Privacy-Preserving-based Distributed State-Decomposition Convex Optimization for Multi-DESS Operations

Yajie Jiang, *Member*, *IEEE*, Noven Lee, Yici Wang, Xiangrong Zhang, Eddy Y. S. Foo, *Member*, *IEEE*, and Yun Yang, *Senior Member*, *IEEE*

***Abstract*—The distributed convex optimization strategies are widely used for voltage regulation and current distribution among distributed energy storage systems (DESSs). Meanwhile, consensus-based secondary control is commonly employed but risks leaking initial state information when exchanged explicitly. To address this issue, a distributed state-decomposition convex optimization (DSDCO) approach is proposed for current distribution in DC networks, ensuring the protection of DESSs' initial states. In DSDCO, a state-decomposition strategy is implemented, where the state variable of each DESS is divided into two sub-state variables with random initial values. One sub-variable is dedicated to external consensus control, safeguarding the node's true initial state, while the other manages internal dynamics to achieve global consensus. The theoretical analysis confirms that DSDCO can achieve state consensus in finite time and effectively maintain privacy. Subsequently, the first state variable that incorporates consensus control is used for current allocation and loss optimization. Finally, the privacy-preserving effectiveness of DSDCO is validated through both simulation and experimental case studies.**

***Index Terms*—Privacy-preserving, distributed energy storage systems (DESSs), state decomposition, average consensus.**

NOMENCLATURE

I_i	output current of DESS$_i$
I_{tol}	total load current
N_i	current allocation coefficient of DESS$_i$
V_i	output voltage of DESS$_i$
R_i	wire resistance of DESS$_i$
P_{lossi}^{conv}	power conversion loss of DESS$_i$
P_{lossi}^{line}	line loss of DESS$_i$
n	total number of DESSs
α_i, β_i, and γ_i	coefficients of loss function
$f_i(N_i)$	loss of DESS$_i$
$f(N_i)$	loss of all DESSs
$g(N_i)$	current coefficient equation
$\frac{\partial f(N_i)}{\partial N_i}$	first-order partial derivative for $f(N_i)$
$\frac{\partial^2 f(N_i)}{\partial N_i^2}$	second-order partial derivative for $f(N_i)$
P_{mini} and P_{maxi}	lower range and upper range of power
V_{mini} and V_{maxi}	lower and upper limits of voltage
k	sampling instant
n_i	adjacent nodes of DESSs
f_j'	the gradient of DESS$_j$
W_{ii}	self-weight of the DESS$_i$
W_{ij}	mutual-weight between DESS$_i$ and DESS$_j$
x_i, x_j, x_m and x_p	states of DESS$_i$, DESS$_j$, DESS$_m$ and DESS$_p$
V_{refi}	reference value of V_i
V_{nom}	nominal value of V_i
$R_{\text{d}i}$	virtual resistance of DESS$_i$
δ_i	adaptive voltage
ε	edge-weight of communication protocol
z_i	inferred state-variable of DESS$_i$
x_i^{α} and x_i^{β}	sub-states of DESS$_i$
x_j^{α} and x_j^{β}	sub-states of DESS$_j$
x_m^{α} and x_m^{β}	sub-states of DESS$_m$
x_q^{α} and x_q^{β}	sub-states of DESS$_q$
$x_i^{\alpha}(0)$, $x_i^{\beta}(0)$, and $x_i(0)$	the initial values of x_i^{α}, x_i^{β}, and x_i
$x_j^{\alpha}(0)$, $x_j^{\beta}(0)$, and $x_j(0)$	the initial values of x_j^{α}, x_j^{β}, and x_j
$x_m^{\alpha}(0)$, $x_m^{\beta}(0)$, and $x_m(0)$	the initial values of x_m^{α}, x_m^{β}, and x_m
$x_q^{\alpha}(0)$, $x_q^{\beta}(0)$, and $x_q(0)$	the initial values of x_q^{α}, x_q^{β}, and x_q
a_{ij}, a_{ip}, a_{ji}, a_{jp}, a_{jm}, and a_{pq}	elements of adjacency matrix
η	a predefined scalar
$\bar{x}_j$, $\bar{x}_m$ and $\bar{x}_p$	inferred states of DESS$_j$, DESS$_m$ and DESS$_p$
$I_i(k)$ and $\bar{I}_i(k)$	information accessible to DESS$_j$
$\bar{x}_i^{\alpha}$ and $\bar{x}_i^{\beta}$	inferred sub-states of DESS$_i$
$\bar{x}_j^{\alpha}$ and $\bar{x}_j^{\beta}$	inferred sub-states of DESS$_j$
$\bar{x}_m^{\alpha}$ and $\bar{x}_m^{\beta}$	inferred sub-states of DESS$_m$
$\bar{x}_q^{\alpha}$ and $\bar{x}_q^{\beta}$	inferred sub-states of DESS$_q$
$a_{i,\alpha\beta}$, $a_{j,\alpha\beta}$, $a_{m,\alpha\beta}$, and $a_{q,\alpha\beta}$	coefficient between sub-states
$\bar{a}_{j,\alpha\beta}$, $\bar{a}_{j,\alpha\beta}$, $\bar{a}_{m,\alpha\beta}$, and $\bar{a}_{q,\alpha\beta}$	inferred coefficients
$\bar{a}_{jm}$, $\bar{a}_{pq}$, and $\bar{a}_{ip}(k)$	inferred elements of adjacency matrix

I. INTRODUCTION

DC electric networks, characterized by high efficiency and a simple structure, are garnering significant attention as effective systems for integrating various renewable energy sources [1] - [3]. However, due to the low inertia, load variations, off-grid switching, and uncertain output power of renewable energy sources (RESs), voltage fluctuations can occur. To enhance system stability, real-time allocation of currents and powers among distributed energy storage systems (DESSs) is necessary [4]. Distributed optimization control has been proposed to achieve voltage regulation and optimize power losses by integrating power electronics and information technology. Nevertheless, the reliance on data exchange makes distributed control susceptible to malicious network intrusions, thereby highlighting data security as another critical issue.

Recently, the consensus-based control is widely applied for secondary cooperative operation, due to its benefits of strong-

scalability, and high-flexibility. By modelling DC electric network as a multi-agent system, the consensus control can be executed by exchanging the state-variables among DESSs [5]. In [6], consensus for voltages and currents is achieved within a specified time by adopting a sign function-based composite controller. A strategy based on a multi-agent consensus algorithm is designed to achieve state balancing by simply exchanging data between adjacent DESSs [7]. In [8], an adaptive anti-attack consensus control is developed for DC microgrids to address unknown unbounded attacks on the control input channel. Recently, considering the damage of data attacks on the secondary control of microgrids, some methods have been proposed to alleviate the imbalance in power and current distribution [9], [10]. Through direct information exchanging between nodes, the consensus protocol combined with secondary controllers is generally adopted for voltage and current regulations.

With the widespread application of RESs, data privacy protection in smart grids has become a research hotspot. This provides the necessary conditions for the reliable and secure operation of smart grids and the orderly regulation of electricity markets. Relying on direct exchange of information among nodes, the privacy protection of each node in the data exchange protocol, such as the initial state values of DESSs, has not been taken into account. In details, two potential risks can be triggered during direct information-exchanging. Firstly, each individual containing private information does not wish to disclose its privacy to other individuals in order to prevent their decision-making process from being affected [11]. For example, when a group uses consensus protocol to seek common opinions, the individuals wish to keep everyone's opinions confidential. Additionally, during bidding for electricity prices, multiple power generators aim to reach agreements on costs while maintaining confidentiality of their respective bidding prices, which is sensitive in the context of bidding for energy sales rights [12]. Secondly, the direct data transmission through communication increases the possibility of data being stolen in the communication link [13]. If privacy information, such as voltage, power generation/consumption, and cost, is obtained by malicious eavesdroppers, it may lead to safety risks and economic losses [14]. With the increasing number of attack events, improving communication protocols to protect data privacy in DC microgrids has become an urgent demand [15].

To protect the privacy of nodes' initial states during the dynamic consensus iteration process, algorithms have been applied to network systems, such as microgrids [14]. Based on specific encryption processes, these methods can be mainly classified into two categories: differential privacy algorithms [16]-[19] and cryptographic techniques [20]-[24]. Differential privacy algorithms mask the true values of state variables by adding predefined noise to the transmitted states [16], [17]. In [18], a differential privacy scheme is proposed in reference, which obscures sensitive information by injecting independent noise sequences. However, this scheme has a recognized weakness in terms of accuracy, as there is a trade-off between privacy level and convergence precision. This differential privacy algorithm poses obstacles to achieving state consensus. [19] introduces the quantum divergence to mask sensitive power information, but the developed scheme fails to achieve fast convergence due to the costs associated with privacy protection. As for cryptographic techniques [20]-[22], the exchanged states among nodes can be encrypted to preserve privacy. It develops a homomorphic encryption-based protocol that enables confidential communication between neighboring nodes by fully utilizing the Pailler encryption system and a random weighting mechanism [23]. Achieving average consensus is impractical for nodes with limited resources due to significant computation and the high demands of the encryption algorithm. Therefore, an algorithm is needed to achieve accurate consensus while safeguarding personal privacy [24].

The distributed algorithms discussed in this context operate under two fundamental principles: first, nodes keep their initial private information confidential from all other nodes in the network; second, each node has knowledge solely of its local connectivity, which includes only its immediate neighbors. Despite these constraints, the algorithms implemented by the nodes are designed to address the overarching system problem while relying on minimal understanding of the objective function and restricted local communication. Considering the above issues, some literature proposes a leader-follower consensus algorithm based on the state decomposition mechanism [25]. However, due to the limitations of the leader-follower protocols, this method cannot be applied to general microgrid topologies and protocols [26], [27]. Based on the aforementioned requirements, this article proposes a more general consistency control strategy for node decomposition, eliminating the need for a leader node while maintaining low computational complexity [28].

To develop the privacy-preserving algorithm for the general DC microgrids, the average consensus-based secondary control is introduced in this work as the preliminary. Then, the risk of each node exposing its initial state is analyzed. It is found that the initial state-variables of DESSs can be extracted by adversaries using some inference algorithms. Then, regarding the optimization of losses, a distributed state-decomposition convex optimization (DSDCO) is proposed to achieve average consensus while protecting the privacy of each DESS. According to the state decomposition strategy, the state-variables used for exchanging are decomposed into two sub-states, each playing different roles in the new consensus protocol. One of them will be sent to adjacent nodes for inter-node interactions. Thereby, it is the only state that can be acquired by the neighboring nodes. For the second sub-state, it is used for interacting with the first sub-state, which is in-visible to the neighboring nodes. Moreover, the initial values of two sub-states are randomly selected while satisfy an equality constraint. Theoretical analysis and experimental evidence have shown that even if the adversaries know the communication topology and protocol, the proposed DSDCO can still protect the privacy of the initial state values. This paper cleverly combines the general consensus protocol with state decomposition and convex optimization, proposing the DSDCO, which simultaneously achieves privacy protection, loss optimization, and stable operation of the DC electric network. The universal consensus protocol proposed in this article does not require a leader node, allowing for adaptive adjustment of the current of each DESS under various operating conditions. The major contributions include that

1) By treating multiple DESSs as a network, a distributed

convex optimization algorithm combined with a consensus protocol is applied for loss minimization.

2) The state-decomposition-based DSDCO is presented to protect the privacy of nodes in DESS-based DC networks.

II. Privacy-Preserving Average Consensus

A. DC Electric Network and Loss Modelling

As shown in Fig. 1(a), this work considers a DC system composed of a set of DESSs, along with RESs such as wind energy generation and photovoltaic systems (seen as un-dispatchable units). Power electronic interfaces facilitate the convenient use of various energy types in the DC system. The load (including chargers and data center servers, among others) can be modeled as a constant power/current load or a constant resistance load, as shown in Fig. 1 (b). In practical applications, DESSs, such as batteries play essential roles in stabilizing voltage and balancing power. By leveraging communication and sensor technology, the DC network transforms into a cyber-physical system. The data-exchanging topology of DESSs within the DC network can generally be represented as a graph with n nodes, where DESSs represent nodes and communication links represent edges. The coefficient a_{ij} signifies the connectivity between DESS$_i$ and DESS$_j$. Each node can exchange its state information—such as voltage, output current, and output power—with its neighbors.

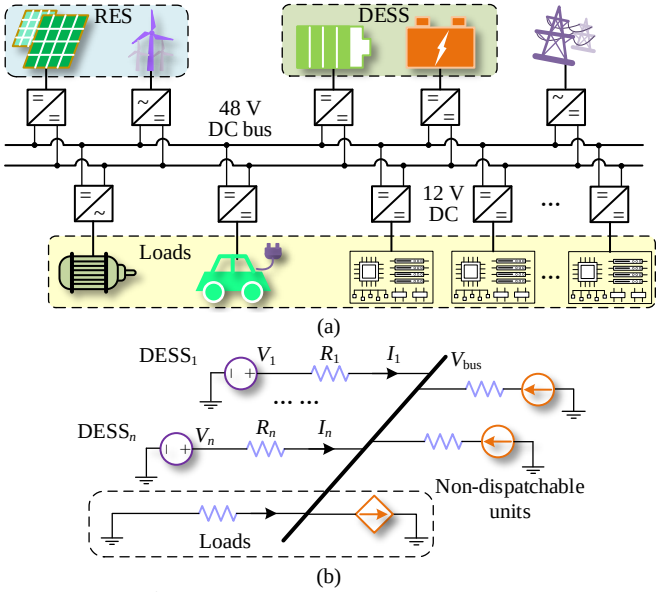


Fig. 1. (a) a simplified DC system, and (b) the equivalent circuit diagram.

In Fig. 1, V_i is the voltage of DESS$_i$, R_i is the wire resistance, I_i is the current of DESS$_i$, and I_{tol} is the total load current. The loss power of one DESS can be generated in power conversion stage and the transmission line [28], as described by

$$f_i(N_i) = P_{lossi}^{conv} + P_{lossi}^{line} = (\alpha_i + R_i)(N_i I_{\text{tol}})^2 + \beta_i |N_i I_{\text{tol}}| + \gamma_i \quad (1)$$

where α_i, β_i, and γ_i are positive coefficients. After summarizing, the loss function is further given as function of N_i

$$f(N_i) = \sum_{i=1}^{n} [(\alpha_i + R_i)(N_i I_{\text{tol}})^2 + \beta_i N_i |I_{\text{tol}}| + \gamma_i] \quad (2)$$

Considering the supply-demand balancing, the equality constraint is added as

$$g(N_i) = \sum_{i=1}^{n} N_i - 1 = 0 \quad (3)$$

By taking the partial derivatives of (2), it gives

$$\frac{\partial f(N_i)}{\partial N_i} = 2N_i(\alpha_i + R_i)(I_{\text{tol}})^2 + \beta_i |I_{\text{tol}}| \quad (4.1)$$

$$\frac{\partial^2 f(N_i)}{\partial N_i^2} = 2(\alpha_i + R_i)(I_{\text{tol}})^2 \quad (4.2)$$

In (4), $(I_{\text{tol}})^2 \geq 0$, $\alpha_i > 0$, and $R_i > 0$. It appears that the first-order partial derivative is differentiable, and the Hessian is positive semidefinite for all N_i. This indicates that the power loss model in (2) is strictly convex [4], [29].

Take the consideration of power and voltage limits, the loss optimization for multi-DESSs is given as follows

$$\begin{aligned} \min \quad & J = f(N_i) \\ \text{s.t.} \quad & g(N_i) = 0 \\ & P_{\text{min}i} \leq P_i \leq P_{\text{max}i}, V_{\text{min}i} \leq V_i \leq V_{\text{max}i} \end{aligned} \quad (5)$$

where $P_{\text{min}i}$ and $P_{\text{max}i}$ are the lower range and upper range of the generation capacity, $V_{\text{min}i}$ and $V_{\text{max}i}$ are the lower range and upper range of the voltage.

To further analyze the convexity of the proposed loss function, the surfaces of a four DESSs-based DC microgrid are plotted in Fig. 2. By using the parameters of the DC system and DESSs in the Section IV, the value of one current coefficient should be fixed (i.e., 0.05). Based on the equality-constraint (3), the loss functions (N_1 = 0.05 for (a), N_2 = 0.05 for (b), N_3 = 0.05 for (c) and N_4 = 0.05 for (d)) are drawn as 3D convex surfaces, as show in Fig. 2. All surfaces are smooth with a unique minimum point, confirming the convexity of the proposed loss function. Together with (4), it supports the theoretical foundation for the DSDCO approach we will present later to solve this convex optimization problem.

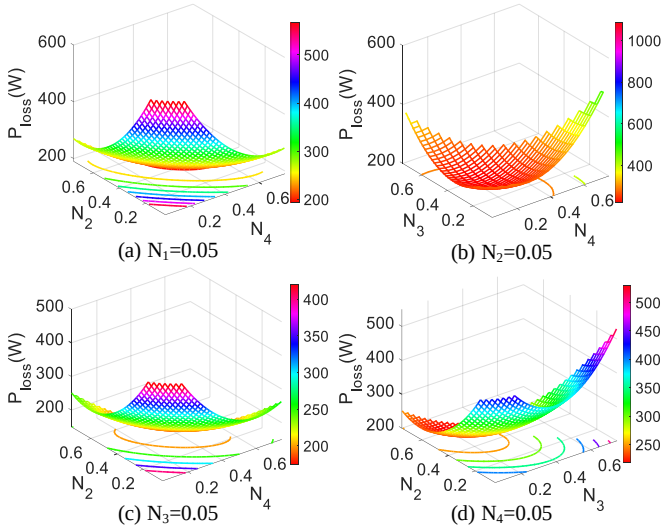


Fig. 2. Convex surfaces of loss function for analysis.

B. Distribution Optimization and Average Consensus Control

Generally, the derivative of individual function (incremental cost) of node i combined with first-order consensus algorithm can be used to solve the problem.

$$N_i(k+1) = N_i(k) - W_{ii} f_i'[N_i(k)] - \sum_{j \in n_i} W_{ij} f_j'[N_j(k)] \quad (6)$$

where k is the sampling instant, n_i is the set of neighboring DESSs, $f_i'[N_i(k)]$ and $f_j'[N_j(k)]$ are the gradients of DESS$_i$ and DESS$_j$, respectively. W_{ii} is a constant self-weight of the DESS$_i$, and W_{ij} are mutual-weights (i.e., W_{ij}=W_{ji}).

In addition, consensus algorithm and secondary controllers are commonly used to allocate output currents between DESS. This approach employs distributed frameworks in which each DESS leverages local state information along with data from its neighbors to meet operational objectives. To apply consensus protocol, one state-variable is defined as

$$x_i = I_i/N_i \tag{7}$$

The iteration equation of consensus algorithm in discrete time is described as

$$x_i(k+1) = x_i(k) + \varepsilon * \sum_{j\in n_i}^{n} a^{ij}\left[x_j(k) - x_i(k)\right] \tag{8}$$

where ε is one edge-weight, x_j is a state-variable of DESS$_j$, and n_i represents adjacent nodes of DESS$_i$. It has been proved that the consensus of state-variables of DESSs can be reached [30]:

$$\lim_{k\to\infty}\left\|x_i(k) - x_j(k)\right\| = 0 \tag{9}$$

In short-distance DC network [4], droop control is widely used in the primary layer. Then, the secondary controller for current allocation is given as

$$V_{\text{refi}} = V_{\text{nom}} - R_{\text{di}}I_i + \delta_i,\ \dot{\delta}_i = x_i(k) - I_i/N_i \tag{10}$$

where R_{di} is the virtual resistance of DESS$_i$, V_{refi} is the reference voltage, V_{nom} is the nominal value of system voltage, and δ_i is the adaptive voltage term. All DESS output currents will be distributed according to the current distribution coefficient obtained through distributed convex optimization.

III. Distributed State Decomposition-based Consensus Control

A. Initial Sate Disclosure During Consensus Process

Despite the discussed consensus method (7) being widely used for secondary regulation in DC electric networks, it has a vulnerability: the initial state variables of nodes can be easily deduced through information exchange among DESSs. Without preventive measures, adversaries can exploit this vulnerability to obtain the private information of distributed nodes. This work considers two main types of adversaries:

1) *An honest-but-curious adversary:* This type of adversary adheres to the consensus protocol and follows updating procedures correctly but attempts to deduce the state information of other nodes using data obtained from itself and its neighboring nodes.
2) *An eavesdropper:* This refers to an external attacker who knows the topology of data exchange, can eavesdrop on communication links, and access exchanged messages.

In this paper, legitimate nodes are defined as adjacent nodes that faithfully follow the scheduling algorithm without attempting to infer the states of other nodes. Thereby, all agents can be categorized into legitimate nodes and honest but curious nodes. References [23] and [24] have demonstrated that when adversaries possess knowledge of the communication topology, consensus protocol, and weight coefficients, they can use specific methods to obtain nodes' initial state variables. By using protocol (8) as an example, the initial state variables of DESS$_i$ can be acquired by the adversaries. It is recognized that following inference algorithm can be adopted:

$$z_i(k) = \frac{x_i(k+1) - \varepsilon * \sum_{j\in n_i} a_{ij}(k)x_j(k)}{1 - \varepsilon * \sum_{j\in n_i} a_{ij}(k)} \tag{11}$$

where $z_i(k)$ is the inferred state-variable of DESS$_i$ at *k-th* iteration. If the adversary is a malicious eavesdropper, the acquired information can be used to harm the DESS's interest.

B. Distributed State-Decomposition Consensus Protocol

This general communication topology of the DC system is depicted in Fig. 3(a). Inspired by the state-decomposition algorithm in [25], a privacy-preserving-based consensus protocol is proposed to achieve average consensus (i.e., current allocation) while safeguarding the privacy of DESSs' initial states. Accordingly, the state-variable x_i of DESS$_i$ is decomposed into two sub-states, x_i^{α} and x_i^{β}, each assigned random initial values. These initial values satisfy a specified equality constraint:

$$x_i^{\alpha}(0) + x_i^{\beta}(0) = 2 * x_i(0) \tag{12}$$

where $x_i^{\alpha}(0)$, $x_i^{\beta}(0)$, and $x_i(0)$ are the initial values of x_i^{α}, x_i^{β}, and x_i respectively.

Based on the conventional consensus protocol and state-decomposition mechanism, an improved topology depicted in Fig. 3(b) has been devised. In this topology, the two sub-state-variables, x_i^{α} and x_i^{β}, serve distinct roles within the consensus protocol. Specifically, x_i^{α} is transmitted to neighboring nodes of node *i* for inter-node interactions, making it the sole state accessible to these neighboring nodes. On the other hand, x_i^{β} remains invisible to neighboring nodes and is utilized solely for interaction with x_i^{α}. This internal interaction between x_i^{α} and x_i^{β} influences the evolution of x_i^{α} and is instrumental in achieving consensus on the final state.

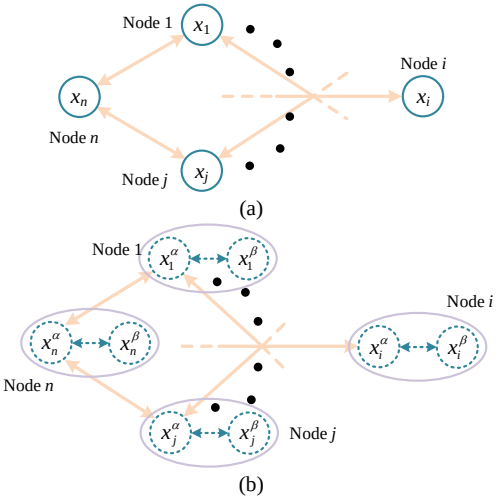


Fig. 3. Communication graphs (a) original topology. (b) topology after state-decomposition.

For DSDCO, a novel state-variable-interacting protocol is proposed as

$$x_i^{\alpha}(k+1) = x_i^{\alpha}(k) + \varepsilon * \sum_{j\in n_i}^{n} a_{ij}(k)\left[x_j^{\alpha}(k) - x_i^{\alpha}(k)\right] + \varepsilon * a_{i,\alpha\beta}(k) * \left[x_i^{\beta}(k) - x_i^{\alpha}(k)\right] \tag{13.1}$$

$$x_i^{\beta}(k+1) = x_i^{\beta}(k) + \varepsilon * a_{i,\alpha\beta}(k) * \left[x_i^{\alpha}(k) - x_i^{\beta}(k)\right] \tag{13.2}$$

where $a_{i,\alpha\beta}$ is the mutual coefficient between x_i^{α} and x_i^{β}. In (13), with a random initial value, x_i^{β} remains invisible to the outside while influencing the evolution of x_i^{α}. Meanwhile, x_i^{α} functions for both external (with x_j^{α}) and internal interactions (with x_i^{β}).

In addition to the novel state-variable-interacting protocol and state-decomposition, coefficient-selection rules are designed for privacy preservation.

1) For k = 1, 2, ..., all $a_{i,\alpha\beta}(k)$ satisfy $\eta \le a_{i,\alpha\beta}(k) < 1$, and all non-zero $a_{ij}(k)$ satisfy $\eta \le a_{ij}(k) < 1$, where $0 < \eta < 1$ is a scalar.
2) At initialization, i.e., k = 0, the coupling coefficients $a_{i,\alpha\beta}(0)$ and inter-node coefficients $a_{ij}(0)$ can be arbitrarily selected under the constraint of $a_{ij}(0) = a_{ji}(0)$;

Based on the proposed DSDCO, x_i^{α} is adopted for current allocation, as given by

$$\dot{\delta}_i = x_i^{\alpha}(k) - I_i/N_{Ii} \tag{14}$$

Fig. 4 shows the overall control block diagram of the secondary current control for DC network. With the assistance

of DSDCO, each individual DESS utilizes state information, such as output current, to generate control signals. Integration regulators then adaptively produce voltage terms. These terms, combined with droop controllers, adjust voltage references for lower loops. This enables proportional output current allocation in DC networks. Notably, internal sub-node interactions and secondary control occur locally.

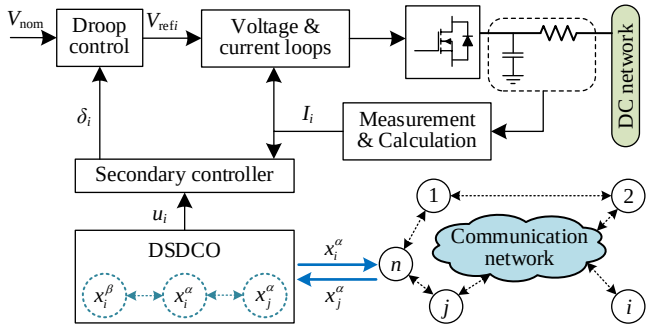


Fig. 4. Average consensus-based cooperative control for DC system.

C. Convergence Analysis of State Consensus

The analysis of consensus convergence of sub-states demonstrates that DSDCO ensures privacy preservation even in the presence of adversaries. Therefore, the initial states of each node are kept confidential without the need to increase communication overhead or alter the system structure.

Theorem 1: Under the DSDCO and weight-selection rules, all sub-states in (13) will converge to average value, as given by

$$\lim_{k\to\infty} x_i^\alpha(k) = \lim_{k\to\infty} x_i^\beta(k) = \frac{1}{n}\sum_{i=1}^{n} x_i(0) \tag{15}$$

Proof: Under the weight selection rules of $a_{ij}(k) = a_{ji}(k)$ and $a_{i,\alpha\beta}(k)$, it can be easily concluded the sum of all sub-states (after decomposition) is time-invariant. Thereby, during the consensus-iteration period, even the weights can be arbitrarily selected, it always has

$$\frac{1}{2n}\sum_{i=1}^{n}\left[x_i^\alpha(0) + x_i^\beta(0)\right] = \frac{1}{2n}\sum_{i=1}^{n}\left[x_i^\alpha(1) + x_i^\beta(1)\right] \tag{16}$$

Since all coupling coefficients $a_{ij}(k) = a_{ji}(k)$ form a connected -graph, the proposed decomposition strategy ensures that all sub-state-variables also form a connected-graph. As proved in [22], the average consensus can still be realized, as given by

$$\frac{1}{2n}\sum_{i=1}^{n}\left[x_i^\alpha(k) + x_i^\beta(k)\right] = \frac{1}{2n}\sum_{i=1}^{n}\left[x_i^\alpha(k+1) + x_i^\beta(k+1)\right] \tag{17}$$

With the help of the initial condition (12), it can be concluded that all sub-states finally converge to their average value, as given in (15).

D. Privacy-Preserving Analysis

Corresponding to previous Section, the privacy-preserving capability of proposed DSDCO is analyzed in terms of the honest but-curious adversaries and external eavesdropping adversaries. Before analyzing, the definition of node's privacy is given as follows.

Definition 1: Node j's initial value $x_j(0)$ remains private as long as an adversary cannot obtain $x_j(0)$ with assured accuracy.

Here, it is assumed that node i is an adversary, which is a neighboring node of node j. By combining with *Definition 1*, the theorem on privacy-preserving is given as follows.

Theorem 2: Under the *DSDCO* and *Coefficient-Selection Rules*, if node j has (at least) one neighboring node m who does not collude with node i to infer $x_j(0)$, node i cannot accurately infer $x_j(0)$ with any guarantee, as depicted in Fig. 5 for node connection configuration.

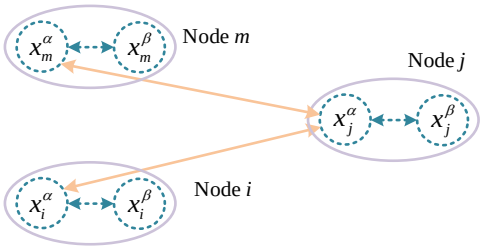


Fig. 5. Node connection topology for Theorem 2.

Proof: In Definition 1, to prove that $x_j(0)$ cannot be extracted with any guaranteed accuracy by node i, we need to prove that any variation in $x_j(0)$ is in-distinguishable for node i. In other words, the information accessible to node i should be exactly invariant even if $x_j(0)$ is changed to an arbitrary value, i.e., $\bar{x}_j(0) \neq x_j(0)$. With a superscript, the state variables and coefficients are obtained after the initial state changes.

When the initial values and weight coefficients of nodes do not have superscripts, the information accessible to node i at *k-th* iteration can be given as

$$I_i(k) = \left\{ \begin{matrix} a_{ip}(k)\big|_{p\in n_i},\ x_p^\alpha(k)\big|_{p\in n_i}, \\ x_i(k),\ x_i^\alpha(k),\ x_i^\beta(k),\ a_{i,\alpha\beta}(k) \end{matrix} \right\} \tag{18}$$

In this way, the cumulated information accessible to node i is expressed as follows

$$I_i = \cup_{k=0}^{\infty} I_i(k) \tag{19}$$

Under different initial values $\bar{x}_j(0) \neq x_j(0)$, if the information available to node i is the same, then the privacy of $x_j(0)$ can be preserved. In this way, node i cannot estimate a range of $x_j(0)$. Therefore, to prove the privacy-preserving capability of the proposed DSDCO, the following condition need to be satisfied:

$$\bar{I}_i = I_i, \forall \bar{x}_j(0) \neq x_j(0) \tag{20}$$

Therefore, we need to prove that the condition in (20) can be achieved by the state initial value and weight coefficient under the proposed protocol. When the initial value of node j is changed to $\bar{x}_j(0)$, the new sub-states are given to satisfy the following equations:

$$\bar{x}_j^\alpha(0) = x_j^\alpha(0), \bar{x}_j^\beta(0) = 2\bar{x}_j(0) - x_j^\alpha(0) \tag{21.1}$$

For node m (does not cooperate with node i for eaves-dropping), the new initial value of state satisfies:

$$\bar{x}_m(0) - x_m(0) = x_j(0) - \bar{x}_j(0) \tag{21.2}$$

In addition, its sub-states satisfy the following equations:

$$\bar{x}_m^\alpha(0) = x_m^\alpha(0), \bar{x}_m^\beta(0) = 2\bar{x}_m(0) - x_m^\alpha(0) \tag{21.3}$$

For the remaining nodes, their initial values, satisfy the following conditions

$$\bar{x}_q(0) = x_q(0), \bar{x}_q^\alpha(0) = x_q^\alpha(0), \bar{x}_q^\beta(0) = x_q^\beta(0), \quad q \neq j, q \neq m \tag{21.4}$$

Meanwhile, the coupling weights among node j and m should satisfy the following conditions:

$$\bar{a}_{j,\alpha\beta}(k) = \begin{cases} \frac{x_j^\beta(k) - \bar{x}_j^\beta(k) + \varepsilon a_{j,\alpha\beta}(k)\left[x_j^\alpha(k) - x_j^\beta(k)\right]}{\varepsilon\left[\bar{x}_j^\alpha(k) - \bar{x}_j^\beta(k)\right]}, k = 0 \\ a_{j,\alpha\beta}(k), \quad k = 1,2,\ldots \end{cases} \tag{22.1}$$

$$\bar{a}_{m,\alpha\beta}(k) = \begin{cases} \frac{x_m^\beta(k) - \bar{x}_m^\beta(k) + \varepsilon a_{m,\alpha\beta}(k)\left[x_m^\alpha(k) - x_m^\beta(k)\right]}{\varepsilon\left[\bar{x}_m^\alpha(k) - \bar{x}_m^\beta(k)\right]}, k = 0 \\ a_{m,\alpha\beta}(k), \quad k = 1,2,\ldots \end{cases} \tag{22.2}$$

The iterative weights between nodes j and m satisfy:

$$\bar{a}_{jm}(k)=\begin{cases}\frac{x_j^{\beta}(k)-\bar{x}_j^{\beta}(k)+\varepsilon a_{jm}(k)\left[x_m^{\alpha}(k)-x_j^{\alpha}(k)\right]}{\varepsilon\left[\bar{x}_m^{\alpha}(k)-\bar{x}_j^{\alpha}(k)\right]}, k=0\\ a_{jm}(k), \quad k=1,2,\ldots\end{cases} \tag{22.3}$$

The coupling weight coefficients and mutual iteration weight coefficients of the remaining nodes are given as

$$\bar{a}_{q,\alpha\beta}(k)=a_{q,\alpha\beta}(k), q\neq j, q\neq m, k=0,1,2,\ldots \tag{22.4}$$

$$\bar{a}_{pq}(k)=a_{pq}(k), \{p,q\}\neq\{j,m\}, k=0,1,2,\ldots \tag{22.5}$$

Notably, the conditions in (21.1) and (21.2) are to ensure that the final convergence value remains the same regardless of the alternative initial values, $\bar{x}_j(0)$ and $\bar{x}_m(0)$. Here, the items in (187) will be analyzed in details.

1) Accessible weights of node i

As given in (22.4) and (22.5), the weight coefficients used for iteration of node i remain unchanged. It yields

$$\bar{a}_{ip}(k)\big|_{p\in n_i}=a_{ip}(k)\big|_{p\in n_i}, a_{i,\alpha\beta}(k)=\bar{a}_{i,\alpha\beta}(k) \tag{23}$$

2) Initial state information of node i

In (21.4), the initial states of node i also remain unchanged:

$$x_i(0)=\bar{x}_i(0), x_i^{\alpha}(k)=\bar{x}_i^{\alpha}(0), x_i^{\beta}(k)=\bar{x}_i^{\beta}(0) \tag{24}$$

3) States from node i's adjacent nodes

Firstly, after the state of node j changes, except for nodes j and m, the states and weights of other nodes remain unchanged. When the initial state value of node j is $x_j(0)$, the state value of node j after the first iteration is:

$$x_j^{\alpha}(1)=x_j^{\alpha}(0)+\varepsilon\sum_{p\in n_j}^{n}a_{jp}(0)\left[x_p^{\alpha}(0)-x_j^{\alpha}(0)\right]+\varepsilon a_{j,\alpha\beta}(k)\left[x_j^{\beta}(0)-x_j^{\alpha}(0)\right]$$
$$=x_j^{\alpha}(0)+\varepsilon\sum_{p\in n_i,p\neq m}^{n}a_{jp}(0)\left[x_p^{\alpha}(0)-x_j^{\alpha}(0)\right]+\varepsilon a_{jm}(0)\left[x_m^{\alpha}(0)-x_j^{\alpha}(0)\right]+\varepsilon a_{j,\alpha\beta}(k)[x_j^{\beta}(0)-x_j^{\alpha}(0)] \tag{25}$$

When the initial state value of node j is change to be $\bar{x}_j(0)$, the sub-state value of node j after the first iteration can be calculated as:

$$\bar{x}_j^{\alpha}(1)=\bar{x}_j^{\alpha}(0)+\varepsilon\sum_{p\in n_j,p\neq m}^{n}a_{jp}(0)\left[x_p^{\alpha}(0)-x_j^{\alpha}(0)\right]$$
$$+\varepsilon\bar{a}_{jm}(0)\left[\bar{x}_m^{\alpha}(0)-\bar{x}_j^{\alpha}(0)\right]+\varepsilon\bar{a}_{j,\alpha\beta}(0)[\bar{x}_j^{\beta}(0)-\bar{x}_j^{\alpha}(k)] \tag{26}$$

By bringing the weight coefficients of (22) into (26), it can be obtained that:

$$\varepsilon\bar{a}_{jm}(0)\left[\bar{x}_m^{\alpha}(0)-\bar{x}_j^{\alpha}(0)\right]=x_j^{\beta}(0)-\bar{x}_j^{\beta}(0)+\varepsilon a_{jm}(0)\left[x_m^{\alpha}(0)-x_j^{\alpha}(0)\right] \tag{27.1}$$

$$\varepsilon\bar{a}_{j,\alpha\beta}(0)\left[\bar{x}_j^{\beta}(0)-\bar{x}_j^{\alpha}(k)\right]=-x_j^{\beta}(0)+\bar{x}_j^{\beta}(0)-\varepsilon a_{j,\alpha\beta}(0)\left[x_j^{\alpha}(0)-x_j^{\beta}(0)\right] \tag{27.2}$$

By combining (26) with (27), it yields

$$\bar{x}_j^{\alpha}(1)=x_j^{\alpha}(0)+\varepsilon\sum_{p\in n_j,p\neq m}^{n}a_{jp}(0)\left[x_p^{\alpha}(0)-x_j^{\alpha}(0)\right]+x_j^{\beta}(0)-\bar{x}_j^{\beta}(0)+\varepsilon a_{jm}(0)\left[x_m^{\alpha}(0)-x_j^{\alpha}(0)\right]\pm x_j^{\beta}(0)+\bar{x}_j^{\beta}(0)-\varepsilon a_{j,\alpha\beta}(0)\left[x_j^{\alpha}(0)-x_j^{\beta}(0)\right]$$
$$=x_j^{\alpha}(0)+\varepsilon\sum_{p\in n_i,}^{n}a_{jp}(0)\left[x_p^{\alpha}(0)-x_j^{\alpha}(0)\right]+x_j^{\beta}(0)+\varepsilon a_{j,\alpha\beta}(0)\left[x_j^{\beta}(0)-x_j^{\alpha}(0)\right] \tag{28}$$

After the first iteration, under the given initial state values and weight coefficients, the first sub-state of node j (used for interaction between nodes) remains unchanged

$$\bar{x}_j^{\alpha}(1)=x_j^{\alpha}(1) \tag{29}$$

As given in (22.4), the states acquired by node i after the first consensus iteration remain unchanged, as given by

$$\bar{x}_p^{\alpha}(1)\big|_{p\in n_i}=x_p^{\alpha}(1)\big|_{p\in n_i} \tag{30.1}$$

In the following iterations (k =1, 2, …), the state of node j, received by adjacent nodes remains unchanged:

$$\bar{x}_j^{\alpha}(k)=x_j^{\alpha}(k) \tag{30.2}$$

As shown in (30), the states from node i's adjacent nodes also remains unchanged:

$$\bar{x}_p^{\alpha}(k)\big|_{p\in n_i}=x_p^{\alpha}(k)\big|_{p\in n_i} \tag{31}$$

4) State information of node i after first iteration

Apart from the unchanged initial states in (24), the state of node i itself, the weights and states of the remaining nodes also remain unchanged. Therefore, it can be concluded that:

$$\bar{x}_i(k)=x_i(k), \bar{x}_i^{\alpha}(k)=x_i^{\alpha}(k), \bar{x}_i^{\beta}(k)=x_i^{\beta}(k) \tag{32}$$

As analyzed above, the accessible information for node i remains unchanged regardless of the variation of $x_j(0)$:

$$I_i=\bar{I}_i, \forall\bar{x}_j(0)\neq x_j(0) \tag{33}$$

Here, the proof is completed. The proposed DSDCO protects the privacy of a node's initial value while requiring only a small amount of computation, thus not increasing the communication burden between nodes.

IV. Case Studies

The validation of the DSDCO is conducted using a constructed DC network as shown in Fig. 6. This system includes six DESSs interconnected on a DC bus, where each DESS incorporates a DC/DC converter and a battery system. The main parameters of the DC electric network, detailed in Table I, adhere to the specifications of the DC converter outlined in [4]. The data exchange topologies are also shown in Fig. 6. The wire resistances of DESSs are 0.48 Ω, 0.37 Ω, 0.32 Ω, 0.62 Ω, 0.22 Ω, and 0.36 Ω. For verification, four cases are proposed by using MATLAB/Simulink simulation (Case 1), OPAL-RT platform (Cases 2 and 3), and experiment (Case 4).

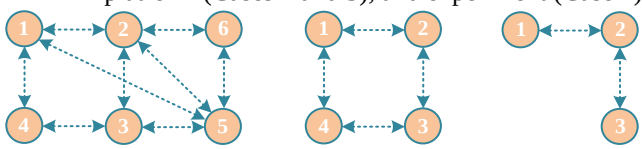


Fig. 6. Communication networks: (a) Case 1, (b) Case 2, (c) Cases 3 and 4.

TABLE I. Parameters of the DC Microgrid and DESSs

Parameters	Value
Nominal bus voltage V_{nom}	48 V
Lower limit of the DC bus voltage V_{min}	45.6 V
Upper limit of the DC bus voltage V_{max}	50.4 V
Rated load current I_{tol}	19 A
DSDCO parameter ε	0.24
Droop coefficient R_{di}	0.05 Ω
Mutual-weight W_{ii}	0.0005
DSDCO execution frequency	0.5 Hz

A. Case 1 – 6 DESSs for Charging

Fig. 7 presents the waveforms of output voltages, current allocation coefficients, output currents, and power losses of the DESSs controlled by the proposed strategy, as shown in Fig. 6(a). From 0 s to 10 s, a conventional control strategy is applied to minimize line losses, while the proposed strategy targets reducing distribution power losses from 10 s to 100 s. All communication channels are subject to an added time delay, leading to a maximum delay of 120 ms. Notably, a delay within a certain range does not affect the system's stability. With a total load current of 19 A and the DSDCO activated, the output currents of the DESSs are distributed based on line resistances

from 0 s to 10 s. Afterwards, the optimal current distribution coefficients are calculated as follows: N_1=0.145, N_2=0.258, N_3=0.081, N_4=0.242, N_5=0.102, and N_6=0.172, respectively. During current distribution, non-negligible communication delays have little impact on the reduction of power loss at steady states, and although dynamic performance deteriorates somewhat, the curves converge asymptotically. Compared to the conventional method, the total loss is reduced from 172.5 W to 135.1 W with the help of the proposed DSDCO.

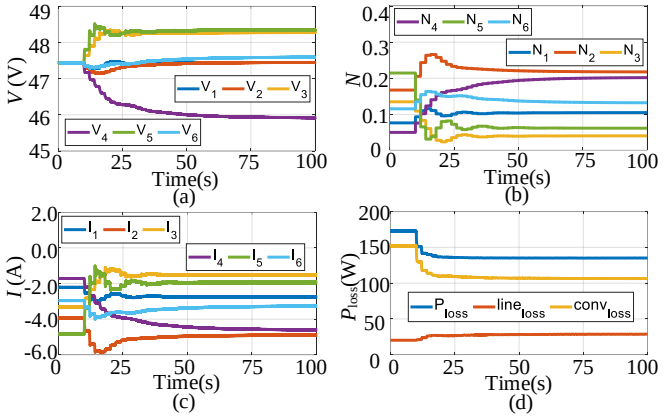


Fig. 7. Waveforms of (a) V_i, (b) N_i, (c) I_i, and (d) P_{loss} in Case 1.

In the proposed DSDCO, the state variables of DESSs are split into two sub-states (x_i^{α} and x_i^{β}) with random values, as shown in Table II. The iteration trajectories of the sub-state variables are plotted in Fig. 8. After successive iterations, all state variables, including actual and sub-state variables, converge to a consensus value. Assuming that external eavesdroppers aim to acquire the initial states of DESSs, these values are inferred using the algorithm described in (11). The trajectories of the state variables after iterations are shown in Fig. 9. Using the conventional consensus protocol, the inferred initial state variables are 20.7, 16.0, 17.3, 22.0, 21.0, and, matching the actual initial states. In contrast, the initial state variables obtained from DSDCO are 13.7, 3.73, 20.2, 22.3, 23.9, and 18.9. This discrepancy demonstrates the privacy-preserving capability of the proposed DSDCO. The iteration trajectories of the sub-state variables using the consensus protocol in [26] are shown in Fig. 10 for comparison. The state variable is obtained by integrating additional inputs, which leads to continuous changes in its value, preventing it from stabilizing near a given target. If this protocol is applied for voltage/current regulation, the microgrid will quickly lose stability.

TABLE II. INITIAL STATE VALUES OF CASE 1

	$DESS_1$	$DESS_2$	$DESS_3$	$DESS_4$	$DESS_5$	$DESS_6$
x_i	20.7	16.0	17.3	22.0	21.0	17.0
x^{α}_i	37.26	14.4	1.73	8.8	17.1	15.3
x^{β}_i	4.14	17.6	32.87	35.2	20.9	18.7

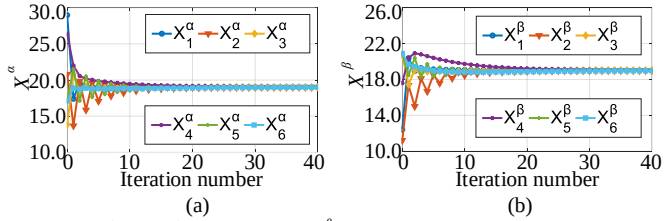


Fig. 8. Waveforms of (a) x_i^{α}, and (b) x_i^{β} in Case 1.

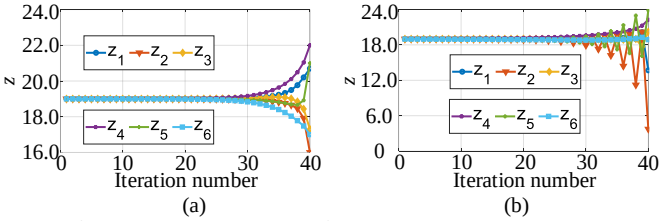


Fig. 9. Inferred initial state-variables for (a) conventional consensus, and (b) DSDCO, in Case 1.

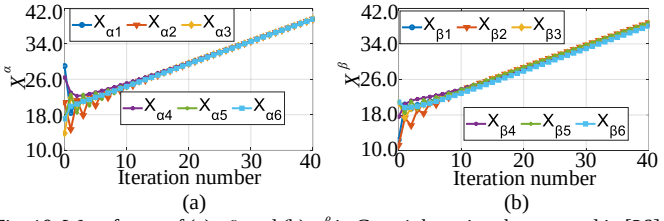


Fig. 10. Waveforms of (a) x_i^{α}, and (b) x_i^{β} in Case 1, by using the protocol in [26].

B. *Case 2 – 4 DESSs for Discharging*

To further verify the effectiveness of the proposed DSDCO, we conducted Cases 2 and 3 on the OPAL-RT-based platform, as shown in Fig. 11. The system variables were exported through the interface board and displayed on the oscilloscope.

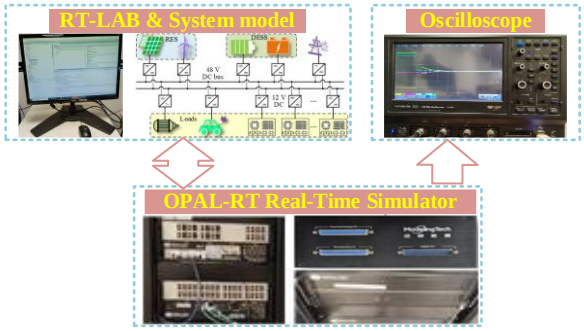
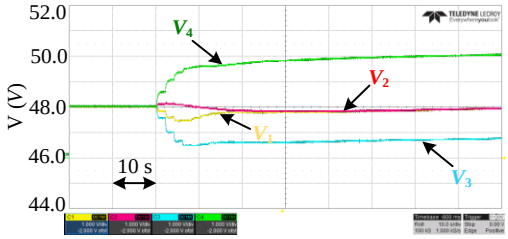


Fig. 11. OPAL-RT platform.

As shown in Fig. 6, two DESSs are removed from the system, due to the limited memory capacity of simulator. For Case 2, during the period from 0 s to 20 s, output currents of DESSs are distributed based on line resistances, with only voltage regulation applied. Subsequently, at 20 s, the proposed DSDCO is implemented until 100 s. Fig. 12 illustrates the waveforms of output voltages, currents, current allocation coefficients, and loss power of DESSs. At 20 s, the DSDCO initiates iterative updates of current coefficients every 2 seconds. This process identifies optimal coefficients for minimum loss: N_1 = 0.202, N_2 = 0.357, N_3 = 0.105, and N_4 = 0.336. Concurrently, as coefficients are updated, DESS output currents are redistributed using secondary adaptive control. Compared to conventional methods (196.6 W), this approach reduces total distribution power loss to 158.6 W.



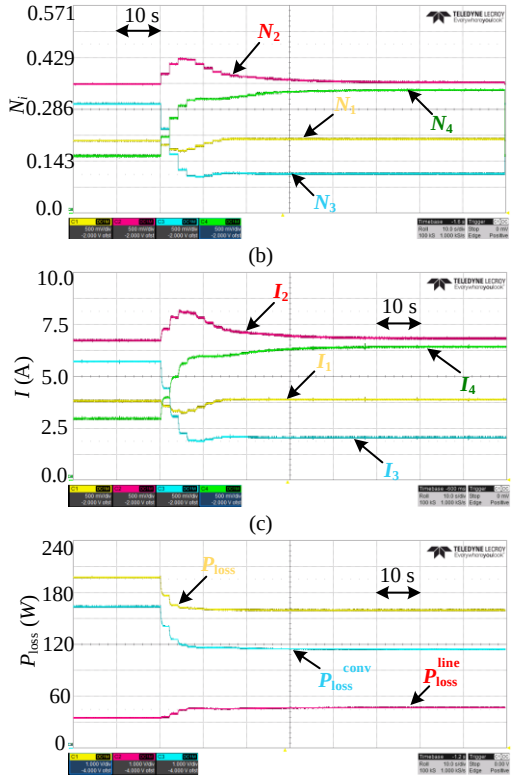


Fig. 12. Waveforms of (a) V_i, (b) N_i, (c) I_i, and (d) P_{loss} in Case 2.

In Case 2, the initial values of the four DESSs are 20.7, 16.0, 17.3, and 22.0, as given in Table III. In Fig. 13, following iterations, all state-variables, encompassing both actual state-variables and sub-state-variables, converge to consensus value. By using the algorithm (11), the inferred trajectories of state-variables are presented in Fig. 14. For conventional consensus protocol, the inferred initial state variables are 20.7, 16.0, 17.3, and 22.0, which are the same as the initial states of $DESS_1$, $DESS_2$, $DESS_3$ and $DESS_4$. For the state-variables obtained by DSDCO, the initial state-variables are 6.69, 17.35, 30.5, and 33.2, respectively.

TABLE III. INITIAL STATE VALUES OF CASE 2

	$DESS_1$	$DESS_2$	$DESS_3$	$DESS_4$
x_i	20.7	16.0	17.3	22.0
x^{α}_i	37.26	14.4	1.73	8.8
x^{β}_i	4.14	17.6	32.87	35.2

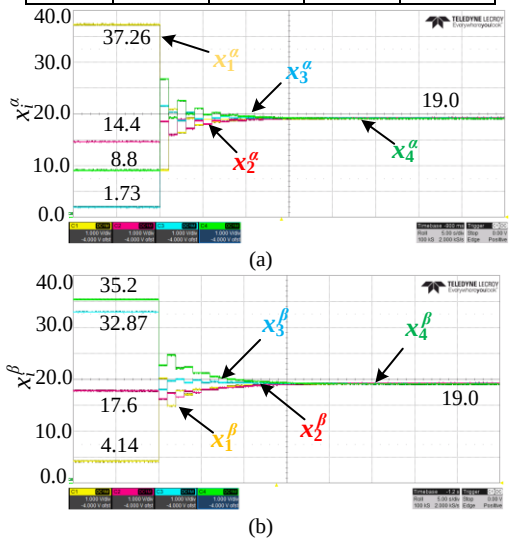


Fig. 13. Waveforms of (a) x_i^{α}, and (b) x_i^{β} in Case 2.

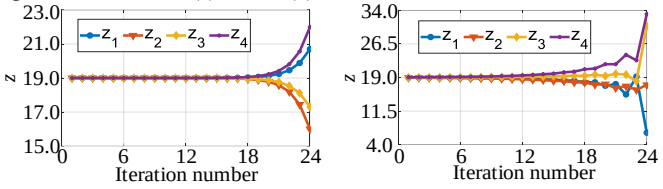


Fig. 14. Inferred initial state-variables for (a) conventional consensus, and (b) DSDCO, in Case 2.

C. *Case 3 - 3 DESSs for Discharging*

Case 3 is conducted using the network in Fig. 6(c) to highlight DSDCO's robustness to different topologies. Fig. 15 shows the output voltages, currents, current coefficients, and loss power for Case 3. With $DESS_4$ is removed, output currents are distributed based on line resistances during the period from 0 s to 20 s. At 20 s, the proposed DSDCO is implemented until 100 s, initiating iterative updates of current coefficients every 2 seconds. This process identifies optimal coefficients for minimum loss: N_1 = 0.295, N_2 = 0.524, and N_3 = 0.181, using DSDCO. As coefficients are updated, DESS output currents are redistributed using secondary adaptive control. Compared to conventional methods (234.7 W), this approach reduces total distribution power loss to 207.8 W.

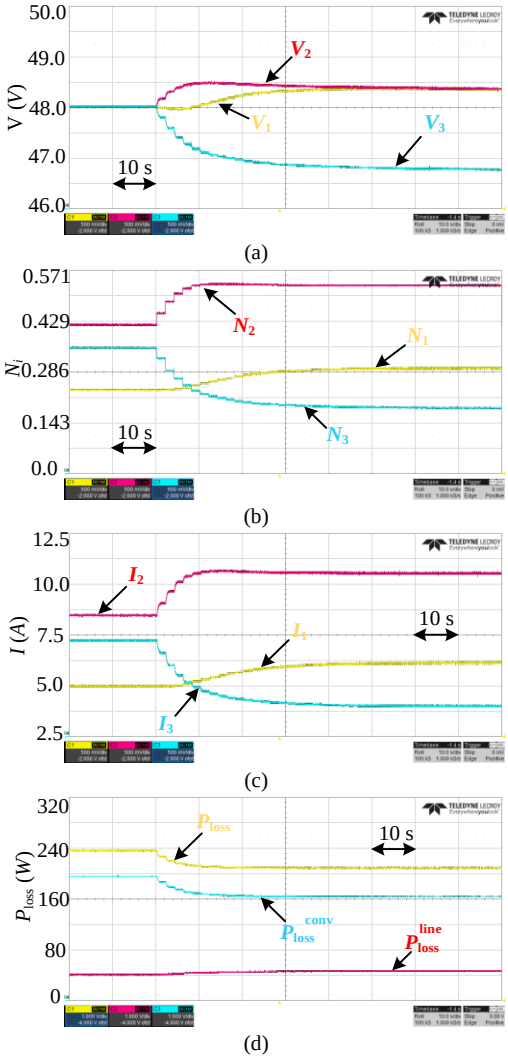


Fig. 15. Waveforms of (a) V_i, (b) N_i, (c) I_i, and (d) P_{loss} in Case 3.

For Case 3, the initial values of three DESSs are 21.0, 17.5, and 18.5, as detailed in Table IV. In Fig. 16, after inter-node and internal actions, all state variables, including x_i^{α} and x_i^{β}, converge to the global average value. The initial states of DESSs are inferred by using (11). The iterative trajectories of state-variables are presented in Fig. 17. When adopting the traditional consensus protocol, the inferred initial state-variables are 21.0, 17.5, and 18.5, which are the same as the initial states. For the state-variables iterated by DSDCO, the initial states are 20.4, 11.6, and 21.4, respectively. In above cases, the inferred initial states are different with the actual values, validating the privacy-preserving capability of proposed method.

TABLE IV. INITIAL STATE VALUES OF CASE 3

	$DESS_1$	$DESS_2$	$DESS_3$
x_i	21.0	17.5	18.5
x^{α}_i	23.1	24.5	9.25
x^{β}_i	18.9	10.5	27.75

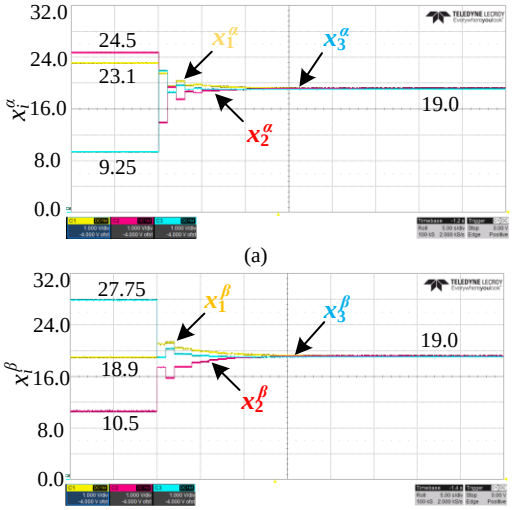


Fig. 16. Waveforms of (a) x_i^{α}, and (b) x_i^{β} in Case 3.

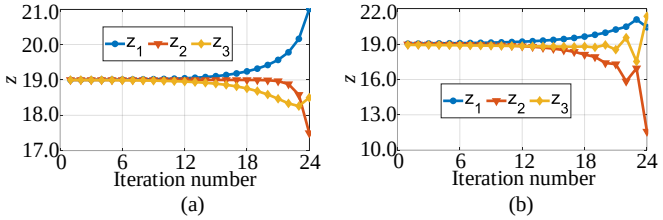


Fig. 17. Inferred initial state-variables for (a) conventional consensus, and (b) DSDCO, in Case 3.

D. *Case 4 - 3 DESSs for Discharging*

In the experiment, three boost converter-based DESSs are adopted to build a DC system. As plotted in Fig. 18, for power conversion between the battery modules and converters, the digital signal processor (DSP), is used for sampling and control. During experimental process, some variables, i.e., voltages and currents can be acquired and displayed by probes. The inter-mediate variables, are calculated and output via the digital-to-analog pins. The controller parameters, parameters of the boost converters, and loss coefficients can be found in [4]. Except for extending the algorithm update cycle to 4 s, the other parameters of the DSDCO are same with the previous simulations.

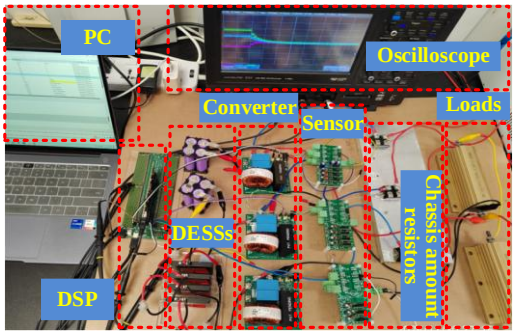


Fig. 18. Experimental testing bench.

Under I_{tol} = 1.5 A, Case 4 is conducted using the network in Fig. 6(c) to highlight DSDCO's robustness against different topologies. Fig. 19 shows the output voltages, currents, current coefficients, and loss power for Case 4. At 20 s, the proposed DSDCO is implemented until 100 s, initiating iterative updates of current coefficients every 4 s. The proposed DSDCO finds optimal coefficients for minimum loss are N_1 = 0.51, N_2 = 0.27, and N_3 = 0.22. As coefficients are updated, DESS output currents are redistributed using secondary adaptive control. Compared to conventional methods (15.3 W), this approach reduces total distribution power loss to 14.8 W.

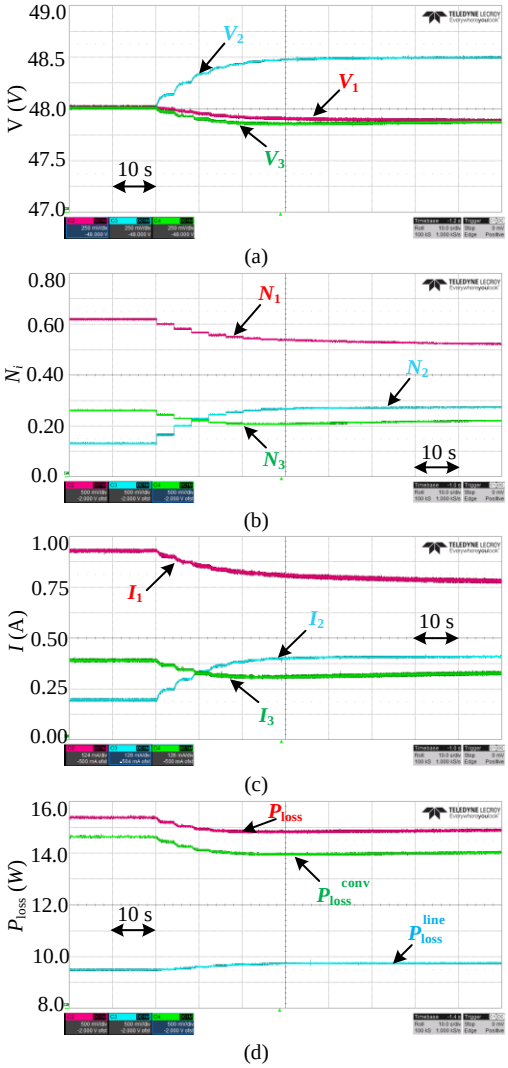


Fig. 19. Waveforms of (a) V_i, (b) N_i, (c) I_i, and (d) P_{loss} in Case 4.

Based on the initial values of 1.15, 1.55, and 1.80, all state variables, including x_i^{α} and x_i^{β}, converge to the global average value, as plotted in Fig. 20. The iterative trajectories of the state variables, generated by inferring algorithm (11), are shown in Fig. 21. When using the traditional consensus control, the inferred initial state-variables are 1.15, 1.55, and 1.8, which are the same as the initial states. For the DSDCO, the inferred initial states are 0.03, 1.25, and 1.38, respectively. Thus, the privacy-preserving capability of proposed method is validated.

TABLE V. INITIAL STATE VALUES OF CASE 4

	$DESS_1$	$DESS_2$	$DESS_3$
x_i	1.15	1.55	1.80
x^{α}_i	1.20	1.90	2.30
x^{β}_i	1.10	1.20	1.3

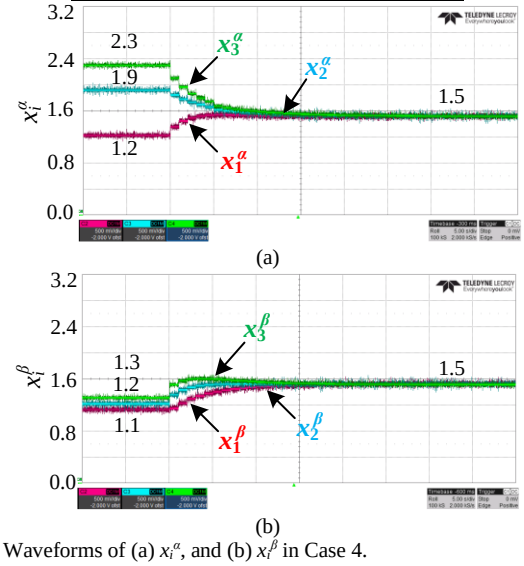


Fig. 20. Waveforms of (a) x_i^{α}, and (b) x_i^{β} in Case 4.

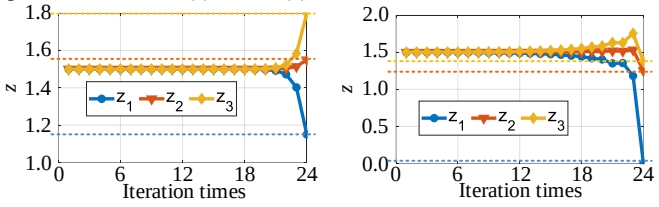


Fig. 21. Inferred initial state-variables for (a) conventional consensus, and (b) DSDCO, in Case 4.

Therefore, the distributed optimization algorithm based on state decomposition proposed in this article demonstrates robustness to different node numbers, communication topologies, and communication delays. Furthermore, Table VI presents a comparison of execution cycles between the proposed DSDCO and the proportional-integral (PI) gradient algorithm [29] across four cases. The convergence of the distributed optimization algorithm is determined using a boundary condition of 0.5% error. When compared to the PI gradient algorithm, the execution cycles of the proposed DSDCO are reduced by over 11% in all scenarios.

TABLE VI. COMPARISONS OF EXECUTION CYCLE

Cases	Cycles by PI gradient algorithm	Cycles by DSDCO	Execution cycle reduction (%)
1	51	45	11.8
2	32	26	18.8
3	27	24	11.1
4	11	9	18.2

V. CONCLUSION

This study develops a state decomposition-based consensus convex optimization strategy for current distribution in DC networks. We address the privacy-preserving current distribution problem in low-voltage DC grids and propose an optimization algorithm to minimize power loss under practical constraints. Using consensus theory, we demonstrate that the DSDCO can find the optimal solution across various operating conditions. To protect the initial information of DESSs, we integrate a privacy protection strategy into the optimization algorithm through state decomposition, ensuring the algorithm's security. To counter adversaries with system knowledge, we use two sub-state variables to conceal the actual state of each DESS during the transmission of state variables, enabling accurate consensus. Combined with a lower-level control strategy, this method allows for precise current distribution and minimizes losses. Through case studies and experiments, we validate the privacy protection capability of DSDCO. Our future research will expand the privacy protection algorithm to a broader range of control systems and implement privacy-preserving.

ACKNOWLEDGEMENT

The authors would like to thank the financial supports from the Ministry of Education (MoE) Academic Research Fund (AcRF) Tier-1 Seed Fund RS12/23.

REFERENCES

[1] R. Bambang, A. Rohman, et. al., "Energy management of fuel cell battery supercapacitor hybrid power sources using model predictive control," *IEEE Trans. Ind. Inform.*, vol. 10, no. 4, pp.1992-2002, Nov. 2014.

[2] Y. Jiang, and Y. Yang, "A distributed proportional-integral observer-based hierarchical control for AC microgrids under FDI attacks," *IEEE Trans. Ind. Electron.*, vol. 71, no. 12, pp. 15780-15792, Dec. 2024.

[3] Q. Wu, R. Guan, X. Sun, Y. Wang, and X. Li, "SoC balancing strategy for multiple energy storage units with different capacities in islanded microgrids based on droop control," *IEEE J. Emerg. Sel. Top. Power Electron.*, vol. 6, no. 4, pp.1932-1941, Dec. 2018.

[4] Y. Jiang, Y. Yang, S.C. Tan, and S.Y.R. Hui, "Distribution power loss mitigation of parallel-connected distributed energy resources in low-voltage DC microgrids using a Lagrange multiplier-based adaptive droop control," *IEEE Trans. Power Electron.*, vol. 36, no. 8, pp. 9105-9118, Jan. 2021.

[5] G. Lin, J. Ma, et. al., "A virtual inertia and damping control to suppress voltage oscillation in islanded DC microgrid," *IEEE Trans. Energy Convers.*, vol. 36, no. 3, pp. 1711-1721, Sep. 2021.

[6] Y. Zhang, Y.W. Wang, J.W. Xiao, and X.K. Liu, "Predefined-time secondary control for DC microgrid," *IEEE Trans. Ind. Electron.*, vol. 69, no. 12, pp. 13504-13513. Dec. 2022.

[7] Y. Zeng, Q. Zhang, Y. Liu, X. Zhuang, X. Lv, and H. Wang, "An improved distributed secondary control strategy for battery storage system in DC shipboard microgrid," *IEEE Trans. Ind. Appl.*, vol. 58, no. 3, pp. 4062-4075, May-June 2022.

[8] S. Zuo, T. Altun, F.L. Lewis, and A. Davoudi, "Distributed resilient secondary control of DC microgrids against unbounded attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3850-3859, Sep. 2020.

[9] Y. Jiang, Y. Yang, S.C. Tan, and S.Y. R. Hui, "Dual-ascent hierarchical control-based distribution power loss reduction of parallel-connected distributed energy storage systems in DC microgrids," *IEEE, J. Emerg. Sel. Top. Ind. Electron.*, vol. 4, no. 1, pp. 137-146, Mar. 2021.

[10] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Multilayer resilience paradigm against cyber-attacks in DC microgrids," *IEEE Trans. Power Electron.*, vol. 36, no. 3, pp. 2522–2532, Mar. 2021.

[11] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Trans. Autom. Contr.*, vol. 62, no. 2, pp. 753–765, Feb. 2017.

[12] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surv. Tut.*, vol. 14, no. 4, pp. 944–980, Fourth Quarter 2012.
[13] A. Cherukuri, and J. Cortés, "Initialization-free distributed coordination for economic dispatch under varying loads and generator commitment," *Automatica*, vol. 74, pp. 183–193, Dec. 2016.
[14] C. Zhao, J. Chen, J. He, and P. Cheng, "Privacy-preserving consensus-based energy management in smart grids," *IEEE Trans. Signal Process.*, vol. 66, no. 23, pp. 6162–6176, Dec. 2018.
[15] S. Mao, Y. Tang, Z. Dong, K. Meng, Z. Y. Dong, and F. Qian, "A privacy preserving distributed optimization algorithm for economic dispatch over time-varying directed networks," *IEEE Trans. Ind. Inform.*, vol. 17, no. 3, pp. 1689–1701, Mar. 2021.
[16] Mo, Y. and Murray, R.M., "Privacy preserving average consensus," *IEEE Trans. Automatic Control*, vol. 62, no. 2, pp.753-765, Feb. 2017.
[17] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Trans. Autom. Contr.*, vol. 64, no. 10, pp. 4035–4049, Oct. 2019.
[18] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Privacy-preserving distributed control strategy for optimal economic operation in islanded reconfigurable microgrids," *IEEE Trans. Power Syst*., vol. 35, no. 5, pp. 3847–3856, Sep. 2020.
[19] C. Hirche, C. Rouzé, and D.S. França, "Quantum differential privacy: An information theory perspective," *IEEE Trans. Inf. Theory*, vol. 69, no. 9, pp.5771-5787, Sep. 2023.
[20] T. Wu, C. Zhao, and Y.-J. A. Zhang, "Privacy-preserving distributed optimal power flow with partially homomorphic encryption," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4506–4521, 2021.
[21] W. Chen, L. Liu, and G.P. Liu, "Privacy-preserving distributed economic dispatch of microgrids: A dynamic quantization-based consensus scheme with homomorphic encryption," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 701–713, Jan. 2023.
[22] C.N. Hadjicostis and A.D. Dom´ınguez-Garc´ıa, "Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus," *IEEE Trans. Autom. Contr*., vol. 65, no. 9, pp. 3887–3894, Sep. 2020.
[23] B. Qu, Z. Wang, B. Shen, H. Dong, and X. Zhang, "Secure particle filtering with paillier encryption–decryption scheme: application to multi-machine power grids," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp.863-873, Jan. 2024.
[24] C. Ying, N. Zheng, Y. Wu, M. Xu, and W.-A. Zhang, "Privacy-preserving adaptive resilient consensus for multi-agent systems under cyberattacks," *IEEE Trans Ind. Inform*., vol. 20, no. 2, pp. 1630-1640, Feb. 2024.
[25] Y. Wang, "Privacy-preserving average consensus via state decomposition," *IEEE Trans. Autom. Contr*., vol. 64, no. 11, pp. 4711 - 4716, Nov. 2019.
[26] K. Zhang, Z. Li, et. al., "Privacy-preserving dynamic average consensus via state decomposition: Case study on multi-robot formation control," *Automatica*, vol. 139, p. 110182, May 2022.
[27] H. Tu, Y. Du, H. Yu, X. Lu, and S. Lukic, "Privacy-preserving robust consensus for distributed microgrid control applications," *IEEE Trans. Ind. Electron.*, vol. 71, no. 4, pp. 3684 - 3697, Apr. 2023.
[28] Y. Jiang, Y. Yang, S. C. Tan, and S. Y. R. Hui, "Power loss minimization of parallel-connected DERs in dc microgrids using a distributed hierarchical control," *IEEE Trans. Smart Grid*, vol. 13, no. 6, pp. 4538-4550, Nov. 2022.
[29] Y. Yu, P. Elango, U. Topcu, and B. Açıkmeşe, "Proportional–integral projected gradient method for conic optimization," *Automatica*, vol. 142, p.110359, Aug. 2022.
[30] F. L., Lewis, H., Zhang, K., Hengster-Movric, and A. Das, "Cooperative control of multi-agent systems: optimal and adaptive design approaches," *Springer Science & Business Media*, (2013).

Yajie Jiang (Member, IEEE) received the Ph.D. degree in electrical engineering from the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong, China, in 2022. He is currently a Research Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include power electronics, smart grid, and machine drives.

Noven Lee received his B.Eng. degree in Electrical & Electronic Engineering from Nanyang Technological University in 2022 and his M.Sc. degree in Electrical Engineering from the National University of Singapore in 2024. He is pursuing his PhD in Electrical Engineering at Nanyang Technological University. His research interests include battery management systems for traction batteries and energy storage systems for smart grids.

Yici Wang is an undergraduate Electrical and Electronic Engineering student at Nanyang Technological University (2021-2025), Singapore. Her research interest is power electronics.

Xiangrong Zhang is a postgraduate Electrical and Electronic Engineering student at Nanyang Technology University (2023-2024), Singapore. His research interest is power electronics.

Eddy Y. S. Foo (Member, IEEE) received the B.Eng. and Ph.D. degrees in electrical and electronic engineering from Nanyang Technological University, Singapore, in 2009 and 2016, respectively. From 2014 to 2016, he was a Research Engineer with the Cambridge Centre for Advanced Research and Education in Singapore, an entity under the National Research Foundations Campus for Research Excellence and Technological Enterprise Program. Since 2016, he has been a Lecturer with the School of Electrical and Electronic Engineering, Nanyang Technological University. His research interests include multiagent systems, microgrid energy management systems, electricity markets, and renewable energy resources.

Yun Yang (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from Wuhan University, Wuhan, China, in 2012, and the Ph.D. degree in electrical engineering from The University of Hong Kong, Hong Kong, in 2017. He was a Research Assistant Professor with the Department of Electrical Engineering, The Hong Kong Polytechnic University. He is currently an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include wireless power transfer, renewable energy technologies, electric vehicles, power electronics, and advanced control.