Detection and Mitigation via Alternative Data for False Data Injection Attacks in DC Microgrid Cluster

Sucheng LIU, Guanggan HU, Mengyu XIA, Qianjin ZHANG, Wei FANG, and Xiaodong LIU

***Abstract*—DC microgrid clusters (DCMGCs), as deeply integrated cyber-physical systems, are formed by interconnection of multiple DC microgrids, and use distributed control to achieve power distribution with high reliability and scalability, and further reflect advantages of distributed energy resources-based generations. However, sharing of information among control agents by distributed manner in the DCMGCs renders the systems vulnerable to cyber-attacks. Among various cyber-attacks, false data injection attacks (FDIAs) can be carefully designed as stealth attacks, which can cause errors in the power management of DCMGCs without manifestation of instability phenomena and even mislead existing detection methods to make incorrect judgments. To address this issue, this paper presents an alternative data-based strategy to detect FDIAs and mitigate the impact of the attacks in cyber network of DCMGCs. The classification conditions of FDIAs are discussed according to the different responses of DCMGCs to the attacks. Furthermore, the core detection problem is transformed into identifying whether the system outputs match by selecting alternative communication data to circumvent complex modeling. Finally, hardware-in-the-loop experimental results on the dSPACE™ MicroLabBox platform with universal digital signal processing (DSP) controllers validate the proposed strategy.**

***Index Terms*—Cyber-attack, DC microgrid cluster, false data injection attack, hierarchical control.**

I. Introduction

MICROGRIDS (MGs), as building blocks of modern distribution grids, have offered efficient solutions in distributed energy generation and supply [1]. In more recent years, DC microgrids (DCMGs) have been experiencing faster growth than ACMGs thanks to higher efficiency, lower cost, and simpler control structures [2]–[5]. Meanwhile, the growing applications of DCMGs points out natural evolution to clusters structures, i.e., interconnected multiple MGs in the neighborhood to achieve the most of MG solutions with economic benefits [6]–[8].

The hierarchical control paradigm that in general consists of three levels, viz. primary, secondary, and tertiary, has been introduced with decoupled design of multiple objectives to ensure efficient and stable operation DCMGs clusters. The primary control performs fundamental voltage and current regulation and current sharing of the converters in parallel. The secondary control implements power quality regulation to maintain the DCMG voltage within acceptable range. The tertiary control is to achieve power management among the multiple DCMGs in the cluster [8]–[12]. Moreover, distributed communications of hierarchical control have been considered as desired means with combined benefits, e.g., reliability, regulation capability and scalability, of centralized and decentralized controls [13]–[15].

However, distributed control of DCMGCs means sharing information among the neighboring control agents, which will inevitably expose the cyber layer of the system to potential security problems [10], [16]–[18]. Again, the weakened capability of global monitoring and awareness with the absence of central controller renders DCMGCs vulnerable to cyber-attacks such as false data injection attacks (FDIAs) [17], [19], replay attacks [20], and denial-of-service (DoS) attacks [21] , and so forth. Among these various cyber-attacks, the FDIAs inject malicious false data in communication links to tamper with the control variables of the system and have become the most prevalent forms of cyber-attacks [15]. Therefore, strategies of detection and mitigation of FDIAs become indispensable part of the control architecture of DCMGCs [22], which is especially critical at tertiary level without centralized control entities in DCMGCs. Unfortunately, there are only some works on FDIA detection and mitigation in single DC or AC MGs, even less in multiple MG clusters [10].

Basically, the existing methods for FDIAs detection and mitigation can be grouped as either model-based or model-free ones. In the model-based methods, prior knowledge of the system for mathematical modeling is required. For example, modeling based on the distributed sliding mode observer is adopted in the secondary control of DCMGs for attack detection and voltage restoration [23]. In [24], the Kalman filter is designed and combined with the proposed Euclidean detector to detect the complicated FDIA in smart grid systems. In [17], the framework of hybrid automaton for detecting FDIAs is presented, where the detection problem is transformed into identifying the inferred candidate invariants. To circumvent the difficulty and complexity in most existing centralized

Manuscript received May 19, 2023; revised August 14, 2023; accepted September 20, 2023. Date of publication March 30, 2024; date of current version October 13, 2023. This work was supported by the National Natural Science Foundation of China under grant 52277169 and in part by the Key Laboratory of Fujian Universities for New Energy Equipment Testing under grant XNY202106, and Natural Science Research Project of Anhui Educational Committee under grant 2022AH050326. *(Corresponding author: Sucheng Liu.)*

All authors are with the Anhui Provincial Key Laboratory of Power Electronics and Motion Control, Anhui University of Technology, Ma'anshan 243032, China (e-mail: liusucheng@ahut.edu.cn; hugaunggan@163.com; ayu224215@163.com; zqj1214@ahut.edu.cn; fwei2k@163.com; liuxiaodong@ahut.edu.cn).

Digital Object Identifier 10.24295/CPSSTPEA.2023.00043

modeling approaches to obtain global state space models, the distributed modeling-based cyber-attack detection method is proposed for the secondary control of DC microgrids, where the local state space models of the distributed generation units plus a few interacting variables from neighboring units are only required [25]. The trust-based distributed cooperative control is proposed to ensure attack-resilient operation by using current sharing mismatch from neighboring converters in DCMGs, and thus propagation of compromised data can be avoided [26]. In [27], the resilient distributed control mechanism through a graph-theoretic approach is proposed, and the Lyapunov-based framework guarantees the stability of the system without the need to know information about the nature or location of the attack. The network attack detection index was defined and the positive characterization of cooperative vulnerability factor was utilized, and then the adaptive proportional gain of the current regulator was selected to eliminate the instability of the system caused by nonlinear FDIAs [28]. The distributed linear adaptive observer was designed to detect and mitigate FDIAs with unknown constant power loads, nonlinearities, noise and other limitations [29].

By contrast, model-free methods are also referred to data-driven ones that rely on input/output data rather than on the prior knowledge of systems [30]. In [31], Hilbert-Huang transform is first adopted to extract the signals feature of the DCMG, and then advanced selective ensemble deep learning procedure with for Krill Herd Optimization Algorithm is used to detect the FDIAs with over 90% accuracy. The artificial neural network-based approach is proposed to detect and mitigate the coordinated FDIAs in a decentralized manner for DCMGs [32]. Sahoo et al. [33] propose a novel cooperative vulnerability factor (CVF) framework based on the deviation values generated by the consistency algorithm, thus detecting possible FDIAs locally. By extracting control quantities through the control loops, the discordant element-based detection approach is designed to detect the nodes with FDIAs, and the risk assessment framework for DC microgrids to resist cyber-attacks is provided as well [34]. In [35], the invisible cyber-attacks in DC microgrids are detected by proposing an unsupervised deep recurrent autoencoder anomaly detection scheme with deep recursive autoencoder, and the comparison of single feature extraction (i.e., current) with multiple feature extraction (i.e., current and voltage data) is also performed to verify the effectiveness of the scheme.

On the other hand, DCMGCs that consist of multiple DCMGs have been only sporadically studied with respect to the cyber-attacks of the systems. For example, the distributed state estimation approach is proposed for each MG to detect possibly manipulated data that receives from neighboring MGs [36]. However, the DCMGCs are typical CPSs that of high-order nonlinear dynamics with multiple inputs and multiple outputs, which poses significant challenges in developing detection and mitigation methods for cyber-attacks like FDIAs [12]. To circumvent this issue, the detection strategy based on the convergent nature of the global error in the control variables is derived [10]. However, the set of well-designed false data that satisfy the equilibrium condition, known as stealth attack, can bypass the global error-based detection strategies in DCMGCs [33]. This is because that the objectives of the DCMGC power allocation are satisfied without involving any power imbalance under the stealth attack of individual false data. Thus, in this case, the existing distributed observers-based detection methods would become ineffective such that the DCMGC will continue to operate under this false consensus without loss of stability. Furthermore, the injected false data can be changed as well, which will produce greater economic losses.

To sum up, the lack of a comprehensive cybersecurity strategy with effective yet simple implementation for power management of DCMGCs motivates the work in this paper. The contributions of this work are summarized as follows:

1) The effects of FIDAs as stealth attacks on power management in DCMGCs are investigated. Specifically, modeling and analysis are carried out for FDIAs by partial information from the cyber layer and the state variables. Hence, the relationship between FDIAs and the global error of the distributed tertiary control is readily revealed without requiring complicated modeling efforts of the DCMGCs of high order and nonlinear nature.

2) An alternative data-based framework is proposed for detection and mitigation of FDIAs in DCMGCs with distributed tertiary control. By the proposed method, the core detection problem is transformed into identifying whether the alternative data in every single DCMG matches with the original data from the state variables, and thus, the computation burden for the detection is significantly reduced. Further, the mitigation strategy based on the matching result of FDIAs is successively derived, where the alternative data is utilized to regain the control of the DCMGC.

The rest of the paper is organized as follows. The general topology of a distributed tertiary controlled-DCMGC as the cyber-physical system is presented in Section II. The modeling and design requirements in case of FDIAs in DCMGCs is discussed in Section III. The detection and mitigation strategy via alternative data for FDIAs in DCMGCs is proposed in Section IV. The hardware-in-the-loop (HIL) experimental results to demonstrate the proposed strategy are shown in Section V. Conclusions of the work are finally drawn in Section VI.

II. Review of the Two-Layer Distributed Tertiary Control for the DCMGC

Fig. 1 shows the topology of a general DCMGC with both cyber and physical layers, where k DCMGs are interconnected through tie-lines in the physical layer and each DCMG consists of photovoltaic (PV), wind turbine (WT), battery energy storage system (BESS), and DC and AC loads. In the cyber layer, the control agents of the DCMGC, i.e., all the DCMGs agents that represented by the square nodes, constitute the distributed global cyber network, and each DCMG agent is composed of multiple BESS converter control agents that represented by the circular nodes to form the local cyber network, the connection between the two cyber networks is via the pinning links. By the cyber network, the power flow of the

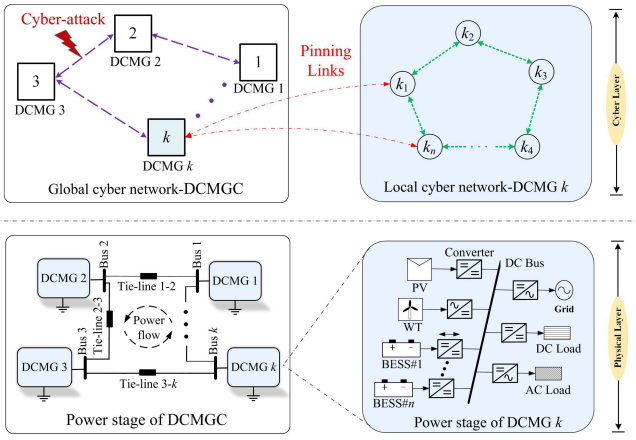

Fig. 1. Topology of a general DCMGC with both cyber and physical layers.

DCMGC among every DCMG will be managed, which is assigned to the distributed tertiary control in the hierarchical control framework. In this scenario, the cyber-attack of FDIAs in the global tertiary network is the primary consideration of this work.

Fig. 2 shows the block diagram of the distributed tertiary control for the DCMGC. As we focus on the system-level power flow management for the DCMGC, the tertiary control that consists of global and local layers is highlighted by the detailed control blocks with the cyber networks, whereas the primary and the secondary controls are simplified by the functional blocks.

In the global tertiary control, each DCMG in the DCMGC generates its voltage set point to enable the system-level power flow based on the sharing data between its local load and the load from the neighboring DCMGs. Taking DCMG k as the example, the global error term e_k is generated based on the consensus protocol, which can be expressed as

$$e_k = \sum_{l \in N_k} (i_{\text{pu}}^l - i_{\text{pu}}^k) \tag{1}$$

where the N_k , i_{pu}^i and i_{pu}^k represent the set of the neighbors of DCMG k, the received data of the neighbor, and the averaged value of all the per-unit currents of the BESS converters, respectively.

Subsequently, the correction term is calculated by the PI controller, and the voltage reference for every DCMG is produced by adding to the nominal reference value, which is given by

$$\delta v_k = k_p e_k + k_i \int e_k = H_1^k(s) \cdot e_k \tag{2}$$

$$v_{\text{ref}}^k = v_{\text{ref}} + \delta v_k \tag{3}$$

where v_{ref}^k is the voltage set point of DCMG k.

In the local tertiary control, the propagation of the voltage set point to the local pinned converter agents is achieved through the pinning link by sharing the distributed network with the secondary control.

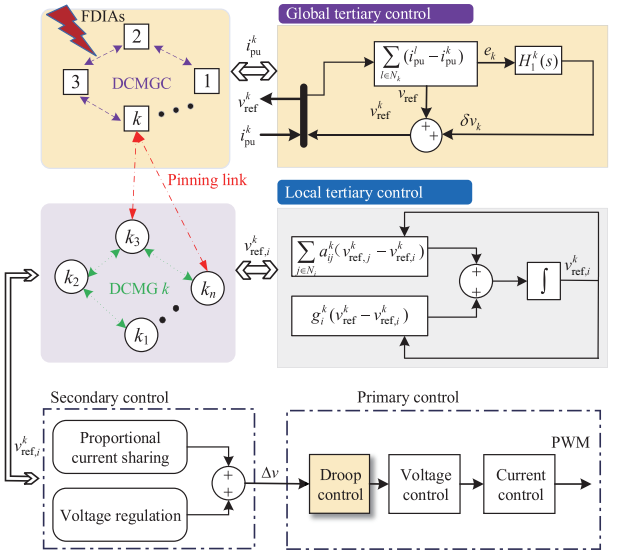

Fig. 2. Block diagram of the distributed tertiary control for the DCMGC.

Therefore, dynamics of the voltage reference for the pinned converter agent by consensus protocol can be described as

$$v_{\text{ref},i}^k = \sum_{j \in N_i^k} a_{ij}^k (v_{\text{ref},j}^k - v_{\text{ref},i}^k) + g_i^k (v_{\text{ref}}^k - v_{\text{ref},i}^k) \tag{4}$$

where $v_{\text{ref},i}^k$ is the voltage reference of the converter i in the DCMG k, and $g_i^k = 1$ or 0 depends on whether the converter i is pinned or not, and represents the set of the neighbors of the converter i, respectively.

In the tertiary control of DCMGCs, FDIAs in the tertiary link can disrupt the power flow in a stealth way by combing the false data with the real data. It is necessary to figure out how the FDIAs affect the power management of DCMGCs before embarking on the solution of detection and mitigation.

III. FDIAs in Power Management of DCMGCs

A. Modeling and Analysis of FDIAs

The FDIAs in the tertiary communication link between DCMG j and DCMG k in the DCMGC can be modeled as

$$x_{k,j}^f = x_{k,j} + k_T \cdot f_{k,j} \tag{5}$$

where $x_{k,j}$ represents the original data sent by its neighboring agents of DCMG j and $f_{k,j}$ denotes the false data, respectively. $x_{k,j}^f$ is the data received by DCMG k with the FDIA. $k_T = 1$ means the presence of FDIAs in the communication link, and $k_T = 0$ means no attack.

Thus, the false data for DCMG k in the tertiary control communication network can be expressed as

$$f_k = \sum_{j \in N_k} f_{k,j} \tag{6}$$

Accounting the FDIA into (1), and the global error can be rewritten as

$$e_k^f = \sum_{j \in N_k} (i_{\text{pu}}^j - i_{\text{pu}}^k) + k_T \cdot f_k \tag{7}$$

where e_k^f is the global error generated after the attack.

Further, we can expand (6) to the complete DCMGC as the matrix format of

$$\mathbf{E_a} = -\mathbf{L_G I_{pu}} + k_T \mathbf{F} \tag{8}$$

where $\mathbf{F}$ and $\mathbf{L_G} \in \mathbb{R}^{k \times k}$ denote the vector of FDIAs and the Laplacian matrix of the global tertiary graph, respectively.

Normally, the DCMGC in steady state without FDIAs can be expressed as

$$\mathbf{E} = -\mathbf{L_G I_{pu}} = 0 \tag{9}$$

For FDIAs, however, the global error of each DCMG in the DCMGC still can converge to zero, and in this case the system in steady state is given by

$$\mathbf{E_a} = -\mathbf{L_G I_{pu}} + k_T \mathbf{F} = \mathbf{0} \tag{10}$$

As such, the DCMGC remains to operate stably within a reasonable range, which renders the FDIAs extremely difficult to be detected.

The FDIAs aimed at power management in DCMGCs can be categorized as two main types, i.e., 1) *stealth attacks*, if the sum of attack data for all attacked DCMGs in the DCMGC is zero, and 2) *common FDIAs*, otherwise.

Now, we attempt to obtain the design requirements of the attack vectors with respect to different types of FDIAs based on the convergence of the global error and the knowledge related to the communication topology.

The minimum eigenvalue of the Laplacian matrix $\mathbf{L_G}$ of global tertiary network the is zero and the corresponding right eigenvector is $\mathbf{1}$, which can be described as

$$\mathbf{L_G} \times \mathbf{1} = \mathbf{0} \tag{11}$$

Defining the left eigenvector as $\boldsymbol{\beta} = [\beta_1 \quad \dots \quad \beta_k] \in \mathbb{R}^{1 \times k}$, and we derive

$$\boldsymbol{\beta} \times \mathbf{L_G} = \mathbf{0} \tag{12}$$

In the case of the stealth attack, the relationship between the attack data and $\boldsymbol{\beta}$ can be expressed as

$$\boldsymbol{\beta} \times \mathbf{F} = \mathbf{0} \tag{13}$$

Furthermore, with the Laplacian matrix being the real symmetric matrix, (11) can be transposed to

$$\mathbf{L_G}^{\mathrm{T}} \times \boldsymbol{\beta}^{\mathrm{T}} = \mathbf{0} \tag{14}$$

Combing (10) with (13), the relationship between $\boldsymbol{\beta}$ and the right eigenvalue is derived as

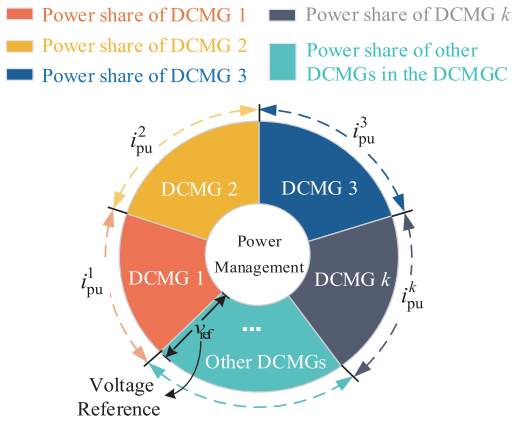

Fig. 3. Pie chart for power management of the DCMGC.

$$\boldsymbol{\beta} = a[1 \quad \dots \quad 1] \tag{15}$$

where $a \neq 0, \forall a \in \mathbb{R}$.

Substituting (14) into (12) derives the design requirement for stealth attacks that is given by

$$\sum_{i=1}^{k} f_i = 0 \tag{16}$$

where $f_i \in \mathbf{F}$ is the attack data for the individual DCMG.

In addition, for FDIAs that do not satisfy (15), the global error will be shifted under the influence of the attack data and communication data, which is described as

$$\mathbf{E_a} = -\mathbf{L_G I_{pu}} + k_T \mathbf{F} = \mathbf{X} \tag{17}$$

where $\mathbf{X} = [x \quad \dots \quad x]^{\mathrm{T}} \in \mathbb{R}^{k \times 1}$, $x \neq 0$ denotes the non-zero global error in the tertiary control.

Similarly, adding $\boldsymbol{\beta}$ to (16) produces

$$\sum_{i=1}^{k} f_i = kx \tag{18}$$

In this case, the attack can change the voltage profile of the DCMGC by controlling the attack data, and this is referred as common FDIAs. Due to the existence of the PI controllers in the tertiary control, the non-zero global error makes the voltage set point of each DCMG continuously increase or decrease, and the bus voltage exceeds the safe range, which will trigger the overvoltage or undervoltage protection.

B.Impact of FDIAs on Power Management in DCMGCs

To describe the impact of FDIAs in a concise manner, we introduce the pie chart to illustrate the power management of the DCMGC as in Fig. 3. The power share of every single DCMG in the DCMGC is represented by the corresponding sector in the pie chart, wherein the arc length and the radius stand for the per-unit current and the voltage reference that

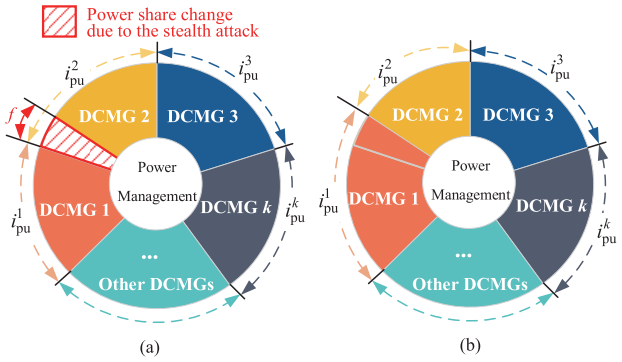

Fig. 4. Power management of the DCMGC subject to the stealth attack. (a) Power share change, (b) Power share after the stealth attack.

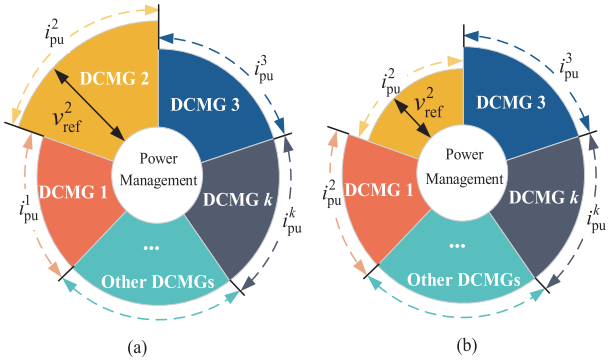

Fig. 5. Power management of the DCMGC subject to the common FDIAs. (a) Power share with the positive FDIA, (b) Power share with the negative FDIA.

generated by the tertiary control, respectively.

In normal operation, the global error of the DCMGC converges to zero with the tertiary control, which can be expressed as

$$i_{\mathrm{pu}}^{1} = i_{\mathrm{pu}}^{2} = i_{\mathrm{pu}}^{3} \ldots = i_{\mathrm{pu}}^{k} \tag{19}$$

Now, assuming the power management of the DCMGC is subject to the FDIA as the stealth attack, which can be illustrated in Fig. 4. Specifically, the false data with the value of f was injected into the tertiary graph of DCMG 1 and $-f$ into that of DCMG 2, respectively. To maintain the new power balance after the stealth attack, the communication data of DCMG 1 can be rewritten as

$$\sum_{j \in N_1} (i_{\mathrm{pu}}^{j} - i_{\mathrm{pu}}^{1}) = -f \tag{20}$$

and

$$i_{\mathrm{pu}}^{1} = \frac{\sum_{j \in N_1} i_{\mathrm{pu}}^{j} + f}{|N_1|} \tag{21}$$

Similarly, the per-unit current for DCMG 2 with the stealth attack can be derived as

$$i_{\mathrm{pu}}^{2} = \frac{\sum_{j \in N_2} i_{\mathrm{pu}}^{j} - f}{|N_2|} \tag{22}$$

Hence, the power share of DCMG 1 will increase according to (20), and meanwhile the power share of DCMG 2 decrease by (21). The power share change due to the stealth attack was illustrated in Fig. 4(a) and the power share after the attack is shown in Fig. 4(b), respectively, which means that the power share change due to the stealth attack is shifted from DCMG 2 to DCMG 1. But the overall power share of the DCMGC remains with zero net change. In a word, the FDIA stealth attack on the DCMGC have the influence upon the partial change of the power share only, and the stability of the system still maintains if the associated change due to the attack is kept within the tolerance range of the steady state.

In contrast, the common FDIAs-induced response of DCMGCs can behave totally different from that of the stealth attack since the common FDIAs will produce a shift in the global error that it no longer converges to zero. Fig. 5 illustrates the power management of the DCMGC subject to the common FDIAs. In the case of the positive FDIA of f on DCMG 2 in Fig. 5(a), the power share of the DCMG 2 will increase, and furthermore, the voltage reference as the results of the non-zero global error will be increased as well because the rest of the MGs in the DCMGC remains unchanged. Similarly, in the case of the negative FDIA of $-f$ on DCMG 2 in Fig. 5(b), the bus voltage will decrease. Whenever the voltage of the DCMG subject to the common FDIAs increases or decreases, the stability of the DCMGC will be deteriorated if the attack continues.

IV. Proposed Detection and Mitigation Strategy

This section proposes the detection and mitigation strategy for FDIAs in distributed tertiary control of DCMGCs. It is quite to be challenging to identify and mitigate the FDIAs in power management of the DCMGCs since the output power of each DCMG is different, the power flow is controlled by tertiary control. Once the distributed communication network is attacked, the control loop of DCMGC will be affected, thus affecting the whole system. To address this issue, the alternative communication data is selected to detect the attacked nodes and derive the mitigation strategy based on the detected results.

A. The Detection of FDIAs in DCMGCs

The proposed strategy starts with selecting alternative communication data, which is based on the synergetic nature of every DCMG control outputs in the distributed control of DCMGCs.

Assuming that DCMG k in the DCMGC is subjected to FDIAs, there is a relationship between the reference current $i_{\mathrm{L},i}^{k}$ and the output current $i_{\mathrm{pu},i}^{k}$ in the tertiary control, which can

be given by

$$i_{\mathrm{L},i}^{k}(t)=i_{\mathrm{pu},i}^{k}(t-\varphi) \tag{23}$$

where φ is the time difference between two variables.

Further, the alternative communication data is calculated as

$$i_{\mathrm{al}}^{k}=\frac{1}{\left|\mathrm{F}_{k}\right|}\sum_{i\in\mathrm{F}_{k}}i_{\mathrm{L},i}^{k} \tag{24}$$

where F_k denotes the set of pinned converter agents in DCMG k.

The error of the alternative quantity can be written as

$$e_{\mathrm{al},k}=\sum_{l\in N_k}(i_{\mathrm{al}}^{l}-i_{\mathrm{al}}^{k}) \tag{25}$$

With the FDIAs, the global error of the tertiary control will be changed as

$$x=e_k+f_k \tag{26}$$

Thus, the alternative data in (24) (25) can be rewritten as

$$i_{\mathrm{al}}^{k}=\frac{\sum_{j\in N_k}i_{\mathrm{al}}^{l}+f}{\left|N_k\right|}-x \tag{27}$$

The detection criterion to measure the difference between the alternative data and the real data is designed as

$$D_k=\left|e_{\mathrm{al},k}-e_k\right| \tag{28}$$

Subsequently, the detection index δ_k is defined to determine the status of DCMG k, i.e., if it is attacked by FDIAs or not, which is expressed as

$$\delta_k=\begin{cases}1, & \text{if } D_k\geqslant\sigma\\ 0, & \text{otherwise}\end{cases} \tag{29}$$

where σ stands for the threshold to avoid incorrect detection, and σ must meet the following conditions:

$$\begin{cases}\sigma\to 0\\ \sigma\geqslant max\{N_{\mathrm{s}},\psi\}\end{cases} \tag{30}$$

where N_s and Ψ represent output noise and sensor error, respectively.

In addition, the FDIA can be further identified after detection, which is given by

$$\begin{cases}\text{Stealth Attack, if } \lim\limits_{t\to\infty}e_k=0\\ \text{and}\\ \text{Common FDIA, if } \lim\limits_{t\to\infty}e_k\neq 0\end{cases} \tag{31}$$

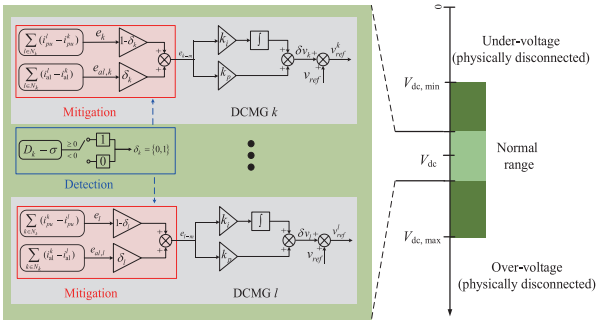

Fig. 6. Proposed mitigation strategy driven by the detection index for the DCMGC.

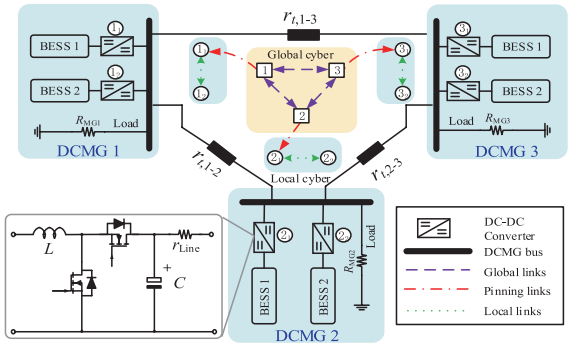

Fig. 7. The layout of the DCMGC experimental setup.

B. The Mitigation of FDIAs in DCMGCs

Fig. 6 illustrates the mitigation strategy for FDIAs in DCMGCs. Based on the detection results, the mitigation strategy will be triggered, and the selected alternative communication data is supposed to replace the original communication data by

$$e_{k-m}=(1-\delta_k)\sum_{l\in N_k}\left(i_{\mathrm{pu}}^{l}-i_{\mathrm{pu}}^{k}\right)+\delta_k\sum_{l\in N_k}\left(i_{\mathrm{al}}^{l}-i_{\mathrm{al}}^{k}\right) \tag{32}$$

where e_{k-m} is the new global tertiary error generated by mitigation.

The communication data in (22) is deployed to generate the new voltage correction term so that the voltage set point of the attacked DCMGs in the DCMGC can be compensated. It is noteworthy that the original communication data is repetitively used to generate the correction term until the condition in (28) is re-satisfied.

In addition to the cyber layer of the DCMGC, the physical layer also adopts the voltage protection scheme in abnormal cases, and to disconnect the physical layer from the cyber layer. With this consideration, the normal voltage range is given by

$$V_{\mathrm{dc,min}}\leqslant V_{\mathrm{dc}}\leqslant V_{\mathrm{dc,max}} \tag{33}$$

In summary, the implementation of the detection and mitigation strategy for the FDIAs in DCMGCs is described by using the pseudocode of Algorithm 1 as follows:

Algorithm 1: Detection and Mitigation of FDIAs.

1. Inputs:

Communication Data: i_{pu}^{k}, i_{pu}^{l} ($l \in N_k$)

Alternative Data: i_{al}^{k}, i_{al}^{l} ($l \in N_k$)

2. Initialization:

e_k, $e_{\mathrm{al},k}$, D_k

3. Communication stage:

$$e_k = \sum_{l \in N_k} (i_{\mathrm{pu}}^{l} - i_{\mathrm{pu}}^{k})$$

$$e_{\mathrm{al},k} = \sum_{l \in N_k} (i_{\mathrm{al}}^{l} - i_{\mathrm{al}}^{k})$$

$$D_k = \left| e_{\mathrm{al},k} - e_k \right|$$

4. FDIAs detection:

Define δ_k as the detection index used for detecting FDIAs

if ($D_k \geq \sigma$){

  if ($e_k = 0$){

  $\sigma = 1$ (There is stealth attack in DCMG k)

  }else{

  $\delta_k = 1$ (There is common FDIA in DCMG k)

  }

}else{

  $\delta_k = 0$ (There is no FDIA in DCMG k)

5: Detection output:

δ_k **(Detection index)**

6: FDIAs Mitigation:

$$e_{k-m} = (1 - \delta_k) \sum_{l \in N_k} (i_{\mathrm{pu}}^{l} - i_{\mathrm{pu}}^{k}) + \delta_k \sum_{l \in N_k} (i_{\mathrm{al}}^{l} - i_{\mathrm{al}}^{k})$$

V. Hardware-in-the-Loop (HIL) Experimental Validation

To validate the proposed detection and mitigation strategy, the DCMGC with interconnection of three DCMGs in Fig. 7 was built in the hardware-in-the-loop platform. The power layer is built in the dSPACE™ MicroLabBox environment, and the cyber layer and all the control loops are implemented in the universal digital signal processors. Every DCMG consists of two BESS interfacing Buck (grid-forming) converters and a local load. Moreover, one converter control agent is selected as the leader agent for the pinning-based two-layer distributed tertiary control. The parameters for the DCMGC are listed in Table I. The verification will be going through three different scenarios, viz., Scenario I: basic test of the distributed tertiary control, Scenario II: study of the FDIAs response, and Scenario III: the detection and mitigation strategy for the FDIAs in the distributed tertiary control of the DCMGC.

Scenario I: Basic Test of the Distributed Tertiary Control

Fig. 8 shows the basic test of the distributed tertiary control of the DCMGC, which consists of three phases of the operation. The system starts with phase I, i.e., the islanded

TABLE I
System Parameters

Parameter	Value	Parameter	Value
Input voltage V_{in}	100 V	Tie-line inductance $L_{t,1\text{-}2}$	1 μH
Rated dc bus voltage V_{dc}	48 V	Tie-line inductance $L_{t,2\text{-}3}$	2 μH
Converter inductance L	1 mH	Tie-line inductance $L_{t,3\text{-}1}$	3 μH
Converter capacitor C	1.8 mF	Switching frequency f_s	10 kHz
Line resistance $r_{\mathrm{line},1}$ in DCMGs	0.01 Ω	Line resistance $r_{\mathrm{line},2}$ in DCMGs	0.02 Ω
Tie-line resistance $r_{t,1\text{-}2}$	0.1 Ω	Nominal load of DCMG 1	48 Ω
Tie-line resistance $r_{t,2\text{-}3}$	0.2 Ω	Nominal load of DCMG 2	24 Ω
Tie-line resistance $r_{t,3\text{-}1}$	0.3 Ω	Nominal load of DCMG 3	16 Ω
The threshold σ_1	0.5	The threshold σ_2	0.5
Secondary control k_p in DCMGs	0.5	Secondary control k_i in DCMGs	20
Tertiary control k_p in DCMGs	0.8	Tertiary control k_i in DCMGs	30

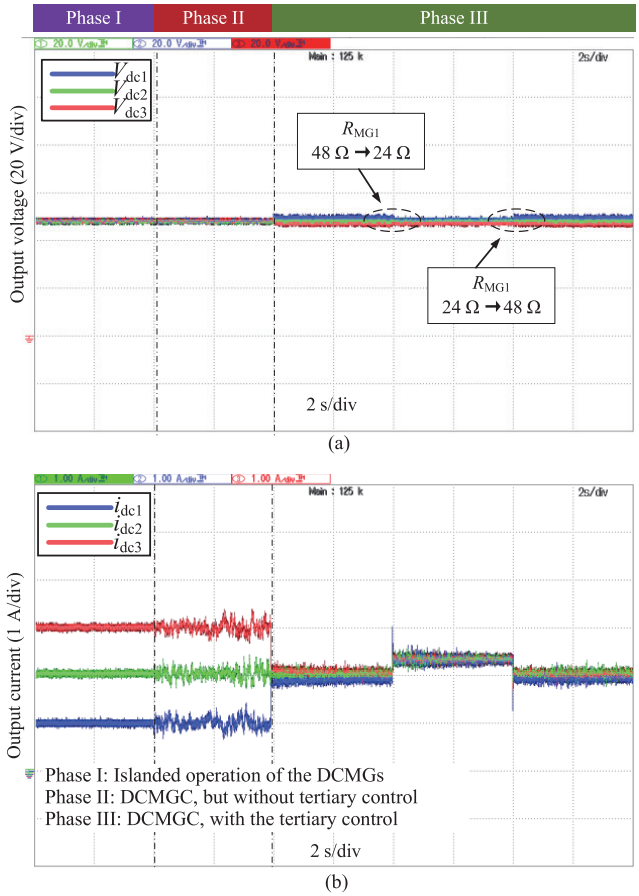

Fig. 8. Proposed mitigation strategy driven by the detection index for the DCMGC.

operation of the three DCMGs that each of them is with local primary and secondary control and operates independently. Then, the system goes into phase II with the three DCMGs are interconnected as the DCMGC, but the tertiary control is still inactive. Lastly, the DCMGC enters phase III with the activation of the distributed tertiary control, and thus the output current of each DCMG reaches the consensus to share the load globally. Moreover, during phase III, the DCMGC goes

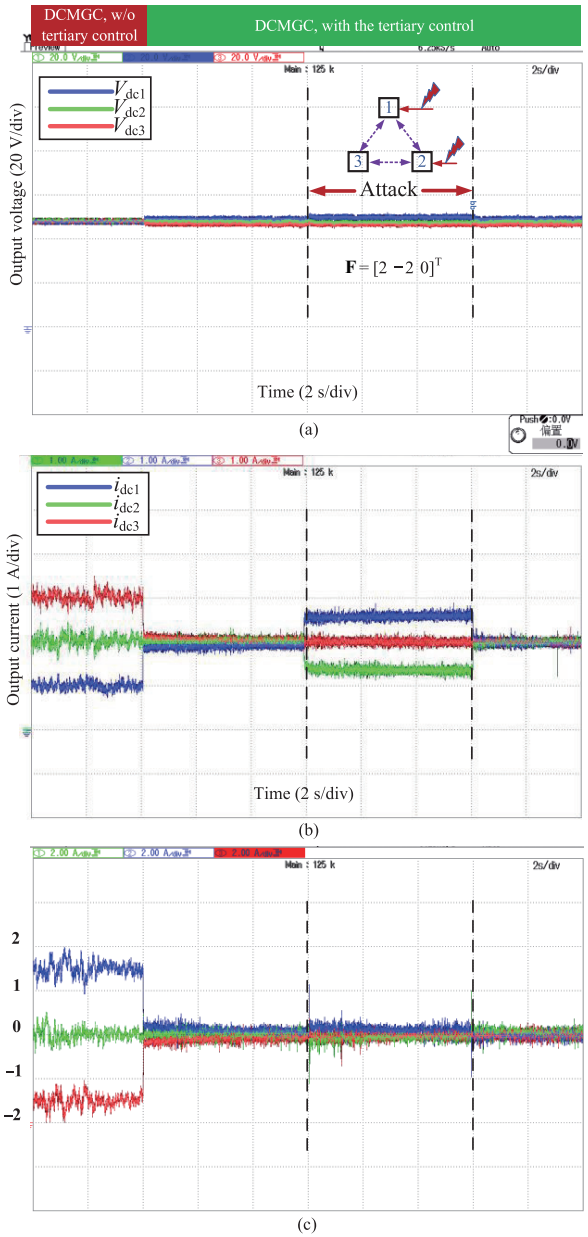

Fig. 9. The stealth attack in the DCMGC: (a) DCMG's bus voltage. (b) DCMG's output current.

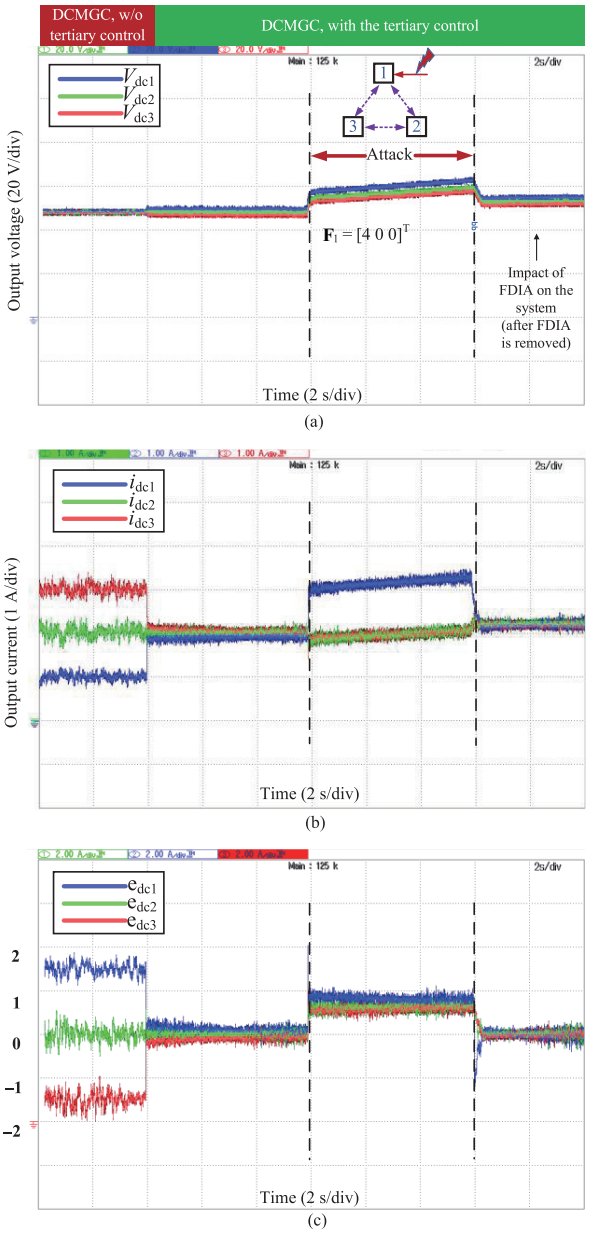

Fig. 10. The common FDIA in the DCMGC. (a) Bus voltage of each DCMG. (b) DCMG's output current.

through the load step transients, and the response demonstrates the distributed tertiary control.

Scenario II: Study of FDIAs Response

The analysis of the impact of the FDIAs on the DCMGC is observed in this scenario that includes two cases, i.e., the stealth attacks and the common FDIAs, as discussed before.

Case 1: Stealth Attacks in the DCMGC

Fig. 9 shows the response of the DCMGC to the stealth attack. In this case, the attack data $\mathbf{F} = [2,-2,0]^T$ is injected into the global tertiary communication of the DCMGC, and the injected stealth data renders the power management of the DCMGC abnormal. Specifically, the output current of DCMG 1 increases by the part that DCMG 2 decreases, which means that DCMG 1 assumes the changing part of the energy supply of DCMG 2 to maintain the power balance. Therefore, the tertiary control consensus is still reached, but with the false consensus at the cost of deviated power sharing from the original system. Then, after the stealth data attack with the interval of 6 seconds, the attack is removed, and the DCMGC returns to its normal operation as before.

Case 2: Common FDIAs

Fig. 10 shows the effect of the common FIDA other than the stealth attacks on the operation of the DCMGC. A constant attack of $\mathbf{F} = [4,0,0]^T$ is attempted also with the interval of

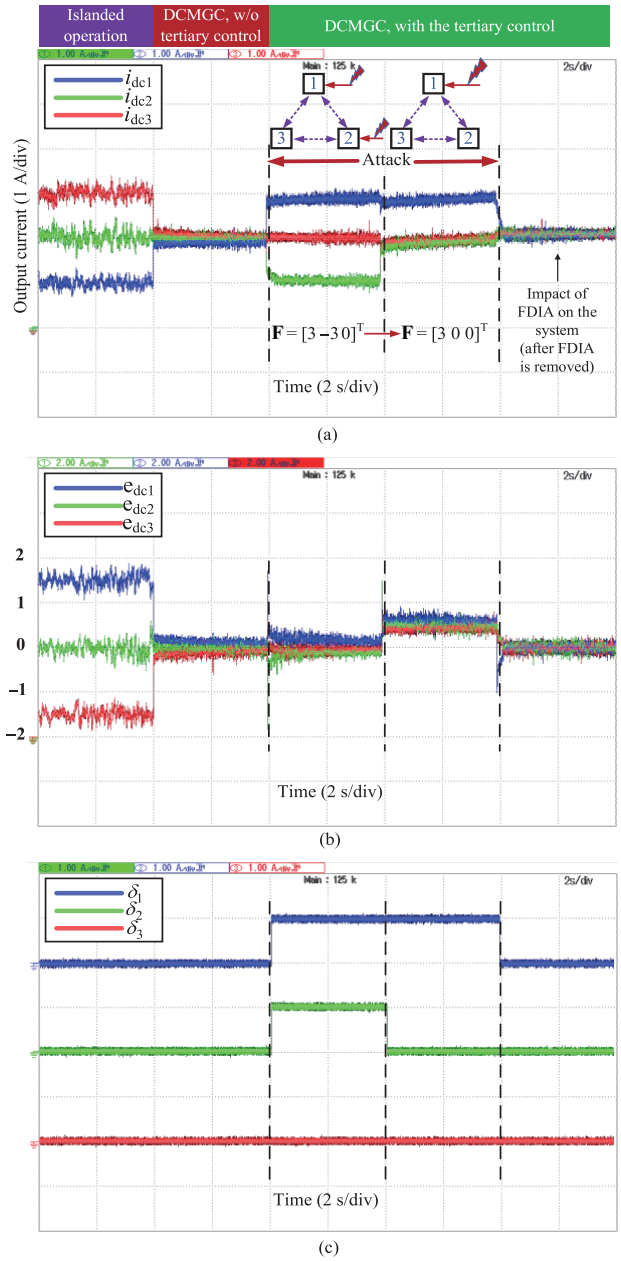

Fig. 11. Detection performance of the DCMGC with resistive load to the FDIA. (a) DCMG's output current. (b) The global error of DCMGs. (c) The detection output of DCMGs.

6 s. However, in contrast to the stealth attack, the bus voltage and output current vary continuously during the interval of the common FDIA. As a result, the voltage set point of every DCMG starts to rise abnormally due to the positive global error, which drives the DCMGC toward the overvoltage state. In addition, after removing the false data, the bus voltage failed to be recovered, and the consensus does not reach the desired value, even the power sharing of the DCMGC is still achieved to the same as the original percentage.

Based on the results, one can see that the FDIAs as stealth attacks are more dormant and difficult to detect than the common FDIAs in the DCMGCs.

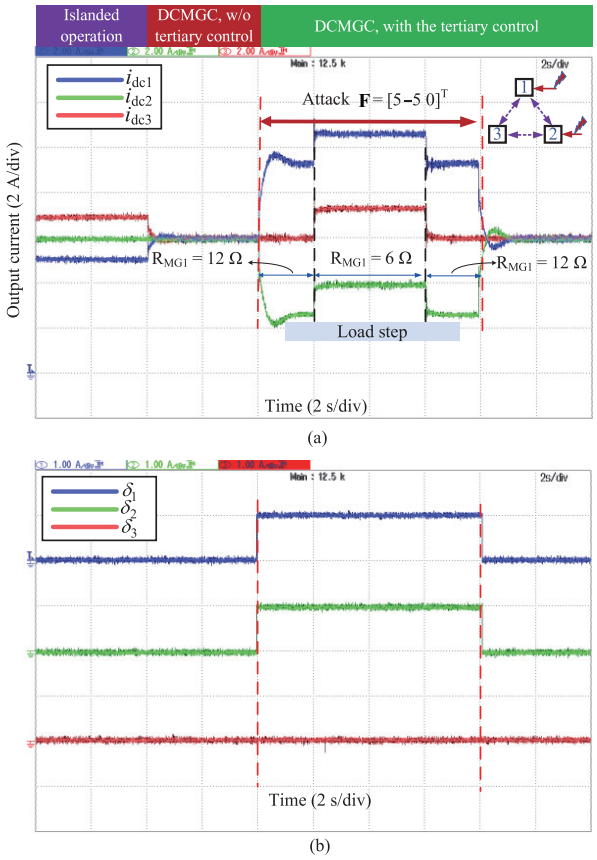

Fig. 12. Detection performance of the DCMGC to the FDIA with load step transients. (a) DCMG's output current. (b) The global error of DCMGs.

Scenario III: The Detection and Mitigation Strategy

Case 1: Detection of FDIAs

Fig. 11 shows the detection performance of the proposed strategy for the FDIA as the stealth attack $\mathbf{F} = [3,-3,0]^T$ that means that the attack data was injected into DCMG 1 and 2 in the DCMGC simultaneously. As the analysis before, the global error still converges in this case, but the attack data causes power shifting between DCMG 1 and 2, which says that the current reference value of the two DCMGs will change, and results in the mismatch between the alternative data and the communication data.

By the detection index in (33), both δ_1 and δ_2 indicate the positive value, as shown in Fig 11(c), for the attacked DCMG 1 and 2. Subsequently, the attack data changes to $\mathbf{F} = [3,0,0]^T$ with only DCMG 1 under the attack. At this point, the detection output of DCMG 2 becomes 0 while DCMG 1 is still shown as under attack. Last, the attack is withdrawn, and all detection outputs go to zero. Therefore, the proposed method has successfully detected the FDIAs based on the validation results.

In addition to constant load condition, Fig. 12 shows the detection performance of the proposed scheme for the FDIAs with load step transients, where in Fig. 12(a) the load of DCMG 1 (R_{MG1}) first steps from 12 Ω to 6 Ω, and then back

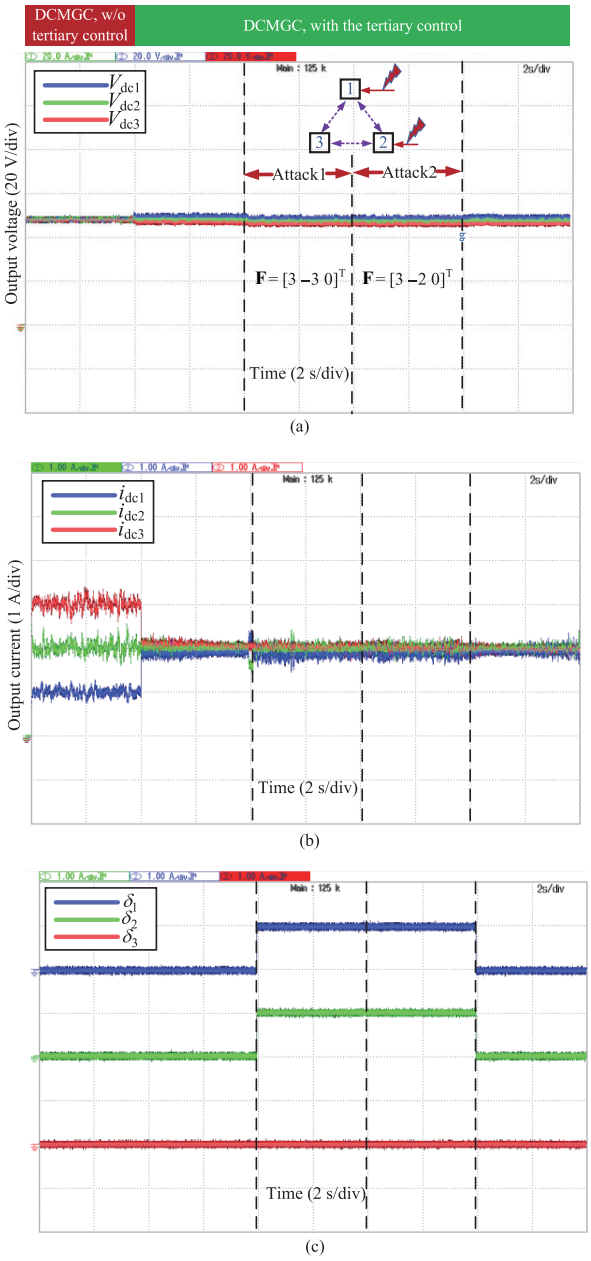

Fig. 13. Mitigation performance of the DCMGC with resistive load to the FDIA. (a) DCMG's output voltage. (b) DCMG's output current. (c) The detection output of DCMGs.

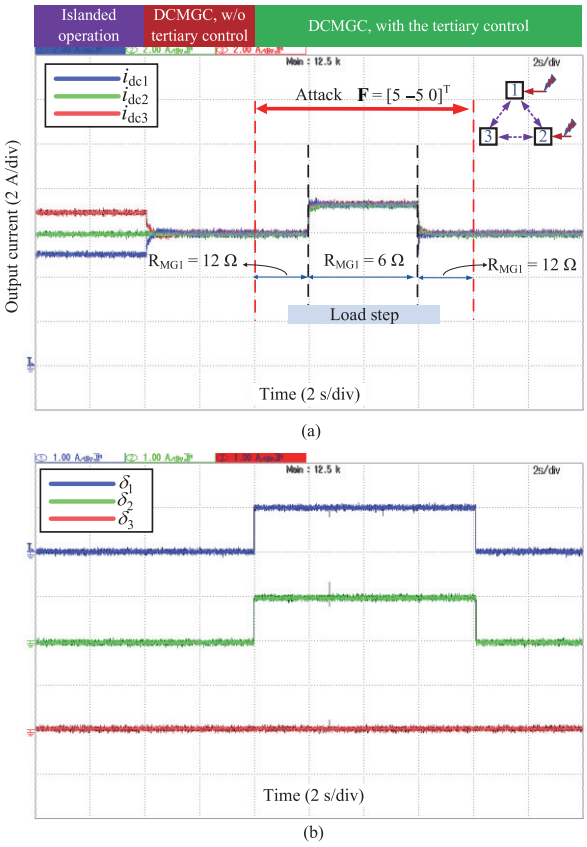

Fig. 14. Mitigation performance of the DCMGC to the FDIA with load step transient. (a) DCMG's output current. (b) The global error of DCMGs.

to 12 Ω, and the attack data of F = [5,−5,0] is injected into DCMG 1 and 2, simultaneously. The detection output in Fig. 12(b) proves that the proposed scheme still succeeds to load step transients.

Case 2: Mitigation of FDIAs

Fig. 13 shows the mitigation of FDIAs with two successive stealth attacks, i.e., $\mathbf{F_1} = [3,-3,0]^T$ and $\mathbf{F_2} = [3,-2,0]^T$, each of 4 s interval for the DCMGC with resistive load.

During the stealth attacks, the original control signal is replaced with the alternative control signal in (35) when the detection output positively. Hence, the effect of the stealth attacks can be cancelled out, and the DCMGC still maintains the original control goal. The bus voltage and the output current of every DCMG remains as that is of without the stealth attacks. Finally, the stealth attacks are removed, and all state outputs are recovered smoothly. Throughout the transient process, the bus voltage, and the output current of every DCMG have always been behaving well with little disturbance.

In addition, Fig. 14 shows mitigation performance of the proposed scheme for the FDIAs with load step transients, where the system undergoes same load transients as in Fig. 12. Still, the results verify the success of the scheme with the load transients.

VI. CONCLUSIONS

This paper proposes the simple FDIAs detection and mitigation strategy via the alternative data for cyber security of power management in DCMGCs. Based on the analysis and the verification, conclusions can be drawn as follows:

(1) The proposed strategy can detect and mitigate the impact of the FDIAs in the cyber network of the distributed tertiary control for the DCMGC and has little side-effect on the operation of the original system. In addition, this algorithm-based strategy does not need any additional investment on the hardware and will be a cost-effective solution.

(2) The proposed strategy circumvents complicated

modeling for the DCMGC, and only several communication variables to have the simple calculations are required, and thus offers a more general way for the cyber security of the system.

(3) The implementation of the strategy is realized based on the distributed tertiary control framework of the DCMGC, which is of high reliability and scalability.

As a result, the prominent advantages of the proposed idea are that it circumvents the complicated modeling process of DCMGCs of high order and nonlinearity, reduces the computational burden, and offers more general application scenarios to DCMGCs with other topologies on power stages and communications.

Reference

[1] D. Tan and D. Novosel, "Energy challenge, power electronics & systems (PEAS) technology and grid modernization," in *CPSS Transactions on Power Electronics and Applications*, vol. 2, no. 1, pp. 3–11, Mar. 2017.

[2] E. Harmon, U. Ozgur, M. H. Cintuglu, R. de Azevedo, K. Akkaya, and O. A. Mohammed, "The internet of microgrids: A cloud-based framework for wide area networked microgrids," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 3, pp. 1262–1274, Mar. 2018.

[3] N. L. Diaz, T. Dragicevic, J. C. Vasquez, and J. M. Guerrero, "Intelligent distributed generation and storage units for DC microgrids—A new concept on cooperative control without communications beyond droop control," in *IEEE Transactions on Smart Grid*, vol. 5, no. 5, pp. 2476–2485, Sept. 2014.

[4] J. Ma, L. Yuan, Z. Zhao, and F. He, "Transmission loss optimization-based optimal power flow strategy by hierarchical control for DC microgrids," in *IEEE Transactions on Power Electronics*, vol. 32, no. 3, pp. 1952–1963, Mar. 2017.

[5] T. Dragičević, X. Lu, J. C. Vasquez, and J. M. Guerrero, "DC microgrids—part I: A review of control strategies and stabilization techniques," in *IEEE Transactions on Power Electronics*, vol. 31, no. 7, pp. 4876–4891, Jul. 2016.

[6] Y. Li, P. Dong, M. Liu, and G. Yang, "A distributed coordination control based on finite-time consensus algorithm for a cluster of DC microgrids," in *IEEE Transactions on Power Systems*, vol. 34, no. 3, pp. 2205–2215, May 2019.

[7] S. Sahoo, S. Mishra, S. M. Fazeli, F. Li, and T. Dragicevic, "A distributed fixed-time secondary controller for DC microgrid clusters," in *IEEE Transactions on Energy Conversion*, vol. 34, no. 4, pp. 1997–2007, Dec. 2019.

[8] Q. Shafiee, T. Dragicevic, J. C. Vasquez, and J. M. Guerrero, "Hierarchical control for multiple DC-microgrids clusters," in *IEEE Transactions on Energy Conversion*, vol. 29, no. 4, pp. 922–933, Dec. 2014.

[9] S. Moayedi and A. Davoudi, "Distributed tertiary control of DC microgrid clusters," in *IEEE Transactions on Power Electronics*, vol. 31, no. 2, pp. 1717–1733, Feb. 2016.

[10] S. Jena, N. P. Padhy, and J. M. Guerrero, "Cyber-resilient cooperative control of DC microgrid clusters," in *IEEE Systems Journal*, vol. 16, no. 2, pp. 1996–2007, Jun. 2022.

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

[12] S. Liu, X. Li, M. Xia, Q. Qin, and X. Liu, "Takagi-sugeno multimodeling-based large signal stability analysis of DC microgrid clusters," in *IEEE Transactions on Power Electronics*, vol. 36, no. 11, pp. 12670–12684, Nov. 2021.

[13] S. Mudaliyar, B. Duggal, and S. Mishra, "Distributed tie-line power flow control of autonomous DC microgrid clusters," in *IEEE Transactions on Power Electronics*, vol. 35, no. 10, pp. 11250–11266, Oct. 2020.

[14] M. Zaery, P. Wang, W. Wang, and D. Xu, "Distributed global economical load sharing for a cluster of DC microgrids," in *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 3410–3420, Sept. 2020.

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

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

[17] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical DC microgrids," in *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.

[18] J. Zhang, S. Sahoo, J. C. -H. Peng, and F. Blaabjerg, "Mitigating concurrent false data injection attacks in cooperative DC microgrids," in *IEEE Transactions on Power Electronics*, vol. 36, no. 8, pp. 9637–9647, Aug. 2021.

[19] L. Wei, D. Gao, and C. Luo, "False data injection attacks detection with deep belief networks in smart grid," in *2018 Chinese Automation Congress (CAC)*, Xi'an, China, 2018, pp. 2621–2625.

[20] Z. Lian and C. Deng, "Distributed security secondary control for cyber-physical microgrids systems under network DoS attacks," in *International Journal of Systems Science*, vol. 52, no. 6, pp. 1237–1250, Mar. 2021.

[21] C. Fang, Y. Qi, P. Cheng, and W. X. Zheng, "Cost-effective watermark based detector for replay attacks on cyber-physical systems," in *2017 11th Asian Control Conference (ASCC)*, Gold Coast, QLD, Australia, 2017, pp. 940–945.

[22] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G. -S. Seo *et al*., "A review of cyber–physical security for photovoltaic systems," in *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 4, pp. 4879–4901, Aug. 2022.

[23] Y. Jiang, Y. Yang, S. -C. Tan, and S. Y. Hui, "Distributed sliding mode observer-based secondary control for DC microgrids under cyber-attacks," in *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 11, no. 1, pp. 144–154, Mar. 2021.

[24] 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," in *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[25] A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, and G. Ferrari-Trecate, "Distributed cyber-attack detection in the secondary control of DC microgrids," in *2018 European Control Conference (ECC)*, Limassol, Cyprus, 2018, pp. 344-349.

[26] S. Abhinav, H. Modares, F. L. Lewis, and A. Davoudi, "Resilient cooperative control of DC microgrids," in *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 1083–1085, Jan. 2019.

[27] M. S. Sadabadi, S. Sahoo, and F. Blaabjerg, "Stability oriented design of cyber attack resilient controllers for cooperative DC microgrids," in *IEEE Transactions on Power Electronics*, vol. 37, no. 2, pp. 1310–1321, Feb. 2021.

[28] M. Leng, S. Sahoo, F. Blaabjerg, and M. Molinas, "Projections of cyberattacks on stability of DC microgrids—modeling principles and solution," in *IEEE Transactions on Power Electronics*, vol. 37, no. 10, pp. 11774–11786, Oct. 2022.

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

[30] K. S. Suprabhath, M. V. S. Prasad, S. Madichetty, and S. Mishra, "A deep learning based cyber attack detection scheme in DC microgrid systems," in *CPSS Transactions on Power Electronics and Applications*, vol. 8, no. 2, pp. 119–127, Jun. 2023.

[31] H. Cui, X. Dong, H. Deng, M. Dehghani, K. Alsubhi, and H. M. A. Aljahdali, "Cyber attack detection process in sensor of DC micro-grids under electric vehicle based on hilbert–huang transform and deep learning," in *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15885–15894, Jul. 2021.

[32] M. R. Habibi, S. Sahoo, S. Rivera, T. Dragicevic, and F. Blaabjerg, "De-

centralized coordinated cyberattack detection and mitigation strategy in DC microgrids based on artificial neural networks," in *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4629–4638, Aug. 2021.

[33] S. Sahoo, S. Mishra, J. C. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for DC microgrids," in *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

[34] S. Sahoo, J. C. Peng, A. Devakumar, S. Mishra, and T. Dragičević, "On detection of false data in cooperative DC microgrids—A discordant element approach," in *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, Aug. 2020.

[35] A. Takiddin, S. Rath, M. Ismail, and S. Sahoo, "Data-driven detection of stealth cyber-attacks in DC microgrids," in *IEEE Systems Journal*, vol. 16, no. 4, pp. 6097–6106, Dec. 2022.

[36] T. V. Vu, B. H. L. Nguyen, T. A. Ngo, M. Steurer, K. Schoder, and R. Hovsapian, "Distributed optimal dynamic state estimation for cyber intrusion detection in networked DC microgrids," *in IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*, Lisbon, Portugal, 2019, pp. 4050–4055.

Sucheng Liu received Ph.D. degree in Electrical Engineering from Chongqing University, Chongqing, China, in 2013. He has been with the Department of Electrical Engineering, Anhui University of Technology, where he is currently a Full Professor. He was a Visiting Research Associate with Queen's University, Kingston, Ontario, Canada, where he conducted two research projects sponsored by GE and NSERC, from Feb. 2015 to Feb. 2016. His research interests include modeling and control of DC microgrids and clusters, and design of switching power converters. He has published more than 60 refereed journal and conference papers and holds 16 patents and has 4 patents pending.

Dr. Liu is an IEEE Member, a CPSS Member, and a Member of IEEE Power Electronics Society. He also serves as an active reviewer for a dozen of international Journals and Conferences, such as *IEEE Transactions on Power Electronics, IEEE Journal of Emerging and Selected Topics in Power Electronics, IEEE Open Journal of Power Electronics, IEEE Transactions on Industrial Electronics*, etc. He was a TPC member of IEEE IPEC-Niigata 2018, and Session Chairs for IEEE WiPDA-Asia, CPSSC, and SPEED. He received Best Paper Awards at the IEEE International Conference on Predictive Control of Electrical Drives and Power Electronics (PRECEDE), Jinan, China, in 2021, IEEE International Conference on DC Microgrids (ICDCM), Matsue, Japan, in 2019, and The China Power Supply Society Conference (CPSSC), Shanghai, China, in 2017, respectively.

Guanggan Hu was born in Anhui, China, in 1997. He received the B.S. degree in Electrical Engineering and Automation from Anhui University of Technology, Ma'anshan, China, in 2021, where he is pursuing the M.S. degree in Electrical Engineering. His research interests include communications and cyber security of DC microgrids systems. He has published 1 refereed conference papers and has 1 patent pending.

Mengyu Xia was born in Anhui, China, in 1998. He received the M.S. degree in Electrical Engineering from Anhui University of Technology, Ma'anshan, China, in 2022. His research interests include communications and cyber security of DC microgrids systems. He has published 2 refereed conference papers and has 2 patents have been granted.

Qianjin Zhang received his Ph.D. degree in power electronics from Chongqing University, Chongqing, China, in 2020. He was a Visiting Scholar in the University of Exeter, Penryn, U.K., from May 2018 to May 2019. He is presently a Lecture with Anhui University of Technology, Anhui, China. His research interests include PV power generation, the modeling, control, and stability analysis of power electronics system.

Wei Fang was born in Anhui Province, China, in 1977. He received the B.S. degree from Anhui university of Technology, Anhui, China, in 1998, and M.S. and Ph.D. degrees from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2004 and 2008, respectively. He has been with Anhui university of Technology, since 2008 and is currently a Professor in the College of Electrical Engineering, Anhui university of Technology. He was a Visiting Scholar at Queen's University, Kinston, Ontario, Canada, from Sept. 2010 to Feb. 2011. His research interests are in the areas of switching power converters, and renewable energy.

Xiaodong Liu was born in Jilin, China, in 1971. He received the Ph.D. degree in Electric Machines and Electric Apparatus from Zhejiang University, Hangzhou, China, in 1999. Since 2003, he has been with School of Electrical and Information Engineering, Anhui University of Technology, Ma'anshan, China, where he is now a Full Professor. He was a visiting scholar at Queen's University, Kinston, Ontario, Canada, from July 2007 to Oct. 2007. His major fields of interest include the dc-dc switching converter, power factor correction techniques, and motor design and driving control.