IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 December 2024, accepted 11 January 2025, date of publication 20 January 2025, date of current version 27 January 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3532172

RESEARCH ARTICLE

Virtual Agents-Based Attack-Resilient Distributed Control for Islanded AC Microgrid

JUN ZHANG[1], (Graduate Student Member, IEEE), SHEIK M. MOHIUDDIN[2], (Member, IEEE), AND JUNJIAN QI[1], (Senior Member, IEEE)

[1]McComish Department of Electrical Engineering and Computer Science, South Dakota State University, Brookings, SD 57007, USA
[2]Energy and Environment Directorate, Pacific Northwest National Laboratory, Richland, WA 99354, USA

Corresponding author: Junjian Qi (Junjian.Qi@sdstate.edu)

The work of Jun Zhang and Junjian Qi was supported by the National Science Foundation under Grant ECCS-2403660.

ABSTRACT Due to its dependence on a communication network, distributed secondary control of microgrids is susceptible to denial-of-service (DoS) attacks in channel shutdown mode, which may negatively impact the network connectivity and thus deteriorate the coordination and power sharing among distributed generators (DGs). Honeypot is a common method for cyber deception by introducing fake targets. However, in the context of microgrid, the misleading information spread by honeypots will also impact the system performance. This paper proposes an attack-resilient distributed control for AC microgrids utilizing virtual agents (VAs) to counteract both DoS edge and node attacks. The VAs are designed to not impact the system's steady state during normal operation but to share information among neighboring real agents and serve as dummy targets for DoS attacks. The control with VAs is implemented by a primal-dual gradient-based distributed algorithm to efficiently obtain a practical solution for voltage/frequency regulation and power sharing. The simulation results on a 4-DG test system and a modified IEEE 34-bus system show that 1) VAs do not impact the normal functionality of the test system, and 2) deploying VAs can enhance the resilience of the microgrid control against DoS edge and node attacks.

INDEX TERMS AC microgrid, cooperative control, denial-of-service (DoS) attack, distributed algorithm, distributed control, primal-dual gradient, resilience, virtual agent.

I. INTRODUCTION

Microgrids are formed when distributed generators (DGs), energy storage systems, loads, and controllable devices are clustered as a single controllable entity to operate either in an islanded or grid-connected mode [1], [2]. As a traditional control, droop control operates at the primary level to achieve power sharing among DGs by emulating the inertial behavior of synchronous generators. Although it is operationally simple, it can suffer from load-dependent frequency and voltage deviations, inappropriate reactive power sharing, and poor dynamic performance [3], [4].

Secondary control is then proposed for better performance on voltage and frequency regulation by coordinating multiple DGs. It can be centralized or distributed. Centralized control requires communication between the central controller and local controllers and suffers from high requirements on communication network, high computational cost, and the risk of single point of failure [4]. By contrast, distributed control only needs to exchange information among neighbors on a sparse communication network, largely reducing the computational complexity and improving the system reliability [5], [6], [7].

Despite the advantages of distributed control, cyber-physical security has become a major concern. Cyber attacks on microgrids can be false data injection (FDI) attacks or denial of service (DoS) attacks [8]. As a common cyber attack, DoS attacks can jeopardize the availability of information by jamming or sabotaging communication channels [8].

There are different types of DoS attacks with different attack targets [9] or intensities [10]. According to attack

The associate editor coordinating the review of this manuscript and approving it for publication was Ning Kang.

targets, there are DoS edge (link) attacks and DoS node attacks. DoS edge attacks aim at removing the connections among nodes, while DoS node attacks target communication nodes and prevent them from sending/receiving any data to/from their neighbors. Moreover, in terms of attack intensity, DoS attacks can have two modes: latency attack mode and channel shutdown attack mode [10]. Latency attack intentionally delays the data transmission to violate its timing requirement, while channel shutdown attack directly disables communication channels.

The defense strategies against DoS attacks on microgrid control can be classified into post-attack and pre-attack methods. Post-attack methods usually utilize the following three strategies or their combinations: 1) channel reconstruction [9], [10], [11]; 2) control gain adjustment [10], [11], [12], [13]; and 3) improved sampling, triggering, and updating [9], [14], [15].

- Strategy 1 is designed for the channel shutdown attack mode. In [9], a communication channel recovery strategy is developed to mitigate the impact of DoS attacks. In [10], a topology reconfiguration controller is activated when some communication edges are disabled. Further in [11], an evolutionary game is used to decide whether to predict channel data or perform channel reconstruction. Although Strategy 1 is effective in addressing the DoS attacks in channel shutdown mode, a central unit is needed for network connectivity monitoring and decision making.
- Strategies 2 and 3 are designed for latency attack mode. In [12], the control gains of the secondary frequency control will be adjusted once attacks are detected. In [13], adaptive communication weight is employed to attenuate the affected signal. In [14], an event-triggered mechanism is developed to determine the need for updating control inputs. Then in [15] a time-varying sampling method is adopted to prevent intelligent DoS attackers from matching the sampling period. However, these methods may not be effective when the communication network remains disconnected for an extended period.

In contrast to the many existing post-attack methods, there are only few pre-attack methods, which attempt to increase the communication network redundancy to provide extra resilience in advance. In [16], an additional parallel control network layer is added for higher network edge redundancies. However, this method cannot handle DoS node attacks which can target both the original and parallel network layers to disable the targeted nodes. To deal with DoS node attacks, node degree deviation is used as a network structural survivability index in [17] and [18] to optimize the network topology. However, it only guarantees the connectivity of the surviving graphs, while the attacked nodes will remain disabled during the attack. The system performance will be greatly impacted if too many nodes are disabled due to long-lasting DoS node attacks in channel shutdown mode. Therefore, this paper tries to add fake attack targets similar to honeypots [19], [20], [21] and their edges to inherently increase network resilience for DoS attack defense.

To this end, this paper proposes a virtual agent (VA) based attack-resilient distributed control as a pre-attack method to provide AC microgrids with inherent attack resilience to deal with the DoS attack in channel shutdown mode. Different from other pre-attack methods, real agents and their connectivity can be intact during DoS node/edge attacks with the presence of VAs and their associated edges. By exchanging the same form of data and modifying the data in sync with real agents, VAs can confuse the attackers and reduce the chance that real agents are targeted by DoS node attacks.

Note that honeypots [19], [20], [21] have been commonly used by defenders for cyber deception, aiming at attracting the attacks, analyzing the attack patterns, and adjusting the defense strategies accordingly. Although VAs function similarly to the honeypots, the specific microgrid application requires the VAs to have additional responsibilities regarding system operation. In a microgrid, the system's stable operation and power quality should be high priorities, requiring the VAs to not only mimic the behavior of the real agents but also not to impact the optimal control goals. Poorly designed VAs can disrupt optimal control, leading to low power quality or even potential system collapse.

In this paper, we design the VAs by considering the specific requirements in microgrid control. The main contributions of this paper are summarized as follows.

1) VAs are designed for AC microgrids, which will not influence the consensus value of real agents but their nodes and edges can serve as fake attack targets for DoS attacks and hence enhance the DoS attack resilience.
2) The control problem is relaxed to guarantee computational efficiency and a practical solution for a system with VAs. A primal-dual gradient-based distributed solving algorithm is developed, in which the global average voltage, voltage variance, and the gradients related to VAs are estimated distributedly.

Compared with the existing methods, the proposed method has the following advantages.

1) The pre-attack methods in [16], [17], and [18] provide communication network with redundant edges or optimize the network topology. However, they cannot deal with DoS node attacks. Different from these methods, the proposed method increases the network redundancy by adding both edges and nodes.
2) In the traditional honeypot concept [19], [20], [21], the honeypots need to broadcast misleading information for attack attraction. However, in the context of AC microgrid, the information sent out by these honeypots may greatly impact the control performance. Differently, our method coordinates VAs with DGs by a distributed algorithm, which can reach a practical solution satisfying the optimal control goals.

Note that the proposed method is compatible with these methods. It can work as the first defense layer to reduce

the probability that the attacks target real agents. The other methods can work as the second layer to further reduce the impact of DoS attacks.

The remainder of this paper is organized as follows. Section II introduces the cyber-physical system modeling of the AC microgrid with distributed control. Section III describes the VA design. Section IV formulates and relaxes the optimization problem for the system with VAs. Section V incorporates the VA design into a primal-dual gradient-based distributed algorithm. Section VI presents the simulation results on two test systems. Finally, conclusions are drawn in Section VII.

II. CYBER-PHYSICAL SYSTEM MODELING OF AN AC MICROGRID WITH DISTRIBUTED CONTROL

A microgrid consists of two layers: the physical layer and the cyber layer. The physical layer includes the DGs, loads, and the power network. The DGs supply power to the loads through the power network. At the cyber layer, the secondary control adjusts the DGs' set points based on the data collected from the local measurements and the cyber network. These adjustments will drive the system towards an operating point to achieve various control objectives, such as proper voltage regulation and proportional power sharing among the DGs.

A. PHYSICAL SYSTEM MODELING

Assume that there are N dispatchable sources. Let the buses as those in the middle of the LCL filter of each source. The other buses are eliminated by Kron reduction. The corresponding bus admittance matrix for the remaining buses is denoted by $\mathbf{Y} = \mathbf{G} + \mathrm{j}\mathbf{B}$. The real and reactive power injections at bus i can be written as [22]:

$$\lambda_{P_i} = \frac{v_i}{\overline{P}_i} \sum_{j \in \mathcal{W}_i} v_j \big(G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij}\big) \tag{1}$$

$$\lambda_{Q_i} = \frac{v_i}{\overline{Q}_i} \sum_{j \in \mathcal{W}_i} v_j \big(G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij}\big), \tag{2}$$

where λ_{P_i} and λ_{Q_i} are the normalized active and reactive power of the ith DG, $\overline{P}_i$ and $\overline{Q}_i$ are the active and reactive power limits of DG i, $\mathcal{W}_i$ is the set of buses that connect with bus i (including bus i), v_i and v_j are, respectively, the voltage magnitudes of buses i and j, $\theta_{ij} = \theta_i - \theta_j$ is the phase angle difference between buses i and j, and G_{ij} and B_{ij} are the real and imaginary parts of the (i, j)-th element in $\mathbf{Y}$.

B. CYBER SYSTEM MODELING

The microgrid communication network can be modeled as a weighted directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with $\mathcal{V} = \{1, 2, \cdots, N\}$ as the node set and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ as the edge set. $\mathcal{G}$ can be described by an adjacency matrix $\mathbf{A} = [a_{ij}] \in \mathbb{R}^{N \times N}$ where a_{ij} is the edge weight between nodes i and j. As in [3], we assume that all edge weights of $\mathcal{G}$ are time-invariant. The Laplacian matrix is defined as $\mathbf{L} = \mathbf{D}^{\text{in}} - \mathbf{A}$ where $\mathbf{D}^{\text{in}} = \text{diag}(d_1^{\text{in}}, \cdots, d_N^{\text{in}})$ is the in-degree matrix with $d_i^{\text{in}} = \sum_{j \in \mathcal{N}_i} a_{ij}$ and $\mathcal{N}_i$ as the set of neighbors of node i on $\mathcal{G}$. Similar to the in-degree matrix, an out-degree matrix $\mathbf{D}^{\text{out}} = \text{diag}(d_1^{\text{out}}, \cdots, d_N^{\text{out}})$ can be defined with $d_i^{\text{out}} = \sum_{j \in \mathcal{N}_i} a_{ji}$. The Laplacian matrix is balanced if the in-degree and out-degree matrices are equal.

For an undirected communication graph, as we always have $a_{ij} = a_{ji}$, its in-degree matrix is always equal to its out-degree matrix, and its Laplacian matrix can be obtained by $\mathbf{L} = \mathbf{D} - \mathbf{A}$ where $\mathbf{D} = \text{diag}(d_1, \cdots, d_N)$ is the degree matrix with $d_i = \sum_{j \in \mathcal{N}_i} a_{ij}$. In this paper, we only consider the communication network as undirected graphs.

C. SECONDARY CONTROL WITHOUT VAS

Without loss of generality, the control in [6] is adopted to demonstrate how microgrid controllers work. The goal of the secondary control in [6] is to 1) restore the microgrid frequency back to the nominal frequency, 2) regulate the system average voltage and voltage variance to the reference values, and 3) achieve proportional active power sharing and relaxed reactive power sharing.

Recently, microgrid controls have been formulated as optimization problems [23], [24], [25], which guarantee mathematically rigorous solutions and good compatibility with different control goals. In light of this, we formulate the control in [6] as an optimization problem. Specifically, for each real agent $i \in \mathcal{V}$, it solves the following optimization problem:

$$\min_{\mathbf{v}, \omega_i} f_i = \frac{1}{2}\Bigg(\sum_{j \in \mathcal{N}_i} a_{ij} \big(\lambda_{P_i} - \lambda_{P_j}\big)^2 + \sum_{j \in \tilde{\mathcal{N}}_i} \tilde{a}_{ij} \big(\lambda_{Q_i} - \lambda_{Q_j}\big)^2 + \frac{1}{\eta}(\omega_i - \omega^{\text{r}})^2 \Bigg) \tag{3a}$$

$$\text{s.t.} \quad \frac{\mathbf{1}^\top \mathbf{v}}{N} - v^{\text{r}} = 0 \tag{3b}$$

$$\frac{1}{N} \sum_{s=1}^{N} \Big(v_s - \frac{1}{N} \sum_{j=1}^{N} v_j \Big)^2 - {\sigma^2}^* = 0, \tag{3c}$$

where ω^{r} and v^{r} are the nominal frequency and rated voltage, respectively, $\eta > 0$ is a design parameter that guarantees the frequency to be regulated to the nominal frequency (detailed discussions can be found in Section V-C), $\mathbf{v} = [v_1, v_2, \cdots, v_N]^\top$ is the voltage magnitude vector for real agents, ω_i is the frequency of DG i with $\omega_i - \omega^{\text{r}} = \dot{\theta}_i$, and ${\sigma^2}^*$ is the voltage variance reference.

The optimization problem in (3) aims at achieving a perfect active power sharing among the DGs. For that reason, in the first term of the objective function we use a_{ij} as the weight of the active power mismatch term. However, as discussed in [6], there is a trade-off between voltage regulation and reactive power sharing. In order to achieve both average voltage and voltage variance regulation, we need to relax one DG from the reactive power sharing. For example, we can choose the kth source, $k \in \{1, \cdots, N\}$, to be the one that is relaxed from reactive power sharing. Then $\mathbf{A}$ is modified to be $\tilde{\mathbf{A}} = [\tilde{a}_{ij}]$ by setting the elements in the kth row and the kth column

to zero. The corresponding communication graph is denoted by $\tilde{\mathcal{G}}$ and the corresponding Laplacian matrix becomes $\tilde{\mathbf{L}} = \tilde{\mathbf{D}} - \tilde{\mathbf{A}}$ where $\tilde{\mathbf{D}} = \text{diag}(\tilde{d}_1, \cdots, \tilde{d}_N)$ is the degree matrix with $\tilde{d}_i = \sum_{j \in \tilde{\mathcal{N}}_i} \tilde{a}_{ij}$ and $\tilde{\mathcal{N}}_i$ is the set of neighbor of node i on $\tilde{\mathcal{G}}$. Then in the second term in the objective function regarding reactive power sharing, we use $\tilde{a}_{ij}$ instead of a_{ij}.

The optimization problem in (3) is formulated to achieve a combined voltage and frequency control for the grid-forming inverters in an islanded AC microgrid. In the objective function, the normalized active and reactive power mismatch is minimized by the first two terms to reach proportional power sharing. The last term is used to regulate the frequency of DG i back to the nominal frequency. The constraint (3b) regulates the global average voltage to the rated voltage v^{r} and the constraint (3c) further ensures the global voltage variance to be the reference value σ^{2*}.

Choose $\forall h \in \{1, \cdots, N\} \backslash k$. Assume that the communication network $\mathcal{G}$ meets the requirement for reaching a consensus. The control in [6] and the optimization problem in (3) are equivalent to solving the following set of nonlinear equations [6]:

$$\begin{cases} \sum_{i=1}^{N} \dfrac{v_i}{N} = v^{\text{r}} & \text{(4a)} \\ \dfrac{1}{N} \sum_{i=1}^{N} \left(v_i - \dfrac{1}{N} \sum_{i=1}^{N} v_i \right)^2 = \sigma^{2*} & \text{(4b)} \\ \lambda_{Q_h} = \lambda_{Q_j}, \ j = 1, \ldots, N, \ j \neq h, \ j \neq k & \text{(4c)} \\ \lambda_{P_h} = \lambda_{P_j}, \ j = 1, \ldots, N, \ j \neq h & \text{(4d)} \end{cases}$$

Here (4a) is corresponding to (3b), (4b) is corresponding to (3c), and (4c) is for relaxed reactive power sharing and (4d) is for proportional active power sharing, which are corresponding to the first two terms in the objective function (3a). As discussed in [26], by introducing $1/\eta$ as weight in (3) the frequency of DG i will return to the nominal frequency ω^{r} when achieving a steady state. This will be further discussed in more detail in Section V-C. For this reason, we have $\omega_i = \omega^{\text{r}}$, $i = 1, \ldots, N$ in the steady state. In (4a), there are a total of $2N - 1$ equations and $2N - 1$ unknown variables, $v_1, v_2, \cdots, v_N, \theta_2, \cdots, \theta_N$. A practical solution can be obtained by solving these equations.

III. VA DESIGN AND STEADY-STATE ANALYSIS

In this paper, we only consider the DoS attacks in channel shutdown mode where the attacked communication channels will be constantly disabled after the attacks begin. To enhance the attack resilience of the distributed control, we add N_{va} VAs to the original communication network $\mathcal{G}$. The total number of agents thus becomes $N_{\text{t}} = N + N_{\text{va}}$. Proper topology design can help improve network survivability. However, topology design is out of the scope of this paper, and we only assume that the undirected communication network with both real and virtual agents, $\hat{\mathcal{G}} = (\hat{\mathcal{V}}, \hat{\mathcal{E}})$, has a spanning tree, with the overall node set $\hat{\mathcal{V}} = \{\mathcal{V}, \mathcal{V}_{\text{va}}\}$ and the VA set $\mathcal{V}_{\text{va}} = \{N + 1, N + 2, \cdots, N_{\text{t}}\}$.

The adjacency matrix, degree matrix, and Laplacian matrix of $\hat{\mathcal{G}}$ are denoted respectively by $\hat{\mathbf{A}} = [\hat{a}_{ij}]$, $\hat{\mathbf{D}}$, and $\hat{\mathbf{L}}$. The corresponding adjacency matrix with a special real agent $k \in \{1, 2, \cdots, N\}$ for relaxed reactive power sharing is $\hat{\tilde{\mathbf{A}}} = [\hat{\tilde{a}}_{ij}]$ for graph $\hat{\tilde{\mathcal{G}}} = (\hat{\mathcal{V}}, \hat{\tilde{\mathcal{E}}})$, which is obtained by setting the elements in the kth row and the kth column of $\hat{\mathbf{A}}$ to zero. The degree matrix and Laplacian matrix corresponding to $\hat{\tilde{\mathbf{A}}}$ are, respectively, denoted by $\hat{\tilde{\mathbf{D}}}$ and $\hat{\tilde{\mathbf{L}}}$.

A. VA DESIGN

A microgrid with VAs is illustrated in Fig. 1. The VAs connect to the communication network. The neighbors of VAs can be either DGs or VAs. Similar to real agents, VAs also receive information from their neighbors and broadcast their information based on the received information. Note that the VAs only connect to the agents at the cyber layer to exchange information while the real agents not only exchange information with the other agents but also control the DGs at the physical layer to maintain the system voltage and frequency to reach the expected control goals. Since VAs are not real power sources, their existence does not impact the power dispatching at the physical layer if they are well coordinated with the DGs at the cyber layer.

With knowledge of specific network topologies, attackers can launch deliberate attacks on nodes. These node attacks will be more harmful to a microgrid compared to edge attacks because targeted DGs will directly lose connection with others and will have to run in local mode. Existing pre-attack methods focus solely on adding redundant edges to the communication network. Differently, VAs can provide both redundant nodes and edges to be DoS attack targets. The existence of these VAs as fake attack targets can inherently increase the network resilience to DoS attacks for a microgrid by reducing the probability that real agents are attacked.

Since the data sent from the VAs can also impact the system's steady state, we design the VAs for the control in Section II-C in such a way that they will not provide additional information to influence the consensus value of the real agents but they can help with the information propagation among the real agents and serve as dummy targets of potential DoS attacks.

The specific design of each VA $l \in \mathcal{V}_{\text{va}}$ is illustrated in Fig. 2. More details of our design are given below.

1) To satisfy (4a), the voltage of VA l is set as rated voltage:

$$v_l = v^{\text{r}}. \tag{5}$$

Let $s \in \hat{\mathcal{V}}$ denote any agent among all real DGs and VAs. Similar to the *average voltage regulator* in [6], an average voltage observer is applied to both real agents and VAs using $\hat{\mathcal{G}}$ to distributedly estimate the average voltage as:

$$v_s^{\text{av}}(t) = v_s(t) + \int_0^t \sum_{j \in \hat{\mathcal{N}}_s} \hat{a}_{sj} \left(v_j^{\text{av}}(\tau) - v_s^{\text{av}}(\tau) \right) d\tau, \tag{6}$$

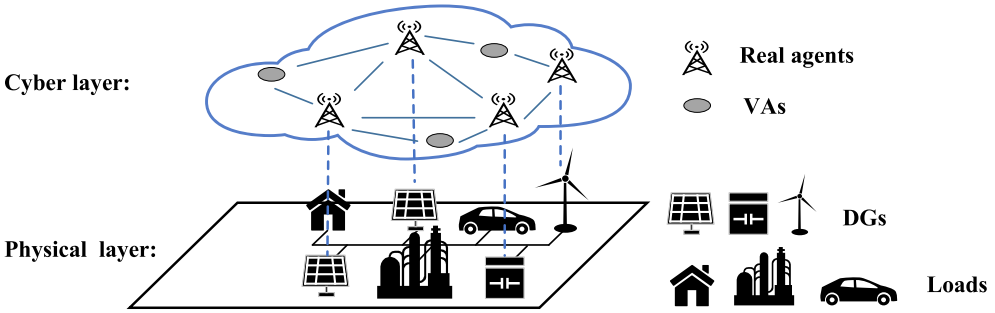


FIGURE 1. A microgrid with VAs.

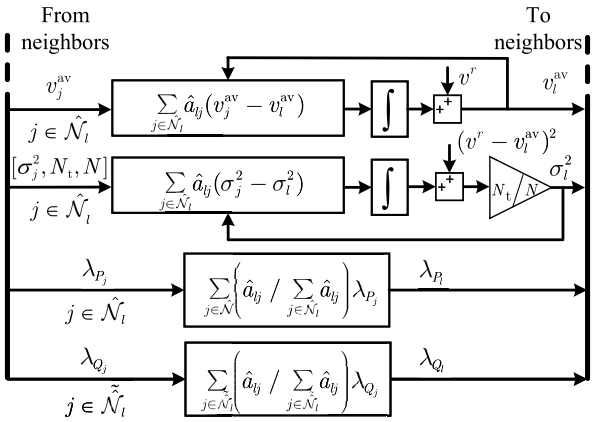


FIGURE 2. The control structure of a VA l.

where $\hat{\mathcal{N}}_s$ is the set of neighbors of node s on $\hat{\mathcal{G}}$ and v_s^{av} is the average voltage estimated by agent s.

2) Adding VAs as in (5) will scale down the voltage variance because the total number of agents increases from N to N_{t}. To satisfy (4b), we need to scale up the estimated variance in order to recover the variance of real agents. Based on the *voltage variance regulator* in [6] we use the scaled voltage variance observer below to estimate the voltage variance by either a real agent or VA $s \in \hat{\mathcal{V}}$:

$$\sigma_s^2(t) = \frac{N_{\text{t}}}{N}\Big[\big(v_s(t) - v_s^{\text{av}}(t)\big)^2 + \int_0^t \sum_{j\in\hat{\mathcal{N}}_s} \hat{a}_{sj}\Big(\sigma_j^2(\tau) - \sigma_s^2(\tau)\Big)\,d\tau\Big], \quad (7)$$

where σ_s^2 is the scaled voltage variance distributedly estimated by agent s.

According to the proof in [3] and [6], if i) the communication graph $\mathcal{G}$ has a spanning tree and ii) the associated Laplacian matrix $\mathbf{L}$ is balanced (always guaranteed for undirected graphs), the average voltage observer and voltage variance observer based on dynamic consensus can, respectively, estimate the global average voltage and global voltage variance dynamically.

In the system with VAs, the communication graph $\hat{\mathcal{G}}$ and the Laplacian matrix $\hat{\mathbf{L}}$ can be set to satisfy these two conditions. Consequently, (6) will converge to the global average voltage dynamically and (7) will converge to the global voltage variance among the real agents dynamically by compensating the scale-down caused by the increase in the number of agents due to the introduction of VAs.

3) To satisfy (4c) and (4d), we make the power output information shared by VAs redundant to (4c) and (4d). Specifically, the normalized real and reactive power outputs of VA l are set as the weighted average of the normalized real and reactive power outputs of its neighbors:

$$\lambda_{P_l} = \sum_{j\in\hat{\mathcal{N}}_l} \frac{\hat{a}_{lj}}{\sum_{j\in\hat{\mathcal{N}}_l}\hat{a}_{lj}}\lambda_{P_j} \quad (8)$$

$$\lambda_{Q_l} = \sum_{j\in\tilde{\hat{\mathcal{N}}}_l} \frac{\tilde{\hat{a}}_{lj}}{\sum_{j\in\tilde{\hat{\mathcal{N}}}_l}\tilde{\hat{a}}_{lj}}\lambda_{Q_j}, \quad (9)$$

where $\hat{\mathcal{N}}_l$ and $\tilde{\hat{\mathcal{N}}}_l$ are the sets of neighbors of node l on $\hat{\mathcal{G}}$ and $\tilde{\hat{\mathcal{G}}}$, respectively. Note that the neighbors of VA l can include both real agents and VAs, which will induce a self-loop for the gradient calculation in the distributed solving algorithm and pose great challenges to the distributed implementation. This will be discussed in more detail in Section V-B.

B. STEADY-STATE ANALYSIS

After integrating VAs, the distributed control is equivalent to solving the following set of nonlinear equations ($h \in \hat{\mathcal{V}}\backslash k$):

$$\begin{cases} \frac{1}{N_{\text{t}}}\big(\sum_{i=1}^{N} v_i + \sum_{l=1}^{N_{\text{va}}} v_l\big) = v^{\text{r}} & (10a)\\ \frac{N_{\text{t}}}{N}\Big[\frac{1}{N_{\text{t}}}\Big(\sum_{i=1}^{N}\Big(v_i - \frac{1}{N_{\text{t}}}\big(\sum_{i=1}^{N} v_i + \sum_{l=1}^{N_{\text{va}}} v_l\big)\Big)^2 & (10b)\\ \quad + \sum_{l=1}^{N_{\text{va}}}\Big(v_l - \frac{1}{N_{\text{t}}}\big(\sum_{i=1}^{N} v_i + \sum_{l=1}^{N_{\text{va}}} v_l\big)\Big)^2\Big)\Big] = \sigma^{2*} & (10c)\\ \lambda_{Q_h} = \lambda_{Q_j},\ j = 1,\ldots,N_{\text{t}},\ j \neq h,\ j \neq k & (10d)\\ \lambda_{P_h} = \lambda_{P_j},\ j = 1,\ldots,N_{\text{t}},\ j \neq h. & (10e) \end{cases}$$

With (5) and $N_t = N + N_{va}$, (10a)–(10c) can be simplified to (4a)–(4b). Specifically,

$$(10a) \iff \sum_{i=1}^{N} v_i = (N_t - N_{va})v^r \iff (4a).$$

Then with (10a), we have

$$(10c) \iff \frac{1}{N}\sum_{i=1}^{N}(v_i - v^r)^2 = {\sigma^2}^* \iff (4b).$$

With (8) and (9), the normalized power outputs associated with the VAs are redundant in (10d) and (10e). Therefore, (10a)–(10e) will have the same solution as that of (4a)–(4d). Therefore, adding VAs will not change the steady-state operating condition to which the distributed control will drive the system.

Although VAs are designed here for the control in [6], it can be designed similarly for other controls. For example, for the droop-free control with average voltage regulation in [3], VAs can be designed by removing (7) and replacing $\tilde{\hat{a}}_{lj}$ and $\tilde{\hat{\mathcal{N}}}$ in (9) by $\hat{a}_{lj}$ and $\hat{\mathcal{N}}$, respectively. This is equivalent to solving:

$$\begin{cases} (10a), (10e) \\ \lambda_{Q_h} = \lambda_{Q_j}, \ j = 1, \ldots, N_t, \ j \neq h, \end{cases}$$

which will give the same steady state as that from the system equations without VAs below:

$$\begin{cases} (4a), (4d) \\ \lambda_{Q_h} = \lambda_{Q_j}, \ j = 1, \ldots, N, \ j \neq h. \end{cases}$$

IV. OPTIMIZATION PROBLEM FORMULATION FOR THE SECONDARY CONTROL WITH VAS

Here we first formulate the optimization problem involving VAs at the cyber layer. In order to ensure optimality, the original problem is converted to a convex optimization problem through approximation and linearization.

A. PROBLEM FORMULATION

According to (5)–(9), the optimization problem in (3) can be redesigned for the system with VAs. For any real agent $i \in \mathcal{V}$, it solves the following optimization problem:

$$\min_{\hat{\mathbf{v}},\omega_i} f_i = \frac{1}{2}\Bigg(\sum_{j\in\hat{\mathcal{N}}_i} \hat{a}_{ij}(\lambda_{P_i} - \lambda_{P_j})^2 + \sum_{j\in\tilde{\hat{\mathcal{N}}}_i} \tilde{\hat{a}}_{ij}(\lambda_{Q_i} - \lambda_{Q_j})^2 + \frac{1}{\eta}(\omega_i - \omega^r)^2\Bigg) \quad (11a)$$

$$\text{s.t.} \quad \frac{\mathbf{1}^\top \hat{\mathbf{v}}}{N_t} - v^r = 0 \quad (11b)$$

$$\frac{N_t}{N}\left(\frac{1}{N_t}\sum_{s=1}^{N_t}\left(v_s - \frac{1}{N_t}\sum_{j=1}^{N_t} v_j\right)^2\right) - {\sigma^2}^* = 0, \quad (11c)$$

where $\hat{\mathbf{v}} = [v_1, v_2, \cdots, v_N, v_{N+1}, \cdots, v_{N_t}]^\top$ is the voltage magnitude vector for all agents. Note that the first coefficient in (11c) is introduced by the scaling in (7). The numerator N_t can be eventually canceled out by $1/N_t$ inside the bracket to ensure that the real agents' voltage variance can remain the same after the VAs are involved.

B. PROBLEM RELAXATION

Due to the non-convexity of the power injection functions (1)–(2) and the nonlinearity of the equality constraint (11c), problem (11) is a nonconvex nonlinear optimization problem, which is hard to solve. Here we make some necessary approximations to obtain a relaxed convex optimization problem.

First, the approximated power injection functions in [27] are introduced for the objective function (11a):

$$\tilde{\lambda}_{P_i} = \frac{1}{\overline{P}_i}\sum_{j=1}^{N}\left(G_{ij}v_j - B_{ij}\theta_j\right) \quad (12)$$

$$\tilde{\lambda}_{Q_i} = -\frac{1}{\overline{Q}_i}\sum_{j=1}^{N}\left(B_{ij}v_j + G_{ij}\theta_j\right), \quad (13)$$

where $i \in \mathcal{V}$ and θ_j is the phase angle of bus j. Using (12) and (13), the convexity of the objective function (11a) can be proved in a similar way as in [23].

To simplify the notations for later sections, for $\forall l \in \mathcal{V}_{va}$ let

$$\tilde{\lambda}_{P_l} = \lambda_{P_l}, \quad \tilde{\lambda}_{Q_l} = \lambda_{Q_l}. \quad (14)$$

Then, to remove the nonlinearity of (11c), we linearize it. Specifically, (11c) is reorganized as:

$$g(\hat{\mathbf{v}}) - {\sigma^2}^* = 0, \quad (15)$$

where $g(\hat{\mathbf{v}}) = \frac{N_t}{N}\sum_{s=1}^{N_t}\left(v_s - \sum_{j=1}^{N_t} v_j/N_t\right)^2/N_t$. Linearizing $g(\hat{\mathbf{v}})$ around $\hat{\mathbf{v}}'$, we have

$$g(\hat{\mathbf{v}}) \approx g(\hat{\mathbf{v}}') + \sum_{s=1}^{N_t}\left.\frac{\partial g(\hat{\mathbf{v}})}{\partial v_s}\right|_{\hat{\mathbf{v}}=\hat{\mathbf{v}}'}(v_s - v_s') \triangleq g(\hat{\mathbf{v}}') + \sum_{s=1}^{N_t}\tilde{g}_s(\hat{\mathbf{v}}, \hat{\mathbf{v}}'), \quad (16)$$

where

$$\tilde{g}_s(\hat{\mathbf{v}}, \hat{\mathbf{v}}') = \left.\frac{\partial g(\hat{\mathbf{v}})}{\partial v_s}\right|_{\hat{\mathbf{v}}=\hat{\mathbf{v}}'}(v_s - v_s'), \quad (17)$$

$$\left.\frac{\partial g(\hat{\mathbf{v}})}{\partial v_s}\right|_{\hat{\mathbf{v}}=\hat{\mathbf{v}}'} = \frac{2}{N}\Bigg[\sum_{k=1}^{N_t}\left(v_k' - \sum_{j=1}^{N_t}\frac{v_j'}{N_t}\right)\left(-\frac{1}{N_t}\right) + \left(v_s' - \sum_{j=1}^{N_t}\frac{v_j'}{N_t}\right)\Bigg]. \quad (18)$$

Then, (11c) can be expressed in a linearized form as:

$$\sum_{s=1}^{N_t}\tilde{g}_s(\hat{\mathbf{v}}, \hat{\mathbf{v}}') + g(\hat{\mathbf{v}}') - {\sigma^2}^* = 0. \quad (19)$$

With (12)–(13) and (19), problem (11) is finally relaxed to the convex optimization problem below:

$$\min_{\hat{\mathbf{v}},\omega_i} f_i = \frac{1}{2}\Bigg(\sum_{j\in\hat{\mathcal{N}}_i}\hat{a}_{ij}\big(\tilde{\lambda}_{P_i}-\tilde{\lambda}_{P_j}\big)^2 + \sum_{j\in\tilde{\hat{\mathcal{N}}}_i}\tilde{\hat{a}}_{ij}\big(\tilde{\lambda}_{Q_i}-\tilde{\lambda}_{Q_j}\big)^2 + \frac{1}{\eta}(\omega_i-\omega^{\mathrm{r}})^2\Bigg) \tag{20a}$$

$$\text{s.t.} \quad \frac{\mathbf{1}^\top\hat{\mathbf{v}}}{N_{\mathrm{t}}} - v^{\mathrm{r}} = 0 \tag{20b}$$

$$\sum_{s=1}^{N_{\mathrm{t}}}\tilde{g}_s(\hat{\mathbf{v}},\hat{\mathbf{v}}') + g(\hat{\mathbf{v}}') - {\sigma^2}^* = 0. \tag{20c}$$

V. PROPOSED DISTRIBUTED SOLVING ALGORITHM

It is challenging to solve the relaxed optimization problem (20) by each DG using only local data and achieve a fully distributed implementation, mainly because:

1) In (20b) and (20c), the calculation of the global average voltage and global voltage variance requires $\hat{\mathbf{v}}$, which is a vector that contains the global voltage information;
2) The power outputs of the VAs depend on their neighbors' power outputs. According to (8) and (9), when a VA has another VA as its neighbor, its gradient calculation will require global information.

In this section, we first address the challenge of estimating the global average voltage and global voltage variance using the existing estimation methods. Second, we propose a linear equation for calculating the VAs' gradients, which can be solved in a distributed manner to tackle the second challenge. Finally, we introduce the overall update policy.

A. LAGRANGE FUNCTION AND CONSTRAINT ESTIMATION

For (20b) and (20c), let $h_1(\hat{\mathbf{v}}) = \mathbf{1}^\top\hat{\mathbf{v}}/N_{\mathrm{t}} - v^{\mathrm{r}}$ and $h_2(\hat{\mathbf{v}},\hat{\mathbf{v}}') = \sum_{s=1}^{N_{\mathrm{t}}}\tilde{g}_s(\hat{\mathbf{v}},\hat{\mathbf{v}}') + g(\hat{\mathbf{v}}') - {\sigma^2}^*$. The Lagrange function for problem (20) is defined as:

$$L_i(\hat{\mathbf{v}},\omega_i,\mu_{1i},\mu_{2i}) = f_i(\hat{\mathbf{v}},\omega_i) + \mu_{1i}|h_1(\hat{\mathbf{v}})| + \mu_{2i}|h_2(\hat{\mathbf{v}},\hat{\mathbf{v}}')|, \tag{21}$$

where μ_{1i} and μ_{2i} are the Lagrange multipliers.

Note that in (21), given the distributed control implementation, the local accessibility of each agent to the voltage vector $\hat{\mathbf{v}}$ is limited. To address this, distributed average voltage and voltage variance observers are employed to estimate the average voltage and voltage variance in $h_1(\hat{\mathbf{v}})$ and $h_2(\hat{\mathbf{v}},\hat{\mathbf{v}}')$.

Specifically, the first term in $h_1(\hat{\mathbf{v}})$, $\mathbf{1}^\top\hat{\mathbf{v}}/N_{\mathrm{t}}$, can be estimated by agent $i \in \hat{\mathcal{V}}$ as $v_i^{\mathrm{av}}[n]$ using the discrete-form distributed average voltage estimator [23]:

$$v_i^{\mathrm{av}}[n] = v_i[n] + \sum_{t=0}^{n}\sum_{j\in\hat{\mathcal{N}}_i}\hat{a}_{ij}\big(v_j^{\mathrm{av}}[t] - v_i^{\mathrm{av}}[t]\big)\Delta t, \tag{22}$$

where n is the current time step and Δt is the step size.

For $h_2(\hat{\mathbf{v}},\hat{\mathbf{v}}')$, let $\hat{\mathbf{v}}' = \hat{\mathbf{v}}[n-1]$. Then the first term in $h_2(\hat{\mathbf{v}},\hat{\mathbf{v}}')$, $\sum_{s=1}^{N_{\mathrm{t}}}\tilde{g}_s(\hat{\mathbf{v}},\hat{\mathbf{v}}')$, can be estimated by

$$\sum_{s=1}^{N_{\mathrm{t}}}\tilde{g}_s[n] = N_{\mathrm{t}}\,\tilde{g}_i^{\mathrm{av}}[n], \tag{23}$$

where $\tilde{g}_i^{\mathrm{av}}[n]$ is the estimate of $\sum_{s=1}^{N_{\mathrm{t}}}\tilde{g}_s(\hat{\mathbf{v}},\hat{\mathbf{v}}')/N_{\mathrm{t}}$ by agent $i \in \hat{\mathcal{V}}$ using the dynamic consensus method:

$$\tilde{g}_i^{\mathrm{av}}[n] = \tilde{g}_i[n] + \sum_{t=0}^{n}\sum_{j\in\hat{\mathcal{N}}_i}\hat{a}_{ij}\left(\tilde{g}_j^{\mathrm{av}}[t] - \tilde{g}_i^{\mathrm{av}}[t]\right)\Delta t. \tag{24}$$

Note that in (24) the first term $\tilde{g}_i[n]$ is not locally available to agent i only by its own voltage v_i through (17)–(18). With $\hat{\mathbf{v}}' = \hat{\mathbf{v}}[n-1]$ and replacing the global average voltage in (18) by its estimate $v_i^{\mathrm{av}}[n-1]$, $\tilde{g}_i[n]$ can be estimated by:

$$\begin{aligned}\tilde{g}_i[n] &= \left.\frac{\partial g(\hat{\mathbf{v}})}{\partial v_i}\right|_{\hat{\mathbf{v}}=\hat{\mathbf{v}}[n-1]}(v_i[n]-v_i[n-1]) \\ &= \frac{2}{N}\big(v_i[n-1]-v_i^{\mathrm{av}}[n-1]\big)(v_i[n]-v_i[n-1]).\end{aligned} \tag{25}$$

The second term in $h_2(\hat{\mathbf{v}},\hat{\mathbf{v}}')$, $g(\hat{\mathbf{v}}')$, can be estimated by agent $i \in \hat{\mathcal{V}}$ using the discrete-form distributed variance estimator. Then the voltage variance can be distributedly estimated by:

$$\sigma_i^2[n-1] = \frac{N_{\mathrm{t}}}{N}\Bigg[\big(v_i[n-1]-v_i^{\mathrm{av}}[n-1]\big)^2 + \sum_{t=0}^{n-1}\sum_{j\in\hat{\mathcal{N}}_i}\hat{a}_{ij}\left(\sigma_j^2[t]-\sigma_i^2[t]\right)\Delta t\Bigg]. \tag{26}$$

If 1) the communication graph has a spanning tree and 2) the associated Laplacian matrix $\hat{\mathbf{L}}$ is balanced (always guaranteed for undirected graphs), the distributed observers in (22), (24), and (26) based on dynamic consensus protocol can globally and dynamically solve the average consensus problems, and employing these distributed observers can ensure the convergence of the average voltage and the voltage variance estimates to their true global average and variance, respectively. This can be readily proved based on the work in [3], [5], and [6].

B. GRADIENT CALCULATION

1) GRADIENT WITH RESPECT TO VOLTAGE

The gradient of the Lagrange function (21) with respect to v_i is calculated by:

$$\begin{aligned}\frac{\partial L_i[n]}{\partial v_i} &= \sum_{j\in\hat{\mathcal{N}}_i, j\notin\mathcal{V}_{\mathrm{va}}}\hat{a}_{ij}\left(\tilde{\lambda}_{P_i}[n]-\tilde{\lambda}_{P_j}[n]\right)\left(\frac{G_{ii}}{\overline{P}_i}-\frac{G_{ij}}{\overline{P}_j}\right) \\ &+ \sum_{j\in\hat{\mathcal{N}}_i\cap\mathcal{V}_{\mathrm{va}}}\hat{a}_{ij}\left(\tilde{\lambda}_{P_i}[n]-\tilde{\lambda}_{P_j}[n]\right)\left(\frac{G_{ii}}{\overline{P}_i}-\frac{\partial\tilde{\lambda}_{P_j}}{\partial v_i}\right) \\ &+ \sum_{j\in\tilde{\hat{\mathcal{N}}}_i, j\notin\mathcal{V}_{\mathrm{va}}}\tilde{\hat{a}}_{ij}\left(\tilde{\lambda}_{Q_i}[n]-\tilde{\lambda}_{Q_j}[n]\right)\left(\frac{-B_{ii}}{\overline{Q}_i}+\frac{B_{ij}}{\overline{Q}_j}\right)\end{aligned}$$

$$+\sum_{j\in\tilde{\mathcal{N}}_i\cap\mathcal{V}_{\rm va}}\tilde{\hat{a}}_{ij}\left(\tilde{\lambda}_{Q_i}[n]-\tilde{\lambda}_{Q_j}[n]\right)\left(\frac{-B_{ii}}{\overline{Q}_i}-\frac{\partial\tilde{\lambda}_{Q_j}}{\partial v_i}\right)$$
$$+\mu_{1i}\mathcal{D}_{v_i}\left|v_i^{\rm av}[n]-v^{\rm r}\right|$$
$$+\mu_{2i}\mathcal{D}_{v_i}\left|N_{\rm t}\tilde{g}_i^{\rm av}[n]+\sigma_i^2[n-1]-\sigma^{2^*}\right|, \quad (27)$$

where $\mathcal{D}_{v_i}$ is the operator for subgradient with respect to v_i. For implementation, the subgradients are calculated as:

$$\mathcal{D}_{v_i}\left|v_i^{\rm av}[n]-v^{\rm r}\right|=\frac{1}{N_{\rm t}}\,{\rm sgn}\left(v_i^{\rm av}[n]-v^{\rm r}\right) \quad (28)$$

$$\mathcal{D}_{v_i}\left|g_i[n]-\sigma^{2^*}\right|=\frac{2}{N}\left(v_i[n-1]-v_i^{\rm av}[n-1]\right)$$
$$\times\,{\rm sgn}\left(N_{\rm t}\tilde{g}_i^{\rm av}[n]+\sigma_i^2[n-1]-\sigma^{2^*}\right), \quad (29)$$

where sgn$(\cdot)$ is the sign function.

$\partial\tilde{\lambda}_{P_j}/\partial v_i$ and $\partial\tilde{\lambda}_{Q_j}/\partial v_i$ in the second and fourth terms of (27) are the partial derivatives of the active and reactive power of VA j with respect to v_i. From (14), $\tilde{\lambda}_{P_j}=\lambda_{P_j}$ for $j\in\mathcal{V}_{\rm va}$ and thus based on (8) $\partial\tilde{\lambda}_{P_j}/\partial v_i$ can be calculated as:

$$\frac{\partial\tilde{\lambda}_{P_j}}{\partial v_i}=\sum_{k\in\hat{\mathcal{N}}_j,k\notin\mathcal{V}_{\rm va}}\frac{\hat{a}_{jk}}{\sum_{j\in\hat{\mathcal{N}}_k}\hat{a}_{jk}}\frac{\partial\tilde{\lambda}_{P_k}}{\partial v_i}$$
$$+\sum_{l\in\hat{\mathcal{N}}_j\cap\mathcal{V}_{\rm va}}\frac{\hat{a}_{jl}}{\sum_{j\in\hat{\mathcal{N}}_l}\hat{a}_{jl}}\frac{\partial\tilde{\lambda}_{P_l}}{\partial v_i}. \quad (30)$$

If VA j only connects to real agents with $\hat{\mathcal{N}}_j\cap\mathcal{V}_{\rm va}=\phi$, $\partial\tilde{\lambda}_{P_j}/\partial v_i$ can be easily calculated. For example, in Fig. 3(a), the neighbors of the VA in node 3 are all real agents. Assuming all $a_{ij}=1$, then $\partial\tilde{\lambda}_{P_3}/\partial v_1=\frac{1}{2}\partial\tilde{\lambda}_{P_1}/\partial v_1+\frac{1}{2}\partial\tilde{\lambda}_{P_2}/\partial v_1$. However, if VA j connects to both types of agents with $\hat{\mathcal{N}}_j\cap\mathcal{V}_{\rm va}\neq\phi$, $\partial\tilde{\lambda}_{P_j}/\partial v_i$ cannot be directly calculated since the gradients of its VA neighbors, $\partial\tilde{\lambda}_{P_l}/\partial v_i$, will depend on $\partial\tilde{\lambda}_{P_j}/\partial v_i$. In Fig. 3(b), VA 3 has both virtual and real agent neighbors. Thus $\partial\tilde{\lambda}_{P_3}/\partial v_1=\frac{1}{3}(\partial\tilde{\lambda}_{P_1}/\partial v_1+\partial\tilde{\lambda}_{P_2}/\partial v_1+\partial\tilde{\lambda}_{P_4}/\partial v_1)$ while $\partial\tilde{\lambda}_{P_4}/\partial v_1=\frac{1}{3}(\partial\tilde{\lambda}_{P_1}/\partial v_1+\partial\tilde{\lambda}_{P_2}/\partial v_1+\partial\tilde{\lambda}_{P_3}/\partial v_1)$.

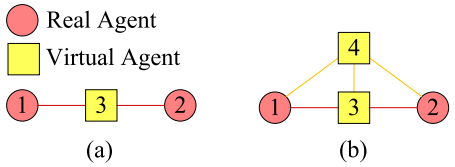


FIGURE 3. VA at node 3 and its neighbors: (a) Node 3 has only real agent neighbors; (b) Node 3 has both real and virtual agent neighbors.

To solve this problem, we describe $\hat{\mathbf{D}}$, $\hat{\mathbf{A}}$, and $\hat{\mathbf{L}}$ as:

$$\hat{\mathbf{A}}=\begin{bmatrix}\hat{\mathbf{A}}_{rr}&\hat{\mathbf{A}}_{rv}\\ \hat{\mathbf{A}}_{vr}&\hat{\mathbf{A}}_{vv}\end{bmatrix},\quad \hat{\mathbf{D}}=\begin{bmatrix}\hat{\mathbf{D}}_{rr}&\mathbf{0}\\ \mathbf{0}&\hat{\mathbf{D}}_{vv}\end{bmatrix},$$
$$\hat{\mathbf{L}}=\begin{bmatrix}\hat{\mathbf{L}}_{rr}&\hat{\mathbf{L}}_{rv}\\ \hat{\mathbf{L}}_{vr}&\hat{\mathbf{L}}_{vv}\end{bmatrix}, \quad (31)$$

where the subscripts r and v represent the part of the matrix corresponding to real and virtual agents, respectively. Then (30) can be rewritten as:

$$\hat{\mathbf{D}}_{vv}\frac{\partial\tilde{\boldsymbol{\lambda}}_P^{\rm va}}{\partial v_i}=\hat{\mathbf{A}}_{vr}\frac{\partial\tilde{\boldsymbol{\lambda}}_P^{\rm ra}}{\partial v_i}+\hat{\mathbf{A}}_{vv}\frac{\partial\tilde{\boldsymbol{\lambda}}_P^{\rm va}}{\partial v_i}, \quad (32)$$

where the partial derivatives of $\tilde{\lambda}_{P_i}$'s and $\tilde{\lambda}_{Q_i}$'s with respect to v_i for real agents and VAs are respectively

$$\frac{\partial\tilde{\boldsymbol{\lambda}}_P^{\rm ra}}{\partial v_i}=\left[\frac{\partial\tilde{\lambda}_{P_1}}{\partial v_i},\frac{\partial\tilde{\lambda}_{P_2}}{\partial v_i},\cdots,\frac{\partial\tilde{\lambda}_{P_N}}{\partial v_i}\right]^\top$$
$$\frac{\partial\tilde{\boldsymbol{\lambda}}_P^{\rm va}}{\partial v_i}=\left[\frac{\partial\tilde{\lambda}_{P_{N+1}}}{\partial v_i},\frac{\partial\tilde{\lambda}_{P_{N+2}}}{\partial v_i},\cdots,\frac{\partial\tilde{\lambda}_{P_{N_{\rm t}}}}{\partial v_i}\right]^\top.$$

Since $\hat{\mathbf{L}}=\hat{\mathbf{D}}-\hat{\mathbf{A}}$, (32) can be rewritten as:

$$\frac{\partial\tilde{\boldsymbol{\lambda}}_P^{\rm va}}{\partial v_i}=-\hat{\mathbf{L}}_{vv}^{-1}\hat{\mathbf{L}}_{vr}\frac{\partial\tilde{\boldsymbol{\lambda}}_P^{\rm ra}}{\partial v_i}. \quad (33)$$

When the system is under DoS attacks, the network topology may change, which will impact the gradient calculation in (33). To solve this problem, since a VA knows its own connections (i.e., its row and column of $\hat{\mathbf{L}}_{vv}$ and $\hat{\mathbf{L}}_{vr}$), the set of linear algebraic equations in (33) with the form $\mathbf{Bx}=\mathbf{c}$ can be solved by distributed algorithms such as those in [28] and [29]. These algorithms can get the dynamic solution even if $\mathbf{B}$, $\mathbf{c}$, and the network topology are changing occasionally.

Similarly, with (9) and $\tilde{\hat{\mathbf{L}}}=\tilde{\hat{\mathbf{D}}}-\tilde{\hat{\mathbf{A}}}$, we can get the partial derivative of the reactive power with respect to v_i as:

$$\frac{\partial\tilde{\boldsymbol{\lambda}}_Q^{\rm va}}{\partial v_i}=-\tilde{\hat{\mathbf{L}}}_{vv}^{-1}\tilde{\hat{\mathbf{L}}}_{vr}\frac{\partial\tilde{\boldsymbol{\lambda}}_Q^{\rm ra}}{\partial v_i}, \quad (34)$$

where

$$\tilde{\hat{\mathbf{L}}}=\begin{bmatrix}\tilde{\hat{\mathbf{L}}}_{rr}&\tilde{\hat{\mathbf{L}}}_{rv}\\ \tilde{\hat{\mathbf{L}}}_{vr}&\tilde{\hat{\mathbf{L}}}_{vv}\end{bmatrix}, \quad (35)$$

and

$$\frac{\partial\tilde{\boldsymbol{\lambda}}_Q^{\rm ra}}{\partial v_i}=\left[\frac{\partial\tilde{\lambda}_{Q_1}}{\partial v_i},\frac{\partial\tilde{\lambda}_{Q_2}}{\partial v_i},\cdots,\frac{\partial\tilde{\lambda}_{Q_N}}{\partial v_i}\right]^\top$$
$$\frac{\partial\tilde{\boldsymbol{\lambda}}_Q^{\rm va}}{\partial v_i}=\left[\frac{\partial\tilde{\lambda}_{Q_{N+1}}}{\partial v_i},\frac{\partial\tilde{\lambda}_{Q_{N+2}}}{\partial v_i},\cdots,\frac{\partial\tilde{\lambda}_{Q_{N_{\rm t}}}}{\partial v_i}\right]^\top.$$

Note that $\partial\tilde{\boldsymbol{\lambda}}_P^{\rm va}/\partial v_i$ and $\partial\tilde{\boldsymbol{\lambda}}_Q^{\rm va}/\partial v_i$ are not locally available because $\partial\tilde{\boldsymbol{\lambda}}_P^{\rm ra}/\partial v_i$ and $\partial\tilde{\boldsymbol{\lambda}}_Q^{\rm ra}/\partial v_i$ need information from all real agents. However, using the approximated power injection functions in (12)–(13), $\partial\tilde{\boldsymbol{\lambda}}_P^{\rm ra}/\partial v_i$ and $\partial\tilde{\boldsymbol{\lambda}}_Q^{\rm ra}/\partial v_i$ become constants related to $\mathbf{G}$ and $\mathbf{B}$ and can thus be pre-assigned. In the gradient calculation, we assume that the admittance is known by the distributed control implementation. It can actually be estimated by data-driven distributed parameter estimation methods such as the one in [30] based on the voltage and power injection data from the local measurements, especially when the system parameters are changing due to either load change or topology change.

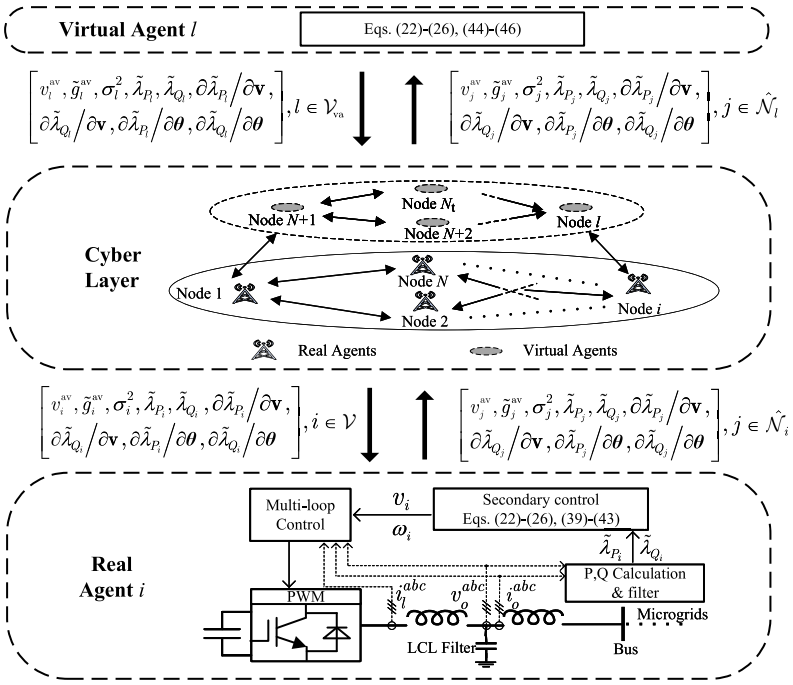


FIGURE 4. Proposed control structure.

2) GRADIENT WITH RESPECT TO FREQUENCY

The gradient of the Lagrange function (21) with respect to ω_i is calculated by:

$$\begin{aligned}\frac{\partial L_i[n]}{\partial \omega_i} = &\Bigg[\sum_{j\in\hat{\mathcal{N}}_i, j\notin\mathcal{V}_{\rm va}} \hat{a}_{ij}(\tilde{\lambda}_{P_i}[n]-\tilde{\lambda}_{P_j}[n])\Big(\frac{-B_{ii}}{\overline{P}_i}+\frac{B_{ij}}{\overline{P}_j}\Big)\\ &+\sum_{j\in\hat{\mathcal{N}}_i\cap\mathcal{V}_{\rm va}} \hat{a}_{ij}(\tilde{\lambda}_{P_i}[n]-\tilde{\lambda}_{P_j}[n])\Big(\frac{-B_{ii}}{\overline{P}_i}-\frac{\partial\tilde{\lambda}_{P_j}}{\partial\theta_i}\Big)\\ &+\sum_{j\in\tilde{\hat{\mathcal{N}}}_i, j\notin\mathcal{V}_{\rm va}} \tilde{\hat{a}}_{ij}(\tilde{\lambda}_{Q_i}[n]-\tilde{\lambda}_{Q_j}[n])\Big(\frac{-G_{ii}}{\overline{Q}_i}+\frac{G_{ij}}{\overline{Q}_j}\Big)\\ &+\sum_{j\in\tilde{\hat{\mathcal{N}}}_i\cap\mathcal{V}_{\rm va}} \tilde{\hat{a}}_{ij}(\tilde{\lambda}_{Q_i}[n]\\ &-\tilde{\lambda}_{Q_j}[n])\Big(\frac{-G_{ii}}{\overline{Q}_i}-\frac{\partial\tilde{\lambda}_{Q_j}}{\partial\theta_i}\Big)\Bigg]\frac{\partial\theta_i}{\partial\omega_i}\\ &+\frac{1}{\eta}(\omega_i[n]-\omega^{\rm r}) \triangleq \frac{\partial L_i[n]}{\partial\theta_i}\frac{\partial\theta_i}{\partial\omega_i}+\frac{1}{\eta}(\omega_i[n]-\omega^{\rm r}),\end{aligned} \tag{36}$$

where $\frac{\partial\theta_i}{\partial\omega_i}=\frac{\partial}{\partial\omega_i}\int_{t-\Delta t}^{t}\big(\omega_i(\tau)-\omega^{\rm r}\big)d\tau=\Delta t$ [26]. $\partial\tilde{\lambda}_{P_j}/\partial\theta_i$ and $\partial\tilde{\lambda}_{Q_j}/\partial\theta_i$ can be calculated by:

$$\frac{\partial\tilde{\boldsymbol{\lambda}}_P^{\rm va}}{\partial\theta_i} = -\hat{\mathbf{L}}_{vv}^{-1}\hat{\mathbf{L}}_{vr}\frac{\partial\tilde{\boldsymbol{\lambda}}_P^{\rm ra}}{\partial\theta_i} \tag{37}$$

$$\frac{\partial\tilde{\boldsymbol{\lambda}}_Q^{\rm va}}{\partial\theta_i} = -\tilde{\hat{\mathbf{L}}}_{vv}^{-1}\tilde{\hat{\mathbf{L}}}_{vr}\frac{\partial\tilde{\boldsymbol{\lambda}}_Q^{\rm ra}}{\partial\theta_i}, \tag{38}$$

where

$$\begin{aligned}\frac{\partial\tilde{\boldsymbol{\lambda}}_P^{\rm ra}}{\partial\theta_i} &= \Big[\frac{\partial\tilde{\lambda}_{P_1}}{\partial\theta_i},\frac{\partial\tilde{\lambda}_{P_2}}{\partial\theta_i},\cdots,\frac{\partial\tilde{\lambda}_{P_N}}{\partial\theta_i}\Big]^\top\\ \frac{\partial\tilde{\boldsymbol{\lambda}}_Q^{\rm ra}}{\partial\theta_i} &= \Big[\frac{\partial\tilde{\lambda}_{Q_1}}{\partial\theta_i},\frac{\partial\tilde{\lambda}_{Q_2}}{\partial\theta_i},\cdots,\frac{\partial\tilde{\lambda}_{Q_N}}{\partial\theta_i}\Big]^\top\\ \frac{\partial\tilde{\boldsymbol{\lambda}}_P^{\rm va}}{\partial\theta_i} &= \Big[\frac{\partial\tilde{\lambda}_{P_{N+1}}}{\partial\theta_i},\frac{\partial\tilde{\lambda}_{P_{N+2}}}{\partial\theta_i},\cdots,\frac{\partial\tilde{\lambda}_{P_{N_t}}}{\partial\theta_i}\Big]^\top\\ \frac{\partial\tilde{\boldsymbol{\lambda}}_Q^{\rm va}}{\partial\theta_i} &= \Big[\frac{\partial\tilde{\lambda}_{Q_{N+1}}}{\partial\theta_i},\frac{\partial\tilde{\lambda}_{Q_{N+2}}}{\partial\theta_i},\cdots,\frac{\partial\tilde{\lambda}_{Q_{N_t}}}{\partial\theta_i}\Big]^\top.\end{aligned}$$

C. OVERALL UPDATE POLICY

Based on (21)–(38), a primal-dual gradient-based distributed algorithm [31] is implemented to solve problem (20). For a real agent $i\in\mathcal{V}$, the variable update equations are:

$$v_i[n+1] = v_i[n]-\alpha\frac{\partial L_i[n]}{\partial v_i} \tag{39}$$

$$\theta_i[n+1] = \theta_i[n]+\big(\omega_i[n]-\omega^{\rm r}\big)\Delta t \tag{40}$$

$$\begin{aligned}\omega_i[n+1] &= \omega_i[n]-\eta\frac{\partial L_i[n]}{\partial\omega_i}\\ &= \omega^{\rm r}-\eta\frac{\partial L_i[n]}{\partial\theta_i}\frac{\partial\theta_i}{\partial\omega_i}\end{aligned} \tag{41}$$

$$\mu_{1i}[n+1] = \mu_{1i}[n]+\gamma_1\big|v_i^{\rm av}[n]-v^{\rm r}\big| \tag{42}$$

$$\mu_{2i}[n+1] = \mu_{2i}[n]+\gamma_2\big|N_{\rm t}\tilde{g}_i^{\rm av}[n]+\sigma_i^2[n-1]-\sigma^{2^*}\big|, \tag{43}$$

where α, η, γ_1, and γ_2 are design parameters. The parameter selection depends on the time step Δt and the system size. Using small values of α, η, γ_1, and γ_2 benefits system stability

but delays the time to reach a steady state. In the simulation in Section VI, we will choose larger design parameters for a small system to ensure fast convergence while smaller design parameters for a large system to ensure stability.

From (41) it is clear that ω_i will become ω^{r} in a steady state, indicating that the frequency of DG i will return to the nominal frequency. This is made possible by introducing $1/\eta$ as weight in (3).

For a VA $l \in \mathcal{V}_{\mathrm{va}}$, based on (5), (8)–(9), and (14), the variable update equations are:

$$v_l[n+1] = v^{\mathrm{r}} \tag{44}$$

$$\tilde{\lambda}_{P_l}[n+1] = \sum_{j\in\hat{\mathcal{N}}_l} \frac{\hat{a}_{lj}}{\sum_{j\in\hat{\mathcal{N}}_l}\hat{a}_{lj}} \tilde{\lambda}_{P_j}[n] \tag{45}$$

$$\tilde{\lambda}_{Q_l}[n+1] = \sum_{j\in\tilde{\hat{\mathcal{N}}}_l} \frac{\tilde{\hat{a}}_{lj}}{\sum_{j\in\tilde{\hat{\mathcal{N}}}_l}\tilde{\hat{a}}_{lj}} \tilde{\lambda}_{Q_j}[n]. \tag{46}$$

Following each update, real DG i sets its voltage set-point v_i^* and frequency set-point ω_i^* to $v_i[n+1]$ and $\omega_i[n+1]$ respectively. They are then sent to the zero-level control (e.g., multi-loop control) to generate pulse width modulation (PWM) signals. The estimated average voltage v^{av}, $\tilde{g}^{\mathrm{av}}$ and σ^2 for voltage variance estimation, as well as the normalized active power output $\tilde{\lambda}_P$ and reactive power output $\tilde{\lambda}_Q$ from both real and virtual agents are then uploaded to the communication network. Once an agent obtains its gradient vectors $\partial\tilde{\lambda}_{P_i}/\partial\mathbf{v}$, $\partial\tilde{\lambda}_{P_i}/\partial\theta$, $\partial\tilde{\lambda}_{Q_i}/\partial\mathbf{v}$, and $\partial\tilde{\lambda}_{Q_i}/\partial\theta$, it broadcasts them to its neighbors. The proposed control structure is shown in Fig. 4.

For a large microgrid system, retaining the zero-level control and detailed inverter models can impose a significant computational burden on simulations. Alternatively, performing variable updates using (39)–(46) alone is a much more efficient way to verify the control effect, assuming that the zero-level control can rapidly track the set-points and the inverters perform ideally. This will be demonstrated for a relatively large microgrid system in Section VI-B.

Remark 1: Given that 1) all VAs are transmitting the same form of data (i.e., v^{av}, $\tilde{g}^{\mathrm{av}}$, σ^2, $\tilde{\lambda}_P$, $\tilde{\lambda}_Q$) as that of the real agents and 2) the output data of VAs undergoes modifications in sync with load variations similar to real agents, distinguishing VAs from real agents will be challenging for the attackers. Therefore, the presence of VAs will decrease the likelihood of DoS attacks targeting real agents and their associated connections.

VI. SIMULATION RESULTS

A. REAL-TIME SIMULATION ON 4-DG TEST SYSTEM

A 4-DG AC microgrid system and its communication network are shown in Fig. 5. The system parameters are the same as those in [6]. DG 4 is selected as the special DG and is relaxed from reactive power sharing. The rated voltage v^{r}, nominal frequency ω^{r}, and voltage variance reference σ^{2*} are set as 1 (p.u.), 120π (rad/s), and 16 (volt^2) respectively.

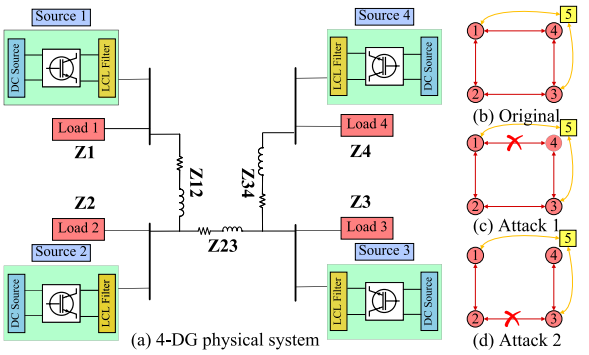


FIGURE 5. 4-DG test system: (a) Physical system; (b) Original communication network (red circles indicate real agents and the yellow square indicates the VA); (c) First attack; (d) Second attack.

All nonzero elements in $\hat{\mathbf{A}}$ and $\tilde{\hat{\mathbf{A}}}$ are set as 0.25. Real-time simulation is performed on OPAL-RT 4510 with Intel Xeon E3 v5 CPU @3.5GHz and 16GB RAM at a time-step of 50 μs using the fixed-step discrete ODE-4 solver. The parameters α, η, γ_1, and γ_2 are chosen as 0.00025, 0.003, 0.15, and 0.01 respectively.

1) INFLUENCE OF VA ON STEADY STATE

As shown in Fig. 5(b), a VA (node 5) is added to the communication network. Load 1 impedance is changed from (25+j18.6) Ω to (16.4+j12.3) Ω at 25 s as a disturbance. Fig. 6 shows $\tilde{\lambda}_{P_i}$, $\tilde{\lambda}_{Q_i}$, v_i, the frequency $\omega_i/(2\pi)$, the estimated average voltage v_i^{av}, and the estimated voltage variance σ_i^2. The steady-state solution is presented in Table 1, in which the solution of the steady-state equation (4a) is also provided for reference. The steady-state values remain unchanged before and after the involvement of VAs.

2) INFLUENCE OF VA ON SYSTEM RESILIENCE UNDER DOS EDGE AND NODE ATTACKS

We assume that the DoS edge attacks shut down the channels all the time. As shown in Figs. 5(c)–5(d), the communication connections between nodes 1–4 and 2–3 are disconnected successively. The attacks happen at 20 s and 60 s and Load 1 impedance is changed from (25+j18.6) Ω to (18.7+j14.1) Ω and (15+j11.3) Ω successively 5 s after each attack. Fig. 7 shows the active and reactive power sharing for the systems with and without VA under DoS edge attack. It is seen that both systems can reach the control goals after the first attack. However, the system with the VA can still achieve the control goals after the second attack and the disturbance while the system without VA cannot.

Since DoS node attacks on real agents directly cause a partition of the original network, in the DoS node attack scenario we only show the attack targeting the VA (node 5). After the attack, Load 1 impedance is changed from (25+j18.60) Ω to (18.7+j14.1) Ω as a disturbance. Fig. 8 shows the active and reactive power sharing for the system with the VA under the DoS node attack and disturbance. It is seen that the system can still achieve the power sharing goals.

TABLE 1. The solution of the system with and without VA.

Variables	Without VA	With VA	Eq. (4)
$\tilde{\lambda}_{P_{1-4}}$	[0.412, 0.412, 0.412, 0.412]	[0.412, 0.412, 0.412, 0.412]	[0.412, 0.412, 0.412, 0.412]
$\tilde{\lambda}_{Q_{1-4}}$	[0.470, 0.470, 0.470, 0.103]	[0.470, 0.470, 0.470, 0.103]	[0.470, 0.470, 0.470, 0.103]
v_{1-4}	[0.962, 0.999, 1.015, 1.024]	[0.962, 0.999, 1.015, 1.024]	[0.962, 0.999, 1.015, 1.024]
$\omega_{1-4}/(2\pi)$	[60, 60, 60, 60]	[60, 60, 60, 60]	N/A
v^{av}_{1-4}	[1, 1, 1, 1]	[1, 1, 1, 1]	[1, 1, 1, 1]
σ^2_{1-4}	[16, 16, 16, 16]	[16, 16, 16, 16]	[16, 16, 16, 16]

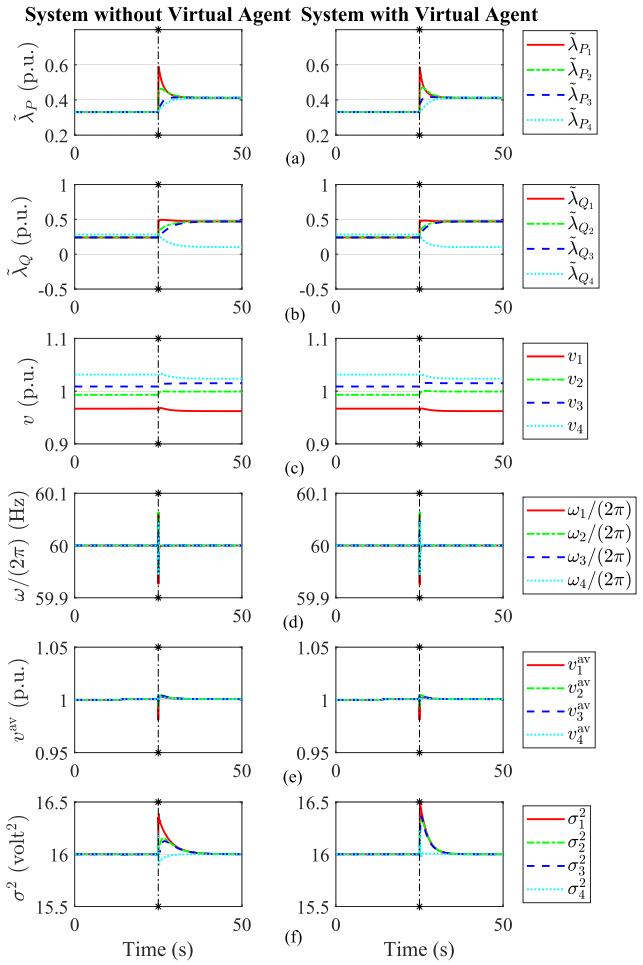


FIGURE 6. System response with and without VAs when Load 1 increases at 25 s: (a) active power sharing; (b) reactive power sharing; (c) voltage; (d) frequency; (e) estimated average voltage; (f) estimated voltage variance.

3) INFLUENCE OF VA ON SYSTEM STABILITY

Here we perform a small-signal evaluation based on Prony analysis [32] to evaluate the VAs' impact on system stability. We first test the DG's impact on the system's stability during normal operation. The first DG's normalized active power sharing data in Fig. 6 after Load 1 increase is used for Prony analysis. The mean squared error (MSE) for the Prony fitting is lower than 0.0001. The critical eigenvalues with the largest real parts and relatively low frequencies (less than 5 Hz) are listed in Table 2. The existence of VA does not significantly impact the critical eigenvalues and the system remains stable during normal operation.

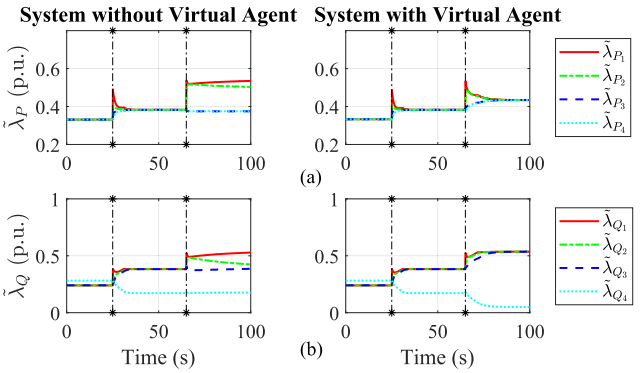


FIGURE 7. DoS edge attacks on 4-DG test system without and with VA: (a) Active power sharing; (b) reactive power sharing. Attacks happen at 20 s and 60 s respectively. After 5 s of each, Load 1 increases.

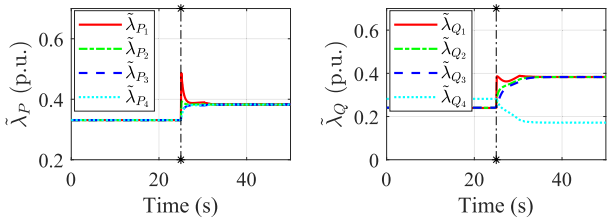


FIGURE 8. DoS node attack on VA in 4-DG Test System. The attack happens at 20 s and Load 1 increases after 5 s.

TABLE 2. Eigenvalue comparison for the first DG.

	Eigenvalue	Damping ratio
system without VA	-0.0005 $-6.7 \pm$ j20.72	100% 30.75%
system with VA	-0.0016 $-14 \pm$ j31.4	100% 40.7%

Then we test the system's stability under DoS attack and load change. The first DG's normalized active power sharing data in Fig. 7 after the second attack and load change is used for Prony analysis. The critical eigenvalues with the largest real parts and relatively low frequencies (less than 5 Hz) are listed in Table 3. With the help of VA, the system can remain stable with positive damping ratios while the system without VA loses stability with a negative damping ratio. It can be concluded that VAs can help stabilize the system during DoS attacks.

B. TESTS ON IEEE 34-BUS SYSTEM

Tests are also performed on a modified IEEE 34-bus system [23]. Fig. 9(a) shows the physical system and Fig. 9(b)

TABLE 3. Eigenvalue comparison for the first DG under DoS edge attack.

	Eigenvalue	Damping ratio
system without VA	0.0009 $-9 \pm$ j25.12	-100% 33.71%
system with VA	-0.0021 $-8.6 \pm$ j23.23	100% 34.69%

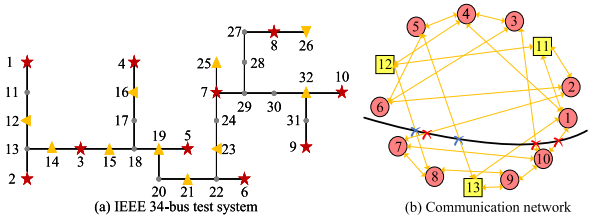


FIGURE 9. Modified IEEE 34-bus test system and its communication network: (a) physical system (stars indicate DGs and triangles indicate loads); (b) communication network (red circle nodes indicate DGs and yellow square nodes indicate VAs).

shows the communication network, assuming three VAs are added. Red circle nodes are real agents and yellow square nodes (nodes 11–13) are VAs. Fig. 9(b) is designed using the topology optimization method in [17] by selecting the total number of edges as 21. The selection of the number of VAs and edges will be discussed in Section VI-E.

Note that this system is too large for OPAL-RT 4510 real-time simulation. In order to improve the computational efficiency for this relatively large system, only the secondary level control is kept while the zero-level control and the inverter models are ignored. DG 5 is the special DG relaxed from reactive power sharing. The rated voltage v^{r}, nominal frequency ω^{r}, and voltage variance reference σ^{2*} are set as 1 (p.u.), 120π (rad/s), and 16 (volt^2) respectively. The design parameters of the proposed algorithm, α, η, γ_1, and γ_2, are chosen as 0.000005, 0.00025, 0.002, and 0.01 respectively. All nonzero elements in $\hat{\mathbf{A}}$ and $\tilde{\hat{\mathbf{A}}}$ are set as 0.15.

To simulate DoS edge attacks, for the system without VAs, we select the cut set consisting of edges 2–7, 3–10, and 1–10 as attack targets and disable them in the order above. For the system with VAs, edges 8–12 and 5–13 are selected as additional attack targets after the above cut set is removed. An attack is launched every 80 s following the preceding one and the overall load impedance is scaled down from 1.4 times the load impedance referenced in [23] to 1.3, 1.2, 1.1, 1.0, and 0.9 successively as a disturbance after each attack.

As shown in Figs. 10–11, the systems with and without VAs can reach the same steady state when the communication network for the real agents is still connected. For example, after the first load change and attack, both systems reach a consensus of 0.423 p.u. for the active power sharing and 0.345 p.u. and 0.214 p.u. for the relaxed reactive power sharing. However, the system with VAs can withstand the attacks mentioned above while the system without VAs cannot achieve proper power sharing after the disconnection of edge 1–10.

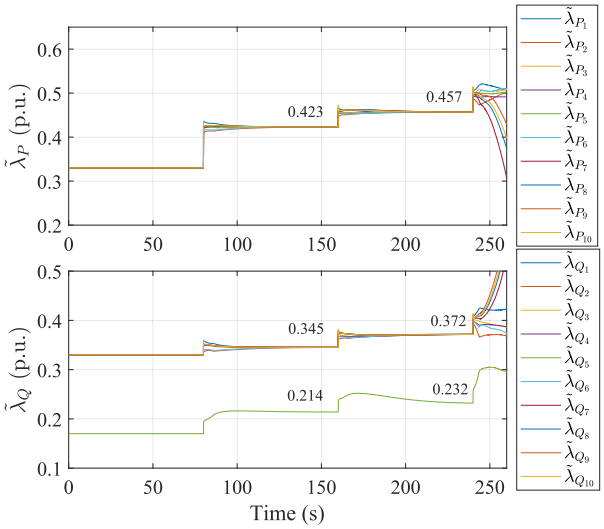


FIGURE 10. DoS edge attacks on IEEE 34-bus system without VAs.

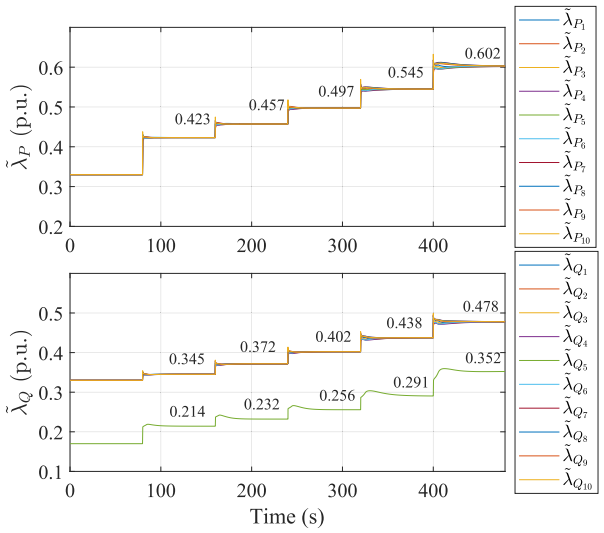


FIGURE 11. DoS edge attacks on IEEE 34-bus system with VAs.

C. THE IMPACT OF RELAXATION

To illustrate the impact of relaxation on accuracy, we produce 20 cases for each of which a load impedance change that follows a normal distribution with zero mean and a standard deviation as 10% of the initial load impedance is added to the initial load impedance. The mean squared error (MSE) of the solution from the proposed method compared with that of the steady-state equation (4a) is calculated. As shown in Fig. 12, the MSE is small, which indicates that the relaxation will not significantly impact the steady state and the proposed method can drive the system to reach the desired control goals.

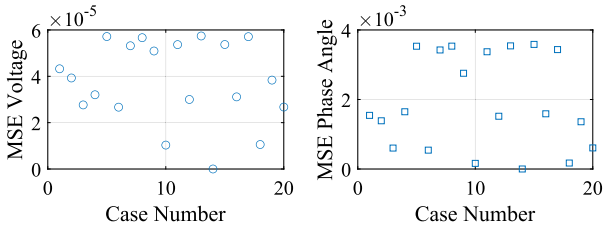


FIGURE 12. MSE of voltage and phase angle compared with the solution of (4a).

D. IMPACT OF DATA LOSS AND COMMUNICATION LATENCY WITH INCREASED SYSTEM SIZE

Here we apply data loss and latency to the test system to show how data loss and latency impact the system with different sizes. To build larger systems, we stack 1, 3, and 5 of the IEEE 34-bus system by connecting buses 12, 14, 15, 16, 19, 21, 23, and 25 from one microgrid to another to form microgrids with 34, 102, and 170 buses. The tie lines between these bus pairs are all 0.286 Ω and 0.4 mH. The N_{va} is selected as 3, 9, and 15. The adjacency matrices for the communication network are constructed by replicating the original adjacency matrix along both rows and columns 1, 3, and 5 times respectively. To evaluate the impact of network conditions, we apply 1) a global latency of 0 ms, 20 ms, and 30 ms and 2) a global packet loss of 0%, 15%, and 30% to the test system, respectively. Note that when a data loss occurs, the last available data will be used for calculation. As shown in Fig. 13, the convergence time increases with system size under varying latencies and data loss conditions. Compared with data loss, latency has a more significant impact on the convergence time as system size increases.

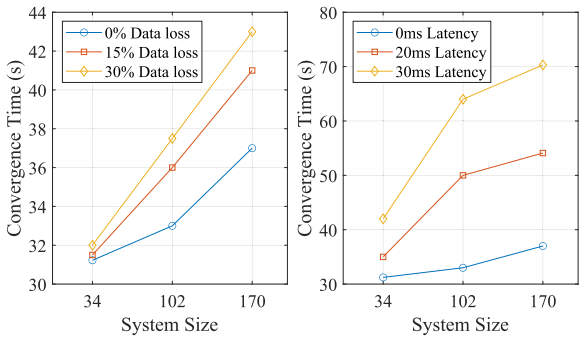


FIGURE 13. Convergence time of the proposed algorithm under data loss and latency.

E. TRADE-OFF BETWEEN COST AND RESILIENCE

DoS attacks can target either communication edges or nodes. Adding extra edges is helpful for dealing with DoS edge attacks while adding virtual nodes is helpful for dealing with DoS node attacks. From a resilience standpoint, adding a large number of VAs and their associated edges can be an effective strategy for reducing the success rate of DoS attacks. However, a large number of dummy agents and edges will result in a high cost. In this paper, we make two mild assumptions: 1) the attacker's resources are limited and small-scale DoS attacks are more likely, and 2) the network resources are constrained, limiting the total number of VAs and edges.

To illustrate the trade-off between cost and resilience, numerical experiments are performed to evaluate the edge and node connectivity of real agents in the following three steps: 1) select the number of edges, $|E|$, ranging from $N_t - 1$ to $N_t(N_t - 1)/2$ and the number of VAs, N_{va}, ranging from 1 to $2N$, and build a communication network using the method in [17]; 2) perform a random attack by removing an edge or a node until the remaining real agents are not interconnected and record the number of removed edges K_e or nodes K_n; 3) perform step 2 for 10,000 times and calculate the cumulative probability $P(k_e \leq \bar{K}_e)$ ($P(k_n \leq \bar{K}_n)$), where $\bar{K}_e$ ($\bar{K}_n$) is the pre-assigned threshold of attack resilience measured by the real agents' edge (node) connectivity.

Figs. 14(a)–14(b) show $P(k_e \leq \bar{K}_e)$ with different $|E|$ and N_{va} given the edge connectivity thresholds $\bar{K}_e = 8$ and 12 respectively. It is seen that the 'safe region' with a low probability (e.g., $P(k_e \leq \bar{K}_e) \leq 0.1$) moves to the top right corner as the threshold goes up. The most cost-effective point (the point with the least $|E|$ and N_{va}) is located at the bottom left corner of the 'safe region', which is close to $|E| = 40$ and $N_{\text{va}} = 8$. A similar conclusion can be drawn from Figs. 14(c)–14(d) that the 'safe region' is smaller when the node connectivity threshold $\bar{K}_n$ goes up and the most cost-effective point is around $|E| = 40$ and $N_{\text{va}} = 8$. This suggests that we can find an economic point satisfying a specific resilience requirement with the lowest cost.

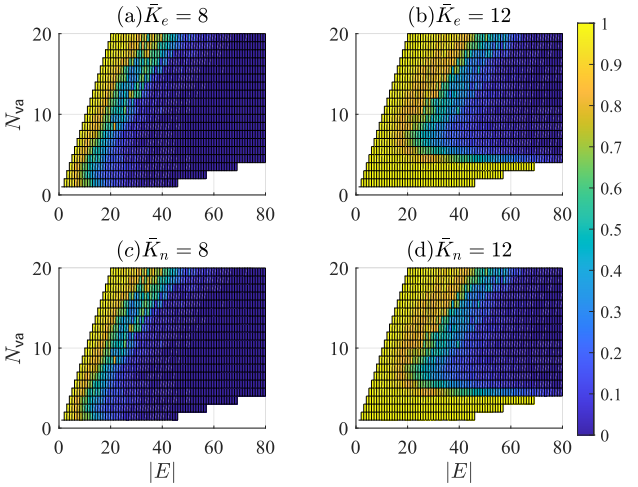


FIGURE 14. Numerical experiments for the trade-off between cost and resilience.

F. VAS' IMPACT ON NETWORK RESILIENCE

In this study, we evaluate the network's resilience under varying numbers of VAs. The network's resilience is quantified using the average number of edge or node attacks required to

disconnect the network for real agents, denoted by N_e^{av} and N_n^{av}, respectively. We examine N_{va} values of 5, 10, 15, and 20, with the number of edges $|E|$ set to $2N_t$. The communication network is constructed following the method in [17]. Attack intensity is defined as the number of edges or nodes targeted during an attack. For each intensity level, we conduct 10,000 random DoS edge or node attacks to calculate N_e^{av} and N_n^{av}. As shown in Fig. 15, both N_e^{av} and N_n^{av} increase with the increase of the number of VAs under the same attack intensity in both edge and node attack scenarios. For instance, when the attack intensity is 10, N_e^{av} is approximately 0.5 for $N_{\text{va}} = 5$, but it rises to nearly 3.5 for $N_{\text{va}} = 20$. It can be concluded that VAs can increase the network resilience against both DoS edge and node attacks.

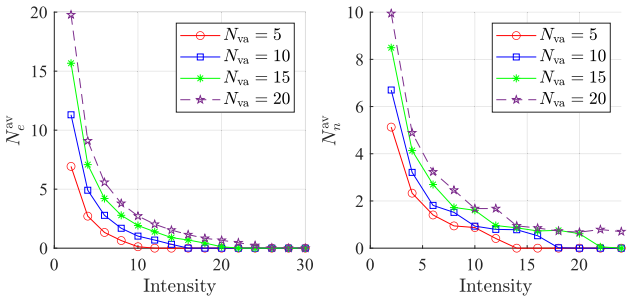


FIGURE 15. N_e^{av} and N_n^{av} under different N_{va}'s.

G. DISCUSSION ON REQUIREMENTS AND TECHNICAL HURDLES

1) Cyber-physical infrastructure requirements for VAs:

a) At the hardware layer, single-board computers equipped with Internet adapters, such as Raspberry Pi and Arduino, can serve as devices to broadcast information from VAs. Network hardware, such as routers and switches, is essential for these devices to obtain IP addresses.

b) At the software layer, a protocol is needed to implement the distributed algorithm. The protocols, such as Transmission Control Protocol/Internet Protocol (TCP/IP) and Message Queuing Telemetry Transport (MQTT), will ensure communication among the agents using a publish/subscribe model [33], which supports flexible network topologies and can largely enhance network resilience by enabling extensive involvement of VAs across the entire microgrid.

2) Regulatory and technical hurdles:

a) Potential regulatory hurdles may include data privacy, certification, and testing requirements. This may impact the widespread adoption of the VAs in reality. As regulations differ from region to region, it is still an open question for realizing these VAs in real-world applications. The employment of VAs needs to follow standards such as North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) to obtain permissions.

b) The technical hurdles may include latency and data loss for data exchange and the cyber camouflage for VAs. Based on Fig. 13, the time for convergence will increase with the system size. For a microgrid system with 170 buses, a data loss rate of less than 15% and a latency below 20 ms are still acceptable for the proposed algorithm. For the cyber camouflage of VAs, game theory could be used for VA locating and network topology switching to attract more attacks on VAs for a better defense effect.

VII. CONCLUSION

This paper proposes an attack-resilient distributed control with VAs as a pre-attack method to reduce the success rate of DoS edge and node attacks. The VAs are designed to have no impact on the system's steady state and work cooperatively with existing controls as dummy targets of DoS attacks. The corresponding distributed solving algorithm is proposed and implemented in a fully distributed manner. Simulations on two test systems validate the effectiveness of the proposed approach in improving the attack resilience of the distributed microgrid control against DoS edge and node attacks. Our future work will be focused on determining the optimal communication topology with VAs and designing online switching strategies for further cybersecurity enhancement.

REFERENCES

[1] Z. Wang, W. Wu, and B. Zhang, "A distributed quasi-Newton method for droop-free primary frequency control in autonomous microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 2214–2223, May 2018.

[2] Z. Cheng, J. Duan, and M.-Y. Chow, "To centralize or to distribute: That is the question: A comparison of advanced microgrid management systems," *IEEE Ind. Electron. Mag.*, vol. 12, no. 1, pp. 6–24, Mar. 2018.

[3] V. Nasirian, Q. Shafiee, J. M. Guerrero, F. L. Lewis, and A. Davoudi, "Droop-free distributed control for AC microgrids," *IEEE Trans. Power Electron.*, vol. 31, no. 2, pp. 1600–1617, Feb. 2016.

[4] Q. Shafiee, V. Nasirian, J. C. Vasquez, J. M. Guerrero, and A. Davoudi, "A multi-functional fully distributed control framework for AC microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3247–3258, Jul. 2018.

[5] V. Nasirian, S. Moayedi, A. Davoudi, and F. L. Lewis, "Distributed cooperative control of DC microgrids," *IEEE Trans. Power Electron.*, vol. 30, no. 4, pp. 2288–2303, Apr. 2015.

[6] S. M. Mohiuddin and J. Qi, "Droop-free distributed control for AC microgrids with precisely regulated voltage variance and admissible voltage profile guarantees," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 1956–1967, May 2020.

[7] N. M. Dehkordi, N. Sadati, and M. Hamzeh, "Distributed robust finite-time secondary voltage and frequency control of islanded microgrids," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3648–3659, Sep. 2017.

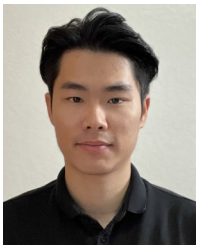
[8] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab, and A. Abusorrah, "Distributed control and communication strategies in networked microgrids," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2586–2633, 4th Quart., 2020.

[9] L. Ding, Q.-L. Han, B. Ning, and D. Yue, "Distributed resilient finite-time secondary control for heterogeneous battery energy storage systems under denial-of-service attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4909–4919, Jul. 2020.

[10] W. Yao, Y. Wang, Y. Xu, and C. Deng, "Cyber-resilient control of an islanded microgrid under latency attacks and random DoS attacks," *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5858–5869, Apr. 2023.

[11] B. Zhang, C. Dou, D. Yue, J. H. Park, and Z. Zhang, "Attack-defense evolutionary game strategy for uploading channel in consensus-based secondary control of islanded microgrid considering DoS attack," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 2, pp. 821–834, Feb. 2022.

[12] S. Liu, P. Siano, and X. Wang, "Intrusion-detector-dependent frequency regulation for microgrids under denial-of-service attacks," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2593–2596, Jun. 2020.
[13] J. Xiao, L. Wang, Z. Qin, and P. Bauer, "A resilience enhanced secondary control for AC micro-grids," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 810–820, Jan. 2024.
[14] M. Jamali, H. R. Baghaee, M. S. Sadabadi, G. B. Gharehpetian, and A. Anvari-Moghaddam, "Distributed cooperative event-triggered control of cyber-physical AC microgrids subject to denial-of-service attacks," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 4467–4478, Mar. 2023.
[15] C. Deng, F. Guo, C. Wen, D. Yue, and Y. Wang, "Distributed resilient secondary control for DC microgrids against heterogeneous communication delays and DoS attacks," *IEEE Trans. Ind. Electron.*, vol. 69, no. 11, pp. 11560–11568, Nov. 2022.
[16] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, A. Abusorrah, L. Che, and X. Liu, "Cross-layer distributed control strategy for cyber resilient microgrids," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 3705–3717, Sep. 2021.
[17] L. Sheng, G. Lou, W. Gu, S. Lu, S. Ding, and Z. Ye, "Optimal communication network design of microgrids considering cyber-attacks and time-delays," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3774–3785, Sep. 2022.
[18] J. Han, W. Lyu, H. Song, Y. Qu, Z. Wu, X. Zhang, Y. Li, and Z. Chen, "Optimization of communication network for distributed control of wind farm equipped with energy storages," *IEEE Trans. Sustain. Energy*, vol. 14, no. 4, pp. 1933–1949, Apr. 2023.
[19] A. H. Anwar, C. A. Kamhoua, N. O. Leslie, and C. Kiekintveld, "Honeypot allocation for cyber deception under uncertainty," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 3, pp. 3438–3452, Sep. 2022.
[20] Y. Sun, Z. Tian, M. Li, S. Su, X. Du, and M. Guizani, "Honeypot identification in softwarized industrial cyber–physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5542–5551, Aug. 2021.
[21] W. Tian, X. Ji, W. Liu, G. Liu, J. Zhai, Y. Dai, and S. Huang, "Prospect theoretic study of honeypot defense against advanced persistent threats in power grid," *IEEE Access*, vol. 8, pp. 64075–64085, 2020.
[22] J. D. Glover, M. S. Sarma, T. J. Overbye, and B. Adam, *Power System Analysis & Design*. Boston, MA, USA: Cengage Learning, 2022.
[23] S. M. Mohiuddin and J. Qi, "Optimal distributed control of AC microgrids with coordinated voltage regulation and reactive power sharing," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 1789–1800, May 2022.
[24] G. Qu and N. Li, "Optimal distributed feedback voltage control under limited reactive power," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 315–331, Jan. 2020.
[25] Z. Wang, F. Liu, Y. Chen, S. H. Low, and S. Mei, "Unified distributed control of stand-alone DC microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 1013–1024, Jan. 2019.
[26] S. M. Mohiuddin, J. Qi, S. Fung, Y. Huang, and Y. Tang, "Deep learning based multi-label attack detection for distributed control of AC microgrids," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2021, pp. 233–238.
[27] J. Yang, N. Zhang, C. Kang, and Q. Xia, "A state-independent linear power flow model with accurate estimation of voltage magnitude," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3607–3617, Sep. 2017.
[28] S. Mou, J. Liu, and A. S. Morse, "A distributed algorithm for solving a linear algebraic equation," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2863–2878, Nov. 2015.
[29] P. Yi, J. Lei, J. Chen, Y. Hong, and G. Shi, "Distributed linear equations over random networks," *IEEE Trans. Autom. Control*, vol. 68, no. 4, pp. 2607–2614, Apr. 2023.
[30] H. Xu, A. D. Domínguez-García, V. V. Veeravalli, and P. W. Sauer, "Data-driven voltage regulation in radial power distribution systems," *IEEE Trans. Power Syst.*, vol. 35, no. 3, pp. 2133–2143, May 2020.
[31] Y. Nesterov, *Introductory Lectures on Convex Optimization: A Basic Course*, vol. 87. Cham, Switzerland: Springer, 2003.
[32] J. F. Hauer, "Application of Prony analysis to the determination of modal content and equivalent models for measured power system response," *IEEE Trans. Power Syst.*, vol. 6, no. 3, pp. 1062–1068, Aug. 1991.
[33] S. A. Alavi, K. Mehran, Y. Hao, A. Rahimian, H. Mirsaeedi, and V. Vahidinasab, "A distributed event-triggered control strategy for DC microgrids based on publish-subscribe model over industrial wireless sensor networks," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4323–4337, Jul. 2019.



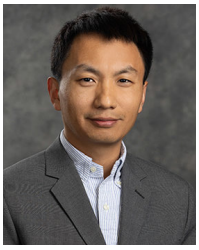
JUN ZHANG (Graduate Student Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Guangxi University, Nanning, China, in 2017 and 2020, respectively. He is currently pursuing the Ph.D. degree in electrical engineering with the McComish Department of Electrical Engineering and Computer Science, South Dakota State University (SDSU), Brookings, SD, USA.

His research interests include microgrid modeling and control, steady-state analysis, microgrid cybersecurity, stability analysis, distributed optimization, and hardware-in-the-loop (HIL) implementation.

SHEIK M. MOHIUDDIN (Member, IEEE) received the B.Sc. degree in electrical and electronic engineering from the Rajshahi University of Engineering and Technology, Bangladesh, in 2013, the master's degree in electrical engineering from the University of New South Wales (UNSW), Australia, in 2017, and the Ph.D. degree in electrical engineering from the Stevens Institute of Technology, in 2021.

He is currently a Senior Power System Research Engineer with the Pacific Northwest National Laboratory. His research interests include fault-ride through control design for inverters and grid-enhancing technologies, control design for solid-state transformers and high-voltage multi-level converters, and distributed control for ac/dc microgrids.

Dr. Mohiuddin received the Best Paper Award at the 2021 IEEE PES ISGT Asia Conference.



JUNJIAN QI (Senior Member, IEEE) received the B.E. degree in electrical engineering from Shandong University, Jinan, China, in 2008, and the Ph.D. degree in electrical engineering from Tsinghua University, Beijing, China, in 2013.

He was an Assistant Professor with the Department of Electrical and Computer Engineering, University of Central Florida, Orlando, FL, USA, from 2017 to 2020, and an Assistant Professor with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, USA, from 2020 to 2023. He is currently the Harold C. Hohbach Endowed Assistant Professor with the McComish Department of Electrical Engineering and Computer Science, South Dakota State University, Brookings, SD, USA. His research interests include cascading blackouts, microgrid control, cyber-physical systems, and synchrophasors.

Dr. Qi was a recipient of the NSF CAREER Award, in 2020, the 2021 Best Paper Award from IEEE TRANSACTIONS ON POWER SYSTEMS, the 2022 Best Paper Award from *Journal of Modern Power Systems and Clean Energy*, and the Best Paper Awards from IEEE Power and Energy Society (PES) General Meetings and IEEE PES ISGT Asia. He is an Associate Editor of IEEE TRANSACTIONS ON POWER SYSTEMS and IEEE POWER ENGINEERING LETTERS.