Distributed Higher Order Differentiator-Based Distributed Secondary Control for DC Microgrids Under Cyber-Attacks

Yajie Jiang[1], Yun Yang[2], Siew-Chong Tan[3], and Shu-Yuen Ron Hui[4]
[1,3,4]Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong, China
[2]Department of Electrical Engineering, The Hong Kong Polytechnic University, Hong Kong, China
[4]Department of Electrical and Electronic Engineering, Imperial College London, London, U.K.
Email: yjjiang@eee.hku.hk[1], cacaloto@hku.hk[2], sctan@eee.hku.hk[3], ronhui@eee.hku.hk[4].

Abstract –The conventional distributed secondary control is widely adopted for distributed energy resources (DERs) to implement bus voltage restorations and output currents/powers sharing in DC microgrids. However, when the DERs are under cyber-attacks, the control variables of the conventional distributed secondary control will deviate from the nominal values such that the control objectives cannot be achieved any more. More seriously, the stability of the DC microgrid may also be threatened by the intrusive cyber-attacks. To this end, a distributed higher order differentiator (DHOD)-based distributed secondary control is proposed in this paper. The DHOD detects the attack signals based on local and neighboring measurements. The estimated attack-signals in the DHOD are further compensated by the control variables of the distributed secondary control to eliminate the negative impact from the cyber-attacks. The stability of the DHOD are verified by the convergence of its state variables. Case studies in simulation have validated that the proposed DHOD-based distributed secondary control can affectively regulate the DERs to track the references of bus voltages and output currents/powers sharing in DC microgrids under various types of cyber-attacks.

Keywords **-Cyber-attacks, DC microgrid, distributed energy resource (DER), distributed high order differentiator (DHOD), distributed secondary control.**

I. Introduction

With a high penetration of power electronics interfaced distributed energy resources (DERs) in DC microgrid, the distribution loss is an increasingly prominent problem, especially in medium- and long-distance low-voltage networks [1]–[6]. In DC microgrids, distributed secondary control has been widely adopted to achieve voltage restoration [7-9], load sharing [9, 10], energy balancing [11, 12], and power loss reduction [12-14], and economic dispatch [15] for DERs However, those conventional distributed secondary control are based on the communication between the two neighboring units, which are vulnerable under 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 can lead to the bus voltage deviations, sharing errors of the output currents and output powers, and even instability of the entire microgrid.

To this end, Kalman-filter-based feedback control and trust/reputation-based control are primarily investigated to eliminate the negative impacts of the attack signals [18-21]. Besides, an efficient density-based global sensitivity analysis is presented to quantify the impacts of variable attack signals on microgrid operations [22, 23]. The analysis can identify the critical attacks on the DERs with limited sensors and eliminate the adverse impacts based on the accurate observers. In [24], constant malicious cyber-attacks are imposed on the control variables to alter the operating points of the microgrid. A trust/confidence-based control is designed to detect the cyber-attacks. The merit of this control scheme is that the inconspicuous malicious cyber-attacks can be compensated. However, the computation burden of this method is relatively higher than the traditional methods. In [25], a noise filtration technique with certain statistical properties is proposed to address time-varying attack signals. Nevertheless, this method is invalidated against cyber-attacks based on full knowledge of physical-cyber networks.

In this paper, a distributed higher order differentiator (DHOD)-based distributed secondary control is proposed for the DER systems to implement bus voltage regulations and output currents/powers sharing in DC microgrids under cyber-attacks. The DHOD is designed based on the extended state observer technique to detect and compensate the attack signals into the control variables of the distributed secondary control. Compared with the conventional first order observer, high order differentiator has advantages of chattering suppression and excellent dynamic performance. The existing hardware of the conventional distributed secondary control can be directly used by the DHOD 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 defended attack signals in this paper cover both constant attack signals and time-varying attack signals on either leader nodes or follower nodes. several case studies on different control objectives and attack signals are conducted in both simulation and experiment to validate the effectiveness of the proposed DHOD-based distributed secondary control to guard the DER systems from the cyber-attacks in DC microgrids.

II. Preliminary of Distributed Secondary Control and Attack

A. Graph theory

The cyber network of the DC microgrid with n converters can be modeled by a directed graph $G_n = (V_n, E_n)$. The converters and the communication links are regarded as the nodes and edges in the graph, respectively. A directed graph is determined by a set of nodes $V_n = \{1, 2, \ldots, n\}$ and a set of edges $E_n = V_n \times V_n$. 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_n, i.e., $(i, i) \notin E$. For each $i \in V_n$, let $V_i = \{j: (j, i) \in E_n\}$ be the set of nodes providing data information to the node i. The adjacency matrix of the directed graph is defined as $\mathbf{A}=[a_{ij}]_{i,j=1}^{n}\in \mathrm{R}^{n\times n}$, where a_{ij} > 0 if (i; j) ∈ E_n and a_{ij} = 0 otherwise. The in-degree matrix of the directed graph $\mathbf{D}^{in}=diag\{d_i^{in}\}$ satisfies the in-degree of the node i $d_i^{in}=\sum_{j\in V}a_{ij}$. Then, Laplacian matrix can be defined as $\mathbf{L}$ = [l_{ij}] ∈ $R^{n\times n}$ can be obtained by $\mathbf{L}$ = $\mathbf{D}^{in}$ - $\mathbf{A}$. The eigenvalues of the Laplacian matrix determine the dynamic performance DER systems with communication in the DC microgrid. If a_{ij} = a_{ji} is satisfied for all i and j in the graph, the corresponding Laplacian matrix is balanced. A directed path is a sequence of edges from a node to the other. A directed graph is called connected when there is always at least one directed path between two arbitrary nodes. If a directed graph has a directed spanning tree, it means that it contains at least one root node which can reach all the other nodes via directed paths.

B. *Distributed secondary control for DC microgrid*

A typical architecture of a single-bus DC microgrid is shown in Fig. 1. It comprises distributed generation (DG) units, loads, ESS, and power electronics interfaces. The wind turbine and solar PV panels serve as clean energy. DC resistive loads such as water heater can be directly connected to DC bus. The constant power load (CPL), i.e., motor drive system, is also considered in the figure. The ESS is introduced to compensate power and alleviate bus voltage fluctuations.

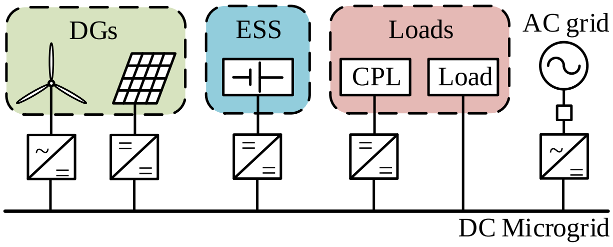


Fig. 1. Configuration of DC microgrid.

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

$$V_{\mathrm{ref}i}=V_{\mathrm{nom}}-R_{\mathrm{d}i}I_i \tag{1}$$

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. However, the droop control alone may result in bus voltage deviations and load sharing errors. To this end, a secondary-layer control is generally adopted in the conventional distributed control to implement bus voltage restoration of DERs at the rated value as

$$\lim_{t\to\infty}V_i\to V_{\mathrm{nom}},\forall i=1,\ldots,n \tag{2}$$

where V_i, is the output voltage of the i-th DER. Another control objective is the proportional output current/power sharing among the DERs as

$$I_i/N_i{=}I_j/N_j,\forall i,j=1,\ldots,n \tag{3.1}$$

$$P_i/N_i{=}P_j/N_j,\forall i,j=1,\ldots,n \tag{3.2}$$

where I_i and I_j are the output currents of the i-th and j-th DERs, P_i and P_j are the output powers of the i-th and j-th DERs, N_1, N_2, … , N_n are the allocation coefficients. By synthesizing the output voltage and output current/power as a control variable x_i, the dynamics of the DER systems can be given as

$$\dot{x}_i(t)=B_iu_i(t) \tag{4}$$

where $u_i(t)$ is the control input and B_i is the control coefficient. To achieve bus voltage restoration, the V_{nom} is often used in some nodes (leader nodes) as the voltage reference. The nodes connected to the leader node and the corresponding connecting edges are called pinned nodes and pinning edges, respectively. A gain is assigned to each pinning edge, e.g., g_i is the pinning gain from the leader to the node i. The pinning gain is zero for an unpinned node. g_i is an indicator to distinguish that the i-th DER is modelled as 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 pinning gain matrix is $\mathbf{G}$ = diag{g_i}. The distributed secondary control can be designed as

$$u_i(t)=-\sum_{j=1}^{n}a_{ij}(x_i(t)-x_j(t))-g_i(x_i(t)-x_{\mathrm{ref}}) \tag{5}$$

where x_{ref} is the reference of the state variables. a_{ij} is the consensus coefficient. The follower nodes are only controlled to achieve consensus of state variable, whereas the lead nodes are also required to track the given references.

It has been proved that all nodes can reach a consensus heading equaling to the initial heading of the leader nodes as [26]

$$\lim_{t\to\infty}\left\|x_i(t)-x_j(t)\right\|=0,\forall i,j=1,\ldots,n \tag{6}$$

A comprehensive control block diagram of the proposed secondary control scheme is depicted in Fig. 2. The proposed control is a hierarchical control, which consists of two layers. In the primary layer, a conventional droop control provides output voltage references of the DERs for the inner-loop voltage and current control. The primary-layer controls are local controls that are independent on the communication. In the secondary layer, a consensus control based on the exchanged information from the neighboring DERs is adopted to provide adaptive voltage references for the conventional droop control.

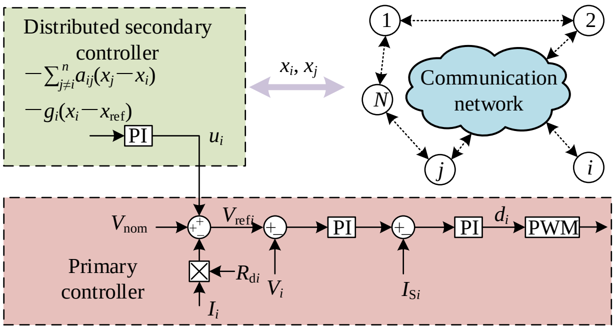


Fig. 2. Control diagram of the distributed secondary control scheme.

Due to the secondary control are widely implemented in embedded controllers with communication, the actuator and data transmission process are vulnerable to cyber-attacks. The attacks may not only variate the bus voltages and output currents of DERs, but also result in the violations of the power limit and stability of entire DC microgrid operations.

C. *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. 3. The attack signals are modeled as a finite superposition of step, sinusoidal, and ramp signals [27], which only falsify the control variables of the distributed secondary control. The attack signal is defined as

$$f_i(t)=\begin{cases}\xi_i & i=1,\ldots,l\\ \zeta_i & i=l+1,\ldots,n\end{cases} \tag{7}$$

where ξ_i is the attack signal on the *i*-th leader node and ζ_i is the attach signal of the *i*-th follower node. Additionally, it satisfies the following assumptions.

Assumption 1: Fault/attack signal and its derivation are bounded.

Assumption 2*:* The attacker does not send on/off commands to the actuators.

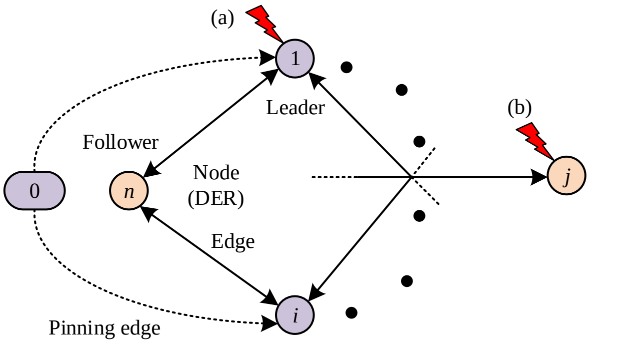


Fig. 3. Potential cyber-attacks on (a) leader nodes or (b) follower nodes in a DC microgrid.

1) Cyber-attacks on leader nodes

When cyber-attacks are conducted on leader nodes, the distributed secondary control for pinned DERs are given as

$$u_i'(t)=-\sum\nolimits_{j\neq i}^{n}a_{ij}(x_i(t)-x_j(t))-g_i\sum\nolimits_{j=1}^{n}(x_i(t)-(x_{\mathrm{ref}}+\xi_i)) \tag{8}$$

By defining the difference between the state variable x_i and the reference x_{ref} as the state variable error e_i (i.e., $e_i = x_i - x_{ref}$) and assuming that the first l DERs are selected to be pinned, the dynamics of the state variable errors with cyber-attacks on the leader nodes can be expressed as

$$\dot{\mathbf{e}}(t)=-(\mathbf{L}+\mathbf{G})\mathbf{e}(t)+\mathbf{G}\boldsymbol{\xi}(t) \tag{9}$$

where $\mathbf{L}$ is the Laplacian matrix of the communication network, $\boldsymbol{\xi}$ = (ξ_1, ξ_2, …, ξ_n) in which $\xi_i \neq 0$ if and only if the communication link from the controller of leader node to the *i*-th pinned DER is corrupted. Accordingly, the dynamics of state variable errors can be derived as

$$\mathbf{e}(t)=exp^{-(\mathbf{L}+\mathbf{G})t}\mathbf{e}(t_0)+\int_{t_0}^{t}e^{-(\mathbf{L}+\mathbf{G})(t-\tau)}\mathbf{G}\boldsymbol{\xi}(\tau)d\tau \tag{10}$$

where *exp* denotes the exponential function. Since the matrix – (**L** + **G**) is negative-definite and invertible, the first term in (11) is converged to zero. Without the loss of generality, all the cyber-attacks on the leader nodes are assumed to be positive (i.e., $\xi_i > \xi_0 > 0$, $\forall\ i \in n$). Apparently, due to the elements of the pinning matrix **G** are non-negative, the state variable errors **e**(*t*) in (10) cannot be converged to zero as

$$\begin{aligned}\lim_{t\to\infty}\mathbf{e}(t)&=\lim_{t\to\infty}\int_{t_0}^{t}exp^{-(\mathbf{L}+\mathbf{G})(t-\tau)}\mathbf{G}\boldsymbol{\xi}(\tau)d\tau\\&>\lim_{t\to\infty}exp^{-(\mathbf{L}+\mathbf{G})t}[exp^{(\mathbf{L}+\mathbf{G})t}-exp^{(\mathbf{L}+\mathbf{G})t_0}](\mathbf{L}+\mathbf{G})^{-1}\mathbf{G}\boldsymbol{\xi}_0\\&=(\mathbf{L}+\mathbf{G})^{-1}\mathbf{G}\boldsymbol{\xi}_0\geq 0\end{aligned} \tag{11}$$

2) Cyber-attacks on follower nodes

when cyber-attacks are conducted on follower nodes, the distributed secondary control for the *i*-th DER and its neighboring nodes are given as

$$\begin{aligned}u_i''&=-\sum\nolimits_{j\neq i}^{n}a_{ij}((x_i-\eta_i)-x_j)-g_i((x_i-\zeta_i)-x_{\mathrm{ref}})\\u_j''&=-\sum\nolimits_{k\neq j}^{n}a_{jk}((x_j-x_k)-(x_j-(x_i-\zeta_i))-g_j(x_j-x_{\mathrm{ref}})\end{aligned} \tag{12}$$

Accordingly, the dynamics of state variable errors with attacks on follower controllers can be expressed as

$$\dot{\mathbf{e}}(t)=-(\mathbf{L}+\mathbf{G})\mathbf{e}(t)+(\mathbf{L}+\mathbf{G})\boldsymbol{\zeta}(t) \tag{13}$$

where ζ = (ζ_1, ζ_2, …, ζ_n). Similarly, the attack signals imposed on follower controller are positive (i.e., $\zeta_i > \zeta_0 > 0$, $\forall i \in n$). The state variable errors cannot converge to zero under the cyber-attack on the follower nodes, which is validated by

$$\begin{aligned}\lim_{t\to\infty}\mathbf{e}(t)&=\lim_{t\to\infty}\int_{t_0}^{t}exp^{-(\mathbf{L}+\mathbf{G})(t-\tau)}(\mathbf{L}+\mathbf{G})\boldsymbol{\zeta}(\tau)d\tau\\&>\lim_{t\to\infty}exp^{-(\mathbf{L}+\mathbf{G})t}[exp^{(\mathbf{L}+\mathbf{G})t}-exp^{(\mathbf{L}+\mathbf{G})t_0}](\mathbf{L}+\mathbf{G})^{-1}(\mathbf{L}+\mathbf{G})\boldsymbol{\zeta}_0\\&=\boldsymbol{\zeta}_0\geq 0\end{aligned} \tag{14}$$

Due to the cyber-attacks on the leader nodes and follower nodes can result in non-convergence of state variable errors, the performance of the distributed secondary control for the voltage restoration and proportional current/power sharing among DERs may be deteriorated.

III. DHOD-Based Distributed Secondary Control

Meanwhile, compared with the conventional first order observer, high order differentiator has advantages of chattering suppression and excellent dynamic performance. The high order differentiator has also been used for estimating derivatives of unknown variables in many industrial applications, especially in mechanical systems [28]. To enhance the robustness of distributed secondary control, a DHOD is incorporated into the control to estimate and compensate the attack signals. Based on system dynamics (4), if the *i*-th DER is suffered from cyber-attacks, its dynamics can be modified as

$$\dot{x}_i(t)=B_i[u_i(t)+f_i(t)] \tag{15}$$

Then, a DHOD based on the extended state observer technique can be designed as [28]

$$\begin{cases}\dot{\hat{x}}_i(t)=B_iu_i(t)+v_0\\ v_0=-\eta_0K^{\frac{1}{3}}\left|e_i\right|^{\frac{2}{3}}\mathrm{sgn}(e_i)+\hat{f}_i\\ \dot{\hat{f}}_i=v_1\\ v_1=-\eta_1K^{\frac{1}{2}}\left|\hat{f}_i-v_0\right|^{\frac{1}{2}}\mathrm{sgn}(\hat{f}_i-v_0)+z\\ \dot{z}=-\eta_2K\,\mathrm{sgn}(z-v_1)\end{cases} \tag{16.1}$$

where $\hat{x}_i$ and $\hat{f}_i$ are the estimated state variables and attack signals of the *i*-th DER, sgn() stands for the sign function. η_0, η_1, η_2 and K are the observer coefficients, z, v_0 and v_1 are the intermediate variables.

$$e_i(t)=\sum\nolimits_{j\neq i}^{n}a_{ij}\left[\tilde{x}_i(t)-\tilde{x}_j(t)\right]+g_i\tilde{x}_i(t) \tag{16.2}$$

$\tilde{x}_i = x_i(t) - \hat{x}_i(t)$. $\tilde{x}_j = x_j(t) - \hat{x}_j(t)$ are the observation errors of the *i*-th and *j*-th DERs. Apparently, if the *i*-th DER is under attack, the estimated state variable $\hat{x}_i$ is biased, as compared to the measured x_i. The difference between $\hat{x}_i$ and x_i can lead to the change of $\mu_i(t)$, which further updates the estimated attack signals to ensure the accuracy of the observer. Similarly, 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 DHOD in (17) can adaptively estimate both state variables and variable attack signals. By substituting the estimated state variables and attack signals into the distributed secondary control in (6), the control variable of the DHOD-based distributed secondary control can be designed as

$$u_i^{'''}(t) = -\sum\nolimits_{j\neq i}^{n} a_{ij}\left[\hat{x}_i(t) - \hat{x}_j(t)\right] - g_i\left[\hat{x}_i(t) - x_{ref}\right] - \hat{f}_i(t) \quad (18)$$

Here, the estimated attack signal is included to compensate the actual attack signal on the control variable. The control block diagram of the DHOD-based distributed secondary control is depicted in Fig. 3. The stability analysis of high order differentiator can be found in [28] and [29].

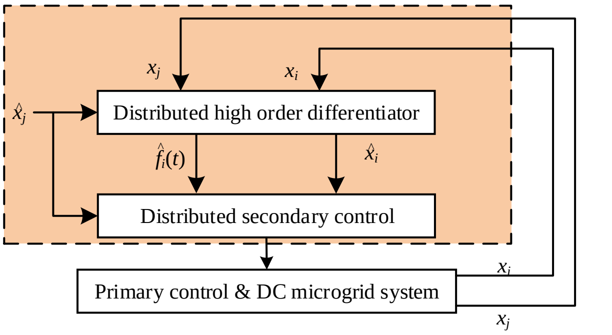
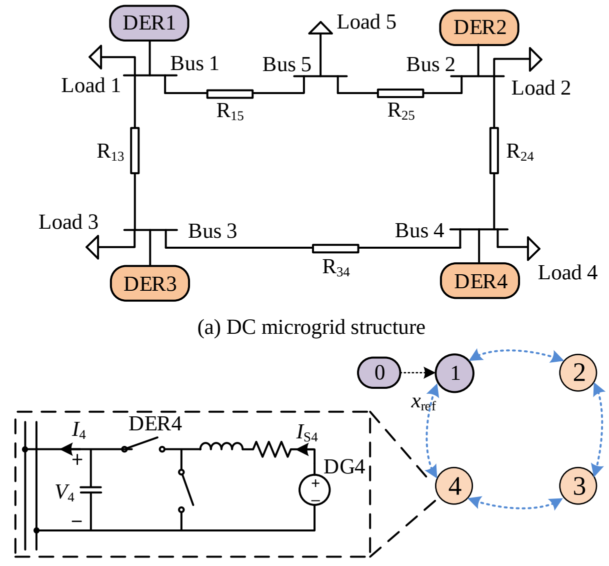

x_j
x_i
$\hat{x}_j$
Distributed high order differentiator
$\hat{f}_i(t)$
$\hat{x}_i$
Distributed secondary control
Primary control & DC microgrid system
x_i
x_j

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

IV. Case Studies

The DHOD-based distributed secondary control is verified based on a 48 V five-bus DC microgrid with four DERs in Matlab/Simulink. The structure of the DC microgrid is shown in Fig. 4(a). Each DER consists of a DC renewable source and a non-isolated bidirectional DC/DC converter. The communication network of the DC microgrid is depicted in Fig. 4(b), which is modelled as four nodes being strongly connected. In Fig. 4(b), 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 control scheme for each DER system are presented in Figs. 2 and 3, which comprises a DHOD-distributed secondary control and a local primary control. The control parameters of the local primary control 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
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 ($R_{\mathrm{L}i}$)	0.1 Ω
Output capacitances of the converter (C_i)	10.1 μF
Output capacitances of the switches ($C_{\mathrm{s}i}$)	102 pF
ON resistances of the switches ($R_{\mathrm{s}i}$)	72 mΩ

To verify the effectiveness of the proposed DHOD-based distributed secondary control against cyber-attacks on the DER systems, four different cases are carried out in simulation. In the cases 1 and 2, the proposed control for voltage restoration of the microgrid under cyber-attacks are studied. In the case 3, the proposed control for proportional load current sharing among the DERs under cyber-attacks are investigated. In the case 4, the proposed control for average load power sharing among the DERs under cyber-attacks is presented. Different attack signals, including constant attack signals and time-varying attack signals, on different DERs are investigated in the four cases, as provided in Table II and Fig. 5. The sampling frequency of the controllers is 100 kHz. The coefficients of the DHOD are K = 10000, η_0 = 3, η_1 = 1.5, and η_2 = 1.1.

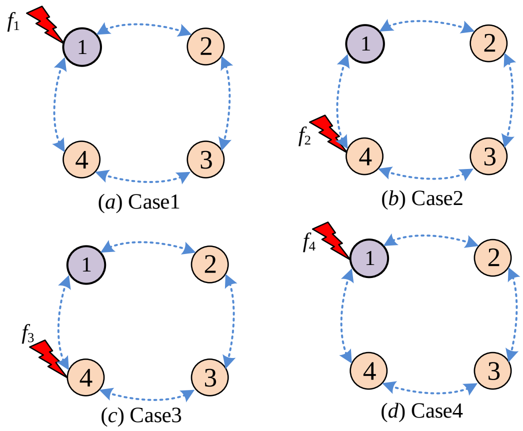


Fig. 5. Attack modes of the cases in simulation.

TABLE II. ATTACK SIGNALS OF DIFFERENT CASES IN SIMULATION

Cases	Attacks	Values
Case 1	f_1 at DER1	$1.6(t-0.5)$
Case 2	f_2 at DER4	-1.5
Case 3	f_3 at DER3	$-16(t-0.5)+16$
Case 4	f_4 at DER2	$30\sin(5.5\pi(t+2.5))$

A. Case 1

Fig. 6 show the waveforms of the output voltages of DERs, the output currents of DERs, the estimated state variables, and the estimated attack signal during the period from 0 s to 4 s in case 1. From 0 s to 0.5 s, only conventional distributed secondary control is adopted for the four DERs while no cyber signals attack the nodes. Apparently, all the bus voltages are controlled in consensus at 48 V. At 0.5 s, the leader node DER1 is attacked by the signal $f_1 = 1.6(t-0.5)$ while the attack is not compensated. Consequently, the leader node voltage deviates from the reference. Since the conventional consensus-based secondary control is still adopted for the four DERs, all the follower node voltages are converged to the leader node voltage, which exceeds the lower limit of the bus voltage. The cyber-attacks cause unsafe operations of the microgrid. The proposed control by DHOD is activated at 2.5 s. During the period from 2.5 s to 4.0 s, the attack signal is estimated and compensated in the control feedback. As a result, the bus voltages and the output currents of the DERs are restored to the nominal values.

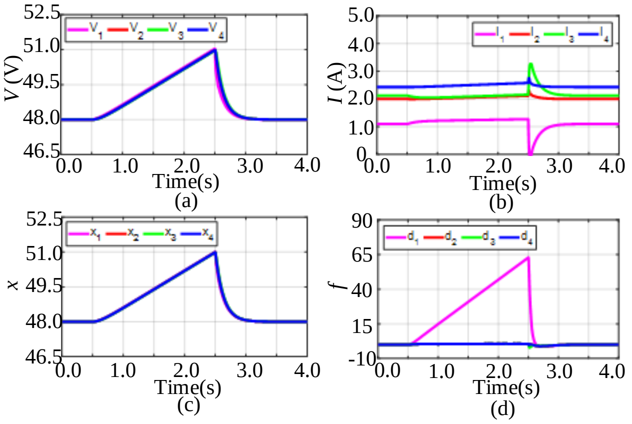


Fig. 6. Waveforms of (a) the output voltages of DERs, (b) the output currents of DERs, (c) the estimated state variables, and (d) the estimated attack signal in case 1.

B. Case 2

The waveforms of the output voltages of DERs, the output currents of DERs, the estimated state variables, and the estimated attack signal in case 2 are shown in Fig. 7. The DER4, which is a follower node, is attacked by the signal $f_2 = -1.5$ at 0.5 s. During the period from 0 s to 0.5 s, without cyber-attacks, the bus voltages are controlled by the conventional distributed secondary control to track the reference. During the period from 0.5 s to 2.5 s, the DER4 is attacked. As a result, the bus voltage of the DERs exceeds the lower limit. Due to the attacked DER4 is a follower node, the bus voltages of the DERs are different from each other under attack, which means the output currents of the DERs will deviate from the nominal values, as can see in Fig. 7(b). During the period from 2.5 s to 4.0 s, the proposed resilience control by DHOD is activated. The state variables and the attack signal are estimated, as shown in Figs. 7(c) and 7(d). The estimated attack signal is compensated in the control feedback. Obviously, the bus voltages and the output currents of DERs are controlled at the nominal values at steady state, which are identical to the corresponding values without cyber-attacks during the period from 0 s to 0.5 s.

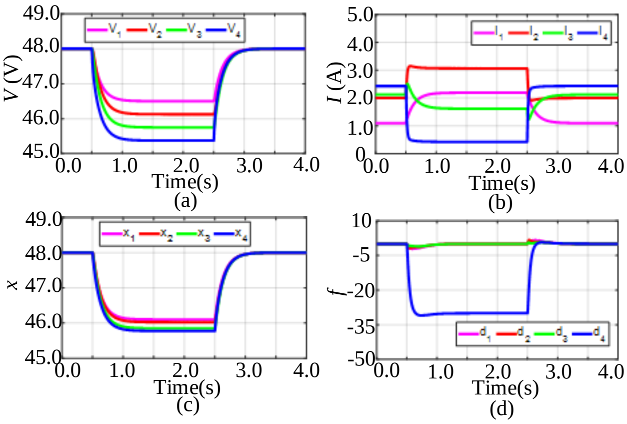


Fig. 7. Waveforms of (a) the output voltages of DERs, (b) the output currents of DERs, (c) the estimated state variables, and (d) the estimated attack signal in case 2.

C. Case 3

The waveforms of the output voltages of DERs, the estimated state variables, the output currents of DERs, and the estimated attack signal in case 3 are shown in Fig.8. During the period from 0 s to 0.5 s, without cyber-attacks, the currents among DERs are allocated as the proportion of, I_1: I_2: I_3: I_4 = 3: 2: 2: 3. The DER4, is attacked by a sine signal: $f_3 = -16(t-0.5)+16$ at 0.5 s. Under the attack, the output currents of DERs deviate from each other, as can be seen in Fig. 8(b). Furthermore, due to the integration effect of the distributed secondary control, the bus voltage will continue to increase linearly in the period of 0.5s ~ 2.5s, as shown Fig. 8(a). During the period from 2.5 s to 4.0 s, the proposed resilience control by DHOD is activated. The state variables and the attack signal are estimated, as shown in Figs. 8(c) and 10(d). Additionally, it can be seen an interesting phenomenon: the attack signals can be estimated in the un-attacked DERs. The reason is that the leader node (provide reference) isn't used in distributed current sharing among DERs. The estimated attack signal is compensated in the control feedback. Obviously, the bus voltages and the output currents of DERs are controlled at the nominal values at steady state, which are identical to the corresponding values without cyber-attacks during the period from 0 s to 0.5 s.

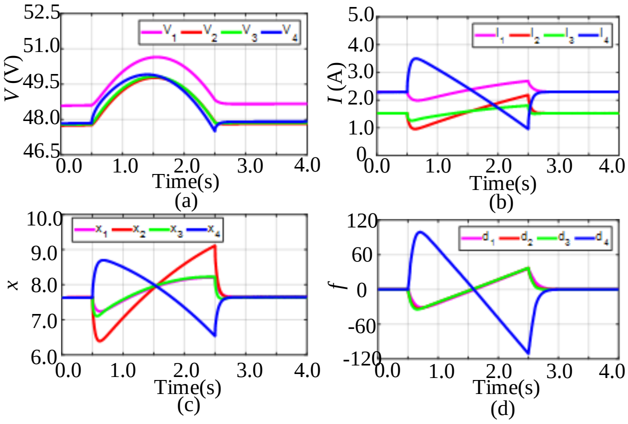


Fig. 8. Waveforms of (a) the output voltages of DERs, (b) the output currents of DERs, (c) the estimated state variables, and (d) the estimated attack signal in case 3.

D. Case 4

In case 4, the distributed secondary control is adopted to implement the average power sharing among the DERs. The waveforms of the output voltages of DERs, the output powers of DERs, the estimated state variables, and the estimated attack signals are shown in Fig. 9. Before the DER1 is attacked by the signal $f_4 = 30\sin(5.5\pi(t + 2.5))$ at 0.5 s, all the output powers are controlled at 91.2W, while all the bus voltages are within the tolerances. During the period from 0.5 s to 2.5 s, the DER1 is attacked but the compensation is not activated. Under the attack, the output currents of DERs deviate from each other, as can be seen in Fig. 9(b). Furthermore, due to the integration effect of the distributed secondary control, the bus voltage will continue to increase linearly in the period of 0.5s ~ 2.5s, as shown Fig. 9(a). During the period from 2.5 s to 4.0 s, the proposed resilience control by DHOD is activated. The state variables and the attack signal are estimated, as shown in Figs. 9(c) and 9(d). The estimated attack signal is compensated in the control feedback. Obviously, the bus voltages and the output currents of DERs are controlled at the nominal values at steady state, which are identical to the corresponding values without cyber-attacks during the period from 0 s to 0.5 s.

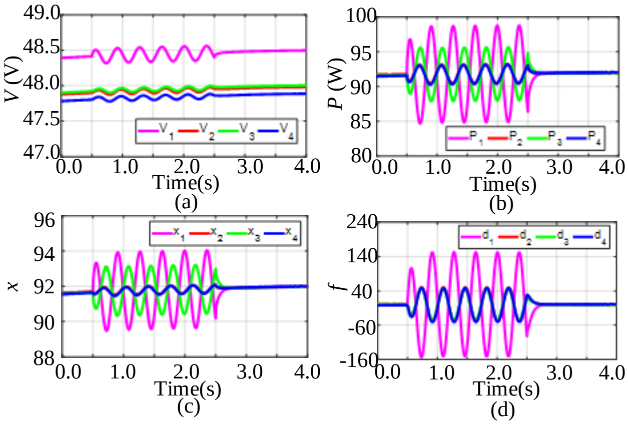


Fig. 9. Waveforms of (a) the output voltages of DERs, (b) the output powers of DERs, (c) the estimated state variables, and (d) the estimated attack signal in case 4.

V. Conclusion

This paper proposes a DHOD-based distributed secondary control to implement bus voltage restorations and output currents/powers sharing of DERs in DC microgrids under cyber-attacks. The DHOD can estimate both constant and time-varying attack signals and compensate the signals to the control variables of the distributed secondary control. Due to the state variables of the DHOD are verified to be converged, the stability of the proposed DHOD-based distributed secondary control can be guaranteed. Case studies in simulation demonstrate that the proposed control strategy can effectively eliminate the negative impact on the DERs in DC microgrids from cyber-attacks.

Acknowledgment

This section should be used to give thanks to people who contributed to the paper but do not have their names in the author list.

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] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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).

[27] 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.

[28] A. Levant, “High-order sliding modes: differentiation and output feedback control,” *Int. J. Control*, vol. 76, no. 9, pp. 924–941, Sep. 2003.

[29] Y. Jiang, W. Xu, and C. Mu, “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.