Distributed Sliding Mode Observer-Based Secondary Control for DC Microgrids Under Cyber-Attacks

Yajie Jiang, Yun Yang, *IEEE, Member*, Siew-Chong Tan, *IEEE, Senior Member*, Shu Yuen Ron Hui, *IEEE, Fellow*

Abstract—**The conventional distributed secondary control is widely adopted for distributed energy resources (DERs) in DC microgrids to achieve bus voltage restorations and output current/power sharing. However, when the DER systems are under cyber-attacks, the control variables of the conventional distributed secondary control will deviate from the nominal parameters and the stability of entire DC microgrids may not be guaranteed anymore. To this end, a distributed sliding mode observer (DSMO)-based secondary control is proposed in this paper. Based on local and neighboring measurements, the DSMO initially detects the false signals. Then, the estimated false signals are compensated by the control variables of the secondary control to eliminate the adverse impact. The stability of DSMO is verified by the convergence of the state variables. Both simulation and experimental results have validated that the proposed DSMO-based secondary control can effectively regulate the DER systems to track the bus voltage references and the desired output current/power under various types of cyber-attacks.**

Index Terms—**Distributed sliding mode observer (DSMO), distributed secondary control, cyber-attacks, distributed energy resource (DER), DC microgrid.**

I. Introduction

With the merits of high flexibility in integrating renewable energy sources (RES), storage devices and modern electronic loads, DC microgrids have been developed rapidly in recent years [1–6]. In DC microgrids, distributed secondary control has been widely adopted for distributed energy resources (DERs) to achieve bus voltage restorations [7-9], load sharing [9, 10], energy balancing [11, 12], power loss reductions [12-14], and economic dispatches [15], etc. However, the conventional distributed secondary control strategies are generally designed based on the communication between the two neighboring units, which are vulnerable to various types of cyber-attacks [16]. Typical cyber-attacks on the communication-based hierarchical control are took place in steady-state control variables [17]. The attacked control variables may lead to bus voltage deviations, output current/power allocation errors, and even instability of the entire DC microgrid. By far, most research activities on cyber-attacks are focused on AC counterparts. In [18], the stability of the AC microgrid is deteriorated by the interpolation of a Gaussian distributed random noise into the control variable of the secondary control. In [19] and [20], similar Gaussian distributed random noise are deliberately imposed on the tuning coefficients of the controllers and the tracking references. As a result, the synchronization of interconnected microgrids could be ended in failure. In [21], the communication channels of distributed generators (DGs) in virtual power plants are maliciously intruded by non-colluding and colluding attacks. Consequently, the microgrid operates in sub-optimal economic conditions.

To address these issues, a combination of Kalman filter and Euclidean detector is adopted to estimate state variables of the microgrid and detect various types of cyber-attacks, such as denial-of-service (DoS) attack, random attack and data-injection attacks [22]. An advanced frequency-state observer with confidence factor structure is proposed to detect and isolate the attacks on the frequency sensors of grid-connected inverters [23]. Besides, a trust-based cooperative controller is proposed to mitigate the adverse effects from false data injection attacks [24]. A three-phase neighborhood watch mechanism for the consensus-based energy management algorithm is designed to detect and counteract the impact of data integrity attacks [25]. The efficient density-based global sensitivity analyses are conducted in [26, 27] to quantify and compensate the impacts of variable attack signals on microgrid operations. In [28], a trust/confidence-based control with relatively high computational complexity is designed to detect and compensate inconspicuous malicious cyber-attacks. In [29], a noise filtration technique with certain statistical properties is adopted to address the zero-mean Gaussian noise on the communication links between the grid-connected inverters. Nevertheless, this method is invalidated against cyber-attacks based on full knowledge of the physical-cyber networks.

Based on the research work of predecessors, a distributed sliding mode observer (DSMO)-based secondary control is proposed in this paper to implement bus voltage restorations and output current/power sharing of DER systems in DC

Manuscript received September 28, 2020; revised December 04, 2020; accepted December 17, 2020. (*Corresponding author*: Yun Yang).

Y. Jiang, and S.C. Tan, are with the is with the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong. (email: yjjiang@eee.hku.hk; sctan@eee.hku.hk).

Y. Yang is with the Department of Electrical Engineering, The Hong Kong Polytechnic University, Hong Kong. (email: yun1989.yang@polyu.edu.hk).

S.Y. Ron Hui is with the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong, and also with the Department of Electrical and Electronic Engineering, Imperial College London, London SW7 2AZ, U.K. (email: ronhui@eee.hku.hk).

microgrids under false signal injection attacks. The DSMO is designed based on the extended state observer technique to detect the attack signals and compensate the control variables of the distributed secondary control. The existing hardware implementations of the conventional distributed secondary control can be directly used for the proposed DSMO to accurately estimate both the state variables and attack signals based on the neighboring measurements. Thus, no additional hardware costs are needed for the proposed control. The investigated constant and time-varying attack signals are imposed on either leader or follower nodes. several case studies for different control objectives and attack signals are carried out in simulation and experiment to validate the effectiveness of the proposed DSMO-based secondary control to protect the DER systems from various types of false signal attacks in DC microgrids. To the best of our knowledge, the investigations in this paper have not been conducted before. The major contributions of this paper include that (i) the vulnerability of conventional distributed secondary control for DER systems in DC microgrids under cyber-attacks is analyzed; (ii) a new DSMO is presented to estimate and compensate various types of attack signals such that the proposed secondary control can achieve bus voltage restorations and output current/power sharing even if the DC microgrid is under cyber-attacks.

II. Modeling of Cyber Attacks on Conventional Distributed Secondary Control

A. Modeling of DERs and Communication Based on Graph Theory

A typical DC microgrid is a two-layer system which consists of a physical layer and a cyber layer. Those hardware components, including power electronics interfaces, sensors, protections, measurements, and auxiliary circuits, are in the physical layer. The control algorithms and communication technique are in the cyber layer. Therefore, each DER system in the DC microgrid can be considered as an agent of the cyber-physical system and the communication network among the DERs can be modelled as a directed graph *G* = (*V*, *E*). Here, *V* and *E* are the sets of agents and edges. In the digraph of the DC microgrid, the DERs and communication links are denoted by the nodes and edges. By considering the DC network with *n* autonomous agents with linear dynamics [30], without loss of generality, we let *V* = {1, 2, …, *n*} and the notation (*j*, *i*) denotes that the directed edge of the graph from the node *j* to the node *i*. It is assumed that no self-loops exist in the diagraph *G*, i.e., (*i*, *i*) ∉ *E*. For each *i* ∈ *V*, let $V_i = \{j:(j, i) \in E\}$ be the set of nodes providing data information to the node *i*. Let $\mathbf{A} = [a_{ij}]_{i,j=1}^{n} \in \mathrm{R}^{n\times n}$ be the adjacency matrix of the digraph *G*. Here, if (*j*, *i*)∈*E*, a_{ij}=1, otherwise, a_{ij} = 0. The cardinality of V_i, also known as the in-degree of the node *i*, is denoted by $d_i^{in} = \sum_{j=1}^{n} a_{ij} = \sum_{j\in V_i} a_{ij}$. Here, d_i^{in} indicates the number of incoming edges to the node *i*. On the contrary, d_i^{out} indicates the number of projected edges from the node *i*, which is also known as the out-degree of the node *i* (i.e., $d_i^{\mathrm{out}} = \sum_{j=1}^{N} a_{ji}$). Then, the Laplacian matrix can be defined as

$$\mathbf{L} = \mathbf{D}^{in} - \mathbf{A} \tag{1}$$

where $\mathbf{D}^{in} = diag\{d_i^{in}\}$ is an in-degree diagonal matrix. The eigenvalues of the Laplacian matrix can determine the dynamic performance of DER systems.

B. A Brief Review of the Conventional Distributed Secondary Control

In the conventional distributed secondary control, the output voltage reference of the *i*-th DER is provided by a droop control as

$$V_{\mathrm{ref}i} = V_{\mathrm{nom}} - R_{\mathrm{d}i} I_i \tag{2}$$

where V_{nom} is the nominal DC bus voltage. I_i and $R_{\mathrm{d}i}$ are the output current and droop coefficient of the *i*-th DER. Based on the droop control, a secondary-layer control is generally adopted to regulate the bus voltages to track the nominal value or proportional output current/power sharing among the DERs. For the bus voltage restorations,

$$V_1 = V_2 = \ldots = V_n = V_{\mathrm{nom}} \tag{3}$$

where V_1, V_2, …, V_n are the output voltages of the DERs. For the output current/power sharing,

$$I_1 / N_1 = I_2 / N_2 = \ldots = I_n / N_n \tag{4.1}$$

$$P_1 / N_1 = P_2 / N_2 = \ldots = P_n / N_n \tag{4.2}$$

where I_1, I_2, …, I_n and P_1, P_2, …, P_n are the output currents and output powers of the DERs, respectively. N_1, N_2, … , N_n are their allocation coefficients. In general, the time constant of the local control is much smaller than that of the secondary-layer control for a DER system. According to [31, 32], by synthesizing the output voltages, output currents, and output powers as a control variable x_i, the dynamics of the DER systems can be given based on the system-level modeling as

$$\dot{x}_i(t) = B_i u_i(t) \tag{5}$$

where $u_i(t)$ is the control input and B_i is the control coefficient. Then, the distributed secondary control can be designed as

$$u_i(t) = -\sum_{j=1}^{n} a_{ij}(x_i(t) - x_j(t)) - g_i(x_i(t) - x_{\mathrm{ref}}) \tag{6}$$

where x_{ref} is the reference of the state variables. a_{ij} is the consensus coefficient. g_i is the indicator of the *i*-th DER being a lead node or a follower node (i.e., $g_i > 0$ for *i* = 1, …, *l* and $g_i = 0$ for *i* = *l*+1, …, *n*). The lead nodes are controlled to track the references, whereas the follower nodes are only regulated to achieve the consensus of state variables. It has been verified that all nodes can reach a consensus heading equaling to the initial heading of the leader nodes as [31]

$$\lim_{t\to\infty} \left\| x_i(t) - x_j(t) \right\| = 0, \forall i, j = 1, \ldots, n \tag{7}$$

The secondary-layer control is generally implemented using embedded digital controllers with communication interfaces. However, the actuators are vulnerable to cyber-attacks, which may not only fluctuate the bus voltages and output currents of DERs, but also exceed power limits and destabilize the entire DC microgrid.

C. Cyber-Attack Model and Analysis

Cyber-attacks on the distributed secondary control of the DERs may occur on the leader nodes or follower nodes, as shown in Fig. 1. The attack signals can be modeled as step signals, sinusoidal signals, ramp signals or a finite superposition of them to falsify the control variables [33, 34]. The attack signals are defined as

$$f_i(t) = \begin{cases} \gamma_i & i = 1,\ldots,l \\ \eta_i & i = l+1,\ldots,n \end{cases} \tag{8.1}$$

where γ_i and η_i are the attacks signals on the i-th leader and follower nodes, respectively. The attack signal $f_t(t)$ and its derivative $\dot{f}_t(t)$ are in the boundaries as the following:

$$|f_i(t)| \in [0, \xi] \tag{8.2}$$

$$|\dot{f}_i(t)| \in [0, \zeta] \tag{8.3}$$

where ξ and ζ are the corresponding upper limits.

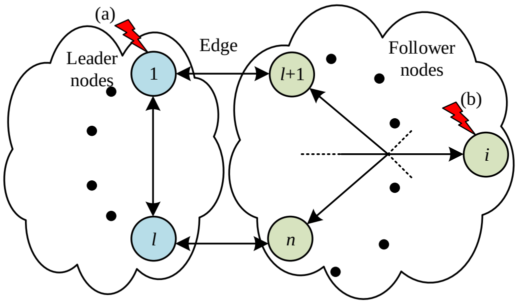


Fig. 1. Cyber-attacks on (a) leader nodes or (b) follower nodes.

1) Cyber-Attacks on Leader Nodes

When the leader nodes are attacked by false signals, based on (6) and (8.1), the distributed secondary control for the controlled DERs (i.e., pinning nodes) can be given as

$$u_i'(t) = -\sum\nolimits_{j\neq i}^{n} a_{ij}\left[x_i(t) - x_j(t)\right] - g_i \sum\nolimits_{j=1}^{n}\left[x_i(t) - (x_{\text{ref}} + \gamma_i)\right] \tag{9}$$

Here, the difference between the state variable x_i and the reference x_{ref} is defined as the state variable error e_i (i.e., $e_i = x_i - x_{ref}$) and the first l DERs are selected to be pinned. Then, the dynamics of the state variable errors can be expressed as

$$\dot{\mathbf{e}}(t) = -(\mathbf{L}+\mathbf{G})\mathbf{e}(t) + \mathbf{G}\boldsymbol{\gamma}(t) \tag{10}$$

where $\mathbf{L}$ is the Laplacian matrix of the communication network. $\mathbf{G} = diag(g_1,\ldots, g_N)$ is the pinning matrix. $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_N)$ in which $\gamma_i \neq 0$ if and only if the communication link from the controller of the leader node to the i-th pinning DER is corrupted. Accordingly, the dynamics of the state variable errors can be derived as

$$\mathbf{e}(t) = exp^{-(\mathbf{L}+\mathbf{G})t}\mathbf{e}(t_0) + \int_{t_0}^{t} e^{-(\mathbf{L}+\mathbf{G})(t-\tau)}\mathbf{G}\boldsymbol{\gamma}(\tau)d\tau \tag{11}$$

where *exp* is the exponential function. Without the loss of generality, the false signals (i.e., $\boldsymbol{\gamma}(\tau)$) are assumed to be positive (i.e., $\gamma_i > \gamma_0 > 0$, $\forall i \in I$). Since the matrix $-(\mathbf{L}+\mathbf{G})$ is negative-definite and invertible, the first term of (11) (i.e., $exp^{-(\mathbf{L}+\mathbf{G})t}\mathbf{e}(t_0)$) is converged to zero. However, due to the elements of the pinning matrix $\mathbf{G}$ are non-negative, the second term of (11) (i.e., $\int_{t_0}^{t} e^{-(\mathbf{L}+\mathbf{G})(t-\tau)}\mathbf{G}\boldsymbol{\gamma}(\tau)d\tau$) cannot be converged to zero. Thus, the state variable errors in (11) (i.e., $\mathbf{e}(t)$) cannot be converged to zero as

$$\begin{aligned} \lim_{t\to\infty}\mathbf{e}(t) &= \lim_{t\to\infty}\int_{t_0}^{t} exp^{-(\mathbf{L}+\mathbf{G})(t-\tau)}\mathbf{G}\boldsymbol{\gamma}(\tau)d\tau \\ &> \lim_{t\to\infty} exp^{-(\mathbf{L}+\mathbf{G})t}[exp^{(\mathbf{L}+\mathbf{G})t} - exp^{(\mathbf{L}+\mathbf{G})t_0}](\mathbf{L}+\mathbf{G})^{-1}\mathbf{G}\boldsymbol{\gamma}_0 \\ &= (\mathbf{L}+\mathbf{G})^{-1}\mathbf{G}\boldsymbol{\gamma}_0 \geq 0 \end{aligned} \tag{12}$$

2) Cyber-Attacks on Follower Nodes

When the follower nodes are attacked by false signals, based on (6) and (8.1), the distributed secondary control for the i-th DER and its neighboring DERs can be given as

$$\begin{aligned} u_i'' &= -\sum\nolimits_{j\neq i}^{n} a_{ij}\left[(x_i - \eta_i) - x_j\right] - g_i\left[(x_i - \eta_i) - x_{\text{ref}}\right] \\ u_j'' &= -\sum\nolimits_{k\neq j}^{n} a_{jk}\left\{(x_j - x_k) - \left[x_j - (x_i - \eta_i)\right]\right\} - g_j(x_j - x_{\text{ref}}) \end{aligned} \tag{13}$$

Accordingly, the dynamics of state variable errors can be expressed as

$$\dot{\mathbf{e}}(t) = -(\mathbf{L}+\mathbf{G})\mathbf{e}(t) + (\mathbf{L}+\mathbf{G})\boldsymbol{\eta}(t) \tag{14}$$

Here, the false signals (i.e., $\boldsymbol{\eta}(\tau)$) are assumed to be positive (i.e., $\eta_i > \eta_0 > 0$, $\forall i \in V$). Similar to the analysis of the leader nodes, the state variable errors in (14) are converged to non-zero values as

$$\begin{aligned} \lim_{t\to\infty}\mathbf{e}(t) &= \lim_{t\to\infty}\int_{t_0}^{t} exp^{-(\mathbf{L}+\mathbf{G})(t-\tau)}(\mathbf{L}+\mathbf{G})\boldsymbol{\eta}(\tau)d\tau \\ &> \lim_{t\to\infty} exp^{-(\mathbf{L}+\mathbf{G})t}[exp^{(\mathbf{L}+\mathbf{G})t} - exp^{(\mathbf{L}+\mathbf{G})t_0}](\mathbf{L}+\mathbf{G})^{-1}(\mathbf{L}+\mathbf{G})\boldsymbol{\eta}_0 \\ &= \boldsymbol{\eta}_0 \geq 0 \end{aligned} \tag{15}$$

According to (12) and (15), the false signal injection attacks on the leader and follower nodes can result in non-convergence of the state variable errors. Therefore, the performances of the distributed secondary control in achieving bus voltage restorations and current/power sharing among the DERs are deteriorated. It is worth noting that the function of consensus of the conventional secondary control is still valid for the cyber-attacks on leader node, while the state variables are not converged for the cyber-attacks on follower nodes.

III. DSMO-Based Secondary Control

To enhance the robustness of the conventional distributed secondary control against cyber-attacks, a DSMO is incorporated to estimate and compensate the false signals. A comprehensive control block diagram of the proposed control scheme is depicted in Fig. 2. The proposed control is a two-layer hierarchical control. In the primary layer, a conventional droop control provides output voltage references of the DERs for the local voltage and current control. The primary-layer control is independent of the communication signals. In the secondary layer, a consensus control is adopted as the distributed secondary control to provide adaptive voltage references for the primary-layer control. The communication signals are only exchanged between the neighboring DERs, as shown in the communication graph (total of n nodes). The solid lines indicate the communication links between the two real nodes, whereas the dotted lines indicate those abbreviated nodes and communication links.

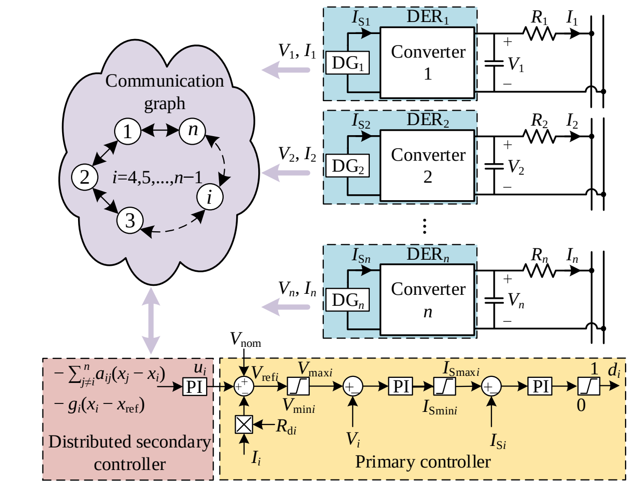


Fig. 2. Circuits and control of the proposed control scheme.

A. Design of the Proposed DSMO

The dynamics of the DER systems under false signal injection attacks can be given based on (5) as

$$\dot{x}_i(t) = B_i[u_i(t) + f_i(t)] \tag{16}$$

Then, based on the extended state observer technique [35, 36], a DSMO can be designed as

$$\begin{cases} \dot{\hat{x}}_i(t) = B_i\left\{u_i(t) + \left[\hat{f}_i(t) + \chi_i\mu_i(t)\right]\right\} \\ \dot{\hat{f}}_i(t) = \mu_i(t) \end{cases} \tag{17}$$

where $\hat{x}_i$ and $\hat{f}_i$ are the estimated state variables and false signals of the i-th DER. χ_i is the observer gain and $\mu_i(t)$ is the observation error. Based on (16) and (17),

$$\mu_i(t) = K\,\mathrm{sgn}\left\{\sum_{j\neq i}^{n} a_{ij}\left[\tilde{x}_i(t) - \tilde{x}_j(t)\right] + g_i\tilde{x}_i(t)\right\} \tag{18}$$

where K is the feedback gain of the sliding mode. The observation errors of the i-th and j-th DERs are denoted as $\tilde{x}_i = x_i(t) - \hat{x}_i(t)$ and $\tilde{x}_j = x_j(t) - \hat{x}_j(t)$, respectively. sgn(•) is the sign function. Apparently, if the i-th DER is attacked by false signals, the estimated state variable $\hat{x}_i$ is biased from the measured x_i. Their differences can lead to the changes of $\mu_i(t)$, which further update the estimated false signals to ensure the accuracy of the observer. Besides, the differences of the state variables between neighboring nodes can also be accounted in $\mu_i(t)$. Hence, by adopting the sliding mode in (18), the DSMO in (17) can adaptively estimate both the state variables and the false signals. By substituting the estimated state variables and attack signals into the distributed secondary control in (6), the control variables of the DSMO-based secondary control can be derived as

$$u_i^{'''}(t) = -\sum_{j\neq i}^{n} a_{ij}\left[\hat{x}_i(t) - \hat{x}_j(t)\right] - g_i\left[\hat{x}_i(t) - x_{ref}\right] - \hat{f}_i(t) \tag{19}$$

Here, the false signals are estimated and compensated in the control variables. The control block diagram of the DSMO-based secondary control is depicted in Fig. 3.

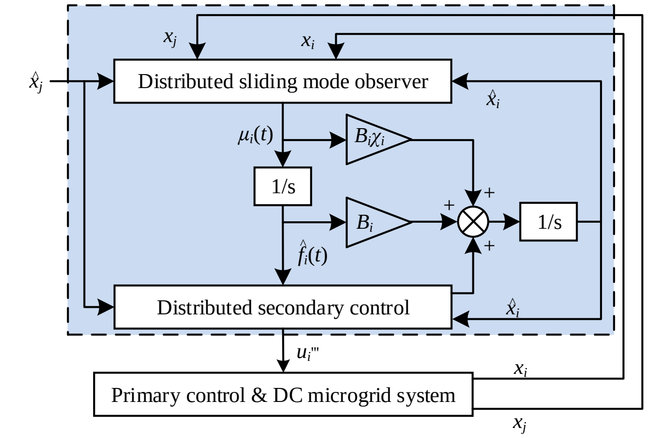


Fig. 3. Control block diagram of the DSMO-based secondary control.

B. Stability Analysis of DSMO

The dynamics of the estimation errors of the state variables and false signals can be derived based on (6), (16), (17) and (18) as (details are provided in the Appendix)

$$\begin{aligned} \dot{\tilde{x}}_i(t) = {} & B_i\left\{-\sum_{j\neq i}^{n} a_{ij}\left[\tilde{x}_i(t) - \tilde{x}_j(t)\right] - g_i\tilde{x}_i(t)\right\} \\ & -B_i\chi_i K\,\mathrm{sgn}\left\{\sum_{j\neq i}^{n} a_{ij}\left[\tilde{x}_i(t) - \tilde{x}_j(t)\right] + g_i\tilde{x}_i(t)\right\} \end{aligned} \tag{20}$$

$$\dot{\tilde{f}}_i(t) = \dot{f}(t) - K\,\mathrm{sgn}\left\{\sum_{j\neq i}^{n} a_{ij}\left[\tilde{x}_i(t) - \tilde{x}_j(t)\right] + g_i\tilde{x}_i(t)\right\} \tag{21}$$

To ensure the stability, the Lyapunov functions of the estimation errors are designed to satisfy

$$\begin{cases} V_1 = \frac{1}{2}\tilde{x}_i^2 \\ \dot{V}_1 = \tilde{x}_i \cdot \dot{\tilde{x}}_i \leq 0 \end{cases} \tag{22}$$

$$\begin{cases} V_2 = \frac{1}{2}\tilde{f}_i^2 \\ \dot{V}_2 = \tilde{f}_i \cdot \dot{\tilde{f}}_i \leq 0 \end{cases} \tag{23}$$

By substituting (20) and (21) into (22) and (23), respectively,

$$\begin{aligned} \dot{V}_1 = {} & B_i\left[-\sum_{j\neq i}^{n} a_{ij}\tilde{x}_i\left(\tilde{x}_i - \tilde{x}_j\right) - g_i\tilde{x}_i^2\right] \\ & -B_i\tilde{x}_i\chi_i K\,\mathrm{sgn}\left[\sum_{j\neq i}^{n} a_{ij}\left(\tilde{x}_i - \tilde{x}_j\right) + g_i\tilde{x}_i\right] \end{aligned} \tag{24}$$

$$\dot{V}_2 = \tilde{f}_i\dot{f} - \tilde{f}_i K\,\mathrm{sgn}\left[\sum_{j\neq i}^{n} a_{ij}\left(\tilde{x}_i - \tilde{x}_j\right) + g_i\tilde{x}_i\right] \tag{25}$$

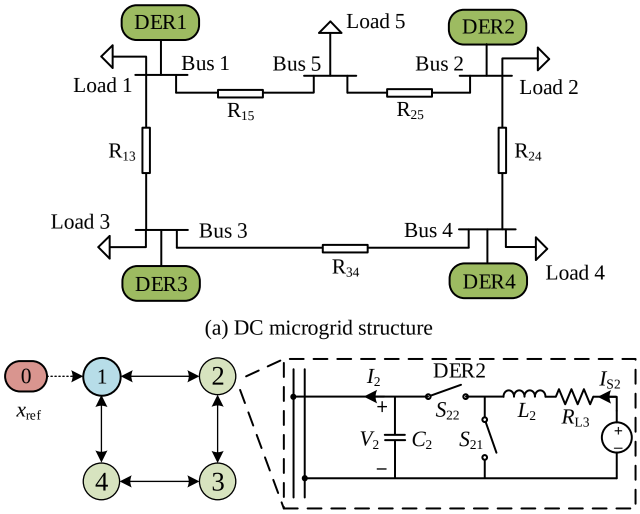
Based on (22)~(25), the stability of DSMO can be guaranteed by designing the parameters χ_i and K to satisfy

$$\begin{cases} K\,\mathrm{sgn}\left[\sum_{j\neq i}^{n} a_{ij}\left(\tilde{x}_i - \tilde{x}_j\right) + g_i\tilde{x}_i\right] \geq \dot{f} & \tilde{f}_i \geq 0 \\ K\,\mathrm{sgn}\left[\sum_{j\neq i}^{n} a_{ij}\left(\tilde{x}_i - \tilde{x}_j\right) + g_i\tilde{x}_i\right] \leq \dot{f} & \tilde{f}_i < 0 \end{cases} \tag{26}$$

$$\begin{cases} -\chi_i K\,\mathrm{sgn}\left[\sum_{j\neq i}^{n} a_{ij}\left(\tilde{x}_i - \tilde{x}_j\right) + g_i\tilde{x}_i\right] \leq \sum_{j\neq i}^{n} a_{ij}\left(\tilde{x}_i - \tilde{x}_j\right) + g_i\tilde{x}_i & \tilde{x}_i \geq 0 \\ -\chi_i K\,\mathrm{sgn}\left[\sum_{j\neq i}^{n} a_{ij}\left(\tilde{x}_i - \tilde{x}_j\right) + g_i\tilde{x}_i\right] \geq \sum_{j\neq i}^{n} a_{ij}\left(\tilde{x}_i - \tilde{x}_j\right) + g_i\tilde{x}_i & \tilde{x}_i < 0 \end{cases} \tag{27}$$

IV. Simulation Results

Simulations are carried out on a 48 V five-bus DC microgrid with four DERs being controlled by the DSMO-based secondary control in Matlab/Simulink. The structure of the DC microgrid is shown in Fig. 4(a). Each DER consists of a DC source and a grid-connected converter. The communication network of the DC microgrid is depicted in Fig. 4(b). The DER systems can be modelled as four connected nodes. The node 1 (i.e., DER1) is the leader node while the other nodes (i.e., DER2, DER3 and DER4) are the follower nodes (the results are insensitive to the selections of leader nodes). The parameters of the local primary control in Fig. 2 are preliminarily tuned to ensure the stability of the DC microgrid. The main specifications of the DC microgrid and the grid-connected converters are provided in Table I. Here, the bus voltages are required to be regulated within the lower bound $V_{\min}$ and the upper bound $V_{\max}$.



(a) DC microgrid structure

(b) Communication network

Fig. 4. The 48 V five-bus DC microgrid with four DERs in simulation.

TABLE I. MAIN SPECIFICATIONS OF THE DC MICROGRID AND CONVERTERS

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
Lower bound of the source current ($I_{\text{Smin}i}$)	0 A
Upper bound of the source current ($I_{\text{Smax}i}$)	15 A
Resistance of Load 1	40 Ω
Rated Power of Load 2	40 W
Resistance of Load 3	60 Ω
Rated Power of Load 4	120 W
Resistance of Load 5	20 Ω
Line resistance between Bus 1 and 2 (R_{13})	0.1 Ω
Line resistance between Bus 1 and 3 (R_{15})	0.15 Ω
Line resistance between Bus 2 and 5 (R_{24})	0.12 Ω
Line resistance between Bus 3 and 4 (R_{25})	0.24 Ω
Line resistance between Bus 4 and 3 (R_{34})	0.2 Ω
Inductances of the converter (L_i)	460 μH
ESR of the inductances ($R_{\text{L}i}$)	0.1 Ω
Output capacitances of the converter (C_i)	10.1 μF
Output capacitances of the switches ($C_{\text{s}i}$)	102 pF
ON resistances of the switches ($R_{\text{s}i}$)	72 mΩ

To verify the effectiveness of the proposed DSMO-based secondary control against false signal injection attacks on the DER systems, five different cases are studied in simulation, as provided in Table II. In the cases 1 and 2, the proposed control is designed for voltage restorations. In the case 3, the proposed control is designed for equal current sharing among the DERs. In the cases 4 and 5, the proposed control is designed for equal power sharing among the DERs. The attack signals are constant in the cases 1, 2 and 3, and time-varying in the cases 4 and 5. The main parameters of the controllers are given in Table III. The parameters of the proportional-integral (PI) compensators in the two-layer control are identical for all the four DERs. The sampling frequency of the controllers is 100 kHz. The parameters of the adopted DSMO are B_1=B_2=B_3=B_4=20, K=15, and χ_1=χ_2=χ_3=χ_4=10000, respectively.

TABLE II. ATTACK SIGNALS OF DIFFERENT CASES IN SIMULATION

Case	Attack Node	False Signal Value	Signal Limits	Derivative Limits
1	f_1 at DER1	−3.0	[0 48]	[0 200]
2	$f_{2,1}$ at DER4	1.4	[0 48]	[0 200]
	$f_{2,2}$ at DER2	0.4		
3	f_3 at DER2	0.8	[0 48]	[0 200]
4	$f_{4,1}$ at DER2	$20(t-0.5)-20$	[0 48]	[0 200]
	$f_{4,2}$ at DER3	$10\sin[5\pi(t-2.5)]$		
5	f_5 at DER1	$4(t-0.5)^2$	[0 48]	[0 200]

TABLE III. PARAMETERS OF THE CONTROLLERS IN SIMULATION

Descriptions	Symbol	Value
Proportional gain of the PI compensation in the secondary control	$K_{\text{P}i}$	0.05
Integral gain of the PI compensation in the secondary control	$K_{\text{I}i}$	0.1
Proportional gain of the PI voltage compensation in the dual-loop control	$K_{\text{P1}i}$	2
Integral gain of the PI voltage compensation in the dual-loop control	$K_{\text{I1}i}$	10
Proportional gain of the current PI current compensation in the dual-loop control	$K_{\text{P2}i}$	40
Integral gain of the PI current compensation in the dual-loop control	$K_{\text{I2}i}$	20

A. Case 1

Fig. 5 show the waveforms of the output voltages of DERs, the estimated state variables, the output currents of DERs, and the estimated attack signal during the period from 0s to 4s in case 1. From 0s to 0.5s, only the conventional distributed secondary control is adopted for the four DERs without cyber-attacks. All the bus voltages are controlled at 48 V, as shown in Fig. 5(a). At 0.5s, the leader node DER1 is attacked by the constant signal f_1=−3.0 without using the proposed DSMO. Consequently, the output voltage of the leader node is controlled at 45 V (6.25% deviation from the reference). However, due to the conventional consensus-based secondary control is adopted, all the output voltages of the follower nodes will converge to the output voltage of the leader node at 45 V, which exceed the lower limit of the bus voltage (i.e., $V_{\min}$). The proposed DSMO-based secondary control is operated at 2.5s. The false signals are estimated and compensated during the period from 2.5s to 4.0s, as shown in Fig. 5(d). As a result, the bus voltages and the output currents of the DERs are restored to the nominal values.

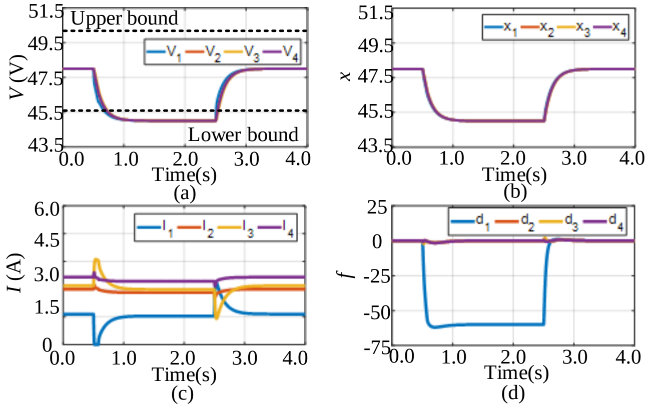


Fig. 5. Waveforms of (a) the output voltages of DERs, (b) the estimated state variables, (c) the output currents of DERs, and (d) the estimated attack signal in case 1.

B. Case 2

The waveforms of the output voltages of DERs, the estimated state variables, the output currents of DERs, and the estimated attack signals in case 2 are shown in Fig. 6. During the period from 0s to 0.5s, without the injections of false signals, the output voltages of the DERs are controlled by the conventional distributed secondary control to track the reference. At 0.5s, the follower node DER4 is attacked by a false signal $f_{2.1}$=1.4. Consequently, the output voltage of the DER4 exceeds the upper limit. At 2.0s, the follower node DER2 is also attacked by a false signal $f_{2.2}$=0.4 (two false signals are imposed simultaneously). As a result, three output voltages (i.e., DER2, DER3 and DER4) exceed the upper limit. Due to the attacked nodes are follower nodes, the output currents of the DERs are deviated from the nominal values, as can be seen in Fig. 6(c). The proposed control strategy is activated at 3.5s. During the period from 3.5 s to 5.0 s, the state variables and the attack signals are accurately estimated, as shown in Fig. 6(b) and Fig. 6(d). By compensating the estimated false signals in the control variables, the bus voltages and output currents of DERs can controlled at the nominal values at steady state (the values without cyber-attacks during the period from 0s to 0.5s).

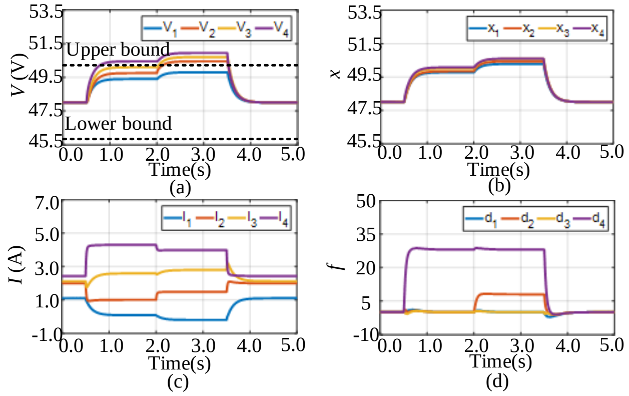


Fig. 6. Waveforms of (a) the output voltages of DERs, (b) the estimated state variables, (c) the output currents of DERs, and (d) the estimated attack signals in case 2.

C. Case 3

In case 3, the output currents of the DERs are controlled in consensus. The waveforms of the output voltages of DERs, the estimated state variables, the output currents of DERs, and the estimated attack signal are shown in Fig. 7. During the period from 0s to 0.5s, without cyber-attacks, the output currents of the DERs are controlled by the conventional secondary control at 1.91 A. During the period from 0.5s to 2.5s, the control signal of the DER2 is falsified by a false signal f_4=0.8, while the conventional control is still used. Under the attack, the output currents of DERs are diversified. Significant deviations from the nominal values can be seen in Fig. 7(c). Accordingly, the output voltages of the DERs exceed the upper limit, as shown in Fig. 7(a). The proposed control is activated at 2.5s. During the period from 2.5s to 4.0s, the state variables and the attack signal are accurately estimated by the DSMO, as shown in Fig. 7(b) and Fig. 7(d). Due to the estimated attack signal is further compensated in the control variable, the output currents of the DERs are controlled in consensus at the nominal values and the output voltages are all controlled within the limits.

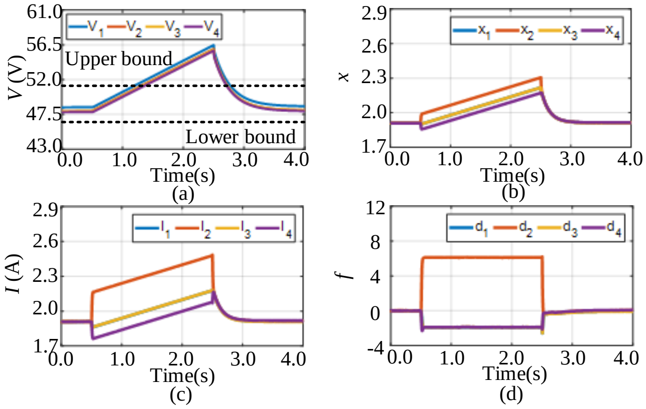


Fig. 7. Waveforms of (a) the output voltages of DERs, (b) the estimated state variables, (c) the output currents of DERs, and (d) the estimated attack signal in case 3.

D. Case 4

Fig. 8 show the waveforms of the output voltages of DERs, the estimated state variables, the output currents of DERs, and the estimated attack signals in case 4. In this case, time-varying false signals, i.e., $f_{4.1}$=20(t−0.5)−20 and $f_{4.2}$=10sin[5π(t−2.5)], are penetrated at 0.5s and 2.5s, respectively. Initially, all the output power of the DERs are controlled in consensus at 91.4W by the conventional secondary control. During the period from 0.5s to 3.5s, due to the injections of the time-varying signals, the output power of the DERs cannot be controlled in consensus. Besides, the output voltages of the DERs exceed both upper and lower limits. By activating the proposed control at 3.5s, the false signals are accurately estimated and compensated during the period from 3.5s to 5s, as shown in Fig. 8(b) and Fig. 8(d). As a result, the bus voltages of the DERs are restored to the references and the output power of the DERs are controlled in the desired consensus.

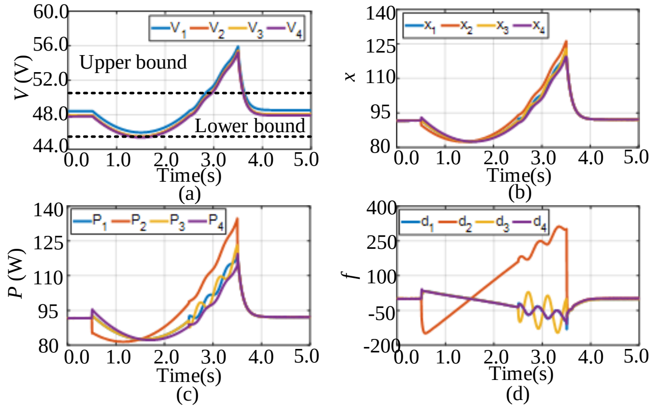


Fig. 8. Waveforms of (a) the output voltages of DERs, (b) the estimated state variables, (c) the output currents of DERs, and (d) the estimated attack signal in case 4.

E. *Case 5*

In case 5, the conventional secondary control is applied during the period from 0s to 2.5s and the proposed control is adopted during the period from 2.5s to 4s. The waveforms of the output voltages of DERs, the estimated state variables, the output currents of DERs, and the estimated attack signal are shown in Fig. 9. During the period from 0s to 0.5s, the output power of the DERs without cyber-attacks are controlled in consensus. The corresponding output voltages are regulated within the limits. However, after the lead node DER1 is attacked by a nonlinear false signal, i.e., f_5=4(t−0.5)^2, at 0.5s, the output power of the DERs are divergent until the adoption of the proposed control at 2.5s. During the period from 2.5s to 4s, the estimated false signal is fed back to the control signal such that the output power of the DERs can be controlled at the nominal values. Accordingly, the output voltages of the DERs can also be regulated within the limits.

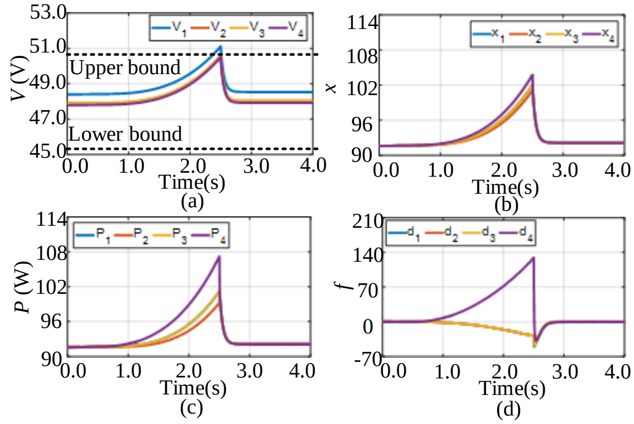


Fig. 9. Waveforms of (a) the output voltages of DERs, (b) the estimated state variables, (c) the output currents of DERs, and (d) the estimated attack signal in case 5.

V. Experimental Verifications

Experiments are conducted on a 48 V DC microgrid with two DERs being connected to the DC bus via non-isolated boost converters, as shown in Fig. 10. DER1 is considered as the leader node and DER 2 is a follower node. The line resistances of the two DER systems are R_1=1.07 Ω and R_2=0.53 Ω, respectively. The load resistance is R_L =49 Ω. The main parameters of the grid-connected boost converters are provided in Table I. The switching frequency is 50 kHz. Details of the attack signals are given in Table IV. All the attacks are constant false signal injection attacks. The upper limits in (8.2) and (8.3) (i.e., ξ and ζ) are 48 and 200 for all the scenarios. The control objectives of the scenarios I and II are bus voltage restoration, while the control objectives of the scenarios III and IV are output current sharing and output power sharing, respectively. The main parameters of the controllers in experiment are provided in Table V. The parameters of the DSMO are B_1=B_2=20, K=3, and χ_1=χ_2=500 for all the scenarios. The control algorithms are implemented using the digital signal processer (DSP) Delfino TMS320F28379D from Texas Instrument.

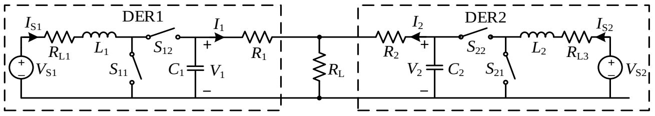


Fig. 10. Circuitry of the DC microgrid with two parallel-connected DER systems in experiment.

TABLE IV. Details of the Attack Signals in Four Scenarios

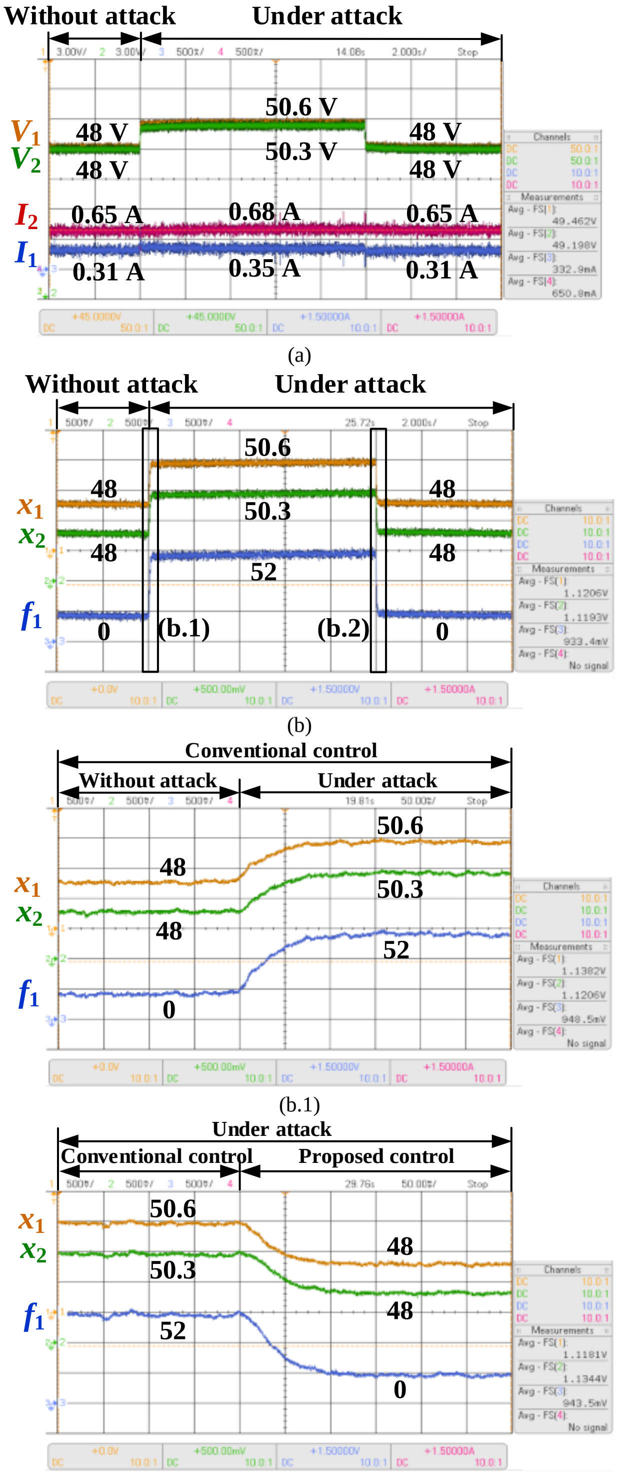
Scenario	Control objectives	Attack positions	Attack values
I	Bus voltage consensus	f_1 at DER1	2.6
II	Bus voltage consensus	f_2 at DER2	−2.5
III	Output current sharing	f_3 at DER1	0.3
IV	Output power sharing	f_4 at DER2	−8

TABLE V. Main Parameters of the Controllers in Experiment

Scenario	PI parameters					
	K_{Pi}	K_{Ii}	K_{P1i}	K_{I1i}	K_{P2i}	K_{I2i}
1	10.0	20.0	0.005	0.1	0.005	0.1
2	10.0	20.0	0.005	0.1	0.005	0.1
3	2.0	4.0	0.005	0.1	0.005	0.1
4	0.005	0.01	0.005	0.1	0.005	0.1

A. Scenario I

In scenario I, the control signal of the DER1 is attacked by a step false signal f_1=2.6 at 4s. The waveforms of the output voltages (i.e., V_1 and V_2) and output currents (i.e., I_1 and I_2) of the DERs are shown in Figs. 11(a). The waveforms of the estimated state variables (i.e., x_1 and x_2) and attack signal (i.e., f_1) are captured in the digital-to-analog (DAC) circuit, as shown in Fig. 11(b). During the period from 0s to 4s, the conventional distributed secondary control is adopted to regulate the output voltages of the DERs without cyber-attacks to track the reference at 48 V. At 4s, the cyber-attack at DER1 occurs. As a result, the output voltage of the DER1 exceeds the upper limit (i.e., V_1=50.6 V). The output currents of the DERs are changed from I_1=0.31 A and I_2=0.65 A to I_1=0.35 A and I_2=0.68 A, respectively. The estimated attack signal, which is amplified by the coefficient B_1, is altered from 0 to 52. The proposed control is adopted from 14s to 20s. During this period, the estimated attack signal is gradually changed from 52 to 0. Both output voltages of the DERs are controlled at the reference. The output currents are regulated at the nominal values (same as the values during the period from 0s to 2s).



(a)

(b)

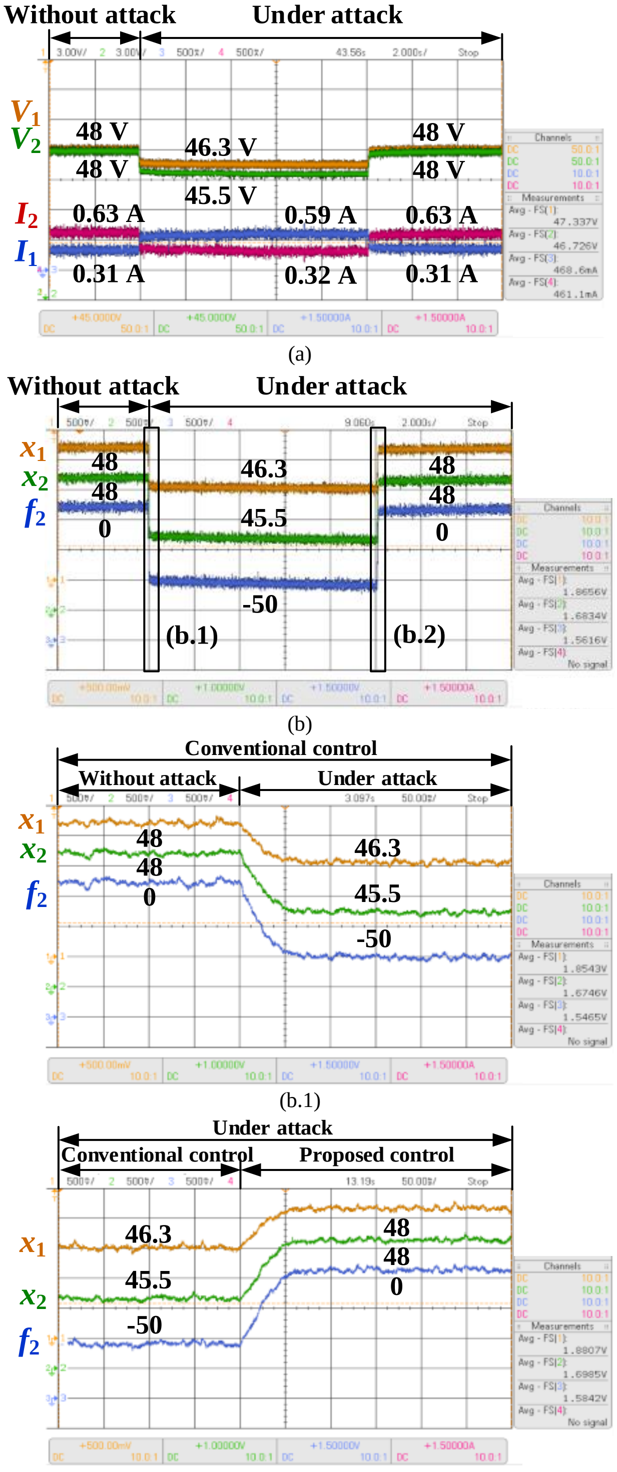
(b.1)

(b.2)

Fig. 11. Waveforms of the (a) output voltages and output currents of the DERs, (b) estimated state variables and false signal in Scenario I.

B. Scenario II

In scenario II, a step false signal f_2=−2.5 is enforced on DER2 at 4s. The waveforms of the output voltages and output currents of the DERs, estimated state variables, and the estimated attack signal are shown in Fig. 12(a) and Fig. 12(b), respectively. The output voltages of the DERs without cyber-attacks are well-regulated to track the reference by the conventional control from 0s to 4s. When the DERs are under cyber-attacks from 4s to 14s, the output voltage of the DER2 exceeds the lower limit (i.e., V_2=45.5 V). The output currents of the DERs are changed from I_1=0.31 A and I_2=0.63 A to I_1=0.59 A and I_2=0.32 A, respectively. The estimated attack signal is altered from 0 to -50. By activating the proposed control at 14s, the estimated attack signal is gradually changed from −50 to 0. Accordingly, the output voltage restorations are achieved and the output currents of the DERs are regulated at the nominal values.



(a)

(b)

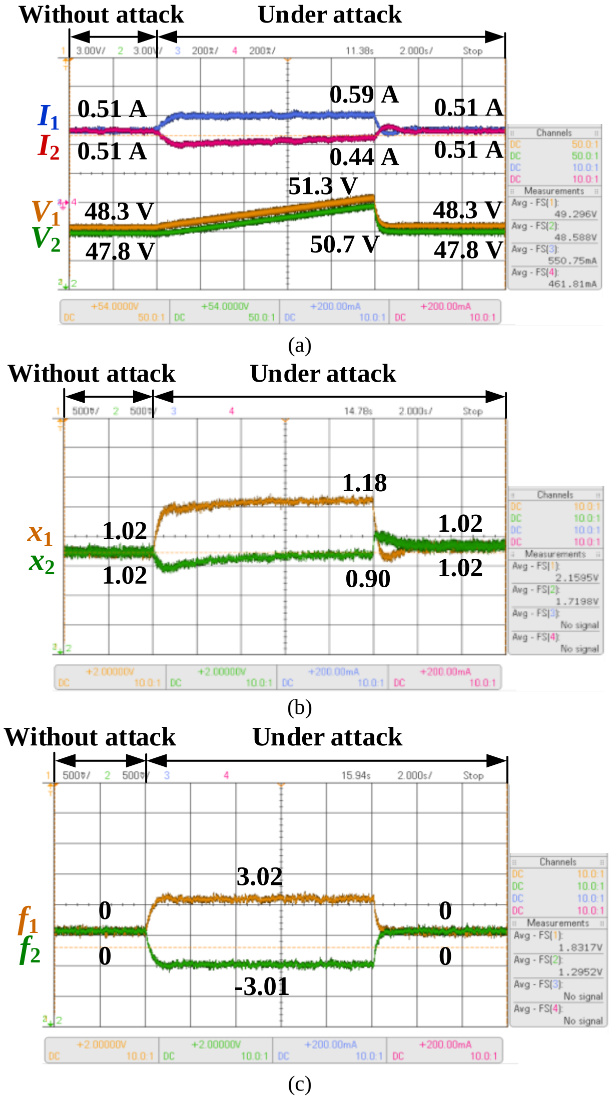
(b.1)

(b.2)

Fig. 12. Waveforms of the (a) output voltages and output currents of the DERs, (b) estimated state variables and attack signal in Scenario II.

C. Scenario III

In Scenario III, a step false signal f_3=0.3 is injected in the control signal of the DER1 at 4s. The conventional secondary control is adopted from 0s to 14s, while the proposed control is adopted from 14s to 20s. The control objective in this scenario is to equally share the output currents of the two DERs. The waveforms of the output voltages and output currents of the DERs, estimated state variables, and estimated attack signals are shown in Fig. 13. By using the conventional control, the output currents of the two DERs under cyber-attacks during the period from 4s to 14s are not in consensus anymore (i.e., I_1=0.59 A and I_2=0.44 A). The corresponding output voltages are increased from V_1=48.3 V and V_2=47.8 V to V_1=51.3 V and V_2=50.7 V, respectively. The estimated attack signals are altered from f_1=f_2=0 to f_1=3.02 and f_2=−3.01. However, by using the proposed control, the estimated attack signals are gradually changed from f_1=3.02 and f_2=−3.01 to f_1=f_2=0. The corresponding output currents of the DERs are controlled in consensus at 0.51 A.



(a)

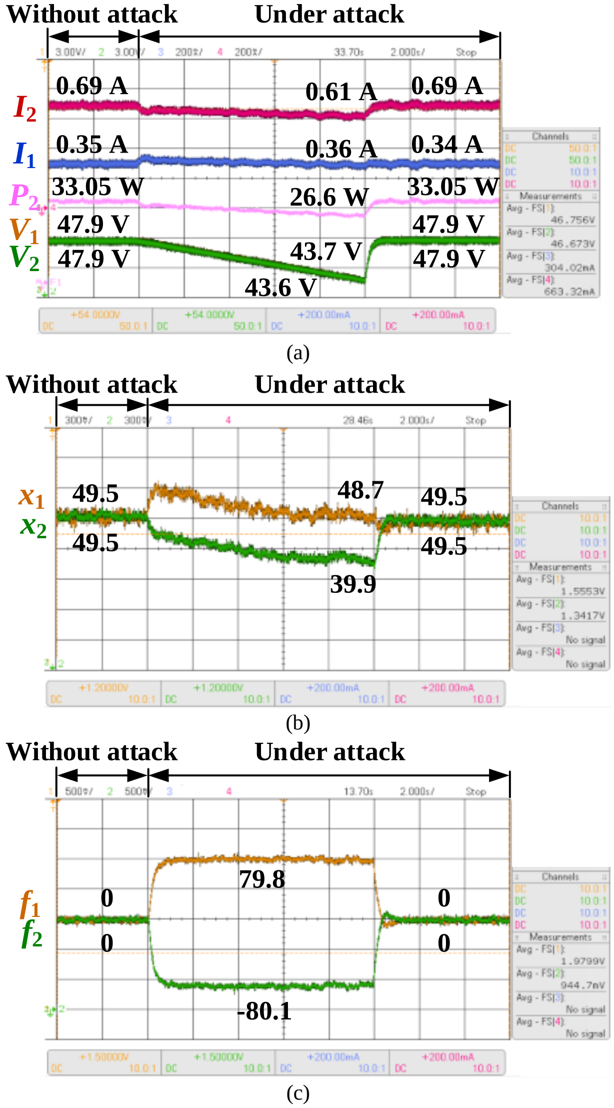
(b)

(c)

Fig. 13. Waveforms of the (a) output voltages and output currents of the DERs, (b) estimated state variables, and (c) attack signals in Scenario III.

D. Scenario IV

In Scenario IV, the DER2 is attacked by a step false signal f_4=−8 at 4s. From 0s to 14s, the conventional secondary control is used. From 14s to 20s, the proposed control is adopted. The control objective in this scenario is to proportionally share the output power of the two DERs by 1:2 (i.e., N_1: N_2 = 1/3: 2/3). The waveforms of the output voltages and output currents of the DERs, output power of the DER2, estimated state variables, and estimated attack signals are shown in Fig. 14. During the period from 0s to 4s, the output power of the DERs are controlled at P_1=16.6 W and P_2=33.05 W. When the false signal is injected at 4s, the output power of both DERs are deviated from the nominal values (i.e., P_1=15.7 W and P_2=26.6 W) and the proportion is no more 1:2 (i.e., 1:1.44). Besides, the output voltages linearly decrease during the period from 4s to 14s. At 14s, the output voltages are decreased to be V_1=43.7 V and V_2=43.6 V, which exceed the lower limit. The estimated attack signals are changed from f_1=f_2=0 to f_1=79.8 and f_2=−80.1. However, by using the proposed control, the estimated attack signals are gradually altered from f_1=79.8 and f_2=−80.1 to f_1=f_2=0. The output power of the DERs are controlled at the nominal values of P_1=16.6 W and P_2=33.05 W. The corresponding output voltages (i.e., V_1=47.9 V and V_2=47.9 V) are well-regulated within the tolerances.



(a)

(b)

(c)

Fig. 14. Waveforms of the (a) output voltages and output currents of the DERs,

(b) estimated state variables, and (c) attack signals in Scenario IV.

VI. Conclusions and Future Work

This paper proposes a DSMO-based secondary control to implement bus voltage restorations and output current/power sharing of DERs in DC microgrids under false signal injection attacks. The proposed DSMO is verified to be strictly stable and can estimate (i) constant or time-varying and (ii) linear or nonlinear false signals accurately. The estimated false signals are further compensated in the control signals of the secondary-layer consensus control which derives adaptive voltage references for the primary-layer local control. Five cases in simulation and four scenarios in experiment have demonstrated that the proposed control strategy can effectively eliminate the negative impact on the DERs in DC microgrids from cyber-attacks. In the future work, the advancements of the proposed control for multiple DERs in large-scale DC microgrids will be conducted.

Appendix

Based on (6), (16) and (17), the dynamics of the estimation errors of the state variables can be derived as

$$\begin{aligned}\dot{\tilde{x}}_i\left(t\right) &= \dot{x}_i(t) - \dot{\hat{x}}_i(t)\\ &= B_i\left\{-\sum\nolimits_{j\neq i}^{n} a_{ij}\left[x_i(t)-x_j(t)\right]-g_i\left[x_i(t)-x_{ref}\,\right]\right]\right\}\\ &\quad -B_i\left\{-\sum\nolimits_{j\neq i}^{n} a_{ij}\left[\hat{x}_i(t)-\hat{x}_j(t)\right]-g_i\left[\hat{x}_i(t)-x_{ref}\,\right]\right]\right\}-B_i\chi_i\mu_i(t)\\ &= B_i\left\{-\sum\nolimits_{j\neq i}^{n} a_{ij}\left[\tilde{x}_i(t)-\tilde{x}_j(t)\right]-g_i\tilde{x}_i(t)\right\}-B_i\chi_i\mu_i(t)\end{aligned} \quad \text{(A1)}$$

By substituting (18) into (A1),

$$\begin{aligned}\dot{\tilde{x}}_i\left(t\right) = B_i&\left\{-\sum\nolimits_{j\neq i}^{n} a_{ij}\left[\tilde{x}_i(t)-\tilde{x}_j(t)\right]-g_i\tilde{x}_i(t)\right\}\\ &-B_i\chi_i K\,\mathrm{sgn}\left\{\sum\nolimits_{j\neq i}^{n} a_{ij}\left[\tilde{x}_i(t)-\tilde{x}_j(t)\right]+g_i\tilde{x}_i(t)\right\}\end{aligned} \quad \text{(A2)}$$

Similarly, the dynamics of the estimation errors of the false signals can be derived based on (17) and (18), as

$$\begin{aligned}\dot{\tilde{f}}_i\left(t\right) &= \dot{f}(t) - \dot{\hat{f}}_i(t)\\ &= \dot{f}(t) - K\,\mathrm{sgn}\left\{\sum\nolimits_{j\neq i}^{n} a_{ij}\left[\tilde{x}_i(t)-\tilde{x}_j(t)\right]+g_i\tilde{x}_i(t)\right\}\end{aligned} \quad \text{(A3)}$$

The derived (A2) and (A3) are (20) and (21) in Section III-B.

References

[1] D. J. Becker and B. J. Sonnenberg, "DC microgrids in buildings and data centers," In *2011 IEEE 33rd International Telecommunications Energy Conference (INTELEC)*, Amsterdam, Netherlands, Oct. 2011, pp. 1-7.

[2] L. Meng, T. Dragičević, J. C. Vasquez, and J. M. Guerrero, "Tertiary and secondary control levels for efficiency optimization and system damping in droop controlled DC–DC converters," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2615-2626, Jun. 2015.

[3] J. Ma, F. He, and Z. Zhao, "Line loss optimization based OPF strategy by hierarchical control for DC microgrid," in *Proc. 2015 IEEE Energy Conversion Congress & Expo. (ECCE)*, Montreal, Canada, Sept. 2015, pp. 6212-6212.

[4] M. K. Zadeh, R. Gavagsaz-Ghoachani, S. Pierfederici, B. Nahid-Mobarakeh, and M. Molinas, "Stability analysis and dynamic performance evaluation of a power electronics-based DC distribution system with active stabilizer," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 4, no. 1, pp. 93-102, Mar. 2016.

[5] K. Natori, T. Tanaka, Y. Takahashi, and Y. Sato, "A study on high-efficiency floating multi-terminal power flow controller for next generation DC power networks," in *Proc. 2017 IEEE Energy Conversion Congress & Expo. (ECCE)*, Cincinnati, USA, Oct. 2017, pp. 2631-2637.

[6] Y. Yang, K. T. Mok, S. C. Tan, and S. Y. R. Hui, "Nonlinear dynamic power tracking of low-power wind energy conversion system," *IEEE Trans. Power Electron*., vol. 30, no. 9, pp. 5223-5236, Sept. 2019.

[7] Q. C. Zhong, "Robust droop controller for accurate proportional load sharing among inverters operated in parallel," *IEEE Trans. Ind. Electron*., vol. 60, no. 4, pp. 1281-1290. Apr. 2013.

[8] Y. Yang, S. C. Tan, and S. Y. R. Hui, "Enhanced digital PI control with state-variable feedback loop for DC electric spring," in *Applied Power Electronics Conference and Exposition (APEC)*, Tampa, FL, Mar. 2017, pp. 1242-1247.

[9] P. Prabhakaran, Y. Goyal, and V. Agarwal, "Novel nonlinear droop control techniques to overcome the load sharing and voltage regulation issues in DC microgrid," *IEEE Trans. Power Electron.*, vol. 33, no. 5, pp. 4477-4487, May 2018.

[10] Y. Jiang, Y. Yang, S. C. Tan, and S. Y. R. Hui, "Adaptive current sharing of distributed battery systems in DC microgrids using adaptive virtual resistance-based droop control," in *Energy Conversion Congress and Exposition (ECCE)*, Baltimore, MD, Sept. 2019, pp. 4262-4267.

[11] C. Persis, E. Weitenberg, and F. Dörfler, "A power consensus algorithm for DC microgrids," *Automatica*, vol. 89, pp. 364-375, Mar. 2018.

[12] Y. Yang, S. C. Tan, and S. Y. R. Hui, "Efficient improvement of photovoltaic-battery systems in standalone DC microgrids using a local hierarchical control for the battery system," *IEEE Trans. Power Electron.*, vol. 34, no. 11, pp. 10796-10807, Nov. 2019.

[13] Y. Yang, S. C. Tan, and S. Y. R. Hui, "Mitigating distribution power loss of DC microgrids with DC electric springs," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5897-5906, Nov. 2018.

[14] J. Deng, Y. Mao, and Y. Yang, "Distribution power loss reduction of standalone DC microgrids using adaptive differential evolution-based control for distributed battery systems," *Energies*, vol. 13, no. 9, pp. 2129, Jan. 2020.

[15] X. Qian, Y. Yang, C. Li, and S. C. Tan, "Operating cost reduction of DC microgrids under real-time pricing using adaptive differential evolution algorithm," *IEEE Access*, vol. 8, pp. 169247-169258, Sept. 2020.

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

[17] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[18] J. Hao, E. Kang, J. Sun, Z. Wang, Z. Meng, X. Li, and Z. Ming, "An adaptive markov strategy for defending smart grid false data injection from malicious attackers," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2398–2408, Jul. 2018.

[19] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "Distributed load sharing under false data injection attack in inverter-based microgrid," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1543–1551, Feb. 2019.

[20] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731–6741, Nov. 2018.

[21] P. Li, Y. Liu, H. Xin, and X. Jiang, "A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks," *IEEE Trans. Ind. Inform.*, vol. 14, no. 10, pp. 4343–4352, Oct. 2018.

[22] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Net. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[23] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731-6741, Nov. 2018.

[24] S. Abhinav, H. Modares, F. L. Lewis and A. Davoudi, "Resilient cooperative control of dc microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 1083-1085, Jan. 2019.

[25] J. Duan and M. Chow, "A resilient consensus-based distributed energy management algorithm against data integrity attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4729-4740, Sep. 2019.

[26] H. Wang, Z. Yan, X. Xu, and K. He, "Probabilistic power low analysis of microgrid with renewable energy," *Int. J. Elect. Power Energy Syst.*, vol. 114, Jan. 2020.

[27] H. Wang, Z. Yan, M. Shahidehpour, X. Xu, and Q. Zhou, "Quantitative evaluations of uncertainties in multivariate operations of microgrids," *IEEE Trans. Smart Grid*, vo. 11, no. 4, Jul. 2020.

[28] L. Lu, H. J. Liu, H. Zhu and C. Chu, “Intrusion detection in distributed frequency control of isolated microgrids,” *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6502-6515, Nov. 2019.

[29] S. Abhinav, I. D. Schizas, F. L. Lewis and A. Davoudi, “Distributed noise resilient networked synchrony of active distribution systems,” *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 836-846, Mar. 2018.

[30] T. Kailath, “Linear Systems,” Englewood Cliffs, NJ, USA: Prentice-Hall, 1980.

[31] R. Olfati-Saber, J. Fax, and R. M. Murray, “Consensus and cooperation in networked multi-agent systems,” *Proc. IEEE*, vol. 95, no. 1, pp. 215-233, Jan. 2007.

[32] M. Shi, X. Chen, J. Zhou, et. al., “Distributed optimal control of energy storages in a DC microgrid with communication delay,” *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2033-2042, May 2020.

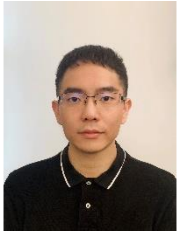
[33] F. L., Lewis, H., Zhang, K., Hengster-Movric, and A. Das, “Cooperative control of multi-agent systems: optimal and adaptive design approaches,” Springer Science & Business Media, (2013).

[34] L. Chen, Y. Wang, X. Lu, et. al., “Resilient active power sharing in autonomous microgrids using pinning-consensus-based distributed control,” *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6802-6811, Nov. 2019.

[35] K. Manandhar, X. Cao, F. Hu, and Y. Liu, “Detection of faults and attacks including false data injection attack in smart grid using Kalman filter,” *IEEE Trans. Contr. Net. Syst.*, vol. 1, no. 4, pp. 370-379, Dec. 2014.

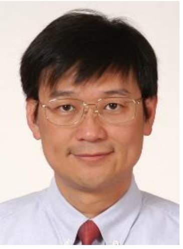
[36] Y. Jiang, W. Xu, C. Mu, and Y. Liu, “Improved deadbeat predictive current control combined sliding mode strategy for PMSM drive system,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 251-263, Jan. 2018.

Yajie Jiang received the B.Eng. degree from the School of Electrical Engineering, Zhengzhou University, Zhengzhou, China in 2015 and the M.Eng. degree in the School of Electrical and Electronic Engineering, Huazhong University of Science and Technology, Wuhan, China in 2018. He is currently pursuing the Ph.D. degree in the Department of Electrical and Electronic Engineering, the University of Hong Kong. His research interests include smart grid and machine drive.



Yun Yang (M’18) received his B.Sc. degree in Electrical Engineering from Wuhan University in 2012 and Ph.D. degree in Electrical Engineering from The University of Hong Kong in 2017. He then became a Postdoctoral-Fellow in the same research group. Now, he is a Research Assistant Professor in the Department of Electrical Engineering, the Hong Kong Polytechnic University and an Honorary Research Assistant Professor in the Department of Electrical and Electronic Engineering, the University of Hong Kong. He has authored or coauthored more than 40 technical papers, including 10 leading journals published as the first author. He also has two book chapters and two U.S. patent applications. His research interests include wireless power transfer, microgrid, power electronics and control.

Siew-Chong Tan (M’06–SM’11) received the B.Eng. (Hons.) and M.Eng. degrees in electrical and computer engineering from the National University of Singapore, Singapore, in 2000 and 2002, respectively, and the Ph.D. degree in electronic and information engineering from the Hong Kong Polytechnic University, Hong Kong, in 2005. He is currently a Professor in Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong. Prof. Tan was a Visiting Scholar at Grainger Center for Electric Machinery and Electromechanics, University of Illinois at Urbana-Champaign, Champaign, from September to October 2009, and an Invited Academic Visitor of Huazhong University of Science and Technology, Wuhan, China, in December 2011. His research interests are focused in the areas of power electronics and control, LED lightings, smart grids, and clean energy technologies.



S. Y. (Ron) Hui (M’87-SM’94-F’03) received his BSc (Eng) Hons in Electrical and Electronic Engineering at the University of Birmingham in 1984 and a D.I.C. and PhD in Electrical Engineering at Imperial College London in 1987. Presently, he holds the Philip Wong Wilson Wong Chair Professorship at the University of Hong Kong and a Chair Professorship at Imperial College London.

He has published over 450 research papers including 280 refereed journal publications. Over 60 of his patents have been adopted by industry. His research interests include power electronics, wireless power, sustainable lighting and smart grid. His inventions on wireless charging platform technology underpin key dimensions of Qi, the world's first wireless power standard, with freedom of positioning and localized charging features for wireless charging of consumer electronics. He also developed the Photo-Electro-Thermal Theory for LED Systems. He received the IEEE Rudolf Chope R&D Award and the IET Achievement Medal (The Crompton Medal) in 2010 and IEEE William E. Newell Power Electronics Award in 2015. He is a Fellow of the Australian Academy of Technological Sciences & Engineering, US National Academy of Inventors and Royal Academy of Engineering, U.K.