}_{\rho - 1} := [\mathcal{M}_{\rho-1}, \hat{\mathcal{M}}_{\rho-1}, \Delta P_G^{i}[\rho], \Delta \omega_{i}[\rho], e_{i}[\rho], \hat{x}_{i}[\rho-1], A', B', C', \hat{\mu}^{*}, \hat{\Sigma}^{*}, \xi_{1}, \xi_{2}] \]

(35)

Algorithm 2 Cyber Resilient \( \mu \text{-AGC} \)

1: \( \mathcal{I}_{W} \leftarrow \cup_{k=1}^{W} [\Delta P_G^{i}[k]] \)
2: while \( \rho = W + 1, W + 2, \ldots \) do
3: \( \hat{\text{flag}}, \mathcal{M}_{\rho}, \hat{\mathcal{M}}_{\rho}, \hat{x}_{\rho} \leftarrow \mathcal{D}_W(\mathcal{I}_{\rho - 1}) \)
4: if \( \hat{\text{flag}} = 0 \) then
5: Compute \( \Delta \omega_{i}[\rho] \) via (18) and (23)
6: else
7: if Neighboring microgrids are unavailable then
8: Compute \( \Delta \omega_{i}[\rho] \) via (24) and (34).
9: \( e_{i}[\rho] \leftarrow 0 \) \( \Rightarrow \) Stop injecting watermark
else
10: \( \Delta \omega_{i}[\rho] \leftarrow 0; e_{i}[\rho] \leftarrow 0 \)
11: Network with the neighboring microgrids
12: end if
13: end if
14: end if
15: return \( \Delta \omega_{i}[\rho] \)
16: end while

Fig. 6. (a) Real power measurement \( P_{L1} \) at load 1; and (b) zoomed-in version of \( P_{L1} \) from time \( t = 0.799 \) sec. to \( t = 0.803 \) sec.
V. CASE STUDY

In this section, the proposed fast μAGC and the associated cyber anomaly detection and correction scheme are tested in a microgrid with three IBRs via Simulink simulations. We first provide a brief description for the software-based microgrid testbed. Then we show the performance of the fast controller that exploits the rank deficiency property of IBRs, under fast renewable/load power fluctuations. Finally, we present the performance of the cyber attack detection and correction scheme that is built upon the model developed in Section IV.

A. Description of Software-Based Microgrid Testbed

Figure 5 illustrates the physical and cyber architecture of two networked microgrids that are used to test the proposed algorithms. For each IBR, its power calculator, voltage controller, current controller, and output filter are modeled according to [18]. All IBRs have the same parameters. Loads 1, 2, and 3 are modeled by resistors with the values of 25 Ω, 20 Ω, and 33 Ω for each phase. There is a tie line that can network Microgrid 1 with Microgrid 2. The line parameters are annotated in Figure 5. Each microgrid has its own μAGC which tunes the setpoint of each IBR in the local microgrid.

B. Control Performance Without Cyber Attack

Here the performance of the controller (23) is tested. The secondary controller μAGC1 takes real power measurements \( P_{G_i} \) every 5 ms and issues control commands \( \omega_{s_i} \) at the same rate, for \( i = 1, 2, 3 \). The tie line in Figure 5 is open.

1) Control Performance With Fast Renewable Fluctuations: Suppose Load 1 varies periodically and Figure 6 shows the real power flowing to Load 1. The spikes in Figure 6(a) show the load changing transients, and the zoomed-in version of one of the spikes is shown in Figure 6(b). As a result, the frequencies at the three nodes of Microgrid 1 fluctuate periodically. This can be observed via the orange dashed curves in Figure 7. The blue curves in Figure 7 show the frequencies at the three nodes with fast load/renewable power fluctuations, when the proposed μAGC1 is enabled. It can be seen that the magnitudes of the frequencies’ fluctuations are significantly reduced by the proposed μAGC under load/renewable power fluctuations.

2) Comparison: The proposed μAGC is compared with a slow LQR μAGC and a fast proportional–integral (PI) μAGC. The slow μAGC issues control commands every 0.1 s, while the two fast μAGC issues control commands every 5 ms. Figure 8 summarizes the comparison results in response to the load power fluctuations shown in Figure 6. In Figure 8, the orange dotted curves are the frequencies under the slow μAGC. It can be observed that the frequencies cannot be regulated. This is not surprising because the time interval between two successive control commands is the same as that between two successive disturbances. The yellow dashed curves are the frequency response with the fast PI μAGC. Since the fast frequency changes cannot be measured accurately, the frequencies under the fast PI controller still cannot be regulated. As the proposed μAGC does not rely on the availability of fast frequency measurements, the frequencies can be regulated tightly around 50 Hz under the fast load/renewable power fluctuations, as it is shown by the blue curves in Figure 8.

C. Cyber Attack Detection and Corrective Control

The proposed scheme for cyber resilient frequency regulator is tested under both renewable/load power fluctuations and cyber attacks.
1) Cyber Attack Detection: One prerequisite for implementing Algorithm 1 is that the matrices $A'$, $B'$, and $C'$ are available. In this paper, these matrices are learned from the measurements of $\Delta \omega_s$ and $\Delta P_G$ based on the system identification procedure. It takes 1.43 seconds to decide the optimal order $d^*$ and to learn the discrete model offline using a MacBook Pro with a 2.6 GHz Dual-Core Intel i5 Processor. The sampling rate of the discrete model is 0.005 seconds. The computation time of learning the models with different orders are shown in Figure 9(a). Next, we show the performance of the model learned by changing the setpoint of one IBR. Without the load/renewable power fluctuations, the set point $\Delta \omega_{s1}$ has a step change at time $t = 0.7$ s. The blue curve in Figure 9(b) represents the evolution of the measurements on $P_G1$ under the step change. With the model learned, the evolution of $P_G1$ can be predicted almost instantaneously. The orange dashed curve in Figure 9(b) represents the prediction. These two curves in Figure 9(b) almost overlap with each other, suggesting that the state-space model learned can accurately predict the response of the real power measurements $P_G1$.

The performance of Algorithm 1 is tested under the noise injection attack and the replay attack. In the simulation, $W$ in Algorithm 1 is set to 100. Figures 10 and 11 show the performance of Algorithm 1 under the noise injection attack. In Figure 10(a), the noise injection attack on $P_G1$ is launched at time $t = 2$ s. Such an attack causes the attack indicator $\xi_2$ to shoot up and triggers the cyber attack alarm. In Figure 11(a), a temporary noise injection attack starts at $t = 2$ s and ends at $t = 2.2$ s. As shown in Figure 11(b), it takes around 0.025 seconds for the indicator to exceed its normal peak value, after the attack occurs. After the attack disappears, it takes around 0.485 seconds for the indicator to fall below its normal peak value. Figure 12 illustrates the performance of Algorithm 1 under the replay attack. A replay attack on the $P_G1$ occurs at time $t = 2$ s. Figure 12(a) shows the $P_G1$ measurements under such an attack. From Figure 12(a), it is hard to determine when the cyber anomaly occurs by simply eyeballing the $P_G1$ measurement curve. However, Figure 12(b) which shows the evolution of the attack indicator $\xi_2$ explicitly suggests that the attack occurs around $t = 2$ s.
2) Observer-Based Cyber Attack Correction: Figure 13 demonstrates the performance of the observer-based corrective controller. The noise injection attacks occur at the sensor measuring $P_{G1}$ at Microgrid 1 at $t = 0.7$ s. Consequently, frequencies at the three nodes of Microgrid 1 become noisy. At $t = 1$ s, the observer-based corrective controller is enabled, and the frequencies are stabilized.

3) Collaborative Cyber Attack Correction: The observer-based corrective control is blind to renewable/load power fluctuations. If Microgrid 2 is available, once cyber attacks at Microgrid 1 are detected, Microgrid 1 can disable $\mu_{AGC1}$ and turn on the switches of the tie line that connects Microgrid 2. The $\mu_{AGC2}$ can regulate the frequencies of both Microgrids 1 and 2. Figure 14 illustrates such a process. Suppose that at $t = 0.5$, $\mu_{AGC1}$ is disabled due to a cyber attack detected. Load 1 also increases at $t = 0.5$, leading frequencies at Microgrid 1 to decrease. To recover the frequencies to 50 Hz, Microgrid 1 networks with Microgrid 2 via the tie line at $t = 0.7$ sec. It can be seen from Figure 14 that the three frequencies at Microgrid 1 are brought back to 50 Hz, and the event of networking Microgrids 1 and 2 only causes negligible frequency ripples at Microgrid 2.

$\mu_{AGC2}$ only serves as a temporary frequency regulator for Microgrid 1 when Microgrid 1 is under cyber attacks. Suppose that $\mu_{AGC1}$ for Microgrid 1 is disabled, and $\mu_{AGC2}$ for Microgrid 2 is enabled. Load at node 1 fluctuates fast according to Figure 6. Figure 15 compares frequencies with and without the collaborative control. It can be seen that while $\mu_{AGC2}$ does not play a big role of regulating the frequency at node 1, it indeed improves the frequency profiles at nodes 2 and 3 by limiting the frequencies of both Microgrids 1 and 2. Figure 14 illustrates such a process. Suppose that at $t = 0.5$, $\mu_{AGC1}$ is disabled due to a cyber attack detected. Load 1 also increases at $t = 0.5$, leading frequencies at Microgrid 1 to decrease. To recover the frequencies to 50 Hz, Microgrid 1 networks with Microgrid 2 via the tie line at $t = 0.7$ sec. It can be seen from Figure 14 that the three frequencies at Microgrid 1 are brought back to 50 Hz, and the event of networking Microgrids 1 and 2 only causes negligible frequency ripples at Microgrid 2.

It is worth noting that with $\mu_{AGC1}$ disabled, $\mu_{AGC2}$ can still regulate frequencies in Microgrid 1 under slow load fluctuations. Figure 17 shows the frequencies at IBRs 1, 2, and 3 with the load at node 1 that changes every 2 s, when $\mu_{AGC1}$ is disabled. It can be observed that the frequencies at IBRs 1, 2, and 3 are tightly regulated around their nominal values by $\mu_{AGC2}$ under the slow load fluctuations at node 1.

The performance of the collaborative control can be justified by examining $\Delta P_{Gi}$ in (16). When the load at node 1 increases at 1 s and the two microgrids are networked, Figure 18 visualizes $\Delta P_{Gi}$ for $i = 1, 2, \ldots, 5$. In Figure 18-(a), it can be observed that the steady-state values of $\Delta P_{Gi}$ for $i = 1, 2, 3$ return zero, which means that no extra real power is produced by IBRs that do not participate in $\mu_{AGC2}$, i.e., IBRs 1, 2 and 3, in order to balance the increased amount of load. The increased amount of load is balanced by the IBRs that participate in $\mu_{AGC2}$, i.e., IBRs 4 and 5. Since IBRs 1, 2 and 3 do not participate in $\mu_{AGC2}$, $\Delta P_{Gi} = 0$ for $i = 1, 2, 3$. In addition, Figure 18-(a) shows $\Delta P_{Gi} = 0$ for $i = 1, 2, 3$ in steady state. Based on (16), $\dot{z}_i$ equals zero for $i = 1, 2, 3$. Because
of Observation 1, $\Delta o_i$ is zero in steady state for $i = 1, 2, 3$. This explains why the frequencies in Microgrid 1 is regulated by $\mu$AGC$_2$, while $\mu$AGC$_2$ does not take any measurements from Microgrid 1. Note that such performance of the collaborative control is built upon the assumption that no congestion occurs in the tie line between Microgrids 1 and 2. Suppose that the congestion occurs, the increase amount of real power cannot be balanced by the IBRs in Microgrid 2. In such a case, $\mu$AGC$_2$ cannot regulate frequencies in Microgrid 1 to the nominal value.

VI. CONCLUSION

In this paper, a cyber-resilient $\mu$AGC is proposed. A new microgrid modeling approach is introduced. The modeling approach exploits the rank-deficient property of IBR dynamics. Such modeling approach leads to a fast $\mu$AGC design that requires no frequency measurements that may not be available in practice under fast load/renewable power fluctuations. An end-to-end cyber security solution to FDI attack detection and mitigation is developed for the proposed $\mu$AGC. The proposed cyber-resilient $\mu$AGC is tested in a system of two microgrids. Simulation shows the proposed $\mu$AGC can regulate microgrid frequencies under fast renewable/load power fluctuations, and its cyber security solution can detect and mitigate FDI attacks. Future work will investigate the impact of microgrid nonlinearity on the cyber-resilient $\mu$AGC design and test and validate the proposed $\mu$AGC in a large-scale system of AC microgrids.

REFERENCES

[1] “Root cause analysis mid-August 2020 extreme heat wave,” California Independent System Operator, Folsom, CA, USA, California Public Utilities Commission, San Francisco, CA, USA, California Energy Commission, Sacramento, CA, USA, 2021.

[2] “The February 2021 cold weather outages in Texas and the South Central United States,” FERC, NERC, Washington, DC, USA, 2021.

[3] T. Huang, S. Gao, and L. Xie, “A neural Lyapunov approach to transient stability assessment of power-electronics-interfaced networked microgrids,” *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 106–118, Jan. 2022.

[4] L. Xie, T. Huang, P. R. Kumar, A. A. Thatte, and S. K. Mitter, “On an information and control architecture for future electric energy systems,” *Proc. IEEE*, vol. 110, no. 12, pp. 1940–1962, Dec. 2022.

[5] M. Farrokhhabadi et al., “Microgrid stability definitions, analysis, and examples,” *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 13–29, Jan. 2020.

[6] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castillo, “Hierarchical control of AC and DC microgrids—A general approach toward standardization,” *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 158–172, Jan. 2011.

[7] J. W. Simpson-Porco, Q. Shafiee, F. Dörfler, J. C. Vasquez, J. M. Guerrero, and F. Bullo, “Secondary frequency and voltage control of islanded microgrids via distributed averaging,” *IEEE Trans. Ind. Electron.*, vol. 62, no. 11, pp. 7025–7038, Nov. 2015.

[8] J. Choi, S. I. Habibi, and A. Bidram, “Detected finite-time event-triggered frequency and voltage control of AC microgrids,” *IEEE Trans. Power Syst.*, vol. 37, no. 3, pp. 1979–1994, May 2022.

[9] Y. Khayat et al., “On the secondary control architectures of AC microgrids: An overview,” *IEEE Trans. Power Electron.*, vol. 35, no. 6, pp. 6482–6500, Jun. 2020.

[10] J. A. P. Lopes, C. L. Moreira, and A. G. Madureira, “Defining control strategies for microgrids islanded operation,” *IEEE Trans. Power Syst.*, vol. 21, no. 2, pp. 916–924, May 2006.

[11] A. G. Tsikalakis and N. D. Hatziargyriou, “Centralized control for optimizing microgrids operation,” in *Proc. IEEE PES General Meeting*, 2011, pp. 241–248.

[12] S. Manaffam, M. Talebi, A. K. Jain, and A. Behal, “Intelligent pinning based cooperative secondary control of distributed generators for microgrid in islanding operation mode,” *IEEE Trans. Power Syst.*, vol. 33, no. 2, pp. 1364–1373, Mar. 2018.

[13] J. Shi, D. Yue, and S. Weng, “Distributed event-triggered mechanism for secondary voltage control with microgrids,” *Trans. Inst. Meas. Control*, vol. 41, no. 6, pp. 1553–1561, 2018.

[14] Y. Han, H. Li, L. Xu, X. Zhao, and J. M. Guerrero, “Analysis of washout filter-based power sharing strategy—an equivalent secondary controller for islanded microgrid without LBC lines,” *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4061–4076, Sep. 2018.

[15] Y. Khayat et al., “Decentralized optimal frequency control in autonomous microgrids,” *IEEE Trans. Power Syst.*, vol. 34, no. 3, pp. 2345–2353, May 2019.

[16] G. Lou, W. Gu, L. Wang, B. Xu, M. Wu, and W. Sheng, “Decentralized secondary voltage and frequency control scheme for islanded microgrid based on adaptive state estimator,” *IET Gener. Transm. Distrib.*, vol. 11, no. 15, pp. 3683–3693, 2017.

[17] Q.-C. Zhong and G. Weiss, “Synchronverters: Inverters that mimic synchronous generators,” *IEEE Trans. Ind. Electron.*, vol. 58, no. 4, pp. 1259–1267, Apr. 2011.

[18] N. Pogaku, M. Prodanovic, and T. C. Green, “Modeling, analysis and testing of autonomous operation of an inverter-based microgrid,” *IEEE Trans. Power Electron.*, vol. 22, no. 2, pp. 613–625, Mar. 2007.

[19] S. Tan, P. Xie, J. M. Guerrero, J. C. Vasquez, and R. Han, “Cyberattack detection for converter-based distributed DC microgrids: Observer-based approaches,” *IEEE Ind. Electron. Mag.*, vol. 16, no. 3, pp. 67–77, Sep. 2022.

[20] G. Hug and J. A. Giampapa, “Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks,” *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[21] M. N. Kurt, Y. Yilmaz, and X. Wang, “Distributed quickest detection of cyber-attacks in smart grid,” *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 2015–2030, 2018.

[22] L. Liu, M. Esmailfalah, Q. Ding, V. A. Emesh, and Z. Han, “Detecting false data injection attacks on power grid by sparse optimization,” *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.

[23] A. O. Aluko, R. P. Carpanen, D. G. Dorrell, and E. E. Ojo, “Real-time cyber attack detection scheme for standalone microgrids,” *IEEE Internet Things J.*, vol. 9, no. 21, pp. 21481–21492, Nov. 2022.

[24] A. Cecilia, S. Sahoo, T. Dragicevic, R. Costa-Castello, and F. Blaabjerg, “On addressing the security and stability issues due to false data injection attacks in DC microgrids—An adaptive observer approach,” *IEEE Trans. Power Electron.*, vol. 37, no. 3, pp. 2801–2814, Mar. 2022.

[25] H. H. Alhelou, M. E. H. Golshan, and N. D. Hatziargyriou, “Deterministic dynamic state estimation-based optimal LFC for interconnected power systems using unknown input observer,” *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1582–1592, Mar. 2020.

[26] M. R. Khalghani, J. Solanki, S. K. Solanki, M. H. Khooban, and A. Sargolzaei, “Resilient frequency control design for microgrids under false data injection,” *IEEE Trans. Power Electron.*, vol. 38, no. 3, pp. 2151–2162, Mar. 2023.

[27] B. Satchidanandan and P. R. Kumar, “Dynamic watermarking: Active defense of networked cyber-physical systems,” *Proc. IEEE*, vol. 105, no. 2, pp. 219–240, Feb. 2017.

[28] Y. Guan and M. Sai, “A novel approach to the design of unknown input observers,” *IEEE Trans. Autom. Control*, vol. 36, no. 5, pp. 632–635, May 1991.

[29] J. M. Rey, P. Martí, M. Velasco, J. Miret, and M. Castilla, “Secondary switched control with no communications for islanded microgrids,” *IEEE Trans. Ind. Electron.*, vol. 64, no. 11, pp. 8534–8545, Nov. 2017.
[30] PMU (PLL-Based, Positive-Sequence) Benchmark, MathWorks, Natick, MA, USA, 2023.

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

[32] EPRI Power System Dynamic Tutorial, Electr. Power Res. Inst., Washington, DC, USA, Jul. 2009.

[33] C.-C. Sun, A. Hahn, and C.-C. Liu, “Cyber security of a power grid: State-of-the-art,” Int. J. Electr. Power Energy Syst., vol. 99, pp. 45–56, Jul. 2018.

[34] A. Barua and M. A. Al Faruque, “Hall spoofing: A noninvasive DoS attack on grid-tied solar inverter,” in Proc. 29th USENIX Conf. Security Symp., 2020, pp. 1273–1290.

[35] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, “A review of false data injection attacks against modern power systems,” IEEE Trans. Smart Grid, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[36] C.-C. Sun, D. J. S. Cardenas, A. Hahn, and C.-C. Liu, “Intrusion detection for cyber-security of smart meters,” IEEE Trans. Smart Grid, vol. 12, no. 1, pp. 612–622, Jan. 2021.

[37] Y. Li and J. Yan, “Cybersecurity of smart inverters in the smart grid: A survey,” IEEE Trans. Power Electron., vol. 38, no. 2, pp. 2364–2383, Feb. 2023.

[38] M. Ilic and X. Liu, “A simple structural approach to modeling and analysis of the inter-area dynamics of the large electric power systems: Part I—Linearized models of frequency dynamics,” in Proc. North Amer. Power Symp., 1993, pp. 560–569.

[39] Q. Liu, “Large-scale systems framework for coordinated frequency control of electric power systems,” Ph.D. dissertation, Dept. Electr. Comput. Eng., Carnegie Mellon Univ., Pittsburgh, PA, USA, 2013.

[40] Y. Liu et al., “Wide-area-measurement system development at the distribution level: An FNET/GridEye example,” IEEE Trans. Power Del., vol. 31, no. 2, pp. 721–731, Apr. 2016.

[41] Y. Xia, Y. He, K. Wang, W. Pei, Z. Blazic, and D. P. Mandic, “A complex least squares enhanced smart DFT technique for power system frequency estimation,” IEEE Trans. Power Del., vol. 32, no. 3, pp. 1270–1278, Jun. 2017.

[42] M. Karimi-Ghartemani, B.-T. Ooi, and A. Bakshai, “Application of enhanced phase-locked loop system to the computation of synchronphasors,” IEEE Trans. Power Del., vol. 26, no. 1, pp. 22–32, Jan. 2011.

[43] M. M. Begovic, P. M. Djuric, S. Dunlap, and A. G. Phadke, “Frequency tracking in power networks in the presence of harmonics,” IEEE Trans. Power Del., vol. 8, no. 2, pp. 480–486, Apr. 1993.

[44] IDM: Multifunction Power System Monitor, Qualtrol, Fairport, NY, USA, [Online]. Available: https://www.qualtrolcorp.com/wp-content/uploads/2016/09/IP-F23-04L-01E_IDM-E.pdf

[45] X. Miao, M. Ilic, and Q. Liu, “Enhanced automatic generation control (E-AGC) for electric power systems with large intermittent renewable energy sources,” in Proc. IEEE PES General Meeting, 2019, pp. 1–5.

[46] P. Van Overschee and B. De Moor, “N4SID: Numerical algorithms for state space subspace system identification,” in Proc. IFAC, 1993, pp. 55–58.

[47] D. Wu, P. Bharadwaj, P. Rowles, and M. Ilic, “Cyber-physical secure observer-based corrective control under compromised sensor measurements,” in Proc. Amer. Control Conf., 2022, pp. 1638–1645.

Tong Huang (Member, IEEE) received the Ph.D. degree from Texas A&M University in 2021. He is an Assistant Professor with the Department of Electrical and Computer Engineering, San Diego State University (SDSU). Before joining SDSU, he was a Postdoctoral Associate with the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology. His industry experience includes an internship with ISO-New England in 2018 and an internship with Mitsubishi Electric Research Laboratories in 2019. His research focuses on cyber–physical resilience enhancement for electricity infrastructure with deep renewables via both data-driven and model-based approaches. As the first author, he received two Best Paper Awards at the 2020 IEEE PES General Meeting and the 54th Hawaii International Conference on System Sciences.

Dan Wu (Member, IEEE) received the B.S. degree in electrical engineering and automation from the Huazhong University of Science and Technology, Wuhan, China, in 2012, and the M.S. and Ph.D degrees in electrical and computer engineering from the University of Wisconsin–Madison, Madison, WI, USA, in 2014 and 2017, respectively. Following his doctoral studies, he worked as a Postdoctoral Associate with the Mechanical Engineering Department, Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, from 2017 to 2019, and then as a Postdoctoral Associate with the Laboratory for Information and Decision Systems, MIT, from 2019 to 2022. He was also a Senior Analyst with Equinor US Holdings Inc. from 2022 to 2023. He is currently a Professor with the School of Electrical and Electronic Engineering, Huazhong University of Science and Technology. His research interests lie in the areas of nonlinear dynamics and optimization, electric power systems, natural gas networks, interdependent complex systems, and geometric and topological methods in engineering applications. He has published several peer-reviewed research papers in top-tier journals and has served as an invited guest editor. He has also presented his research at various international conferences and has served as the conference panel chair. He actively collaborates with researchers and industry professionals to solve real-world problems and create innovative solutions that make a positive social impact.

Marija Ilic (Life Fellow, IEEE) is a Professor Emerita with Carnegie Mellon University (CMU). She currently holds a joint appointment of an Adjunct Professor with EECS Department and of a Senior Research Scientist with the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology (MIT). She has coauthored several books on the subject of large-scale electric power systems, and has co-organized an annual multidisciplinary Electricity Industry conference series at CMU with participants from academia, government, and industry. She was the Founder and the Co-Director of the Electric Energy Systems Group (EESG), CMU. She is currently building EESG, MIT, in the same spirit as EESG, CMU. Most recently, she has offered an open EdX course at MIT titled “Principles of Modeling, Simulations and Control in Electric Energy Systems.” She is the Founder and the Chief Scientist with New Electricity Transmission Software Solutions, Inc., currently, SmartGridz, Inc. She was the first recipient of the NSF Presidential Young Investigator Award for Power Systems in the U.S. She is an Elected Member of the U.S. National Academy of Engineering and the Academia Europaea.