Converter-based Moving Target Defense Against Deception Attacks in DC Microgrids

Mengxiang Liu, *Student Member, IEEE*, Chengcheng Zhao, *Member, IEEE*, Zhenyong Zhang, *Member, IEEE*, Ruilong Deng, *Senior Member, IEEE*, Peng Cheng, *Member, IEEE*, and Jiming Chen, *Fellow, IEEE*

***Abstract*—With the rapid development of information and communications technology in DC microgrids (DCmGs), the deception attacks, which typically include false data injection and replay attacks, have been widely recognized as a significant threat. However, existing literature ignores the possibility of the intelligent attacker, who could launch deception attacks once obtaining necessary information by exploiting zero-day vulnerabilities or bribing insiders, to affect the system in an unforeseeable manner. In this paper, based on the observation that the primary control law of the power converter device in DCmGs is usually programmable, we propose a novel converter-based moving target defense (CMTD) strategy by proactively perturbing the primary control gains to defend against deception attacks. First, we study the impact of perturbing the primary control gains on the voltage stability in DCmGs and provide explicit conditions for the perturbation magnitude and frequency under which the voltage stability can be ensured. Then, we investigate the improved detectability against deception attacks under CMTD and present sufficient conditions under which these attacks can be detected. Finally, we conduct extensive Matlab Simulink/PLECS based simulations and systematic hardware-in-the-loop based experiments to validate the effectiveness of CMTD.**

***Index Terms*—Converter-based moving target defense, deception attacks, DC microgrids.**

I. Introduction

In the recent decade, the DC microgrid (DCmG) has attracted much attention for the advantage in accommodating for distributed energy resources (DERs) through power converter devices [1], which have been widely utilized to address the operational challenges induced by the inherent intermittency and variability of DERs [2]. The main tasks of converter devices include adjusting the output voltages of DERs to the power line voltage of the DCmG, the operating control of DERs (e.g., the maximum power point tracking in solar power plants) and the system level control, such that the DCmG can operate autonomously in a reliable and efficient status [3]. Since the controller of the converter device (e.g., the digital signal processor) is usually equipped with certain computation resource and appropriate communication interfaces, the distributed coordination between DERs is becoming an increasingly promising trend in the future power distribution system, which can significantly reduce the burden of the control center and hence improve the reliability and flexibility of DCmGs [4]. Nevertheless, the communication network required by the distributed coordination will inevitably expose DCmGs to the threat of cyberattacks, which could destroy the synchronization between DERs and thus cause economic losses or even converter outages [5].

Two typical cyberattacks are denial of service (DoS) and deception attacks [6]. The DoS attack prevents the exchange of information between DERs, while the deception attack destroys the data integrity of packets by modifying their payloads. Generally speaking, the deception attacks, including false data injection (FDI) and replay attacks, possess stronger stealthiness than the DoS attacks as the attacker can carefully design the injected bias to deceive the system operator. In this paper, we mainly focus on the detection and identification of the deception attacks in DCmGs, which has become a prevailing topic in the most recent literature.

In the power and energy society, Zhang *et al.* [5] considered the FDIs and theoretically investigated the stability region of microgrids with respect to the utilization level. While no countermeasure is proposed to defend against the destructive FDI attack. Sahoo *et al.* [7] proposed a cooperative vulnerability factor framework for each DER to identify malicious DERs. Yet the cross-coupling verification of the cooperative vulnerability factor needs to be concealed from the attacker to prevent it from being surreptitiously compromised. In the presence of local unknown constant power loads, Cecilia *et al.* [8] introduced a distributed non-linear observer approach that can robustly detect and reconstruct the applied FDI attacks in DCmGs, where the knowledge of the observer should be maintained unknown to the attacker. Habibi *et al.* [9] proposed a new artificial intelligent based method for the detection and identification of the FDI attacks in DCmGs. While the artificial intelligent model should also be kept confidential to prevent it from being fooled by the attacker with adversarial examples. In the control society, Gallo *et al.* [10] presented a distributed monitoring scheme to provide attack detection and identification capabilities for linear large-scale systems, which can be directly applied to DCmGs. But the system parameters of DERs should be hidden from the attacker to thwart the construction of covert (stealthy) FDI

This work was supported in part by the Science and Technology Innovation 2030 Program under Grant 2018AAA0101605, in part by the Zhejiang Provincial Key R&D Program under Grant 2021C01032, in part by the National Natural Science Foundation of China under Grants 62073285, 62061130220, 61833015, 61903328, in part by the Zhejiang Provincial Natural Science Foundation under Grant LZ21F020006, and in part by the Fundamental Research Funds for the Central Universities (Zhejiang University NGICS Platform). (*Corresponding author: Ruilong Deng.*)

Mengxiang Liu, Chengcheng Zhao, Ruilong Deng, Peng Cheng, and Jiming Chen are with State Key Lab. of Industrial Control Technology, College of Control Science and Engineering, Zhejiang University, Hangzhou, China (e-mails: {lmx329, chengchengzhao, dengruilong, lunarheart, cjm}@zju.edu.cn).

Zhenyong Zhang is with State Key Lab. of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang, China (e-mail: zyzhangnew@gmail.com).

attacks. Furthermore, a distributed watermarking scheme was proposed for the secure control of the DCmG under replay attacks [11]. To successfully preclude replay attacks, the added watermarking should be protected from being inferred by the attacker. More recently, Liu *et al.* [12] proposed a distributed countermeasure against the stealthy FDI attacks in DCmGs based on the estimated average point and common coupling (PCC) voltage, which should also be protected from being disturbed by the attacker.

In summary, most literature seriously underestimates the capabilities of the attacker, and assumes that the attacker has zero/little knowledge of the system model and the detection scheme. Nevertheless, the notorious Stuxnet security incident against nuclear facilities indicated that an intelligent attacker can obtain necessary information through exploiting zero-day vulnerabilities in communication and computation devices or bribing insiders, such that the deception attacks with strong stealthiness could be launched to cause accurate and specific adverse impact [13]. Hence, new attack detection and identification methods are required to deal with this thorny threat.

Moving Target Defense (MTD) has been shown to be a potentially effective method in thwarting the FDI attacks against the state estimation process in AC power systems [14]–[18], which is achieved by proactively perturbing the reactances of power lines with the distributed flexible AC transmission system (D-FACTS) devices. The basic idea behind MTD is to make the attacker's understanding of the system model outdated such that the FDI attack constructed with antiquated system parameters may be exposed to the bad data detector. However, the existing MTD strategy cannot be directly applied to DCmGs due to the following two limitations: a) The X/R ratio of the power line in DCmGs is significantly smaller than that in AC power systems, under which the D-FACTS device may be invalid as merely trivial perturbation can be made on the impedance of the DC power line; b) The installation of D-FACTS devices is costly especially when the number of power lines increases, which will limit the practicality of MTD in scalable DCmGs. Fortunately, we observe that the primary control law of the power converter device, which is originally designed for the adjustment of the voltage reference provided to the inner control loops [19], is usually programmable by the host computer [20]. Therefore, in this paper, we propose a novel converter-based MTD (CMTD) strategy by proactively perturbing the primary control gains (PCGs) in converter devices to defend against the deception attacks with strong stealthiness, which requires no extra installation cost. Compared to the existing MTD strategies based on the D-FACTS devices, the investigation of CMTD should address the voltage stability issue under perturbation and the detection and identification of deception attacks, which are still challenging and require extra efforts. Towards this end, we make the following contributions:

- We provide explicit conditions on the perturbation magnitude and frequency to guarantee the voltage stabilization under PCG perturbation;
- We investigate the enhanced detectability against FDI and replay attacks with CMTD, and introduce the sufficient conditions under which these attacks can be detected;
- We conduct extensive simulations in Matlab Simulink/PLECS and systematic hardware-in-the-loop (HIL) experiments in the Typhoon HIL emulator based testbed to validate the effectiveness of CMTD.

In the remainder of this paper, Section II introduces the DCmG model, the unknown input observer (UIO) based detector, the attack model, and our problems of interest. Section III analyzes the voltage stability under PCG perturbation, and Section IV investigates the enhanced detectability against FDI and replay attacks with CMTD. Section V presents simulation and experiment results to validate the effectiveness of CMTD, and Section VI concludes this paper.

Notation: $\mathbb{R}^n/\mathbb{R}^{n\times n}$ is the set of real vectors/matrices. The symbol $|\cdot|$ denotes the component-by-component absolute value of a vector/matrix, and $\|\cdot\|$ represents the norm of a vector/matrix. Inequalities of vectors/matrices are compared component-by-component, and $\lim_{t\to\infty} y(t)$ is denoted by $y(\infty)$ for brevity. Let $\mathbb{1}^n/\mathbb{1}^{n\times n}$ and $\mathbb{0}^n/\mathbb{0}^{n\times n}$ denote vectors/matrices with all 1 and 0 entries, respectively, and I^n denotes the $n\times n$ identity matrix. Scalar $v_{[m]}$ denotes the m-th entry of $\boldsymbol{v}\in\mathbb{R}^n$.

II. System Model and Problem Formulation

A. Electrical Model of DCmG

We consider a DCmG composed of $N\geq 2$ DERs, where the buck converter is commanded to supply the local ZIP load connected to the PCC bus as shown in Fig. 1. The electrical network among DERs are denoted by a weighted undirected graph $\mathcal{G}_{el}=\{\mathcal{A},\mathcal{E}_{el}\}$, where $\mathcal{A}$ is the set of DERs and $\mathcal{E}_{el}$ is the set of power lines connecting them. Specifically, DERs i and j are neighbors if power line $\{i,j\}\in\mathcal{E}_{el}$, and the set of neighbors of DER i in $\mathcal{G}_{el}$ is represented by $\mathcal{N}_i^{el}$. Moreover, the weight of $\{i,j\}$ is the branch conductance, which is denoted by $\frac{1}{R_{ij}}$.

At each PCC bus, the ZIP load includes constant impedance load (CIL), constant current load (CCL), and constant power load (CPL). As illustrated in Fig. 1, Z_i, I_{CCLi}, and P_{CPLi} signify the CIL (Z), CCL (I), and CPL (P) inside DER i, respectively. Since the objective of the buck converter is to keep the PCC voltage near the nominal reference value $V_{ref,i}$, it is reasonable to linearize CPL around the reference voltage [21]. Then, in DER i, the equivalent model for CPL can be expressed as

$$I_{CPLi}=\underbrace{-\frac{P_{CPLi}}{V_{ref,i}^2}}_{(a)}V_i+\underbrace{2\frac{P_{CPLi}}{V_{ref,i}}}_{(b)}, \tag{1}$$

where V_i is the i-th PCC voltage and I_{CPLi} is the total current for the CPL, arose from the negative impedance part (a) and the constant current part (b) in (1). Combining (1) with CIL and CCL, the ZIP load in DER i can be equivalently represented with impedance Z_{Li} and current load I_{Li} as

$$\begin{cases}\dfrac{1}{Z_{Li}}=\dfrac{1}{Z_i}-\dfrac{P_{CPLi}}{V_{ref,i}^2}\\ I_{Li}=I_{CCLi}+2\dfrac{P_{CPLi}}{V_{ref,i}}\end{cases}. \tag{2}$$

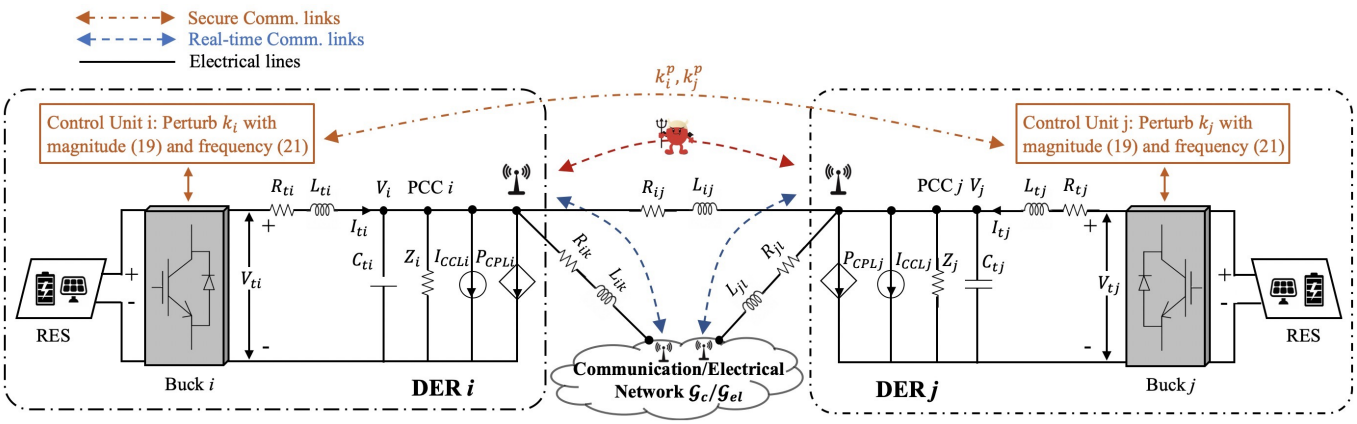


Fig. 1: This figure depicts the system diagram of the DCmG equipped with the proposed CMTD. Here the real-time communication link is to enable the collaborative distributed control among DERs, while the secured communication link with advanced encryption technologies is to exchange the perturbed control gains every hour.

According to Fig. 1, after applying the Kirchhoff voltage and current laws and exploiting the quasi-stationary line (QSL) approximation (i.e., $L_{ij} \approx 0$) [22], the electrical model of DER i is obtained as

$$\begin{cases} \dfrac{dV_i}{dt} = \dfrac{1}{C_{ti}} I_{ti} + \sum\limits_{j \in \mathcal{N}_i^{el}} \dfrac{1}{C_{ti} R_{ij}} (V_j - V_i) + \\ \qquad\qquad - \dfrac{1}{C_{ti}} (I_{Li} + \dfrac{V_i}{Z_{Li}}) \\ \dfrac{dI_{ti}}{dt} = -\dfrac{1}{L_{ti}} V_i - \dfrac{R_{ti}}{L_{ti}} I_{ti} + \dfrac{1}{L_{ti}} V_{ti} \end{cases}, \tag{3}$$

where I_{ti} is the output current from the renewable energy source (RES), R_{ti}, L_{ti}, and C_{ti} are the converter electrical parameters (CEPs), and R_{ij} is the resistance of the power line connecting DERs i and j.

Considering the bounded process noise $|\boldsymbol{\omega}_i(t)| \leq \bar{\boldsymbol{\omega}}_i$ and the bounded measurement noise $|\boldsymbol{\rho}_i(t)| \leq \bar{\boldsymbol{\rho}}_i$, model (3) can be expressed as the following state-space form:

$$\begin{cases} \dot{\boldsymbol{x}}_i(t) = A_{ii} \boldsymbol{x}_i(t) + \boldsymbol{b}_i u_i(t) + M_i \boldsymbol{d}_i(t) + \\ \qquad\qquad + \boldsymbol{\xi}_i(t) + \boldsymbol{\omega}_i(t) \\ \boldsymbol{y}_i(t) = \boldsymbol{x}_i(t) + \boldsymbol{\rho}_i(t) \end{cases}, \tag{4}$$

where $\boldsymbol{x}_i(t) = [V_i(t), I_{ti}(t), v_i(t)]^{\mathrm{T}}$ is the state vector of DER i, $u_i(t) = V_{ti}$ is the primary control input, $\boldsymbol{d}_i(t) = [I_{Li}, V_{ref,i} + \alpha_i(t)]^{\mathrm{T}}$ is the exogenous input vector, and $\boldsymbol{y}_i(t)$ is the measurement output vector. The last element of the state vector, i.e., $v_i(t)$, signifies the integral of the voltage tracking error and satisfies $\dot{v}_i(t) = V_{ref,i} + \alpha_i(t) - V_i(t)$, with $\alpha_i(t)$ being the secondary control input. Moreover, vector $\boldsymbol{\xi}_i(t) = \sum_{j \in \mathcal{N}_i^{el}} A_{ij} \boldsymbol{x}_j(t)$ accounts for the electrical coupling with neighboring DERs. Vector $\boldsymbol{b}_i = [0, \frac{1}{L_{ti}}, 0]^{\mathrm{T}}$ and the matrices involved in (4) are

$$\begin{aligned} A_{ii} &= \begin{bmatrix} -\frac{1}{Z_{Li} C_{ti}} - \sum\limits_{j \in \mathcal{N}_i^{el}} \frac{1}{R_{ij} C_{ti}} & \frac{1}{C_{ti}} & 0 \\ -\frac{1}{L_{ti}} & -\frac{R_{ti}}{L_{ti}} & 0 \\ -1 & 0 & 0 \end{bmatrix}, \\ M_i &= \begin{bmatrix} -\frac{1}{C_{ti}} & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}, A_{ij} = \begin{bmatrix} \frac{1}{R_{ij} C_{ti}} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}. \end{aligned} \tag{5}$$

B. Structure of Primary and Secondary Controllers

To track the reference PCC voltage, each DER $i \in \mathcal{A}$ is equipped with a primary controller, which is a typical state-feedback controller and satisfies

$$u_i(t) = \boldsymbol{k}_i^{\mathrm{T}} \boldsymbol{y}_i(t), \tag{6}$$

where $\boldsymbol{k}_i = [k_{[i1]}, k_{[i2]}, k_{[i3]}]^{\mathrm{T}}$ denotes the PCG vector required to be carefully designed. In literature [21]–[24], the local design of $\boldsymbol{k}_i$ to ensure the voltage stability in DCmGs has been well studied.

To compensate for the power/current sharing error induced in the primary controller, a consensus-like secondary controller is employed, i.e.,

$$\dot{\alpha}_i(t) = [0, k_I, 0] \sum_{j \in \mathcal{N}_i^c} a_{ij}^c \left(\frac{\boldsymbol{y}_{i,j}^c(t)}{I_{tj}^s} - \frac{\boldsymbol{y}_i(t)}{I_{ti}^s} \right), \tag{7}$$

where $\boldsymbol{y}_{i,j}^c(t)$ is the measurement output vector of DER j communicated to DER i, $I_{ti}^s > 0$ and $I_{tj}^s > 0$ are the rated currents corresponding to DERs i and j, respectively, and $k_I > 0$ is a parameter invariant among all DERs. The communication network among DERs is denoted by a weighted undirected graph $\mathcal{G}_c = \{\mathcal{A}, \mathcal{E}_c\}$, where set $\mathcal{E}_c$ collects all communication links and the weight of link $\{i, j\} \in \mathcal{G}_c$ is denoted by a_{ij}^c. Moreover, the neighbors set of DER i in $\mathcal{G}_c$ is signified by $\mathcal{N}_i^c$.

According to Theorems 1-2 in [25], the primary controllers (6) and secondary controllers (7) $\forall i \in \mathcal{A}$ in the DCmG

can achieve voltage balancing and current sharing, which are formally defined as follows:

Definition 1 (Voltage Balancing): Voltage balancing is achieved if $\frac{1}{N}\sum_{i=1}^{N} V_i(\infty) = V_{op}$, where V_{op} is the operating point set by the tertiary control layer.

Definition 2 (Current Sharing): For the DCmG equipped with the equivalent ZIP loads (2), current sharing is achieved if $\frac{I_{ti}(\infty)}{I_{ti}^s} = \frac{I_{tj}(\infty)}{I_{tj}^s}, \forall i,j \in \mathcal{A}$.

if the following two Assumptions are satisfied:

Assumption 1: The DCmG operates in the isolated mode, and the average of nominal reference PCC voltages is equal to V_{op}, i.e., $\frac{1}{N}\sum_{i=1}^{N} V_{ref,i} = V_{op}$.

Assumption 2: The weighted undirected graphs $\mathcal{G}_{el}$ and $\mathcal{G}_c$ are both connected, and have the same topology and branch/link weights.

Remark 1: Assumption 2 requires that DER $i \in \mathcal{A}$ should know the resistances of all power lines connecting it to the electrical neighbors $j, \forall j \in \mathcal{N}_i^{el}$. Given the QSL approximation [22], R_{ij} can be estimated through $R_{ij} = \frac{|V_j - V_i|}{I_{ij}}$, where V_i and the current on power line $\{i,j\}$, i.e., I_{ij}, are measured locally, and V_j is the measurement transmitted from DER j.

C. UIO-based Detector

To protect DCmGs from being affected by cyberattacks, a bank of UIO-based detectors is employed in each DER to check the integrity of the communicated data from neighbors [10]. Since only the measurement outputs are interacted between DERs, the exogenous input and electrical coupling vectors are lumped as an unknown input vector, denoted by $\bar{\boldsymbol{d}}_i(t)$. Hence, state-space model (4) is transformed to

$$\begin{cases} \dot{\boldsymbol{x}}_i(t) = A_{ki}\boldsymbol{x}_i(t) + M_i\bar{\boldsymbol{d}}_i(t) + \boldsymbol{\omega}_i(t) + \boldsymbol{b}_i\boldsymbol{k}_i\boldsymbol{\rho}_i(t) \\ \boldsymbol{y}_i(t) = \boldsymbol{x}_i(t) + \boldsymbol{\rho}_i(t) \end{cases}, \tag{8}$$

where $A_{ki} = A_{ii} + \boldsymbol{b}_i\boldsymbol{k}_i$ and $M_i\bar{\boldsymbol{d}}_i(t) = M_i\boldsymbol{d}_i(t) + \boldsymbol{\xi}_i(t)$. According to (8), it is verified that matrix $\begin{bmatrix} s\mathrm{I}^3 - A_{ki} & M_i \\ \mathrm{I}^3 & \mathbb{0}^{3\times 2} \end{bmatrix}$ has full column rank $\forall s \in \mathbb{C}$. Thus, a full order UIO can be constructed in DER $j \in \mathcal{N}_i^c$ as

$$\mathrm{UIO}_{j,i} \begin{cases} \dot{\boldsymbol{z}}_{j,i}(t) = F_i\boldsymbol{z}_{j,i}(t) + \hat{K}_i\boldsymbol{y}_{j,i}^c(t) \\ \hat{\boldsymbol{x}}_{j,i}(t) = \boldsymbol{z}_{j,i}(t) + H_i\boldsymbol{y}_{j,i}^c(t) \end{cases}. \tag{9}$$

In the absence of system noises and cyberattacks, the estimated system state $\hat{\boldsymbol{x}}_{j,i}(t)$ will converge asymptotically to $\boldsymbol{x}_i(t)$ regardless of the unknown input vector $\bar{\boldsymbol{d}}_i(t)$ [26]. In $\mathrm{UIO}_{j,i}$, $\boldsymbol{z}_{j,i}(t) \in \mathbb{R}^3$ is the internal state vector and $\boldsymbol{y}_{j,i}^c(t)$ denotes the output vector that DER j receives from DER i. The parameters $F_i, \hat{K}_i, H_i \in \mathbb{R}^{3\times 3}$ are designed according to

$$T_iM_i = \mathbb{0}^{3\times 2}, \tag{10a}$$
$$T_i = \mathrm{I}^3 - H_i, \tag{10b}$$
$$\hat{K}_i = K_{i1} + K_{i2}, \tag{10c}$$
$$F_i = T_iA_{ki} - K_{i1}, \tag{10d}$$
$$K_{i2} = F_iH_i, \tag{10e}$$

where H_i satisfies

$$H_i = \begin{bmatrix} 1 & 0 & 0 \\ h_{12} & h_{22} & h_{32} \\ 0 & 0 & 1 \end{bmatrix}^{\mathrm{T}}, \tag{11}$$

h_{12}, h_{22}, h_{32} are arbitrary scalars, and K_{i1} should be appropriately chosen based on (10d) to make the eigenvalues of F_i all lie in the open left half-plane. Under normal operations, given (8)-(10), the detection residual vector $\boldsymbol{r}_{j,i}(t) = \boldsymbol{y}_{j,i}^c(t) - \hat{\boldsymbol{x}}_{j,i}(t)$ is obtained as

$$\boldsymbol{r}_{j,i}(t) = e^{F_it}\big(\boldsymbol{\sigma}_{2j,i}(0) + \boldsymbol{\sigma}_{3j,i}(t)\big) + T_i\boldsymbol{\rho}_i(t), \tag{12}$$

where $\boldsymbol{\sigma}_{2j,i}(0) = \boldsymbol{x}_i(0) - \hat{\boldsymbol{x}}_{j,i}(0) + H_i\boldsymbol{\rho}_i(0)$ and $\boldsymbol{\sigma}_{3j,i}(t) = \int_0^t e^{-F_i\tau}\big(T_i\boldsymbol{\omega}_i(\tau) + (T_i\boldsymbol{b}_i\boldsymbol{k}_i - \hat{K}_i)\boldsymbol{\rho}_i(\tau)\big)\mathrm{d}\tau$. Moreover, as F_i is Hurwitz stable, there exist positive scalars κ, μ such that $||e^{F_it}|| \le \kappa e^{-\mu t}, \forall t \ge 0$. Then, the time-varying upper bound of $|\boldsymbol{r}_{j,i}(t)|$ can be obtained as

$$|\boldsymbol{r}_{j,i}(t)| \le \bar{\boldsymbol{r}}_{j,i}(t) = \kappa e^{-\mu t}\big(\bar{\boldsymbol{\sigma}}_{2j,i}(0) + \bar{\boldsymbol{\sigma}}_{3j,i}(t)\big) + |T_i|\bar{\boldsymbol{\rho}}_i, \tag{13}$$

where $|\boldsymbol{\sigma}_{2j,i}(0)| \le \bar{\boldsymbol{\sigma}}_{2j,i}(0) = \big(\mathrm{I}^3 + |H_i|\big)\bar{\boldsymbol{\rho}}_i$ and $|\boldsymbol{\sigma}_{3j,i}(t)| \le \bar{\boldsymbol{\sigma}}_{3j,i}(t) = \int_0^t |e^{-F_i\tau}|\big(|T_i|\bar{\boldsymbol{\omega}}_i + |T_i\boldsymbol{b}_i\boldsymbol{k}_i - \hat{K}_i|\bar{\boldsymbol{\rho}}_i\big)\mathrm{d}\tau$ [10]. Once (13) is violated, it is considered that the integrity of $\boldsymbol{y}_{j,i}^c(t)$ is corrupted and the data will be discarded.

D. Attack Model

In this paper, we consider the deception attacks against the communication links among DERs, which include FDI and replay attacks. We note that the malicious intruders inside DERs are not studied here. To avoid being perceived by the UIO-based detector, we assume that the attacker has the following capabilities:

- The attacker can obtain some system parameters like $A_{ki}, M_i, i \in \mathcal{A}$ from insiders, who have legal access to the critical information. But the attacker cannot update the parameters in real time, as the insiders only leak them at a specific time to guarantee their hiddenness [27];
- The attacker can eavesdrop the communication data, and inject appropriate biases into the TCP/IP based communication links through Man-in-the-Middle attacks [28].

For the communication link $\{i,j\}$ under FDI attack, the tempered data received by DER j is expressed as

$$\boldsymbol{y}_{j,i}^c(t) = \boldsymbol{y}_i(t) + \boldsymbol{\phi}_{j,i}(t), \tag{14}$$

where $\boldsymbol{\phi}_{j,i}(t)$ is the injected bias vector and for $t \ge T_a$ satisfies

$$\begin{cases} \dot{\boldsymbol{\phi}}_{j,i}(t) = A_{ki}\boldsymbol{\phi}_{j,i}(t) + M_i\bar{\boldsymbol{d}}_{ji}^a(t) \\ \boldsymbol{\phi}_{j,i}(T_a) = \mathbb{0}^3 \end{cases}, \tag{15}$$

with T_a and $\bar{\boldsymbol{d}}_{ji}^a(t)$ being the activation time of the attack and the fake unknown input vector, respectively. As shown in [12], the FDI attack generated with (15), called as the zero trace stealthy (ZTS) attack, causes zero impact on $\boldsymbol{r}_{j,i}(t)$, indicating that the ZTS attack is unforeseeable to the UIO-based detector.

The replay attack simply replaces the currently communicated data with the historically recorded data. For the communication link $\{i,j\}$ under replay attack, the distorted data received by DER j is obtained as

$$\boldsymbol{y}_{j,i}^c(t) = \boldsymbol{y}_i(t - n \times T_{rep}), \forall t \ge T_a, \tag{16}$$

where the integer $n \geq 1$ and $n \times T_{rep}$ denotes the time shift induced by the replay attack. According to [11], (16) can be particularly stealthy to the UIO-based detector as the recorded data conforms the physical dynamics of the DCmG. Compared with the ZTS attack, the replay attack requires no model knowledge (e.g., the system parameters A_{ki} and M_i) but the attack impact is more limited. Nevertheless, it is noted that the threat of the replay attack lies in the ability in covering the attack impact caused by other destructive attacks like the general FDI attacks. If the attacker launches the replay and FDI attacks together, then the system operator, fooled by the replay attack, would be unaware of the destructive impact caused by the FDI attacks. Besides, it has been demonstrated that multiple replay attacks can have similar impact on PCC voltages as that of FDI attacks [29]. Hence, considerable attention is also paid to the replay attack in this study.

E. Our Problems of Interest

Since the primary control law of the buck converter is usually programmable by the host computer, it is feasible to design a customized control algorithm to proactively perturb the PCG vector $\boldsymbol{k}_i, i \in \mathcal{A}$ with a fixed interval T_{kp}, such that the ZTS and replay attacks can be perceived by the UIO-based detector. For this purpose, an appropriate perturbation manner of $\boldsymbol{k}_i$, under which the voltage stability in DCmGs will not be affected while the detectability of the UIO-based detector can be significantly enhanced, is needed. Two problems are therefore formulated as follows: 1) What are the conditions under which the PCG perturbation will not affect the voltage stability? 2) Whether can the detectability of the UIO-based detector be enhanced with the PCG perturbation?

III. Voltage Stability Analysis Under PCG Perturbation

In this section, we investigate the explicit conditions on the perturbation magnitude and frequency to ensure the voltage stability in DCmGs. In the first step, the range of the perturbed PCG vector (denoted by $\boldsymbol{k}_i^p$) is presented to make the PCC voltages asymptotically stable. Then, the DCmG under PCG perturbation is considered as a switched linear system, and a sufficient condition of the perturbation frequency, which is characterized by the perturbation interval T_{kp}, is provided to make the switched system asymptotically stable.

A. Ranges of the Perturbed PCGs

The local design of PCGs to stabilize the PCC voltages in DCmGs has received widespread attention. In [22], [23], the local control design was cast into a linear matrix inequality problem, whose computation requires to choose appropriate parameters. More recently, the authors in [21], [24] provided the explicit inequalities on PCGs to design the local controllers, i.e.,

Lemma 1: For the DCmG with DER dynamics (4), the primary controllers (6) $\forall i \in \mathcal{A}$ with perturbed PCG vectors $\boldsymbol{k}_i^p$ can achieve asymptotic voltage stability if

$$\begin{cases} k_{[i1]}^p < 1 \\ k_{[i2]}^p < R_{ti} \\ 0 < k_{[i3]}^p < \dfrac{1}{L_{ti}}(k_{[i1]}^p - 1)(k_{[i2]}^p - R_{ti}) \end{cases}, \tag{17}$$

and the CIL and CPL verify

$$P_{CPLi} < \frac{V_{ref,i}^2}{Z_i}. \tag{18}$$

Proof: The proof can be completed by utilizing the Lyapunov stability criterion and is referred to Theorem 1 in [21]. ■

To prevent $||\boldsymbol{k}_i^p||$ from being too large, we further assume $|k_{[i1]}^p| \leq 1$ and $|k_{[i2]}^p| \leq R_{ti}$ and by merging (17) obtain

$$\begin{cases} -1 < k_{[i1]}^p < 1 \\ -R_{ti} < k_{[i2]}^p < R_{ti} \\ 0 < k_{[i3]}^p < \dfrac{1}{L_{ti}}(k_{[i1]}^p - 1)(k_{[i2]}^p - R_{ti}) \end{cases}. \tag{19}$$

Remark 2: Indeed, shrinking the perturbation ranges of PCGs from (17) to (19), which limits the magnitudes of $|k_{[i1]}^p|$ and $|k_{[i2]}^p|$, will result in some conservativity for the CMTD strategy. In particular, when detecting a certain deception attack, a large perturbation magnitude on $k_{[i3]}^p$ may be required to compensate for the shrunk perturbation ranges on $k_{[i1]}^p$ and $k_{[i2]}^p$. Nevertheless, it is verified in Section V that the conservativity will not significantly degrade the detectability against deception attacks, i.e., the CMTD strategy with the perturbed PCGs satisfying (19) can still effectively expose the deception attacks to the UIO-based detector. Moreover, the restriction on $||\boldsymbol{k}_i^p||$ is useful in preventing the control action from being aggressive [22], as the pulse-width modulation (PWM) reference signal of the converter device should be within $[0, 1]$ to ensure the feasibility.

With $\boldsymbol{k}_i^p$ satisfying (19), the state-space model of the overall DCmG dynamics after perturbation, which is denoted by

$$\dot{\mathbf{x}}(t) = \mathbf{A}_p \mathbf{x}(t) + \mathbf{M}\mathbf{d}(t) + \boldsymbol{\omega}(t), \tag{20}$$

is asymptotically stable, i.e., matrix $\mathbf{A}_p$ is Hurwitz stable. In (20), $\mathbf{x}(t) = [\boldsymbol{x}_1^{\mathrm{T}}(t), \cdots, \boldsymbol{x}_N^{\mathrm{T}}(t)]^{\mathrm{T}}$, $\mathbf{u}(t) = [u_1(t), \cdots, u_N(t)]^{\mathrm{T}}$, $\mathbf{d}(t) = [\boldsymbol{d}_1^{\mathrm{T}}(t), \cdots, \boldsymbol{d}_N^{\mathrm{T}}(t)]^{\mathrm{T}}$, $\boldsymbol{\omega}(t) = [\boldsymbol{\omega}_1^{\mathrm{T}}(t), \cdots, \boldsymbol{\omega}_N^{\mathrm{T}}(t)]^{\mathrm{T}}$, and

$$\mathbf{A}_p = \begin{bmatrix} A_{k1}^p & A_{12} \cdots A_{1N} \\ A_{21} & A_{k2}^p \cdots A_{2N} \\ \vdots & \vdots \ddots \vdots \\ A_{N1} A_{N2} \cdots A_{kN}^p \end{bmatrix},$$

where $A_{ki}^p = A_{ii} + \boldsymbol{b}_i(\boldsymbol{k}_i^p)^{\mathrm{T}}, \forall i \in \mathcal{A}$. Moreover, the diagonal matrix $\mathbf{M} = \mathrm{diag}\{M_1, \cdots, M_N\}$.

B. Condition for the Perturbation Interval

The DCmG under PCG perturbation is considered as a switched linear system, whose individual subsystem is expressed as (20) and the interval between any two consecutive switching times is T_{kp}. It is a fairly well-known fact that when all subsystems are asymptotically stable, the switched linear system will be globally and exponentially stable if T_{kp} is large enough [30]. In particular, the required lower bound on T_{kp} can be explicitly calculated from the parameters of individual subsystems as in Lemma 2.

Lemma 2: Let the set $\{\mathbf{A}_p, p \in \mathcal{P}\}$ include all possible system matrices satisfying (19). Moreover, for any positive definite matrix $\mathbf{Q}_p$, it is always feasible to find a symmetrical positive definite matrix $\mathbf{R}_p = \int_0^\infty e^{\tau \mathbf{A}_p^{\mathrm{T}}} \mathbf{Q}_p e^{\tau \mathbf{A}_p} d\tau$ such that $\mathbf{A}_p^{\mathrm{T}}\mathbf{R}_p + \mathbf{R}_p\mathbf{A}_p + \mathbf{Q}_p = \mathbf{0}$. Thus, once T_{kp} verifies

$$T_{kp} > \tau_p = \sup_{p\in\mathcal{P}}\{\frac{\lambda_{\max}(\mathbf{R}_p)}{\lambda_{\min}(\mathbf{Q}_p)}\ln\frac{\lambda_{\max}(\mathbf{R}_p)}{\lambda_{\min}(\mathbf{R}_p)}\}, \tag{21}$$

where the symbols $\lambda_{\min}(\cdot)$ and $\lambda_{\max}(\cdot)$ denote the minimum and maximum eigenvalues of a matrix, respectively, then the switched DCmG will be globally and asymptotically stable.

Proof: The proof is referred to Theorem 3.1 in [31]. ■

Based on Lemmas 1-2, we provide the following result to guarantee the voltage stability under PCG perturbation.

Proposition 1: For the DCmG with ZIP loads satisfying (18), if the perturbed PCGs and the perturbation interval satisfy (19) and (21), respectively, then the primary controllers (6) can achieve asymptotic voltage stability.

Proof: According to Lemma 1, if the ZIP loads satisfy (18) and the perturbed PCGs satisfy (19), then the DCmG *after any single perturbation* is asymptotically stable. Furthermore, as shown in Lemma 2, when the DCmG is consecutively perturbed with the fixed interval T_{kp} satisfying (21), then the DCmG *under the consecutive perturbation* is asymptotically stable. Thus, the statement holds. ■

IV. Detectability Enhancement With PCG Perturbation

In this section, we analyze the enhanced detectability of the UIO-based detector against ZTS and replay attacks under PCG perturbation. In particular, the sufficient conditions under which these attacks can be detected are analytically provided. Since the system parameters from the insiders cannot be updated in a timely manner, it is possible to invalidate the leaked A_{ki} by perturbing the PCGs with a short interval satisfying (21). Specifically, we have

Assumption 3: Perturbing PCGs with the interval satisfying (21) can make the A_{ki} obtained from insiders outdated.

Besides, the secure communication links[1] between DERs are in presence to transmit $\boldsymbol{k}_i^p$ to neighboring DERs $\forall j \in \mathcal{N}_i^c$. Here we note that $\boldsymbol{k}_i^p$ cannot be identified by the attacker based on the information obtained from the unencrypted links, as only the output information of the DER dynamics (8) is transmitted. With the received $\boldsymbol{k}_i^p$, $\mathrm{UIO}_{j,i}$ (9) is updated as

$$\mathrm{UIO}_{j,i}^p \begin{cases} \dot{\boldsymbol{z}}_{j,i}^p(t) = F_i^p \boldsymbol{z}_{j,i}^p(t) + \hat{K}_i^p \boldsymbol{y}_{j,i}^c(t) \\ \hat{\boldsymbol{x}}_{j,i}^p(t) = \boldsymbol{z}_{j,i}^p(t) + H_i^p \boldsymbol{y}_{j,i}^c(t) \end{cases}, \tag{22}$$

where $F_i^p, \hat{K}_i^p$, and H_i^p are the updated UIO parameters, and $\boldsymbol{z}_{j,i}^p(t)$ and $\hat{\boldsymbol{x}}_{j,i}^p(t)$ are the corresponding internal state and estimated state vectors, respectively.

A. ZTS Attack

In this subsection, we theoretically analyze the increment of the residual vector against the ZTS attack (15) under PCG perturbation, which is denoted by $\Delta\boldsymbol{r}_{j,i}^{zts}(t)$.

Proposition 2: Under Assumption 3, for the updated $\mathrm{UIO}_{j,i}^p$ encountering the ZTS attack (15), $\Delta\boldsymbol{r}_{j,i}^{zts}(t), t \geq T_a$ can be analytically calculated as

$$\Delta\boldsymbol{r}_{j,i}^{zts}(t) = \int_{T_a}^t e^{F_i^p(t-\tau)} T_i^p (A_{ki} - A_{ki}^p)\boldsymbol{\phi}_{j,i}(\tau)d\tau. \tag{23}$$

where $T_i^p = \mathrm{I}^3 - H_i^p$ and $\boldsymbol{\phi}_{j,i}(t) = \int_{T_a}^t e^{A_{ki}(t-\zeta)} M_i \bar{\boldsymbol{d}}_{ji}^a(\zeta)d\zeta$.

Proof: Let $\boldsymbol{r}_{j,i}^{pa}(t)$ and $\boldsymbol{r}_{j,i}^{a}(t)$ denote the alterations of the residual vector caused by the ZTS attack with and without PCG perturbation, respectively, and then we have

$$\Delta\boldsymbol{r}_{j,i}^{zts}(t) = \boldsymbol{r}_{j,i}^{pa}(t) - \boldsymbol{r}_{j,i}^{a}(t). \tag{24}$$

Based on the DER dynamics (8), the $\mathrm{UIO}_{j,i}^p$ (22), and the ZTS attack (15), we can derive that, for $t \geq T_a$,

$$\dot{\boldsymbol{r}}_{j,i}^{pa}(t) = F_i^p \boldsymbol{r}_{j,i}^{pa}(t) + T_i^p(A_{ki} - A_{ki}^p)\boldsymbol{\phi}_{j,i}(t).$$

Since $\boldsymbol{r}_{j,i}^{pa}(T_a) = \mathbb{0}^3$, the $\boldsymbol{r}_{j,i}^{pa}(t)$ for $t \geq T_a$ is determined by the term $T_i^p(A_{ki} - A_{ki}^p)\boldsymbol{\phi}_{j,i}(t)$ and follows

$$\boldsymbol{r}_{j,i}^{pa}(t) = \int_{T_a}^t e^{F_i^p(t-\tau)} T_i^p (A_{ki} - A_{ki}^p)\boldsymbol{\phi}_{j,i}(\tau)d\tau. \tag{25}$$

Similarly, according to (8), (9), and (15), we derive $\dot{\boldsymbol{r}}_{j,i}^{a}(t) = F_i \boldsymbol{r}_{j,i}^{a}(t), t \geq T_a$. With $\boldsymbol{r}_{j,i}^{a}(T_a) = \mathbb{0}^3$, we further obtain

$$\boldsymbol{r}_{j,i}^{a}(t) = \mathbb{0}^3. \tag{26}$$

Thus, the result (23) holds directly by substituting (25) and (26) into (24). ■

Remark 3: According to (23), $|\Delta\boldsymbol{r}_{j,i}^{zts}(t)|$ is jointly determined by the perturbation related term $|T_i^p(A_{ki} - A_{ki}^p)|$ and the attack vector associated term $|M_i\bar{\boldsymbol{d}}_{ji}^a(t)|$, whose growth both promotes the growth of the detection residual vector, i.e., the ZTS attack is more likely to be detected. Two insights are received from the result. The first one is intuitive, that is, the perturbation can result in nontrivial steady-state residual vector against the ZTS attack. In particular, the larger perturbation $|T_i^p(A_{ki} - A_{ki}^p)|$ is able to expose the ZTS attack generated with the smaller $|\bar{\boldsymbol{d}}_{ji}^a(t)|$. Secondly, the nontrivial residual vector is difficult to be eliminated if the attacker has no knowledge of T_i^p and A_{ki}^p in advance. To demonstrate the

[1]The transmitted data may be secured by employing the advanced encryption/decryption technology, whose keys are dynamically altered to protect the encrypted data from being understood by the attacker [32].

second insight, we show the special case of (23) with constant $\bar{\boldsymbol{d}}^a_{ji}$ as follows

$$\Delta \boldsymbol{r}^{zts}_{j,i}(t) = \int_{T_a}^{t} e^{F^p_i(t-\tau)} T^p_i (A_{ki} - A^p_{ki}) A^{-1}_{ki} \times \\ \times (\mathrm{I}^3 - e^{A_{ki}(\tau - T_a)}) M_i \bar{\boldsymbol{d}}^a_{ji} d\tau.$$

The necessary condition for $\Delta \boldsymbol{r}^{zts}_{j,i}(\infty) = \mathbb{0}^3$ is $T^p_i (A_{ki} - A^p_{ki}) A^{-1}_{ki} M_i \bar{\boldsymbol{d}}^a_{ji} = \mathbb{0}^3$, which is difficult to be fulfilled according to equations (5), (10b), and (11) if A^p_{ki} and T^p_i are unknown to the attacker.

B. Replay Attack

In this subsection, we theoretically investigate the improved residual vector against the replay attack (16) under PCG perturbation, which is represented by $\Delta \boldsymbol{r}^{rep}_{j,i}(t)$.

Proposition 3: Under Assumption 3, for the updated $\mathrm{UIO}^p_{j,i}$ suffering from the replay attack (16), whose replayed data is consistent with A_{ki}, $\Delta \boldsymbol{r}^{rep}_{j,i}(t)$ can be explicitly calculated as

$$\begin{aligned} \Delta \boldsymbol{r}^{rep}_{j,i}(t) = & \underbrace{e^{F^p_i(t-T_a)} \boldsymbol{\epsilon}^p_{j,i}(T_a) - e^{F_i(t-T_a)} \boldsymbol{\epsilon}_{j,i}(T_a)}_{\boldsymbol{\Delta}^{\epsilon}_{j,i}(t)} + \\ & + \underbrace{(e^{F^p_i(t-T_a)} H^p_i - e^{F_i(t-T_a)} H_i) \boldsymbol{\rho}_i(t - T_{rep})}_{\boldsymbol{\Delta}^{\rho 1}_{j,i}(t)} + \\ & + \underbrace{\int_{T_a}^{t} e^{F^p_i(t-\tau)} T^p_i (A_{ki} - A^p_{ki}) \boldsymbol{x}_i(\tau - T_{rep}) d\tau}_{\boldsymbol{\Delta}^{x}_{j,i}(t)} + \\ & + \underbrace{\int_{T_a}^{t} (e^{F^p_i(t-\tau)} S^p_i - e^{F_i(t-\tau)} S_i) \boldsymbol{\rho}_i(\tau - T_{rep}) d\tau}_{\boldsymbol{\Delta}^{\rho 2}_{j,i}(t)} + \\ & + \underbrace{\int_{T_a}^{t} (e^{F^p_i(t-\tau)} T^p_i - e^{F_i(t-\tau)} T_i) \boldsymbol{\omega}_i(\tau - T_{rep}) d\tau}_{\boldsymbol{\Delta}^{\omega}_{j,i}(t)} + \\ & + \underbrace{(H_i - H^p_i) \boldsymbol{\rho}_i(t - T_{rep})}_{\boldsymbol{\Delta}^{\rho 3}_{j,i}(t)} \end{aligned} \tag{27}$$

for $t \in [T_a, T_a + T_{rep}]$, where $\boldsymbol{\epsilon}^p_{j,i}(t) = \boldsymbol{x}_i(t - T_{rep}) - \hat{\boldsymbol{x}}^p_{j,i}(t)$ and $\boldsymbol{\epsilon}_{j,i}(t) = \boldsymbol{x}_i(t - T_{rep}) - \hat{\boldsymbol{x}}_{j,i}(t)$ denote the vectors of the state estimation error with and without PCG perturbation, respectively, $S^p_i = T^p_i \boldsymbol{b}_i \boldsymbol{k}_i - \hat{K}^p_i$, and $S_i = T_i \boldsymbol{b}_i \boldsymbol{k}_i - \hat{K}_i$.

Proof: With some abuse of notations, let $\boldsymbol{r}^p_{j,i}(t) = \boldsymbol{\epsilon}^p_{j,i}(t) + \rho_i(t - T_{rep})$ and $\boldsymbol{r}_{j,i}(t) = \boldsymbol{\epsilon}_{j,i}(t) + \rho_i(t - T_{rep})$ be the residual vectors under the replay attack (16) with and without PCG perturbation, respectively. According to the DER dynamics (8), the update $\mathrm{UIO}^p_{j,i}$ (22), and the replay attack (16), the dynamics of $\boldsymbol{\epsilon}^p_{j,i}(t)$ obey

$$\begin{aligned} \dot{\boldsymbol{\epsilon}}^p_{j,i}(t) = & F^p_i \boldsymbol{\epsilon}^p_{j,i}(t) + T^p_i (A_{ki} - A^p_{ki}) \boldsymbol{x}_i(t - T_{rep}) + \\ & - H^p_i \dot{\boldsymbol{\rho}}_i(t - T_{rep}) + T^p_i \boldsymbol{\omega}_i(t - T_{rep}) + \\ & + (S^p_i + F^p_i H^p_i) \boldsymbol{\rho}_i(t - T_{rep}) \end{aligned}$$

for $t \in [T_a, T_a + T_{rep}]$. By direct calculation, we obtain

$$\begin{aligned} \boldsymbol{\epsilon}^p_{j,i}(t) = & e^{F^p_i(t-T_a)} \big[\boldsymbol{\epsilon}^p_{j,i}(T_a) + H^p_i \boldsymbol{\rho}_i(t - T_{rep}) \big] + \\ & + \int_{T_a}^{t} e^{F^p_i(t-\tau)} T^p_i (A_{ki} - A^p_{ki}) \boldsymbol{x}_i(\tau - T_{rep}) d\tau + \\ & + \int_{T_a}^{t} e^{F^p_i(t-\tau)} S^p_i \boldsymbol{\rho}_i(\tau - T_{rep}) d\tau + \\ & + \int_{T_a}^{t} e^{F^p_i(t-\tau)} T^p_i \boldsymbol{\omega}_i(\tau - T_{rep}) d\tau + \\ & - H^p_i \boldsymbol{\rho}_i(t - T_{rep}) \end{aligned} \tag{28}$$

Without PCG perturbation, the estimation error vector can be calculated in a similar manner as

$$\begin{aligned} \boldsymbol{\epsilon}_{j,i}(t) = & e^{F_i(t-T_a)} \big[\boldsymbol{\epsilon}_{j,i}(T_a) + H_i \boldsymbol{\rho}_i(t - T_{rep}) \big] + \\ & + \int_{T_a}^{t} e^{F_i(t-\tau)} S_i \boldsymbol{\rho}_i(\tau - T_{rep}) d\tau + \\ & + \int_{T_a}^{t} e^{F_i(t-\tau)} T_i \boldsymbol{\omega}_i(\tau - T_{rep}) d\tau + \\ & - H_i \boldsymbol{\rho}_i(t - T_{rep}). \end{aligned} \tag{29}$$

The statement follows after substituting (28) and (29) into $\Delta \boldsymbol{r}^{rep}_{j,i}(t) = \boldsymbol{\epsilon}^p_{j,i}(t) - \boldsymbol{\epsilon}_{j,i}(t)$. ■

Remark 4: According to (27), the improved residual vector is dominated by the term $\boldsymbol{\Delta}^x_{j,i}$. The term $\boldsymbol{\Delta}^{\epsilon}_{j,i}$ decays exponentially to zeros with the growth of t, and the terms $\boldsymbol{\Delta}^{\rho 1}_{j,i}, \boldsymbol{\Delta}^{\rho 2}_{j,i}, \boldsymbol{\Delta}^{\rho 3}_{j,i}, \boldsymbol{\Delta}^{\omega}_{j,i}$ merely have negligible impact due to the bounded noises. As indicated by the expression of $\boldsymbol{\Delta}^x_{j,i}$, the PCG perturbation can also cause nontrivial steady-state residual vector against the replay attack. Specifically, with nontrivial $\boldsymbol{x}_i(\tau - T_{rep})$, the larger $|T^p_i (A_{ki} - A^p_{ki})|$ can significantly contribute to the growth of $|\boldsymbol{\Delta}^x_{j,i}|$, such that the replay attack is more likely to be detected.

Based on Propositions 2-3, we can obtain the sufficient conditions for the detection of deception attacks in DCmGs.

Theorem 1: Under Assumption 3, the ZTS attack (15) can be detected if

$$|\Delta \boldsymbol{r}^{zts}_{j,i}(t)| > 2 |\bar{\boldsymbol{r}}_{j,i}(t)|, \tag{30}$$

and the replay attack (16) will be perceived once

$$|\Delta \boldsymbol{r}^{rep}_{j,i}(t)| > 2 |\bar{\boldsymbol{r}}_{j,i}(t)|. \tag{31}$$

Proof: For clarity, let $\tilde{\boldsymbol{r}}^{zts}_{j,i}(t)$ and $\tilde{\boldsymbol{r}}^{rep}_{j,i}(t)$ represent the residual vectors against the ZTS attack (15) and the replay attack (16) without PCG perturbation, respectively, and then the ones with PCG perturbation can be obtained as

$$\begin{aligned} \boldsymbol{r}^{zts}_{j,i}(t) &= \tilde{\boldsymbol{r}}^{zts}_{j,i}(t) + \Delta \boldsymbol{r}^{zts}_{j,i}(t), \\ \boldsymbol{r}^{rep}_{j,i}(t) &= \tilde{\boldsymbol{r}}^{rep}_{j,i}(t) + \Delta \boldsymbol{r}^{rep}_{j,i}(t). \end{aligned}$$

When (30) and (31) hold, the following inequalities establish immediately:

$$\begin{aligned} |\boldsymbol{r}^{zts}_{j,i}(t)| \geq |\Delta \boldsymbol{r}^{zts}_{j,i}(t)| - |\tilde{\boldsymbol{r}}^{zts}_{j,i}(t)| > |\bar{\boldsymbol{r}}_{j,i}(t)|, \\ |\boldsymbol{r}^{rep}_{j,i}(t)| \geq |\Delta \boldsymbol{r}^{rep}_{j,i}(t)| - |\tilde{\boldsymbol{r}}^{rep}_{j,i}(t)| > |\bar{\boldsymbol{r}}_{j,i}(t)|, \end{aligned}$$

indicating that the ZTS and replay attacks will be detected. The proof is completed. ■

Remark 5: Indeed, either (30) or (31) requires the improvement of the residual to be larger than twice the detection bound, which is a relatively loose sufficient condition for attack detection. Some attacks that do not satisfy the condition can still trigger the attack alarm. Nevertheless, the condition can work effectively in determining the detectability of the UIO-based detector against a type of specific attacks. Moreover, since the bounds of noises are usually small, the detection bound will not be too large. According to Fig. 6, the residuals under attacks can be far larger than twice the detection bounds.

Algorithm 1 The Implementation of CMTD in DER $j \in \mathcal{A}$

Input: The received $\boldsymbol{k}_i^p, \forall i \in \mathcal{N}_j^c$ from neighbors; The minimal T_{kp} satisfying (21)
Update the UIO-based detectors with received $\boldsymbol{k}_i^p$;
Send the current $\boldsymbol{k}_j^p$ to neighbors;
Record current time as t_0;
Output: The detection of deception attacks
if $t - t_0 < T_{kp}$ **then**
  Calculate the residual vectors $\boldsymbol{r}_{j,i}(t), \forall i \in \mathcal{N}_j^c$;
  if (13) is violated **then**
    Isolate the corresponding link (i, j);
  else
    Return to step 4;
  end if
else
  Update $\boldsymbol{k}_j^p$ with elements randomly chosen from (19);
end if

Remark 6: The plug-in/out of DERs is frequent in DCmGs and can happen at any time regardless of the PCG perturbation. If the DER is plugged into the DCmG, then the first PCG perturbation can only be activated when the perturbed PCGs are received from the neighbors rather than based on the local time, as the DER does not know the time when the last PCG perturbation happened. For the DER plugged out from the DCmG, the PCG perturbation should be stopped to avoid the unnecessary performance degradation.

Remark 7: In this work, we merely consider the isolated DCmG that operates in the independent mode. As the other operating mode, when the DCmG is in the grid-supportive mode, there must exist DC-AC voltage source inverters (VSIs) to be connected to the main grid and to supply possible AC loads. Besides, there may exist AC-DC voltage source converters (VSCs) to integrate wind turbine generators. Generally, the control structures and algorithms involved in VSIs and VSCs are much more complex than those in DC-DC buck converters [33]. Thus, further efforts are required to investigate the impact of PCG perturbation on voltage stability when considering the general DCmGs equipped with VSIs and VSCs.

Remark 8: The proposed CMTD is dedicated to the detection of possible deception attacks against communication links between DERs. However, as the integration of the information communications technology inside the DER, like transmitting the measurements generated by the analog-to-digital (ADC) converters to the controller, the threat of the deception attacks inside DERs is becoming severe. Moreover, the coordinated deception attack, which corrupts the local measurements to deteriorate the status of one specific DER and compromises the communicated measurements to hide the bad status, can easily cause converter outages and is extremely harmful. To defend against the mentioned general deception attacks, it is necessary to integrate the physical invariant information into the defense strategy, which is left as our future work.

V. Simulation and Experiment Results

In this section, we test the impact of PCGs, CEPs, and the network topology on the perturbation interval, and validate the effectiveness of the proposed CMTD against ZTS and replay attacks through Matlab Simulink/PLECS based simulations and Typhoon HIL 602+ based experiments. In particular, we consider 4 representative DCmGs with commonly used network topologies as shown in Fig. 2, i.e., the 4-DER DCmG with a ring topology [7], [21], [34], the 6-DER DCmG with a radial topology [35], [36], the 6-DER DCmG with a mesh topology [22], and the 16-DER DCmG with a mesh topology [37], where the CEPs shown in TABLE I are chosen according to [38]–[40]. The resistances of power lines between DERs are $R_{ij} = 0.2\Omega, \forall \{i, j\} \in \mathcal{E}_{el}$. Moreover, the PCG vectors without perturbation are $\boldsymbol{k}_i = [0.85, 0.01, 2]^{\mathrm{T}}, \forall i \in \mathcal{A}$, and the secondary control parameter is $k_I = 0.4$. The bounds for the noises are $\bar{\boldsymbol{\omega}}_i = \bar{\boldsymbol{\rho}}_i = 0.1 \times [1, 1, 1]^{\mathrm{T}}, \forall i \in \mathcal{A}$. The nominal reference PCC voltages are $V_{ref,i} = 48\mathrm{V}, \forall i \in \mathcal{A}$, and the equivalent impedance loads are $Z_{Li} = 200\Omega, \forall i \in \mathcal{A}$.

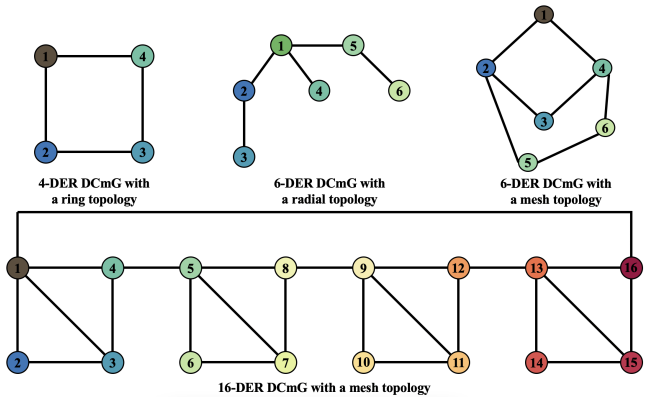


Fig. 2: This figure shows the network topologies of 4 representative DCmGs.

TABLE I: CEPs of DER i

Parameter	Symbol	Value
Output capacitance	C_{ti}	2.2mF
Inductance	L_{ti}	1.8mH
Inductor + switch loss resistance	R_{ti}	0.2Ω
Switching frequency	f_{sw}	10kHz

A. Perturbation Interval

Although it is difficult to derive an analytical lower bound of T_{kp} for DCmGs with *general* PCGs, CEPs, and network topologies based on (21), it indeed provides the capability of evaluating the lower bound of T_{kp} for a *deterministic* DCmG. In the sequel, based on the 4 representative DCmGs shown in Fig. 2 with the typical CEPs provided in TABLE I, we conduct numerical simulations to show the value τ_p, which determines the lower bound of T_{kp}, under different settings of PCGs, CEPs, and network topologies.

1) Case 1: The first case illustrates the relationships between τ_p and $\boldsymbol{k}_i^p$, and τ_p and the network topology of $\mathcal{G}_{el}$. For convenience, the ranges of $k_{[il]}^p, \forall l \in \{1,2,3\}$ defined by (19) are normalized to the range $(0,1)$, after which the vector space of $\boldsymbol{k}_i^p$ is a cube. Then, the cube is evenly sampled and $15 \times 15 \times 15$ discrete points are obtained. Specifically, for DER $i \in \mathcal{A}$ with the discrete point defined by the ternary set $\{k_{[i1,x]}^p, k_{[i2,y]}^p, k_{[i3,z]}^p\}$, the actual PCG vector is calculated as $\boldsymbol{k}_i^p = \big[-1+2k_{[i1,x]}^p, -R_{ti}+2R_{ti}k_{[i2,y]}^p, k_{[i3,z]}^p \frac{1}{L_{ti}}(k_{[i1,x]}^p - 1)(k_{[i2,y]}^p - R_{ti})\big]^{\mathrm{T}}$. The value of τ_p is calculated assuming that the PCGs of DERs in the DCmG share the values derived from the discrete point.

According to Fig. 3, in general, the increases of $k_{[i1,x]}^p$ and $k_{[i2,y]}^p$ both have negative impact on τ_p, while $k_{[i3,z]}^p$ is positively related to τ_p. The is because that the large *proportional* PCGs $k_{[i1,x]}^p$ and $k_{[i2,y]}^p$ both contribute to speeding up the asymptotic convergence rate of (20), and thus only short time (i.e., the small τ_p) is required to stabilize the individual subsystem. Differently, the large *integral* PCG $k_{[i3,z]}^p$ may oscillate the system, under which (20) needs more time to converge (i.e., the large τ_p). In addition, the network topology of $\mathcal{G}_{el}$ with more branches, i.e., the stronger physical couplings among DERs, can slightly enlarge τ_p.

2) Case 2: The second case shows the relationships between τ_p and CEPs, and τ_p and the network topology of $\mathcal{G}_{el}$. The CEPs of DERs $\forall i \in \mathcal{A}$ satisfying (32) are considered, which are chosen around the typical ones in [38]–[40]. Similar as in case 1, the vector space $[R_{ti}, L_{ti}, C_{ti}]^{\mathrm{T}}$ satisfying (32) is firstly normalized to a cube, and then $15 \times 15 \times 15$ discrete points are obtained by evenly sampling over the cube, where each point is denoted by the ternary set $\{R_{ti,x}, L_{ti,y}, C_{ti,z}\}$. The value of τ_p is calculated assuming that the DERs in the DCmG share the CEPs described by the discrete point, and $\boldsymbol{k}_i^p, \forall i \in \mathcal{A}$ are randomly chosen as $[\frac{1}{2}, \frac{0.1+0.9R_{ti,x}}{2}, \frac{0.1+0.9R_{ti,x}}{(4+36L_{ti,y})\text{e-}3}]^{\mathrm{T}}$.

According to Fig. 4, the increases of resistive CEP $R_{ti,x}$ and capacitive CEP $C_{ti,z}$ both have positive impact on τ_p, and the inductive CEP $L_{ti,y}$ is negatively related to τ_p. The phenomenon can be explained by the damping factor $\zeta_{ti} = \frac{R_{ti}}{2}\sqrt{\frac{C_{ti}}{L_{ti}}}$, which determines the type of transient that the RLC circuit will exhibit [41]. That is, the larger ζ_{ti}, which can be caused by the increases of $R_{ti,x}$ and $C_{ti,z}$ or the decrease of $L_{ti,y}$, demands longer time (i.e., the larger τ_p) to converge. Besides, the results also imply that the impact of the network topology of $\mathcal{G}_{el}$ on τ_p is neglectable.

$$\begin{cases} 0.1\Omega < R_{ti} < 1\Omega \\ 1\text{mH} < L_{ti} < 10\text{mH} \\ 1\text{mF} < C_{ti} < 10\text{mF} \end{cases}. \tag{32}$$

In summary, given the analysis above, we obtain that the PCGs and CEPs both significantly affect τ_p with physically interpretable manners, while the network topology of $\mathcal{G}_{el}$ with more branches can slightly enlarge τ_p. Moreover, from the results, we have the following condition for T_{kp}. Considering the 4 representative DCmGs shown in Fig. 2 with the PCGs and CEPs satisfying (19) and (32), respectively,

$$T_{kp} \geq 3000\text{s} \geq 50\text{min} \tag{33}$$

is sufficient to make the DCmG under PCG perturbation asymptotically stable. Although the maximum τ_p can be 3000 when $R_{ti,x} \to 1, C_{ti,z} \to 1$, and $L_{ti,y} \to 0$, we note that it is merely an upper bound and is impossible in practice. For example, when the CEPs are set according to TABLE I, $|k_{[i1,x]}| > 0.8$, and $|k_{[i2,y]}| > 0.8R_{ti}$, the value of τ_p will not exceed 1000.

B. Simulation Results for the Effectiveness of CMTD

In Matlab Simulink/PLECS, we establish the 16-DER DCmG with a mesh topology as shown in Fig. 2. The evolution of the DCmG is divided into several stages: At $t = T_{\text{pri}} = 0$s, the power lines among DERs are interconnected and the primary controllers are started; At $t = T_{\text{sec}} = 20$s, the secondary controllers are activated. The continuous variables like V_i and I_{ti} are sampled with the fixed period $T_{\text{samp}} = 0.05$s and are fed into the discrete UIO-based detectors. At $t = T_{\text{swi}} = 45$s, all current loads are increased by 20%; At $t = T_{\text{att}} = 55$s, the ZTS attack against communication link $\{1,2\} \in \mathcal{E}_c$ or the replay attack against communication links $\{1,2\}$ and $\{1,3\} \in \mathcal{E}_c$ is launched. Specifically, the fake unknown input is $\bar{\boldsymbol{d}}_{21}^a = [0.2, 0.2]^{\mathrm{T}}$ and the period of the recorded data is $(25\text{s}, 35\text{s})$. Here the switch of current loads is included to simulate the daily operation of real-world DCmGs. Moreover, the PCG perturbation is introduced at $t = T_{\text{per}} = 35$s, and the perturbed PCG vector is $\boldsymbol{k}_i^p = [0.8670, -0.19, 2.2]^{\mathrm{T}}$.

1) ZTS Attack: The results under the ZTS attack are shown in (a) of Fig. 5. In the absence of PCG perturbation, voltage balancing and current sharing can be achieved before T_{att}, while the activation of the ZTS attack will make the PCC voltages grow like ramp signals and destroy current sharing. Moreover, the ZTS attack will not alter the detection residuals and thus is unforeseeable to the UIO-based detector. In the presence of PCG perturbation, nontrivial instantaneous fluctuations emerge on the PCC voltages and output currents, but voltage balancing and current sharing can be finally achieved after the perturbation. Besides, the detection residuals increase significantly and exceed the detection bounds at $t = 56.2$s, after which the attacked link $\{1,2\}$ is isolated and voltage balancing and current sharing are recovered.

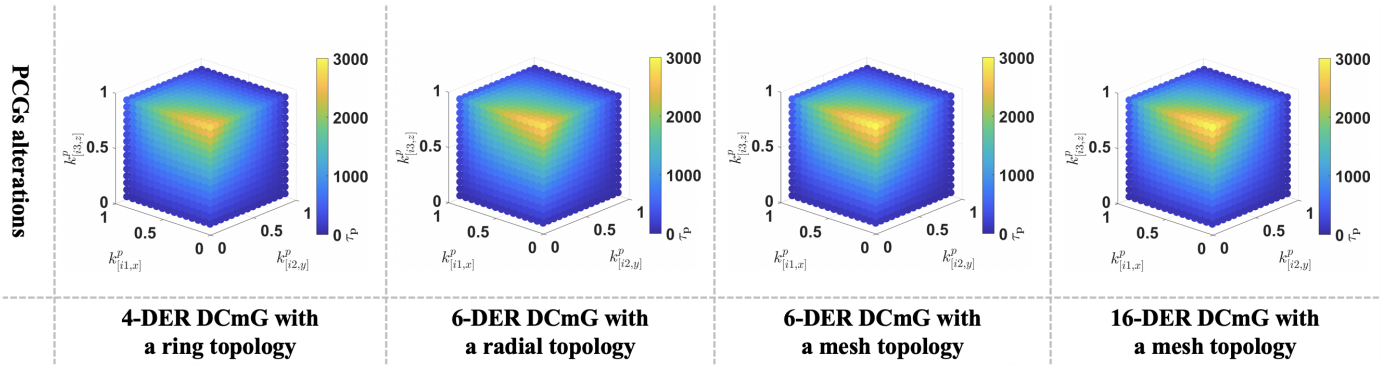


Fig. 3: This figure visualizes the variation of τ_p under different settings of PCGs and network topologies.

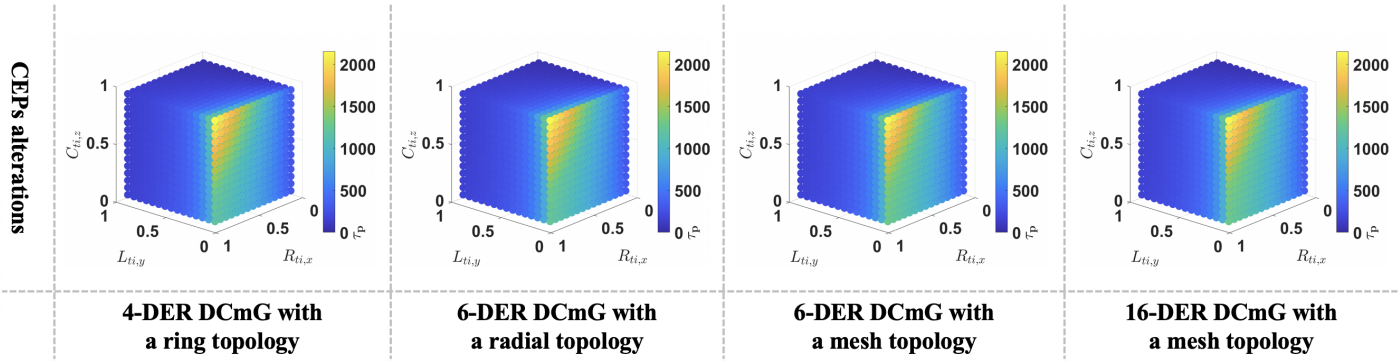


Fig. 4: This figure visualizes the variation of τ_p under different settings of CEPs and network topologies.

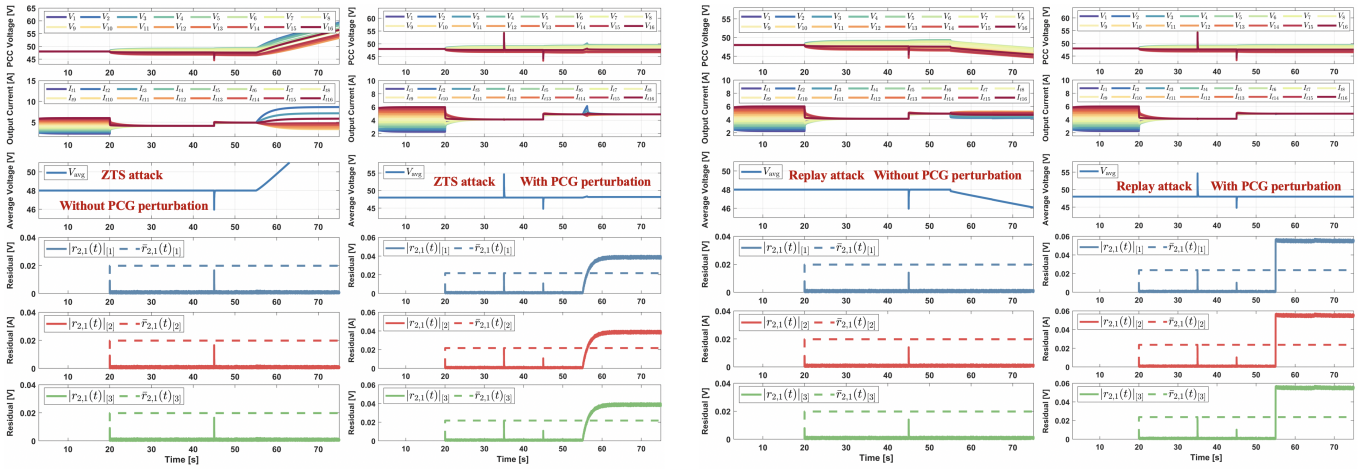
2) Replay Attack: The results under the replay attack are demonstrated in (b) of Fig. 5. In the absence of PCG perturbation, the replay attack will make the PCC voltages decrease constantly and enlarge the current sharing error, which are comparable to those caused by the ZTS attack. While the UIO-based detector is totally unconscious about the existence of the replay attack. In the presence of PCG perturbation, the detection residuals are disturbed with instantaneous fluctuations but are still within the detection bounds. In addition, the detection residuals under the replay attack increase instantaneously and exceed the detection bounds at $t = 55.03$s, after which the abnormal links $\{1, 2\}$ and $\{1, 3\}$ are isolated and voltage balancing and current sharing are reestablished.

C. Experiment Results for the Effectiveness of CMTD

Based on the Typhoon HIL 602+ emulator, which is specialized in the ultra-low-latency, ultra-high-fidelity, real-time emulation of power electronics enabled microgrids [37], [42], [43], we establish the 6-DER DCmG with a radial topology as shown in Fig. 2. The implementation overview of the DCmG testbed is illustrated in Fig. 7. In particular, the SCADA center runs a dedicated software for the Typhoon emulator, and can edit the model schematic and monitor the real-time operating status. The Raspberry PI based data transmission unit implements the self-loop TCP/IP Modbus communication link to emulate the communication network in the DCmG. Specifically, in each conservation, the Raspberry PI (Modbus client) receives the packet containing the states of all DERs from the Typhoon HIL emulator (Modbus server), and then writes the received states into the holding registers in the Typhoon HIL emulator. Since only one communication link is established between the server and client, the process of writing multiple registers simultaneously would be time-consuming. In the experiments, the average time of each conversation is calculated as 0.34s, under which the discrete state-space model of DER dynamics and the discrete UIO-based detector are obtained. Moreover, the PCC voltages and output currents are acquired from the SCADA center with the sampling rate of 10kHz. Here the evolution of the 6-DER DCmG and the perturbed PCGs are the same as those of the 16-DER DCmG. The ZTS attack is launched against link $\{1, 2\} \in \mathcal{E}_c$ and the replay attack is launched against links $\{1, 2\}$ and $\{1, 4\} \in \mathcal{E}_c$.

1) ZTS Attack: The results under the ZTS attack are shown in (a) of Fig. 6, which match the simulation results. But the oscillations on PCC voltages, output currents, and residuals are much heavier due to the non-ideal buck converters. Without PCG perturbation, the ZTS attack can cause large deviations on the system states without being perceived. With PCG perturbation, the ZTS attack will be exposed to the UIO-based detector at $t = 55.85$s, after which the received abnormal packets are discarded and the attack impact is limited. However, the recovery of voltage balancing and current sharing cannot be guaranteed as the isolated communication link disconnects the graph $\mathcal{G}_c$.

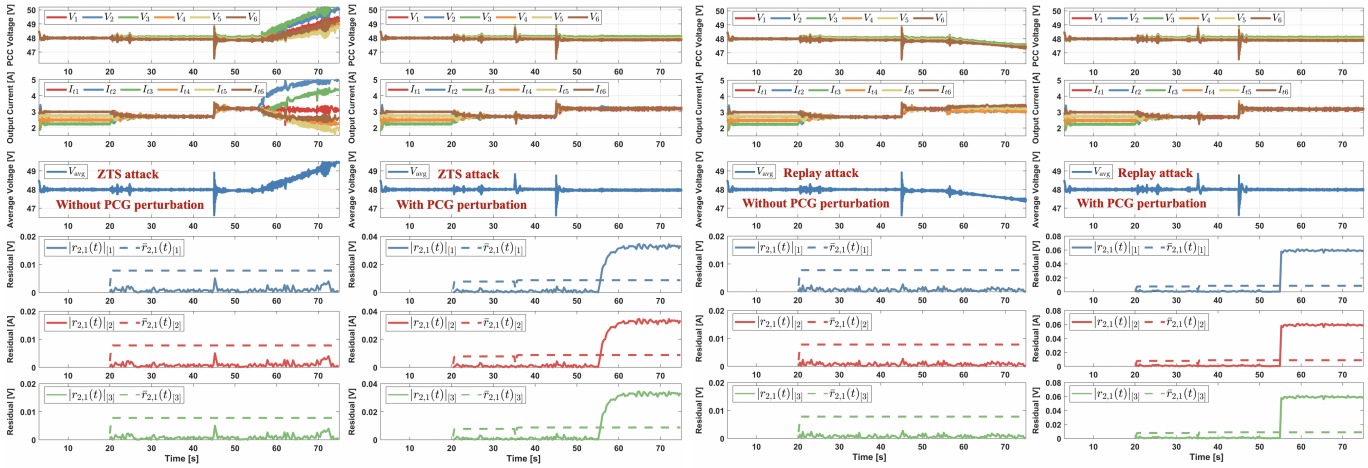
2) Replay Attack: The results under the replay attack are shown in (b) of Fig. 6. Without PCG perturbation, the UIO-based detection cannot detect the replay attack while the



(a) ZTS attack without and with PCG perturbation

(b) Replay attack without and with PCG perturbation

Fig. 5: This figure shows the simulation results on validating the effectiveness of CMTD. In particular, the left sub-figure depicts the results against the ZTS attack, while the right one illustrates the results against the replay attack.



(a) ZTS attack without and with PCG perturbation

(b) Replay attack without and with PCG perturbation

Fig. 6: This figure shows the experiment results on validating the effectiveness of CMTD. In particular, the left sub-figure depicts the results against the ZTS attack, while the right one illustrates the results against the replay attack.

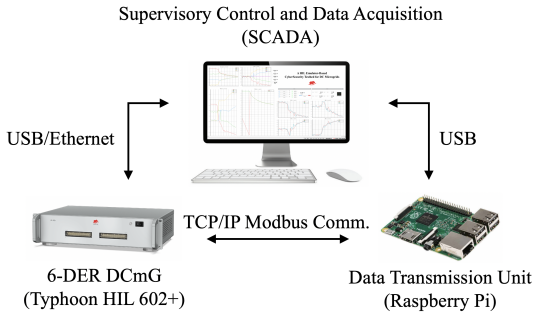


Fig. 7: Implementation overview of the DCmG testbed.

system states deviate a lot from the desired ones. With PCG perturbation, the UIO-based detector can detect the replay attack at almost the time when the attack is launched. Thus, after discarding the corrupted packets, the PCC voltages and output currents are nearly invariant even under the attack.

Remark 9: In subsections V-B and V-C, the perturbed PCG vector $\boldsymbol{k}_i^p$ is chosen by comprehensively considering the following two aspects: 1) The increments of detection residuals under PCG perturbation should be as large as possible; 2) The instantaneous fluctuations caused by the PCG perturbation on PCC voltages and output currents, which may cause unexpected alterations on detection residuals and result in the false alarm, should be acceptable. The first objective can be satisfied referring to (23) and (27), while the second objective is fulfilled through trial and error. In particular, we observe that the opposite changes of $k_{[i1]}^p$ and $k_{[i2]}^p$ usually lead to small fluctuations on system states, and the large alteration on $k_{[i3]}^p$ can significantly improve the detection residuals against deception attacks. Nevertheless, we note that an analytical design method for $\boldsymbol{k}_i^p$ is indispensable for the implementation of CMTD in real-world DCmGs, which still requires further efforts and is left for our future work.

VI. Conclusion and Future Works

In this paper, we proposed a novel CMTD strategy against deceptive FDI and replay attacks in the context of DCmGs. Through theoretical and numerical analysis, we verified that perturbing the PCGs of converter devices with appropriate magnitudes and frequency can remarkably enhance the detectability of the UIO-based detector against deception attacks without destroying the voltage stability in DCmGs. Moreover, extensive Matlab Simulink/PLECS simulation and systematic Typhoon HIL emulator based experiment results were presented to validate the effectiveness of CMTD. In our future work, we will implement CMTD in a laboratory-level 4-node DCmG testbed equipped with real-world converter devices, and investigate an appropriate recovery scheme to avoid the isolation of abnormal communication links.

References

[1] L. Meng, Q. Shafiee, G. F. Trecate, H. Karimi, D. Fulwani, X. Lu, and J. M. Guerrero, "Review on control of DC microgrids and multiple microgrid clusters," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 5, no. 3, pp. 928–948, 2017.

[2] W. Su, J. Wang, and J. Roh, "Stochastic energy scheduling in microgrids with intermittent renewable energy resources," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1876–1883, 2014.

[3] P. Biczel, "Power electronic converters in DC microgrid," in *2007 Compatibility in Power Electronics*, 2007, pp. 1–6.

[4] Z. Cheng, J. Duan, and M. Chow, "To centralize or to distribute: That is the question: A comparison of advanced microgrid management systems," *IEEE Industrial Electronics Magazine*, vol. 12, no. 1, pp. 6–24, 2018.

[5] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "Distributed load sharing under false data injection attack in an inverter-based microgrid," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1543–1551, 2018.

[6] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *IEEE AAC*, 2009, pp. 911–918.

[7] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.

[8] A. Cecilia, S. Sahoo, T. Dragičević, R. Costa-Castelló, and F. Blaabjerg, "Detection and mitigation of false data in cooperative DC microgrids with unknown constant power loads," *IEEE Transactions on Power Electronics*, vol. 36, no. 8, pp. 9565–9577, 2021.

[9] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–1, 2020.

[10] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3800–3815, 2020.

[11] A. J. Gallo, M. S. Turan, F. Boem, G. Ferrari-Trecate, and T. Parisini, "Distributed watermarking for secure control of microgrids under replay attacks," *IFAC-PapersOnLine*, vol. 51, no. 23, pp. 182–187, 2018.

[12] M. Liu, P. Cheng, C. Zhao, R. Deng, W. Wang, and J. Chen, "False data injection attacks and corresponding countermeasure in DC microgrid," *arXiv preprint arXiv:2001.01984*, 2020.

[13] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[14] Z. Zhang, R. Deng, D. K. Yau, P. Cheng, and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2320–2335, 2019.

[15] ——, "On hiddenness of moving target defense against false data injection attacks on power grid," *ACM Transactions on Cyber-Physical Systems*, vol. 4, no. 3, pp. 1–29, 2020.

[16] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying fdi attacks in power system state estimation," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, pp. 763–776, 2018.

[17] M. Cui and J. Wang, "Deeply hidden moving-target-defense for cyber-secure unbalanced distribution systems considering voltage stability," *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 1961–1972, 2020.

[18] M. Liu, C. Zhao, Z. Zhang, R. Deng, and P. Cheng, "Analysis of moving target defense in unbalanced and multiphase distribution systems considering voltage stability," in *IEEE SGC*, 2021, to appear.

[19] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids—a general approach toward standardization," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 1, pp. 158–172, Jan 2011.

[20] J. He, Y. W. Li, J. M. Guerrero, F. Blaabjerg, and J. C. Vasquez, "An islanding microgrid power sharing approach using enhanced virtual impedance control scheme," *IEEE Transactions on Power Electronics*, vol. 28, no. 11, pp. 5272–5282, 2013.

[21] R. Han, M. Tucci, A. Martinelli, J. M. Guerrero, and G. Ferrari-Trecate, "Stability analysis of primary plug-and-play and secondary leader-based controllers for DC microgrid clusters," *IEEE Transactions on Power Systems*, vol. 34, no. 3, pp. 1780–1800, 2018.

[22] 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.

[23] M. Tucci, S. Riverso, and G. Ferrari-Trecate, "Line-independent plug-and-play controllers for voltage stabilization in DC microgrids," *IEEE Transactions on Control Systems Technology*, vol. 26, no. 3, pp. 1115–1123, 2017.

[24] P. Nahata, R. Soloperto, M. Tucci, A. Martinelli, and G. Ferrari-Trecate, "A passivity-based approach to voltage stabilization in DC microgrids with ZIP loads," *Automatica*, vol. 113, p. 108770, 2020.

[25] 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.

[26] J. Chen, R. J. Patton, and H.-Y. Zhang, "Design of unknown input observers and robust fault detection filters," *International Journal of Control*, vol. 63, no. 1, pp. 85–105, 1996.

[27] J. Hunker and C. Probst, "Insiders and insider threats - an overview of definitions and mitigation techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, pp. 4–27, 2011.

[28] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[29] M. Liu, Z. Jin, J. Xia, M. Sun, R. Deng, and P. Cheng, "Demo abstract: A HIL emulator-based cyber security testbed for DC microgrids," in *INFOCOM WKSHPS*, 2021, pp. 1–2.

[30] A. S. Morse, "Supervisory control of families of linear set-point controllers-part i. exact matching," *IEEE Transactions on Automatic Control*, vol. 41, no. 10, pp. 1413–1431, 1996.

[31] Wei Ni, Daizhan Cheng, and Xiaoming Hu, "Minimum dwell time for stability and stabilization of switched linear systems," in *2008 7th World Congress on Intelligent Control and Automation*, 2008, pp. 4109–4115.

[32] D. Kang, J. Lee, B. Kim, and D. Hur, "Proposal strategies of key management for data encryption in SCADA network of electric power systems," *International Journal of Electrical Power & Energy Systems*, vol. 33, no. 9, pp. 1521–1526, 2011.

[33] M. Kumar, S. Srivastava, and S. Singh, "Control strategies of a DC microgrid for grid connected and islanded operations," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1588–1601, 2015.

[34] G.-Y. Lee, B.-S. Ko, J. Cho, and R.-Y. Kim, "A distributed control method based on a voltage sensitivity matrix in DC microgrids with low-speed communication," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3809–3817, 2018.

[35] Z. Wang, F. Liu, Y. Chen, S. H. Low, and S. Mei, "Unified distributed control of stand-alone DC microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 1013–1024, 2017.

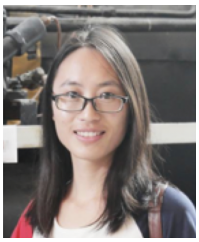
[36] S. Papathanassiou, N. Hatziargyriou, K. Strunz *et al.*, "A benchmark low voltage microgrid network," in *Proceedings of the CIGRE symposium: power systems with dispersed generation*. CIGRE, 2005, pp. 1–8.

[37] S. Abhinav, H. Modares, F. L. Lewis, and A. Davoudi, "Resilient cooperative control of DC microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 1083–1085, 2018.

[38] Q. Shafiee, T. Dragicevic, J. C. Vasquez, and J. M. Guerrero, "Modeling, stability analysis and active stabilization of multiple DC-microgrid clusters," in *IEEE ENERGYCON*, 2014, pp. 1284–1290.

[39] T. Dragičević, J. M. Guerrero, J. C. Vasquez, and D. Škrlec, "Supervisory control of an adaptive-droop regulated DC microgrid with battery management capability," *IEEE Transactions on Power Electronics*, vol. 29, no. 2, pp. 695–706, 2014.
[40] M. Hamzeh, M. Ghafouri, H. Karimi, K. Sheshyekani, and J. M. Guerrero, "Power oscillations damping in DC microgrids," *IEEE Transactions on Energy Conversion*, vol. 31, no. 3, pp. 970–980, 2016.
[41] J. D. Irwin and R. M. Nelms, *Basic engineering circuit analysis*. John Wiley & Sons, 2010, vol. 900.
[42] M. Nazir, K. Burkes, and J. H. R. Enslin, "Converter-based power system protection against DC in transmission and distribution networks," *IEEE Transactions on Power Electronics*, vol. 35, no. 7, pp. 6701–6704, 2020.
[43] P. Maloney, "Building a better microgrid with hardware in the loop," *Microgrid Knowledge White Paper Library*, 1996.

Mengxiang Liu (S'20) received the B.Sc. degree in automation from Tongji University, Shanghai, in 2017. He is currently pursuing the Ph.D. degree with the College of Control Science and Engineering, Zhejiang University, Hangzhou, China. His research interests include cybersecurity, microgrid, and smart grid.



Chengcheng Zhao (M'18) received the B.Sc. degree in measurement and control technology and instrument from Hunan University, Changsha, China, in 2013 and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2018, respectively. She worked as a postdoctoral fellow in the College of Control Science and Engineering, Zhejiang University, from 2018 to 2021, and a postdoctoral fellow at the ECE department, University of Victoria, from 2019 to 2020. Currently, she is an Associate Researcher in the College of Control Science and Engineering, Zhejiang university. Her research interests include consensus and distributed optimization, distributed energy management and synchronization in smart grids, and security and privacy in networked systems.

Zhenyong Zhang (M'20) received his Ph.D. degree from Zhejiang University, Hangzhou, China, in 2020, and bachelor degree from Central South University, Changsha, China, in 2015. He was a visiting scholar in Singapore University of Technology and Design, Singapore, from 2018 to 2019. Currently, he is a professor in the college of Computer Science and Technology, Guizhou University, Guiyang, China. His research interests include cyber-physical system security, applied cryptography and machine learning security.

Ruilong Deng (S'11-M'14-SM'19) received the B.Sc. and Ph.D. degrees in control science and engineering from Zhejiang University, Hangzhou, China, in 2009 and 2014, respectively. He was a Research Fellow with Nanyang Technological University, Singapore, from 2014 to 2015; an AITF Postdoctoral Fellow with the University of Alberta, Edmonton, AB, Canada, from 2015 to 2018; and an Assistant Professor with Nanyang Technological University, from 2018 to 2019. Currently, he is a Professor with the College of Control Science and Engineering, Zhejiang University, where he is also affiliated with the School of Cyber Science and Technology. He serves/served as Associate Editors for IEEE Transactions on Smart Grid, IEEE Power Engineering Letters, IEEE/CAA Journal of Automatica Sinica, and IEEE/KICS Journal of Communications and Networks, and Guest Editors for IEEE Transactions on Emerging Topics in Computing, IEEE Transactions on Cloud Computing, and IET Cyber-Physical Systems: Theory & Applications. His research interests include cybersecurity, smart grid, and wireless networking.

Peng Cheng (M'10) received the B.Sc. and Ph.D. degrees in control science and engineering from Zhejiang University, Hang Zhou, China, in 2004 and 2009, respectively. From 2012 to 2013, he was a Research Fellow with the Information System Technology and Design Pillar, Singapore University of Technology and Design, Singapore. He is currently a Professor with the College of Control Science and Engineering, Zhejiang University. He served as the TPC Co-Chair for IEEE IOV 2016, the Local Arrangement Co-Chair for ACM MobiHoc 2015, and the Publicity Co-Chair for IEEE MASS 2013. He serves as Associate Editors for the IEEE Transactions on Control of Network Systems, Wireless Networks, and International Journal of Communication Systems. He also serves/served as Guest Editors for the IEEE Transactions on Automatic Control and the IEEE Transactions on Signal and Information Processing over Networks. His research interests include networked sensing and control, cyber-physical systems, and control system security.

Jiming Chen (M'08-SM'11-F'18) received the B.Sc. and Ph.D. degrees in control science and engineering from Zhejiang University, Hangzhou, China, in 2000 and 2005, respectively. He was a visiting researcher at University of Waterloo from 2008 to 2010. Currently, he is a Professor with the College of Control Science and Engineering, Zhejiang University. He serves/served Associate Editors for ACM Transactions on Embedded Computing Systems, IEEE Transactions on Parallel and Distributed Systems, IEEE Network, IEEE Transactions on Control of Network Systems, IEEE Transactions on Industrial Informatics, etc. He has been appointed as a distinguished lecturer of IEEE vehicular technology society 2015, and selected in National Program for Special Support of Top-Notch Young Professionals, and also funded Excellent Youth Foundation of National Natural Science Foundation of China. His research interests include the Internet of Things, sensor networks, networked control, and control system security.