Nonzero-Dynamics Stealthy Attack and Its Impacts Analysis in DC Microgrids

Mengxiang Liu[1], Chengcheng Zhao[1], Ruilong Deng[2], Peng Cheng[1], Wenhai Wang[1] and Jiming Chen[1]

***Abstract*— In this paper, we explore the potential stealthy attacks in the DC microgrid (DCmG) equipped with unknown input observer (UIO) based detectors, which are widely adopted for the detection and identification of cyber-attacks. We first prove that once the attacker knows the bounds of the initial state estimation error and the measurement noise, he/she can launch the nonzero-dynamics stealthy (NDS) attack in the DCmG, which can affect the detection residual while keep stealthy. Considering the complexity of the multi-layer control framework in the DCmG, we simplify the primary control loops as static unit gains and obtain the systematic dynamic model of the DCmG under the NDS attack. Then, we obtain the analytical expressions of the Point of Common Coupling (PCC) voltages, which are utilized to analyze the effects of the NDS attack on voltage balancing and current sharing, respectively. Moreover, we prove that under the NDS attack, the voltage and current convergence can still be achieved exponentially in the DCmG. Finally, extensive simulations are conducted in Simulink/PLECS to validate our theoretical results.**

I. INTRODUCTION

Due to the increasing penetration of distributed generation units (DGUs) such as solar photovoltaics (PVs), fuel cells, and microturbines into the power network, microgrids have become the most promising solution to make the power network stable, safe, resilient and efficient [1]. Generally, microgrids can be divided into AC microgrids and DC microgrids (DCmGs). And DCmGs have recently received much attention for their advantages including losses reduction for DC loads, easier integrations of DC DGUs, costs reduction for synchronizing generators, etc.

The basic objectives of DCmGs are voltage balancing and current sharing [2]. Normally, the hierarchical control framework based on specific communication technology is deployed to achieve these objectives [1]. According to different control laws, i.e., centralized and distributed methods, corresponding communication technologies are employed in DCmGs, e.g., the Narrowband Internet of Things technology [3] and the wireless rechargeable sensor network technology [4]. In this paper, we focus on the distributed control law, which has attracted much attention for its scalability and flexibility. However, the communication flows between DGUs are prone to cyber-attacks, which can adversely affect the integrity, availability, and confidentiality of the communication data, and thus cause economic losses or destabilize the voltages/currents. In the main grid, numerous works on the cyber security have been done in recent years [5], [6], since Liu *et al.* proposed the false data injection attack scheme against the state estimation process in the power network [7]. Meanwhile, due to the combination of characteristics like the low inertial distributed generators and the hierarchical control frameworks in DCmGs, small disturbance can cause devastating damage and it is challenging to give theoretical analysis considering the complex multi-layer dynamics. Therefore, the cyber-security issue of the DCmG has aroused widespread interests among researchers.

By utilizing the candidate invariants, Beg *et al.* [8] proposed a framework to detect the cyber-attacks in DCmGs, which inject false data into the global variables randomly. Then, Lu *et al.* [9] designed a distributed method to detect the cyber-attacks injecting constant signals into the communication links in microgrids, by checking the dual-ascent update iterations. As for model-based detection methods, the unknown input observer (UIO) techniques, which allow the design of observers with the existence of unknown inputs (e.g., injected malicious signals), are widely adopted to detect and identify malicious nodes/compromised links in unreliable networks [10]. Recently, a novel UIO-based detector was proposed to detect and identify specific cyber-attacks in DCmGs [11], where each DGU estimates neighbors' states and requires only neighbors' knowledge.

However, most existing works (like the aforementioned ones [8]–[11]) assumed that attackers have little knowledge of the system model. Actually, intelligent attackers can learn critical system parameters by hiding themselves in the system, and launch the attacks at appropriate time, which can cause devastating damage like the Stuxnet and even threaten human life. In this paper, we investigate the zero-dynamics stealthy (ZDS) attack and the nonzero-dynamics stealthy (NDS) attack in current DCmG [12]. The ZDS attack, which injects the zero output signals into systems, has been deeply investigated in cyber-physical systems [13]. Since the ZDS attack is invisible at the output, it can bypass the detector and cause disturbance on system states. Whereas the NDS attack is firstly explored in the DCmG, which can bypass the detector by masking itself as the state estimation error and the measurement noise. Considering the novel detector proposed in [11], we firstly investigate the potential stealthy

This work was partially supported by National Key Research and Development Program under Grant 2018YBF0803501, the NSFC under Grant 61833015, the NTU Internal Funding - SUG - CoE under Grant M4082287 and the A*STAR-NTU-SUTD AI Partnership under Grant RGANS1906.

[1]Mengxiang Liu, Chengcheng Zhao, Peng Cheng, Wenhai Wang, and Jiming Chen are with State Key Lab. of Industrial Control Technology, Zhejiang University, Hangzhou, 310027, P. R. China. Emails: {liumengxiang329, zccsq90}@gmail.com; {pcheng, whwang,jmchen}@iipc.zju.edu.cn

[2]Ruilong Deng is with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. Email: rldeng@ntu.edu.sg

attacks in the DCmG, and main contributions are listed as follows:

1) We prove that there exists no ZDS attack in current DCmG, and provide the NDS attack by exploiting the state estimation error and the measurement noise.
2) By approximating the primary control loops as static unit gains, we analyze the dynamics of the DCmG under the NDS attack, and obtain analytical expressions of the Point of Common Coupling (PCC) voltages.
3) The steady-state PCC voltages and output currents are analyzed to verify the voltage balancing and current sharing, respectively. Moreover, exponential convergence rates of voltages/currents are proved to be guaranteed under the NDS attack. Finally, simulations are conducted to validate our theoretical results.

The rest of this paper is organized as follows. Section II presents the DCmG system model, the UIO-based detector, and the problem formulation. Then, we provide the NDS attack and analyze its effects on the voltage balancing, current sharing, and convergence rates of voltages/currents in Section III. Extensive simulations are presented in Section IV and Section V concludes this paper.

II. PRELIMINARIES AND PROBLEM FORMULATION

Notation: In this paper, $|\cdot|$ denotes the cardinality of a finite set and the component-by-component absolute value of a matrix/vector, $\|\cdot\|$ is the norm of a matrix/vector, the inequality between matrices/vectors is compared component-by-component, and $y(\infty)=\lim_{t\to\infty} y(t)$, where $y(t)$ denotes a scalar/vector. Moreover, $\mathbb{1}^{n\times n}/\mathbb{1}^n$ and $\mathbb{0}^{n\times n}/\mathbb{0}^n$ are matrices/vectors with all 1 and 0 entries respectively, and $\mathbf{I}^n$ denotes a unit matrix with $n\times n$ dimension. $\mathbb{H}^1$ denotes a subspace of $\mathbb{R}^n$ and $\forall \boldsymbol{v}\in\mathbb{H}^1, \langle \boldsymbol{v}\rangle=0$, where $\langle \boldsymbol{v}\rangle=\frac{1}{n}\sum_{i=1}^n v_i$ returns the average of vector $\boldsymbol{v}$ and the dimension of $\mathbb{H}^1$ is calculated as $\dim\{\mathbb{H}^1\}=n-1$. $\mathbb{H}^1_\perp$ is the orthogonal vector space of $\mathbb{H}^1$, where $\boldsymbol{v}=\alpha\mathbb{1}^n, \alpha\in\mathbb{R}, \forall \boldsymbol{v}\in\mathbb{H}^1_\perp$ and $\dim\{\mathbb{H}^1_\perp\}=1$. Therefore, the decomposition can be obtained as $\mathbb{R}^n=\mathbb{H}^1\oplus\mathbb{H}^1_\perp$, where $\oplus$ denotes the direct sum of vector spaces.

A. Network Model

Physical Network: The DCmG is consisted of N DGUs interconnected through power lines, and a digraph $\mathcal{G}_{el}=\{\boldsymbol{\nu},\boldsymbol{\varepsilon_{el}},\boldsymbol{W}\}$ is used to characterize the electrical model of the DCmG. $\boldsymbol{\nu}=\{1,2,...,N\}$ is the set of nodes (DGUs), and $\boldsymbol{\varepsilon_{el}}\subset\boldsymbol{\nu}\times\boldsymbol{\nu}$ denotes the set of edges (power lines), whose orientations are defined arbitrarily for reference directions of positive currents. Moreover, $\boldsymbol{W}=\text{diag}\{\frac{1}{R_{ij}}\}\in\mathbb{R}^{|\boldsymbol{\varepsilon_{el}}|\times|\boldsymbol{\varepsilon_{el}}|}$, where R_{ij} denotes the resistance of power line $(i,j)\in\boldsymbol{\varepsilon_{el}}$. The neighbor set of DGU i is denoted by $\mathcal{N}_i^{el}=\{j|(i,j)\in\boldsymbol{\varepsilon_{el}}$ or $(j,i)\in\boldsymbol{\varepsilon_{el}},\forall j\in\boldsymbol{\nu}\}$. $\boldsymbol{B}\in\mathbb{R}^{|\boldsymbol{\nu}|\times|\boldsymbol{\varepsilon_{el}}|}$ denotes the incidence matrix, with which the Laplacian Matrix can be calculated independently of edges' orientations, i.e., $\boldsymbol{M}=\boldsymbol{BWB}^{\mathrm{T}}$.

Communication Network: As for the communication network in the DCmG, an undirected graph $\mathcal{G}_c=\{\boldsymbol{\nu},\boldsymbol{\varepsilon_c},\boldsymbol{W_c}\}$ is used to model the bidirectional communication among DGUs. Here, $\boldsymbol{\nu}$ is the set of DGU nodes, and $\boldsymbol{\varepsilon_c}$ denotes the set of edges (communication links). Moreover, $\boldsymbol{W_c}=\text{diag}\{a_{ij}\}\in\mathbb{R}^{|\boldsymbol{\varepsilon_c}|\times|\boldsymbol{\varepsilon_c}|}$, where a_{ij} is the weight of communication link $(i,j)\in\boldsymbol{\varepsilon_c}$. And $\mathcal{N}_i^c=\{j|(i,j)\in\boldsymbol{\varepsilon_c},\forall j\in\boldsymbol{\nu}\}$ denotes the neighbor set of DGU i. The Laplacian Matrix of $\mathcal{G}_c$ is given by $\boldsymbol{L}$. Furthermore, $\mathcal{G}_{el}$ and $\mathcal{G}_c$ should satisfy Assumption 1 to guarantee stable control of voltages/currents in the DCmG [12].

Assumption 1: The digraph $\mathcal{G}_{el}$ is weakly connected and the undirected graph $\mathcal{G}_c$ is connected. Moreover, $\mathcal{G}_{el}$ and $\mathcal{G}_c$ have the same topology, and $\boldsymbol{L}=\gamma\boldsymbol{M},\gamma>0$.

B. Dynamic Model

Each DGU is modeled as a DC voltage source and a buck converter to supply the local load current connected to the Point of Common Coupling (PCC) through an RLC filter [14] as shown in Fig.1. The dynamic of DGU i is given as

$$\begin{cases}\dfrac{dV_i}{dt}=\dfrac{1}{C_{ti}}I_{ti}+\displaystyle\sum_{j\in\mathcal{N}_i^{el}}\frac{1}{C_{ti}R_{ij}}(V_j-V_i)-\frac{1}{C_{ti}}I_{Li}\\ \dfrac{dI_{ti}}{dt}=-\dfrac{1}{L_{ti}}V_i-\dfrac{R_{ti}}{L_{ti}}I_{ti}+\dfrac{1}{L_{ti}}V_{ti},\end{cases}\tag{1}$$

where V_{ti} is the output voltage of buck converter i, I_{Li} is the load current unknown to DGU i, V_i and I_{ti} are the measured voltage and the output current at PCC i respectively (see Fig.1), R_{ti},L_{ti},C_{ti} are parameters of the RLC filter, and V_j is the PCC voltage of neighbor node $j\in\mathcal{N}_i^{el}$.

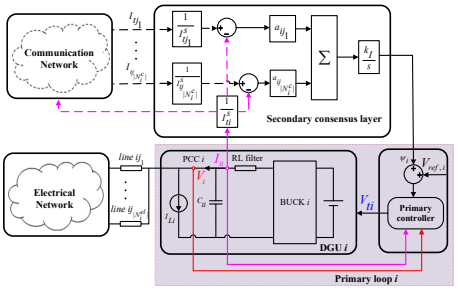

Fig. 1. The hierarchical control framework of DGU i, where the communication network models its interactions with neighbors $\mathcal{N}_i^c$ and the electrical network models the physical couplings with neighbors $\mathcal{N}_i^{el}$.

A hierarchical control framework is adopted to achieve the regulation of voltages and currents, where the primary Proportional Integral (PI) controller tracks the reference voltage and the secondary controller achieves the global proportional current sharing by employing the consensus algorithm (As Fig.1 shows) [12]. Considering the secondary inputs, the exogenous inputs, and the system noise, the state space model of DGU i can be obtained as

$$\begin{cases}\dot{\boldsymbol{x}}_{\boldsymbol{i}}(t)=\boldsymbol{A_{ii}x_i}(t)+\boldsymbol{b}_{\boldsymbol{i}}u_i(t)+\boldsymbol{g_i}\psi_i(t)+\\ \qquad\qquad+\boldsymbol{M_i d_i}(t)+\boldsymbol{\xi_i}(t)+\boldsymbol{\omega_i}(t)\\ \boldsymbol{y_i}(t)=\boldsymbol{C_i x_i}(t)+\boldsymbol{\rho_i}(t),\end{cases}\tag{2}$$

where $\boldsymbol{x_i}=[V_i,I_{ti},v_i]^{\mathrm{T}}$ is the local state vector, and v_i is the voltage error integral item. The dynamic of v_i is $\dot{v}_i=V_{ref,i}+\psi_i-V_i$, where $V_{ref,i}$ is the reference voltage of DGU i, ψ_i is the secondary input and the corresponding parameter vector $\boldsymbol{g_i}=[0,0,1]^{\mathrm{T}}$. Besides, $\boldsymbol{d_i}=[I_{Li},V_{ref,i}]^{\mathrm{T}}$ is the exogenous input vector, and $\boldsymbol{y_i}\in\mathbb{R}^3$ denotes the

measurement output vector. The physical coupling with neighbor DGUs is modeled as $\boldsymbol{\xi_i} = \sum_{j\in\mathcal{N}_i^{el}} \boldsymbol{A_{ij}x_j} \in \mathbb{R}^3$. Moreover, the process noise and measurement noise are modeled as $|\boldsymbol{\omega_i}(t)| \leq \bar{\boldsymbol{\omega}}_{\boldsymbol{i}} \in \mathbb{R}^3, |\boldsymbol{\rho_i}(t)| \leq \bar{\boldsymbol{\rho}}_{\boldsymbol{i}} \in \mathbb{R}^3, \forall t \geq 0$ respectively, which are bounded by some certain bounds. And interested readers can refer to [14] for information of $\boldsymbol{A_{ii}}, \boldsymbol{A_{ij}}, \boldsymbol{C_i}, \boldsymbol{M_i}, \boldsymbol{b_i}$ in detail.

The primary control input $V_{ti} = u_i(t) = \boldsymbol{k_i}^{\mathrm{T}}\boldsymbol{y_i}(t)$, where the control gain vector $\boldsymbol{k_i} \in \mathbb{R}^3$ is designed by using local information to achieve the plug-and-play operation [14]. And the secondary control input $\psi_i(t)$ is computed by the following consensus scheme to adjust the reference voltage,

$$\dot{\psi}_i(t) = -[0, k_I, 0] \sum_{j\in\mathcal{N}_i^c} a_{ij}\left(\frac{\boldsymbol{y_i}(t)}{I_{ti}^s} - \frac{\boldsymbol{y_{i,j}^c}(t)}{I_{tj}^s}\right), \tag{3}$$

where $\boldsymbol{y_{i,j}^c}(t) \in \mathbb{R}^3$ is the output vector of DGU j transmitted to DGU i through link (i, j), $I_{ti}^s > 0$ is the rated current of DGU i, $k_I > 0$ is the consensus value common to all communication links, and $a_{ij} = a_{ji} > 0$ is the link weight. Under Assumption 2, the definitions of voltage balancing and current sharing are given.

Assumption 2: The reference voltages are equal among all DGUs, i.e., $V_{ref,i} = V_{ref}, \forall i \in \boldsymbol{\nu}$.

Definition 1 (Voltage Balancing): Voltage balancing is achieved if $\langle \boldsymbol{v}(\infty)\rangle = V_{ref}$, where $\langle \boldsymbol{v}(\infty)\rangle$ is the steady-state average voltage of all PCCs.

Definition 2 (Current Sharing): Current sharing is achieved if $\frac{I_{ti}^{\infty}}{I_{ti}^s} = \frac{I_{tj}^{\infty}}{I_{tj}^s}$, $\forall i, j \in \boldsymbol{\nu}$, i.e., the load currents are shared proportionally to DGUs' rated currents.

C. UIO-based Detector

We consider the cyber-attacks injecting false data into the communication links. Since DGU j shares the full measurement output vector to its neighbors, we can model the attack compromising the communication link from DGU j to i as

$$\boldsymbol{y_{i,j}^c}(t) = \boldsymbol{y_j}(t) + \tau(t - T_a)\boldsymbol{\phi_{i,j}}(t), \tag{4}$$

where $\boldsymbol{\phi_{i,j}}(t)$ is the injected attack vector, $\boldsymbol{y_{i,j}^c}(t)$ is the data that DGU i receives from DGU j, and $\tau(t - T_a)$ is a step function with T_a time delay, i.e., the attack is started at $t = T_a$. And the attacker only compromises the communication data between DGUs, which means that the measurements inside DGUs are secure, and thus the primary control loops are not affected.

The UIO techniques are adopted to detect and identify the cyber-attacks in DCmG, where each DGU estimates neighbor DGUs' states without the knowledge of their inputs [11]. And a full order UIO in DGU i is given as follows,

$$\begin{cases} \dot{\boldsymbol{z}}_{\boldsymbol{i,j}}(t) = \boldsymbol{F_j z_{i,j}}(t) + \boldsymbol{T_j b_j}\bar{u}_j(t) + \hat{\boldsymbol{K}}_{\boldsymbol{j}}\boldsymbol{y_{i,j}^c}(t) \\ \hat{\boldsymbol{x}}_{\boldsymbol{i,j}}(t) = \boldsymbol{z_{i,j}}(t) + \boldsymbol{H_j y_{i,j}^c}(t), \end{cases} \tag{5}$$

where $\boldsymbol{z_{i,j}}(t)$ denotes the internal state vector of UIO i, $\hat{\boldsymbol{x}}_{\boldsymbol{i,j}}(t)$ denotes the output vector of UIO i, i.e., the estimated state vector of DGU j, $\bar{u}_j = 0$, and $\boldsymbol{F_j}, \boldsymbol{T_j}, \hat{\boldsymbol{K}}_{\boldsymbol{j}}, \boldsymbol{H_j} \in \mathbb{R}^{3\times 3}$ are parameters of the observer.

According to the characteristics of the system matrix $\boldsymbol{C_j} = \mathbf{I}$, the convergence conditions of UIO i can obviously be satisfied [14]. And matrices $\boldsymbol{F_j}, \boldsymbol{T_j}, \hat{\boldsymbol{K}}_{\boldsymbol{j}}, \boldsymbol{H_j}$ are designed as that in [11], from which a stable matrix $\boldsymbol{F_j}$ is obtained. In the absence of cyber-attacks, the state estimation error vector $\boldsymbol{\epsilon_{i,j}}(t) = \boldsymbol{x_j}(t) - \hat{\boldsymbol{x}}_{\boldsymbol{i,j}}(t)$ can be obtained as

$$\boldsymbol{\epsilon_{i,j}}(t) = e^{\boldsymbol{F_j}t}\boldsymbol{\sigma_{i,j}^1}(0) - \boldsymbol{H_j\rho_j}(t) + \int_0^t e^{\boldsymbol{F_j}(t-\tau)}\boldsymbol{\sigma_{i,j}^2}(\tau)d\tau, \tag{6}$$

where $\boldsymbol{\sigma_{i,j}^1}(0) = \boldsymbol{\epsilon_{i,j}}(0) + \boldsymbol{H_j\rho_j}(0)$ and $\boldsymbol{\sigma_{i,j}^2}(t) = \boldsymbol{T_j\omega_j}(t) + (\boldsymbol{T_j b_j k_j} - \hat{\boldsymbol{K}}_{\boldsymbol{j}})\boldsymbol{\rho_j}(t)$. Since $\boldsymbol{F_j}$ is stable, there always exists positive κ, μ such that $||e^{\boldsymbol{F_j}t}|| \leq \kappa e^{-\mu t}$. And the residual vector is $\boldsymbol{r_{i,j}}(t) = \boldsymbol{y_{i,j}^c}(t) - \boldsymbol{C_j}\hat{\boldsymbol{x}}_{\boldsymbol{i,j}}(t) = \boldsymbol{\epsilon_{i,j}}(t) + \boldsymbol{\rho_j}(t)$, from which the upper bound of $|\boldsymbol{r_{i,j}}(t)|$ can be obtained as

$$\bar{\boldsymbol{r}}_{\boldsymbol{i,j}}(t) = \kappa e^{-\mu t}\bar{\boldsymbol{\sigma}}_{\boldsymbol{i,j}}^{\boldsymbol{1}}(0) + |\boldsymbol{T_j}|\bar{\boldsymbol{\rho}}_{\boldsymbol{j}} + \int_0^t \kappa e^{-\mu(t-\tau)}\bar{\boldsymbol{\sigma}}_{\boldsymbol{i,j}}^{\boldsymbol{2}}(\tau)d\tau, \tag{7}$$

where $\bar{\boldsymbol{\sigma}}_{\boldsymbol{i,j}}^{\boldsymbol{1}}(0) = \bar{\boldsymbol{\epsilon}}_{\boldsymbol{i,j}}(0) + |\boldsymbol{H_j}|\bar{\boldsymbol{\rho}}_{\boldsymbol{j}}$, $\bar{\boldsymbol{\sigma}}_{\boldsymbol{i,j}}^{\boldsymbol{2}}(t) = |\boldsymbol{T_j}|\bar{\boldsymbol{\omega}}_{\boldsymbol{j}} + |\boldsymbol{T_j b_j k_j} - \hat{\boldsymbol{K}}_{\boldsymbol{j}}|\bar{\boldsymbol{\rho}}_{\boldsymbol{j}}$, and $\bar{\boldsymbol{\epsilon}}_{\boldsymbol{i,j}}(0)$ is the bound of the initial state estimation error such that $\bar{\boldsymbol{\epsilon}}_{\boldsymbol{i,j}}(0) \geq |\boldsymbol{\epsilon_{i,j}}(0)|$ always holds. Then, we can obtain the new residual vector under the attack (4) as $\tilde{\boldsymbol{r}}_{\boldsymbol{i,j}}(t) = \boldsymbol{r_{i,j}}(t) + \boldsymbol{r_{i,j}^a}(t), t \geq T_a$, where $\boldsymbol{r_{i,j}^a}(t)$ is the attack impact on the detection residual, i.e.,

$$\begin{aligned} \boldsymbol{r_{i,j}^a}(t) = {} & e^{\boldsymbol{F_j}(t-T_a)}\boldsymbol{H_j\phi_{i,j}}(T_a) + \boldsymbol{T_j\phi_{i,j}}(t) + \\ & - \int_{T_a}^t e^{\boldsymbol{F_j}(t-\tau)}\hat{\boldsymbol{K}}_{\boldsymbol{j}}\boldsymbol{\phi_{i,j}}(\tau)d\tau. \end{aligned} \tag{8}$$

Lemma 1: If there holds

$$|\boldsymbol{r_{i,j}^a}(t)| > 2\bar{\boldsymbol{r}}_{\boldsymbol{i,j}}(t), t > T_d, \tag{9}$$

the UIO-based detector (5) can detect the attack (4) in communication link (i, j).

Remark 1: The developed detection threshold $\bar{\boldsymbol{r}}_{\boldsymbol{i,j}}(t)$ can ensure the absence of the false alarm [11]. However, due to the restrictive trade-off between the false-alarm and the missed-alarm in the model-based detection method [15], it is obvious that the detection threshold $\bar{\boldsymbol{r}}_{\boldsymbol{i,j}}(t)$ cannot simultaneously guarantee zero missed-alarm, which means that the detection condition (9) is only sufficient and the stealthy attacks may exist.

D. Problem Formulation

If the attacker knows some static parameters of the DGU model and the UIO-based detector, it is possible to design the ZDS attack, which can introduce disturbance to the system state without affecting the detection residual. Moreover, once the attacker can infer the bounds of the initial state estimation error and the measurement noise by eavesdropping DGUs' output measurements, it is likely to design the NDS attack, which will affect the detection residual while keep stealthy. Accordingly, the first problem is to investigate the existence of the ZDS and NDS attacks in current DCmG [12]. If there exists potential stealthy attacks, it is urgent to analyze how the stealthy attacks will affect the performances of the DCmG. We mainly concern about performances of two aspects, which include the steady-state performances (e.g., the voltage balancing and current sharing) and the dynamic performances (e.g., the convergence rates of currents/voltages). Therefore, the second problem is to fully investigate the impacts of the potential stealthy attacks on the DCmG.

III. MAIN RESULTS

In this section, we present main results of this paper, including the potential stealthy attacks and their impacts analysis. We mainly consider stealthy attacks that can bypass the UIO-based detector and still cause disturbance to the DCmG. The definitions of the ZDS and NDS attacks are given as follows:

Definition 3 (ZDS Attack): The attack is ZDS if the estimation residual vector is unaffected and the injected attack vector is not always zero, i.e.,

$$\begin{cases} |\boldsymbol{r}^{\boldsymbol{a}}_{\boldsymbol{i,j}}(t)| = \mathbb{0}^3, \forall t \geq T_a \\ \boldsymbol{\phi_{i,j}}(t) \neq \mathbb{0}^3, \exists t \geq T_a \end{cases}, (i,j) \in \boldsymbol{\varepsilon_c}. \tag{10}$$

Definition 4 (NDS Attack): The attack is NDS if the estimation residual vector is affected but still within the detection threshold, and the attack vector is not always zero, i.e.,

$$\begin{cases} |\boldsymbol{r}^{\boldsymbol{a}}_{\boldsymbol{i,j}}(t)| \neq \mathbb{0}^3, \exists t \geq T_a \\ |\tilde{\boldsymbol{r}}_{\boldsymbol{i,j}}(t)| \leq \bar{\boldsymbol{r}}_{\boldsymbol{i,j}}(t), \forall t \geq T_a, (i,j) \in \boldsymbol{\varepsilon_c}. \\ \boldsymbol{\phi_{i,j}}(t) \neq \mathbb{0}^3, \exists t \geq T_a \end{cases} \tag{11}$$

A. Potential Stealthy Attacks

First, we prove that there exists no ZDS attack in the DCmG, and then obtain the NDS attack by exploiting the state estimation error and the measurement noise.

Theorem 1: Under the constraints of the UIO-based detector, there exists no ZDS attack in current DCmG [12].

Proof: By combining (8) with the residual condition in (10), the constraints can be obtained as

$$\begin{cases} \boldsymbol{T_j}\dot{\boldsymbol{\phi}}_{\boldsymbol{i,j}}(t) = (\boldsymbol{F_j T_j} + \hat{\boldsymbol{K}}_{\boldsymbol{j}})\boldsymbol{\phi_{i,j}}(t) \\ (\boldsymbol{H_j} + \boldsymbol{T_j})\boldsymbol{\phi_{i,j}}(T_a) = \mathbf{0}. \end{cases} \tag{12}$$

Moreover, from the design rules of the UIO-based detector [11], we have $\boldsymbol{F_j T_j} + \hat{\boldsymbol{K}}_{\boldsymbol{j}} = \boldsymbol{T_j A_{kj}}, \boldsymbol{H_j} + \boldsymbol{T_j} = \mathbf{I^3}$, where $\boldsymbol{A_{kj}} = \boldsymbol{A_{jj}} + \boldsymbol{b_j k_j^{\mathrm{T}}} \in \mathbb{R}^{3\times 3}$ denotes the control parameter matrix of (2). And then combining with (12), we can get

$$\boldsymbol{\phi_{i,j}}(t) = \mathbb{0}^3, t \geq T_a, \tag{13}$$

which contradicts with the attack vector condition in (10). And thus there exists no ZDS attack in current DCmG. ■

Actually, a similar definition of the ZDS attack has been proposed in [11], but the existence of the ZDS attack was not solved. In this paper, we find that there exists no ZDS attack in current DCmG which is based on the consensus algorithm. Whereas the existence of ZDS attacks in DCmGs under other control algorithms, e.g., the sliding control [16], is remained to be investigated in future work. And the NDS attack is obtained in Theorem 2.

Theorem 2: By exploiting the state estimation error and measurement noise, the NDS attack on communication link (i,j) is given as

$$\begin{cases} \boldsymbol{\phi_{i,j}}(t) = e^{\boldsymbol{A_{kj}}(t-T_a)}\boldsymbol{\phi_{i,j}}(T_a), t \geq T_a \\ \boldsymbol{\phi_{i,j}}(T_a) = e^{\boldsymbol{F_j}T_a}\tilde{\boldsymbol{I}}\tilde{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0), \end{cases} \tag{14}$$

where the non-zero vector $|\tilde{\boldsymbol{I}}\tilde{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)| \leq |\boldsymbol{\sigma}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)| + \bar{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)$, and $\tilde{\boldsymbol{I}} \in \mathbb{R}^3$ is derived from a unit matrix $\mathbf{I}^3$ with its $(2,2)_{th}$ diagonal entry replaced by 0.

Proof: Since $\boldsymbol{T_j}\boldsymbol{\phi_{i,j}}(T_a) = \mathbf{0}$ and $\boldsymbol{T_j} = \boldsymbol{I} - \boldsymbol{H_j}$, we can get $\boldsymbol{H_j}\boldsymbol{\phi_{i,j}}(T_a) = \boldsymbol{\phi_{i,j}}(T_a)$. Moreover, if $e^{\boldsymbol{F_j}T_a}\tilde{\boldsymbol{I}} = \tilde{\boldsymbol{I}}e^{\boldsymbol{F_j}T_a}$ is satisfied[1], then we can obtain the following equation by substituting (14) into (8):

$$\boldsymbol{r}^{\boldsymbol{a}}_{\boldsymbol{i,j}}(t) = e^{\boldsymbol{F_j}t}\tilde{\boldsymbol{I}}\tilde{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0), t \geq T_a, \tag{15}$$

and the residual vector under the attack (14) can be obtained as

$$\begin{aligned} \tilde{\boldsymbol{r}}_{\boldsymbol{i,j}}(t) =& e^{\boldsymbol{F_j}t}(\tilde{\boldsymbol{I}}\tilde{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0) + \boldsymbol{\sigma}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)) + \boldsymbol{T_j}\boldsymbol{\rho_j}(t) + \\ &+ \int_0^t e^{\boldsymbol{F_j}(t-\tau)}\boldsymbol{\sigma}^{\boldsymbol{2}}_{\boldsymbol{i,j}}(\tau)d\tau, t \geq T_a. \end{aligned} \tag{16}$$

With $|\boldsymbol{\sigma}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)| \leq \bar{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)$, there always exists a non-zero vector $|\tilde{\boldsymbol{I}}\tilde{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)| \leq |\boldsymbol{\sigma}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)| + \bar{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)$ such that $|\tilde{\boldsymbol{I}}\tilde{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0) + \boldsymbol{\sigma}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)| \leq \bar{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)$, and $|\boldsymbol{r}^{\boldsymbol{a}}_{\boldsymbol{i,j}}(t)| \neq \mathbb{0}^3, \exists t \geq T_a$. Therefore,

$$|\tilde{\boldsymbol{r}}_{\boldsymbol{i,j}}(t)| \leq \bar{\tilde{\boldsymbol{r}}}_{\boldsymbol{i,j}}(t) \leq \bar{\boldsymbol{r}}_{\boldsymbol{i,j}}(t), t \geq T_a \tag{17}$$

where $\bar{\tilde{\boldsymbol{r}}}_{\boldsymbol{i,j}}(t) = \kappa e^{-\mu t}|\tilde{\boldsymbol{I}}\tilde{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0) + \boldsymbol{\sigma}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)| + |\boldsymbol{T_j}|\bar{\boldsymbol{\rho}}_{\boldsymbol{j}} + \int_0^t \kappa e^{-\mu(t-\tau)}\bar{\boldsymbol{\sigma}}^{\boldsymbol{2}}_{\boldsymbol{i,j}}(\tau)d\tau, t \geq T_a$ denotes the tighter residual threshold caused by the carefully designed attack vector (14). Thus, the residual vector $\tilde{\boldsymbol{r}}_{\boldsymbol{i,j}}(t)$ under the attack is still within the detection threshold, and it is proved that the attack (14) is NDS. ■

Remark 2: Since $\boldsymbol{A_{kj}}$ is stable, the magnitude of $\boldsymbol{\phi_{i,j}}(t)$, which determines the attack impacts on the DCmG, can be approximated as the initial value $\boldsymbol{\phi_{i,j}}(T_a)$. Under the constraints of (14), $\boldsymbol{\phi_{i,j}}(T_a)$ is positive proportional to the bounds of the initial state estimation error and the measurement noise, negative proportional to the attack start time T_a. Apparently, the state estimation error will be closer to zero with a larger attack start time T_a, and thus the initial value of the attack vector $\boldsymbol{\phi_{i,j}}(T_a)$ will be more restricted. Moreover, the bound of the initial state estimation error could be considerably large if the DGU cannot infer neighbors' initial states accurately, especially with the disturbance of unknown inputs in neighbor DGUs. Moreover, the detection redundancy[2] $\bar{\boldsymbol{r}}_{\boldsymbol{i,j}}(t) - |\boldsymbol{r_{i,j}}(t)|$ may allow the existence of the NDS attack with $|\tilde{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)| \geq |\boldsymbol{\sigma}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)| + \bar{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{i,j}}(0)$, which will be investigated in simulations. And the value of the detection redundancy is related to the state estimation error, measurement noise, and the parameters in residual thresholds(e.g., $\kappa, \mu, \boldsymbol{T_j}, \boldsymbol{H_j}$, etc.).

B. Attack Impacts Analysis

Under the NDS attack in Theorem 2, we theoretically analyze the attack impacts on the voltage balancing, current sharing, and the convergence rates of voltages/currents in

[1] $\boldsymbol{F_j}$ is designed to be stable simultaneously.

[2] The detection redundancy denotes the gap between the residual and its detection threshold. On the one hand, an appropriate detection redundancy can decrease the false-alarm caused by the uncertainties, e.g., the initial state estimation error. On the other hand, a high detection redundancy will increase the missed-alarm and the trade off relationship need to be carefully considered.

current DCmG [12]. The secondary inputs of the DCmG can be obtained from (3) as

$$\dot{\boldsymbol{\psi}}(t) = -\tilde{\boldsymbol{L}}\boldsymbol{D}\boldsymbol{i_t}(t), \tag{18}$$

where $\boldsymbol{\psi}(t) = [\psi_1(t), ..., \psi_N(t)]^{\mathrm{T}}, \tilde{\boldsymbol{L}} = k_I\boldsymbol{L}, \boldsymbol{D} = \mathrm{diag}\{\frac{1}{I^s_{t1}}, ..., \frac{1}{I^s_{tN}}\}$, and $\boldsymbol{i_t}(t) = [I_{t1}, ..., I_{tN}]^{\mathrm{T}}$. And the primary control loops can be approximated as unit gains [12], i.e.,

$$\boldsymbol{v}(t) = \boldsymbol{v_{ref}} + \boldsymbol{\psi}(t), \tag{19}$$

where $\boldsymbol{v} = [V_1, ..., V_N]^{\mathrm{T}}$, and $\boldsymbol{v_{ref}} = [V_{ref,1}, ..., V_{ref,N}]^{\mathrm{T}}$. By utilizing the Kirchhoff's laws, the dynamics of the DCmG can be obtained as

$$\dot{\boldsymbol{\psi}}(t) = -\boldsymbol{Q}\boldsymbol{\psi}(t) - \tilde{\boldsymbol{L}}\boldsymbol{D}\boldsymbol{i_l} - \boldsymbol{Q}\boldsymbol{v_{ref}}, \tag{20}$$

where $\boldsymbol{i_l} = [I_{L1}, ..., I_{LN}]^{\mathrm{T}}$ and $\boldsymbol{Q} = \tilde{\boldsymbol{L}}\boldsymbol{D}\boldsymbol{M}$ integrates Laplacian Matrices of $\mathcal{G}_c$ and $\mathcal{G}_{el}$. Under Assumption 1, $\boldsymbol{Q} = k_I\gamma\boldsymbol{M}\boldsymbol{D}\boldsymbol{M}$, $a_{ij} = \frac{\gamma}{R_{ij}}$, and moreover, voltage balancing and current sharing are exponentially achieved [12].

Since the attacker only compromises communication data between DGUs, the measurements inside DGUs are not affected. Therefore, the primary control loops can also be approximated as unit gains $\tilde{\boldsymbol{v}}(t) = \boldsymbol{v_{ref}} + \tilde{\boldsymbol{\psi}}(t)$, where $\tilde{\boldsymbol{v}}(t)$ and $\tilde{\boldsymbol{\psi}}(t)$ are the PCC voltage vector and the secondary input vector under the NDS attack, respectively. Given the additivity of attack impacts when compromising multi-links (multiply communication links), we only analyze the scenario that only one communication link (i, j) is compromised, and specifically $\boldsymbol{\phi_{i,j}}(t)$ is injected into the data transmitted from DGU j to i. Under the NDS attack on link (i, j), the dynamics of the DCmG are re-modeled as follows:

$$\dot{\tilde{\boldsymbol{\psi}}}(t) = -\boldsymbol{Q}\tilde{\boldsymbol{\psi}}(t) - \tilde{\boldsymbol{L}}\boldsymbol{D}\boldsymbol{i_l} - \boldsymbol{Q}\boldsymbol{v_{ref}} + C_a\phi_2(t)\boldsymbol{l}, \tag{21}$$

where $C_a = \frac{k_I a_{ij}}{I^s_{tj}}$, $\boldsymbol{l} = \tilde{\mathbb{0}}^n_i \in \mathbb{R}^n$, $\tilde{\mathbb{0}}^n_i$ is derived from a zero vector with its i_{th} entry replaced by 1 to denote the destination of the compromised data (i.e., DGU i), and $\phi_2(t)$ is the second entry of $\boldsymbol{\phi_{i,j}}(t)$. The secondary input vector is decomposed as $\tilde{\boldsymbol{\psi}}(t) = \boldsymbol{\psi}(t) + \boldsymbol{\psi_a}(t)$, where $\boldsymbol{\psi_a}(t)$ denotes the attack impacts on secondary inputs modeled by the last element $C_a\phi_2(t)\boldsymbol{l}$ in (21).

Theorem 3: When there exists a NDS attack in link (i, j), current sharing can still be achieved while voltage balancing is violated, i.e., the steady-state average voltage of all PCCs $\langle\tilde{\boldsymbol{v}}(\infty)\rangle$ is increased by $\langle\boldsymbol{\psi_a}(\infty)\rangle$. Moreover, the currents/voltages in the DCmG can still converge exponentially at rate $\min\{|Re(\beta_3)|^3, \lambda_2\}$, where β_3 is the minimal eigenvalue of $\boldsymbol{A_{kj}}$ satisfying $|Re(\beta_3)| \leq |Re(\beta_2)| \leq |Re(\beta_1)|$ and λ_2 is the minimal nonzero eigenvalue of $\boldsymbol{Q}$.

$$\boldsymbol{\psi_a}(\infty) = -\frac{k_I a_{ij}}{NI^s_{tj}}\boldsymbol{k}\boldsymbol{A^{-1}_{kj}}\boldsymbol{\phi_{i,j}}(T_a)\mathbb{1}^N. \tag{22}$$

Proof: The proof is omitted due to space limitation. ■

[3] $Re(\beta_3)$ represents the real part of β_3.

Remark 3: Once any link in the DCmG is compromised by the NDS attack, the steady-state voltages at all PCCs will be increased by the same magnitude $\langle\boldsymbol{\psi_a}(\infty)\rangle$, which is related to the initial value of the attack vector $\boldsymbol{\phi_{i,j}}(T_a)$, system matrix $\boldsymbol{A_{kj}}$, link weight a_{ij}, etc. Whereas current sharing can still be achieved and the convergence rates of currents/voltages are still exponentially fast. Moreover, the steady-state voltage deviation at each PCC caused by the NDS attack can change the operating point set by the tertiary control [17], which is related to the economically optimal operation. Accordingly, the attack may cause economic losses like increasing the generation costs [18].

IV. SIMULATION

In this section, we demonstrate impacts of the NDS attack on detection residuals, PCC voltages, and output currents through extensive simulations. The DCmG is conducted in Simulink/PLECS, composed of 4 DGUs and the topology is showed in Fig. 2. Specifically, electrical parameters and primary controllers of DGUs are designed according to [14]. Process and measurement noise bounds are set as $\bar{\boldsymbol{\rho}}_{\boldsymbol{j}} = [0.001, 0.01, 0]^T$ and $\bar{\boldsymbol{\omega}}_{\boldsymbol{j}} = [0.001, 0.01, 0]^T, j \in \boldsymbol{\nu} = \{1, 2, 3, 4\}$, respectively. According to [11], the second columns of $\boldsymbol{H_j}$ are chosen as $[-0.02, 0.98, -0.02]^T$, $\boldsymbol{F_j} = \mathrm{diag}\{-1, -1, -1\}$, and then $\boldsymbol{T_j}, \hat{\boldsymbol{K}}_{\boldsymbol{j}}, j \in \boldsymbol{\nu}$ can be obtained.

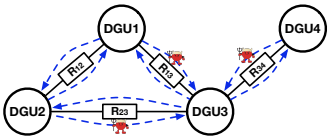

Fig. 2. Electrical coupling and communication link model of the DCmG, where black solid lines denote power lines with resistances and blue dotted lines denote bidirectional communication links. The attacker injects attack vectors into communication links between DGU 3 and its neighbor DGUs $j, j \in \mathcal{N}^c_3 = \{1, 2, 4\}$.

We construct the NDS attacks with the maximum attack vector magnitude, under which the detection residuals are always within the detection thresholds as shown in Fig. 3. The isolated DGUs are interconnected by power lines at $t = 0$, the secondary control is activated at $T_s = 3s$ and the attack is started at $T_a = 6s$. The attacker compromises communication data transmitted between DGU 3 and its neighbor DGUs j, and the bounds of the initial state estimation error are all $\bar{\boldsymbol{\epsilon}}_{\boldsymbol{3,j}}(T_s) = 0.3 * [1, 1, 1]^T, \forall j \in \mathcal{N}^c_3$. Specifically, we investigate the maximum $\tilde{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{3,j}}(T_s), \forall j \in \mathcal{N}^c_3$ under the constraints of the UIO detector, which depend not only on the state estimation error and the measurement noise, but also on the parameters of the detection thresholds (e.g., $\kappa, \mu, \boldsymbol{T_j}, \boldsymbol{H_j}, j \in \mathcal{N}^c_3$, etc.). As shown in Fig. 3, when $\tilde{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{3,j}}(T_s) = \alpha_{max}\bar{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{3,j}}(T_s) = 5.5\bar{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{3,j}}(T_s)$, the estimation residuals are still within the detection thresholds, and the attack vectors are designed as $\boldsymbol{\phi_{3,j}}(t) = e^{\boldsymbol{A_{kj}}(\boldsymbol{t-T_a})}\tilde{\boldsymbol{I}}e^{\boldsymbol{F_j}(T_a-T_s)}\tilde{\boldsymbol{\sigma}}^{\boldsymbol{1}}_{\boldsymbol{3,j}}(T_s), t \geq T_a, \forall j \in \mathcal{N}^c_3$.

Under the NDS attacks, the PCC voltages and output currents are depicted in Fig.4, from which the voltage balancing and current sharing are analyzed. For the secondary

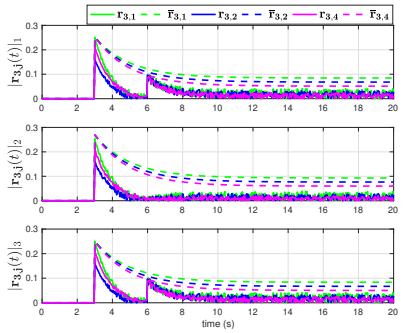

Fig. 3. Element-by-element comparison of estimation residuals $|\boldsymbol{r_{3,j}}(t)|, j \in \mathcal{N}_3^c$ with residual bounds $\bar{\boldsymbol{r}}_{\boldsymbol{3,j}}(t)$, where $|\boldsymbol{r_{3,j}}(t)|_i$ denotes the i_{th} element of $|\boldsymbol{r_{3,j}}(t)|$. Solid lines denote the estimation residuals and dotted lines denote the residual bounds, and moreover, the colors of lines represent different DGUs as the legend shows. The secondary control is activated at $T_s = 3$s, before which the residuals are all zero, and the attack is started at $T_a = 6$s.

control, we set $k_I = 1$, $a_{ij} = \frac{1}{R_{ij}}, \forall i, j \in \boldsymbol{\nu}, i \neq j$ according to Assumption 1. Moreover, the reference voltage is $V_{ref} = 40V$, the load currents are $I_{L1} = 10A, I_{L2} = 8A, I_{L3} = 12A, I_{L4} = 14A$ and the rated output currents are $I_{ti}^s = 20A, i \in \{1, 2, 4\}, I_{t3}^s = 35A$. As Fig. 4 shows, the current sharing and voltage balancing are both achieved after activating the secondary control at T_s second. When the NDS attacks are launched at T_a second, the dynamics of currents/voltages are affected and eventually the steady-state average PCC voltage is increased by $|\langle\tilde{\boldsymbol{\psi}}(\infty)\rangle| = |\sum_{j\in\{1,2,4\}} \frac{C_a}{4} \boldsymbol{k A_{kj}^{-1}} \boldsymbol{\phi_{3,j}}(T_a)| = 0.4107V$, which will increase the generation costs. And the current sharing is still achieved.

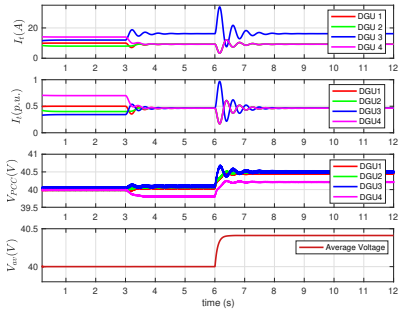

Fig. 4. After DGUs are interconnected by power lines, evolutions of output currents in A (Ampere), output currents in per-unit ($p.u.$, i.e. $\frac{I_{ti}}{I_{ti}^s}$), output voltages at PCCs and average output voltage in V (Volt) are shown.

V. CONCLUSIONS

In this paper, we investigated the NDS attack against the UIO-based detector in current DCmG [12], and theoretically analyzed the attack impacts on current sharing, voltage balancing, and convergence rates of currents/voltages. Interestingly, we found that the attack impacts are closely related to the bounds of the initial state estimation error and the measurement noise. The steady-state average voltage of all PCCs could be deviated from the reference point, which may increase the output power of the DC-DC buck converter and thus cause more generation costs; Whereas the current sharing is still achieved and currents/voltages in the DCmG can converge with exponential rates. Compared with the ZDS attack, the state disturbance caused by the NDS attack is limited by the bounds of the initial state estimation error and the measurement noise. However, this paper provides a novel perspective to investigate stealthy attacks in DCmGs, which exploit the common state estimation error/measurement noise in physical plants and can cause economic losses. In the future work, countermeasures against the NDS attack will be investigated for the DCmG.

REFERENCES

[1] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control system," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1963–1976, 2012.

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

[3] J. Chen, K. Hu, Q. Wang, Y. Sun, Z. Shi, and S. He, "Narrowband internet of things: Implementations and applications," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2309–2314, 2017.

[4] R. Deng, S. He, P. Cheng, and Y. Sun, "Towards balanced energy charging and transmission collision in wireless rechargeable sensor networks," *Journal of Communications and Networks*, vol. 19, no. 4, pp. 341–350, 2017.

[5] R. Deng, P. Zhuang, and H. Liang, "Ccpa: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420–2430, 2017.

[6] R. Deng and H. Liang, "False data injection attacks with limited susceptance information and new countermeasures in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1619–1628, 2018.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, p. 13, 2011.

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

[9] H. J. Liu, M. Backes, R. Macwan, and A. Valdes, "Coordination of ders in microgrids with cybersecure resilient decentralized secondary frequency control," in *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS)*, 2018.

[10] A. Teixeira, H. Sandberg, and K. H. Johansson, "Networked control systems under cyber attacks with applications to power networks," in *American Control Conference (ACC)*. IEEE, 2010.

[11] 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 *European Control Conference (ECC)*, 2018.

[12] M. Tucci, L. Meng, J. M. Guerrero, and G. Ferrari-Trecate, "Stable current sharing and voltage balancing in dc microgrids: A consensus-based secondary control layer," *Automatica*, vol. 95, pp. 1–13, 2018.

[13] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 90–104, 2012.

[14] M. Tucci, S. Riverso, J. C. Vasquez, J. M. Guerrero, and G. Ferrari-Trecate, "A decentralized scalable approach to voltage control of dc islanded microgrids," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 6, pp. 1965–1979, 2016.

[15] S. Attuati, M. Farina, F. Boem, and T. Parisini, "Reducing false alarm rates in observer-based distributed fault detection schemes by analyzing moving averages," *IFAC-PapersOnLine*, vol. 51, no. 24, pp. 473–479, 2018.

[16] M. Cucuzzella, G. P. Incremona, and A. Ferrara, "Design of robust higher order sliding mode control for microgrids," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 5, no. 3, pp. 393–401, 2015.

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

[18] C. Zhao, J. He, P. Cheng, and J. Chen, "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5107–5117, 2017.