PDDL: Proactive Distributed Detection and Localization Against Stealthy Deception Attacks in DC Microgrids

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

***Abstract*—With the rapid development of the information and communication technology in DC microgrids (DCmGs), the threat of deception attacks has been widely recognized. However, the stealthy deception attacks, which can hide the actual attack impact from the system operator as in the Stuxnet accident, have not yet been well studied. Towards this end, this paper proposes a proactive distributed detection and localization (PDDL) framework to defend against the stealthy deception attacks. The attack detection is achieved by observing the attack impact that is quantified as the voltage balancing deviation (VBD) and current sharing deviation (CSD) in DCmGs. Once any anomaly is perceived, the proactive perturbation on primary control gains (PCGs) will be activated to invalidate the previously inferred PCGs of the attacker, under which the constructed stealthy deception attacks may be located by the unknown input observer (UIO) based locators. To maximize the locatability of attacks while limiting the induced transient fluctuations on system states, an optimization problem is formulated to determine the PCG perturbation magnitude. Finally, the effectiveness of the PDDL framework is verified through extensive hardware-in-the-loop (HIL) based simulations and systematic full-hardware experimental studies.**

***Index Terms*—DC microgrid, proactive detection and localization, stealthy deception attack.**

I. Introduction

With the popularity of DC DERs and DC loads including the photovoltaic unit, battery unit, electrical vehicle, data center, etc. [1], [2], the DC microgrid (DCmG), which is an important branch of the microgrid, is expected to play a vital role in the future distribution system. To efficiently coordinate the DERs in microgrids to achieve the system-level tasks including voltage balancing and current sharing, the communication and computation capabilities are indispensable [3]. At the same time, the adoption of open standard communication protocols [4] and the support for numerous remote access points (such as dial-up, VPN, and wireless) [5] inevitably expose DCmGs to the threat of various cyber vulnerabilities.

The security accidents like the Stuxnet and BlackEnergy indicated that the attacker could intrude into the cyber network by exploiting zero-day vulnerabilities and tamper with commands to affect the power system. The Stuxnet accident was reported to ruin almost one-fifth Iran's nuclear centrifuges by causing them to spin out of control [6]. The BlackEnergy accident caused approximately 225,000 customers to lose power across various areas in Ukrainian for three hours [7]. Once the attacker intrudes into the cyber network of DCmGs, then she/he could easily deteriorate the control performance and even destabilize the voltages and currents [8].

Compared with the general distributed multi-agent system model [9], the DCmG has extra cyber-physical interconnections among DERs, with which the analysis of cyberattacks and the design of corresponding defensive strategies would be more challenging. Hence, considerable attention has been paid to the unique cybersecurity issue in DCmGs. Roughly speaking, the existing literature focuses on either the detection and localization of cyberattacks or the resilient control under cyberattacks [10], [11], both of which play an important role in defending against cyberattacks. Here, the detection and localization method aims to perceive and isolate the compromised components to mitigate the attack impact [12]. The cyberattacks can be generally classified into the denial-of-service (DoS) attack and deception attack [13], where the DoS attack blocks the data transmission in the communication link and the deception attack injects biases into the payloads of transmitted data packets. The deception attack, which can be further divided into the false data injection attack (FDIA) and replay attack, has stronger stealthiness than the DoS attack.

In this paper, we mainly focus on the detection and localization of the deception attacks in DCmGs and the relevant literature review is as follows. Considering the cybersecurity issue in the distributed load shedding procedure of microgrids, Yan *et al.* proposed an unknown input observer (UIO) based detector to perceive the FDIAs [14]. To improve the resilience of the distributed economic dispatch

Manuscript received 24 January 2022; revised 18 May 2022; accepted 27 June 2022. Date of publication 5 July 2022; date of current version 22 December 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 61833015, Grant 62073285, Grant 62061130220, Grant 61903328, and Grant 62103367; in part by the Zhejiang Provincial Natural Science Foundation under Grant LZ21F020006 and Grant LZ22F030010; in part by the Fundamental Research Funds for the Central Universities under Grant 226-2022-00120; and in part by the Key Laboratory of Collaborative Sensing and Autonomous Unmanned Systems of Zhejiang Province. Paper no. TSG-00110-2022. *(Corresponding author: Ruilong Deng.)*

The authors are with the State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China (e-mail: lmx329@zju.edu.cn; chengchengzhao@zju.edu.cn; jinhuixia@zju.edu.cn; dengruilong@zju.edu.cn; lunarheart@zju.edu.cn; cjm@zju.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2022.3188489.

Digital Object Identifier 10.1109/TSG.2022.3188489

in cyber-physical DCmGs, Cheng and Chow proposed a reputation-based distributed detection and localization method against non-colluding and colluding FDIAs [2]. Given the deception attacks faced by photovoltaic farms, Zhang *et al.* proposed a physics-data-based detection and localization method using the power electronics-enabled harmonic state space models [15]. To exclude the vulnerability of the distributed microgrid control framework to the hijacking attack, which is comparable to the replay attack as they both replace original data with new one, Sahoo *et al.* proposed a novel distributed screening methodology for attack detection [16]. Considering the threat of the concurrent attack that compromises the local and communicated data simultaneously, Zhang *et al.* proposed an energy-based detection method using the ensemble empirical model decomposition method [17]. For the awareness of deception attacks in the distributed voltage control architecture of DCmGs, Shi *et al.* proposed an analytical consistency-based anomaly detection scheme [18]. To address the vulnerability of a well-planned set of balanced FDIAs that do not violate the control objectives of DCmGs, Sahoo *et al.* proposed a cooperative vulnerability factor framework to locate the compromised DER [19]. To enhance the resilience of the distributed voltage and frequency control against FDIAs in microgrids, Mustafa *et al.* proposed a Kullback-Liebler divergence-based criterion for attack detection [20]. Yang *et al.* designed a novel non-invasive intrusion detection and localization system for the controllers of DCmGs, based on a set of control invariants [21], [22]. Zhao *et al.* designed a dynamical detection method with an updated threshold to detect and locate the FDIAs against variable-speed wind turbines [23]. Based on the aperiodically intermittent control strategy, Zhou *et al.* proposed a timely detection and localization scheme against the FDIAs in islanded microgrids [24]. By twining the UIOs and Luenberger observers, Gallo *et al.* proposed a distributed detection scheme against the deception attacks in DCmGs [25].

However, the above mentioned literature does not consider the possibility of the intelligent attacker, who can first obtain some knowledge of the system model (including system parameters, control gains, defensive strategy, etc.) and then carefully designs a stealthy attack strategy to achieve his/her malicious goals in an unperceived way. We consider two well-known stealthy deception attacks, i.e., the zero trace stealthy (ZTS) attack [26] and Stuxnet-like attack [27], [28]. The ZTS attack is designed by simulating the system dynamics of DCmGs when the attacker has full knowledge of the system model and detection scheme. The Stuxnet-like attack includes two parts. The first part affects the normal operations of DCmGs by tampering with the current measurement, and the second part replays the historical normal data to hide the bad status from the upper host. The idea of proactively perturbing the parameters of power lines has been widely adopted in defending against the stealthy FDIAs in power system state estimation [29], [30]. To defend the stealthy deception attacks in DCmGs, Liu *et al.* proposed a converter-based moving target defense (CMTD) strategy, where the primary control gains (PCGs) are proactively perturbed [12]. Nevertheless, the CMTD strategy has the following three limitations: 1) the PCG perturbation needs to be frequently activated, which may induce many useless fluctuations; 2) a systematic design method that determines the PCG perturbation magnitude is not provided; 3) the feasibility of CMTD on the full-hardware testbed is not validated.

In this paper, we propose a novel proactive distributed detection and localization (PDDL) framework against the stealthy deception attacks in DCmGs. The contributions of this paper are summarized as the following aspects:

- Two attack detection indicators, i.e., voltage balancing deviation (VBD) and current sharing deviation (CSD), are established for each DER to quantify the attack impact of stealthy deception attacks on the two control objectives in DCmGs. Specifically, the dynamic average consensus (DAC) observer is employed to estimate the average point of common coupling (PCC) voltage in a distributed manner, and the sliding time window (STW) technology is adopted to decrease the impact of daily operations on VBD and CSD.
- The PCGs are perturbed with the optimal magnitudes, which are determined by maximizing the locatability of attacks while limiting the induced transient fluctuations on PCC voltage and currents, to expose the compromised DERs to the UIO-based locators. Concretely, the locatability of attacks is quantified as the residual increments of UIOs under PCG perturbation and the induced transient fluctuations are quantified as the primary control input (PCI) variations caused by PCG perturbation.
- The attack detection and localization phases are integrated into a PDDL framework, where the PCG perturbation will be activated once any anomaly is detected. Moreover, the PDDL framework can be easily deployed in the upper host and requires no extra installation cost.
- Extensive hardware-in-the-loop (HIL) based simulations and systematic full-hardware experimental studies are conducted to validate the effectiveness of the proposed PDDL framework.

II. Cyber-Physical DCmG Model and Vulnerability Analysis

In this section, we illustrate the Cyber-Physical DCmG model and analyze the cyber vulnerability of DCmG.

A. Cyber-Physical DCmG Model

DCmGs are typical cyber-physical systems that contain a variety of interconnected devices that sense, control, and supervise DERs, loads, and power distribution devices [31]. The detailed structure of DCmG is shown in Fig. 1. The control layer includes controllers that receive inputs from sensors, process the inputted data through control algorithms, and send the output data to buck converters. The supervisory layer includes upper hosts that supervise the local statuses of DERs by observing the data from controllers [32]. Besides the local capabilities, the cyber networks among controllers and upper hosts enable their data transmission capabilities, which promote the achievement of global control and supervisory objectives. The corporate network, vendor personal, and site

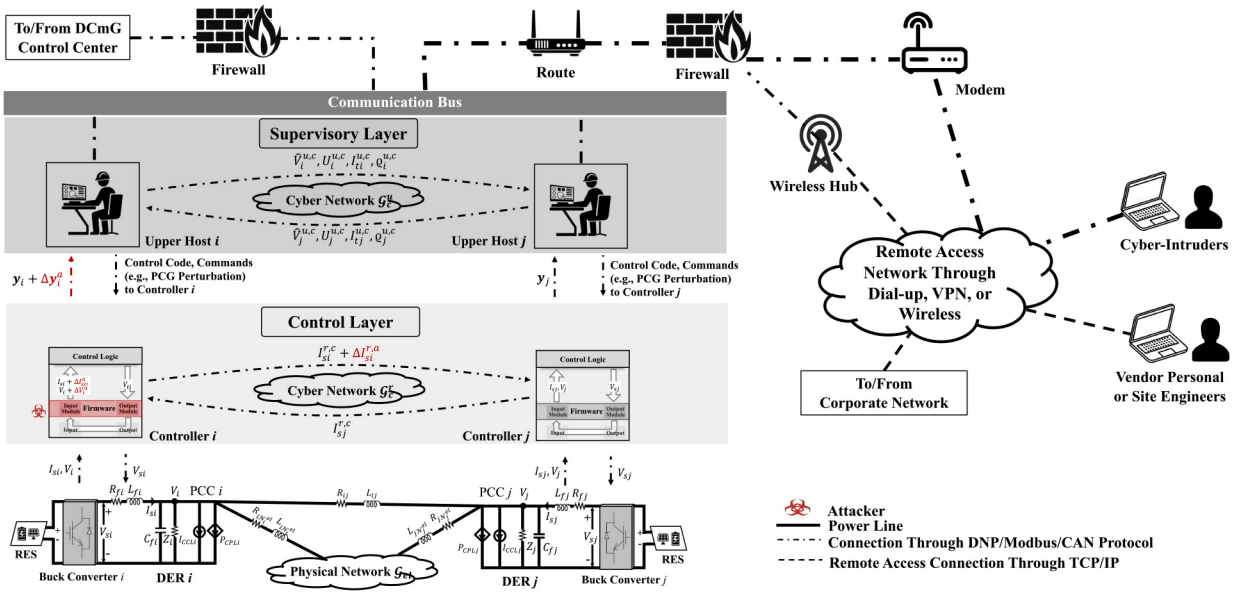


Fig. 1. This figure illustrates the structure of the cyber-physical DCmG.

engineer can get remote access to the DCmG through dial-up, VPN, or wireless connection [5].

This paper mainly considers the isolated DCmG that operates in the independent mode. DER i is composed of a DC voltage source (representing the renewable energy source, RES), a buck converter i, and a series RLC filter (described by resistance R_{fi},[1] inductance L_{fi}, and capacitance C_{fi}). DERs i and j are connected through a power line with non-zero impedance (R_{ij}, L_{ij}). Buck converter i regulates the source voltage V_{si}[2] to supply the ZIP load at PCC i through a RLC filter. The ZIP load includes the constant impedance load (Z_i), constant current load (I_{CCLi}), and constant power load (P_{CPLi}). Since the PCC voltage V_i is kept near the nominal reference value $V_{ref,i}$ [33], it is reasonable to linearize the constant power load as

$$I_{CPLi} = -\frac{P_{CPLi}}{V_{ref,i}^2} V_i + 2\frac{P_{CPLi}}{V_{ref,i}}, \tag{1}$$

where I_{CPLi} is the linearized current load for the constant power load. Then, the linearized ZIP load can be represented by impedance load Z_{Li} and current load I_{Li} [12]. After adopting the Kirchhoff voltage and current laws and the quasi-stationary line (QSL) approximation ($L_{ij} \approx 0$) [34], the physical dynamics of DER $i \in \mathscr{A}$ are obtained as

$$\begin{cases} \frac{dV_i(t)}{dt} = \frac{1}{C_{fi}} I_{si}(t) + \sum_{j\in\mathscr{N}_i^{el}} \frac{1}{C_{fi}R_{ij}}\big(V_j(t) - V_i(t)\big) + \\ \quad - \frac{1}{C_{fi}}\left(I_{Li} + \frac{V_i(t)}{Z_{Li}}\right) \\ \frac{dI_{si}(t)}{dt} = -\frac{1}{L_{fi}} V_i(t) - \frac{R_{fi}}{L_{fi}} I_{si}(t) + \frac{1}{L_{fi}} V_{si}(t), \end{cases} \tag{2}$$

where I_{si}^2 signifies the source current from RES and R_{ij} is the resistance of the power line connecting DERs i and j. Let $\boldsymbol{x}_i(t) = [V_i(t), I_{si}(t), v_i(t)]^{\mathrm{T}}$ be the state vector, where $v_i(t)$ is the integral of the PCC voltage tracking error, the following linear state-space (SS) dynamic equations are obtained:

$$\begin{cases} \dot{\boldsymbol{x}}_i(t) = A_{ii}\boldsymbol{x}_i(t) + \boldsymbol{b}_i u_i(t) + M_i \boldsymbol{d}_i(t) + \boldsymbol{\xi}_i(t) + \boldsymbol{\omega}_i(t), \\ \boldsymbol{y}_i(t) = \boldsymbol{x}_i(t) + \boldsymbol{\rho}_i(t), \end{cases} \tag{3}$$

where $\boldsymbol{y}_i(t)$ is the output vector, $\boldsymbol{d}_i(t) = [I_{Li}, V_{ref,i} + \alpha_i(t)]^{\mathrm{T}}$ denotes the exogenous input vector, and $u_i(t) = V_{si}(t)$ and $\alpha_i(t)$ signify the primary and secondary control inputs, respectively. Vectors $|\boldsymbol{\omega}_i(t)| \le \bar{\boldsymbol{\omega}}_i$ and $|\boldsymbol{\rho}_i(t)| \le \bar{\boldsymbol{\rho}}_i$ denote the bounded process and measurement noises, respectively. The term $\boldsymbol{\xi}_i(t) = \sum_{j\in\mathscr{N}_i^{el}} A_{ij}\boldsymbol{x}_j(t)$ accounts for the electrical couplings among DERs. The physical network among DERs is denoted by a weighted undirected graph (WUG) $\mathscr{G}_{el} = \{\mathscr{A}, \mathscr{E}_{el}\}$, where $\mathscr{A}$ is the set of DERs and $\mathscr{E}_{el}$ is the set of power lines connecting them. DERs i and j are neighbors if the power line satisfies $\{i, j\} \in \mathscr{E}_{el}$, and the set of neighbors of DER i in $\mathscr{G}_{el}$ is represented by $\mathscr{N}_i^{el}$. The weight of $\{i, j\}$ is $\frac{1}{R_{ij}}$. Moreover, the involved matrix parameters are

$$A_{ii} = \begin{bmatrix} -\frac{1}{Z_{Li}C_{fi}} - \sum_{j\in\mathscr{N}_i^{el}} \frac{1}{R_{ij}C_{fi}} & \frac{1}{C_{fi}} & 0 \\ -\frac{1}{L_{fi}} & -\frac{R_{fi}}{L_{fi}} & 0 \\ -1 & 0 & 0 \end{bmatrix},$$

$$M_i = \begin{bmatrix} -\frac{1}{C_{fi}} & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}, A_{ij} = \begin{bmatrix} \frac{1}{R_{ij}C_{fi}} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Under appropriate simplifications, the original complex and nonlinear dynamics of the DER can be described by the derived linear SS model (3), which effectively captures the local dynamics (responses to load variations) and the interactive dynamics (responses to plugging-in/out of DERs). Based on the linear SS model, the feasibility of many advanced applications like the plug-and-play robust control [35], self-sustained and flexible control [36], and distributed attack detection [25] can be easily investigated, providing theoretical guarantee for the deployment of these applications in future DCmGs. Besides, the linearity of the SS model makes

[1]The subscript f denotes the electrical elements of RLC filter.
[2]The subscript s denotes the source voltage/current from RES.

TABLE I
COMMON VULNERABILITIES OF THE CYBER-PHYSICAL DCMG

Application Software	Communication Network	Field Device
Improper input validation	Inadequate segregation and segmentation	Unprotected physical access
Poor code quality	Weak access control of wireless communication	Improper device configuration
Inadequate access control	Adoption of open standard protocols	Inadequate firmware protection
Insufficient verification of data authenticity	Weak encryption mechanism	Lack of tamper-resistance hardware
Poor patch management	Weak firewall rules	
Insufficiently protected credentials	Poor host-based intrusion detection	

it possible to apply mature linear control theory to the design of primary controllers and observer-based anomaly locators. Hence, the linear SS model (3) is adopted in this work.

The calculation of the PCI $u_i(t)$ is completed through a feedback controller, i.e.,

$$u_i(t) = V_{si}(t) = \boldsymbol{k}_i^{\mathrm{T}} \boldsymbol{y}_i(t) = \boldsymbol{k}_i^{\mathrm{T}} \boldsymbol{x}_i(t) + \boldsymbol{k}_i^{\mathrm{T}} \boldsymbol{\rho}_i(t), \tag{4}$$

where $\boldsymbol{k}_i = [k_{[i1]}, k_{[i2]}, k_{[i3]}]^{\mathrm{T}}$ is the PCG vector and should satisfy

$$\begin{cases} k_{[i1]} < 1 \\ k_{[i2]} < R_{fi} \\ 0 < k_{[i3]} < \frac{1}{L_{fi}} \big(k_{[i1]} - 1\big)\big(k_{[i2]} - R_{fi}\big) \end{cases} \tag{5}$$

to guarantee the voltage stability [33]. The secondary control input $\alpha_i(t)$ is calculated with the following consensus scheme

$$\dot{\alpha}_i(t) = k_I \sum_{j \in \mathscr{N}_i^{r,c}} a_{ij}^{r,c} \left(\frac{I_{sj}^{r,c}(t)}{I_{sj}^{rac}} - \frac{I_{si}(t)}{I_{si}^{rac}} \right), \tag{6}$$

where $I_{sj}^{r,c}(t)$ is the current measurement of DER j communicated to controller i, $I_{si}^{rac} > 0$ and $I_{sj}^{rac} > 0$ are rated currents of DERs i and j, respectively, and $k_I > 0$ is a parameter invariant among DERs. The communication network among controllers is denoted by a WUG $\mathscr{G}_c^r = \{\mathscr{A}, \mathscr{E}_c^r\}$, where set $\mathscr{E}_c^r$ collects all communication links and the weight of $\{i, j\} \in \mathscr{E}_c^r$ is $a_{ij}^{r,c}$.

According to [37], the two control objectives of the DCmG, i.e., voltage balancing and current sharing can be achieved if Assumption 1 is satisfied.

Definition 1 (Voltage Balancing): Voltage balancing is achieved if $\langle \mathrm{v}(\infty) \rangle = V_{op}$, where $\mathrm{v}(t) = [V_1(t), \ldots, V_N(t)]^{\mathrm{T}}$ and V_{op} is the operating point set by the tertiary control layer.

Definition 2 (Current Sharing): For the equivalent ZIP load, current sharing is achieved if $\frac{I_{si}(\infty)}{I_{si}^{rac}} = \frac{I_{sj}(\infty)}{I_{sj}^{rac}}, \forall i, j \in \mathscr{A}$.

Assumption 1: The average of nominal reference PCC voltages is equal to V_{op}, i.e., $\frac{1}{N} \sum_{i=1}^{N} V_{ref,i} = V_{op}$. The WUGs $\mathscr{G}_{el}$ and $\mathscr{G}_c^r$ are both connected, and they have the same topology and edge weights. The ZIP load verifies $P_{CPLi} < \frac{V_{ref,i}^2}{Z_i}$.

B. Cyber Vulnerability Analysis

Cyber vulnerabilities are flaws that may be exploited by the attacker to penetrate into and cause physical damage to the DCmG. Cyber vulnerabilities could exist across the cyber-physical DCmG, ranging from the application software, communication network, and field device. The common cyber vulnerabilities are summarized in Table I [38], [39].

1) Application Software Vulnerabilities: Improper input validation can make the content provided to an application software grant the attacker unexpected functionalities or privilege escalation. The attacker thus can achieve remote code execution, DoS, data manipulation, etc. Poor code quality refers to the code issues, such as the use of potentially dangerous functions and null pointer dereference. Inadequate access control can be exploited by the attacker to gain unauthorized access to application functionalities. Insufficient verification of data authenticity can make an application accept forged and malicious requests and code. Poor patch management makes the applications with old versions vulnerable to published and available exploit code. Insufficiently protected credentials like the clear-text passwords can be easily leaked to the attacker.

2) Communication Network Vulnerabilities: Inadequate segregation and segmentation between the internal network and corporate network allow the attacker to easily gain full control of DCmGs, which could cause high-level consequences. The vulnerability is becoming severe as the DCmG requires more and more ancillary information (e.g., weather forecasts, fuel price) from the external network to optimize the overall system performance. The widely adopted wireless communication options (e.g., ZigBee, Wi-Fi) in DCmGs largely expand the access points that could be exploited by the attacker [38]. The open standard protocols (e.g., Modbus, IEC 61850) have also been widely adopted to facilitate the interoperability among various vendor products [4]. The inherent vulnerabilities of these protocols can collectively result in huge cyber threats. The use of weak encryption algorithm can be easily cracked by the published attack. Weak firewall rules can allow unreliable data transmission between the internal network and external network, and make the remote code execution on upper hosts possible. The host-based intrusion detection relies heavily on the normal data transmitted from the controller, and can be easily invalidated once the controller is compromised.

3) Field Device Vulnerabilities: Unprotected physical access of numerous controllers and network devices included in the DCmG makes it possible for the attacker to inject malicious code into controllers and plug into the internal network. Improper device configuration can make the security mechanisms provided by vendors invalidated. Inadequate firmware protection can make the attacker manipulate the firmware through either remote network connection or local joint test action group (JTAG) connection [40]. Lack of tamper-resistance hardware makes field devices vulnerable to physical attacks (e.g., information leakage, unauthorized access) [41].

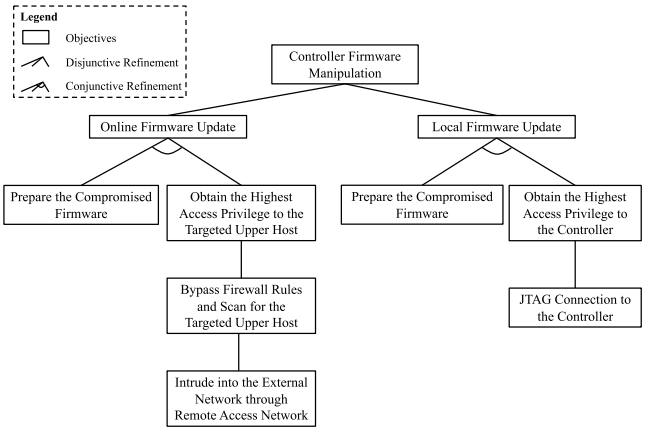


Fig. 2. This figure illustrates the attack tree against the vulnerability of controller firmware manipulation.

In the cyber-physical DCmG, the controllers play an important role in connecting the cyber part to the physical part. The controllers observe the operation statuses of DERs through sensors, calculate commands to buck converters based on appropriate control algorithms, and feed the status information back to upper hosts for anomaly supervision. Hence, the controllers are attackers' primary targets. As illustrated in Fig. 1, the controller includes two main software components, i.e., the control logic program and firmware. The control logic program reads input values from memory and stores the output values to memory. The underlying firmware is responsible for the interchange of these updated values to and from the controller's general purpose input/output (GPIO) ports [40]. The modern embedded devices like the programmable logic controller are commonly designed with a firmware update feature [42]. Once the controller's firmware is manipulated, the attacker can arbitrarily tamper with the output to affect the normal operations of DCmGs and appropriately forge the input to hide the bad status from the upper host. That is, the launched attack can constantly affect the DCmG without being immediately perceived.

Fig. 2 shows the attack tree against the vulnerability of controller firmware manipulation. Generally speaking, the attacker can manipulate the controller firmware through either online firmware update or local firmware update mechanism. To remotely replace the firmware with the compromised one, the attacker is required to follow the attack path: intrude into the external network→find the targeted upper host in the internal network→fully control the upper host→activate the online firmware update mechanism. To locally achieve the firmware manipulation, the attacker needs to get physical access to the controller and connect to the controller through JTAG interface. After obtaining full access privilege to the controller, the local firmware update mechanism can be activated. The compromised firmware is prepared through the reverse engineering process such that the cryptographic-based validation methods can be passed and the modified firmware can achieve attacker's malicious intentions [42], [43].

III. Existing Security Scheme and Problem Formulation

To perceive the physical damage that may be caused by the cyber vulnerabilities, the UIO-based locators have been widely deployed in upper hosts to monitor the data from the upper hosts. In particular, each UIO-based locator is merely responsible for the local controller, and any triggered attack alarm can locate the compromised controller. The following subsections are to introduce the UIO-based locator and problem formulation.

A. UIO-Based Locator

The UIO-based locator is to perceive the local abnormal activities through the observation, i.e., $\boldsymbol{y}_i(t)$, from the controller. After lumping the unknown exogenous input and electrical coupling vectors into one vector and substituting (4) into (3), one has

$$\begin{cases} \dot{\boldsymbol{x}}_i(t) = A_{ki}\boldsymbol{x}_i(t) + \bar{M}_i\bar{\boldsymbol{d}}_i(t) + \boldsymbol{\omega}_i(t) + \boldsymbol{b}_i\boldsymbol{k}_i^{\mathrm{T}}\boldsymbol{\rho}_i(t) \\ \boldsymbol{y}_i(t) = \boldsymbol{x}_i(t) + \boldsymbol{\rho}_i(t), \end{cases} \tag{7}$$

where $A_{ki} = A_{ii} + \boldsymbol{b}_i\boldsymbol{k}_i^{\mathrm{T}}$, $\bar{\boldsymbol{d}}_i(t)$ is the lumped unknown input vector, $\bar{M}_i\bar{\boldsymbol{d}}_i(t) = M_i\boldsymbol{d}_i(t) + \boldsymbol{\xi}_i(t)$, and $\bar{M}_i$ is chosen to have full column rank. The intuition of the anomaly perception is to check the consistency between $\boldsymbol{y}_i(t)$ and the underlying system dynamics. To address the unknown inputs, the following full order UIO is adopted [44], i.e.,

$$\mathrm{UIO}_i \begin{cases} \dot{\boldsymbol{z}}_i(t) = F_i\boldsymbol{z}_i(t) + \hat{K}_i\boldsymbol{y}_i(t) \\ \hat{\boldsymbol{x}}_i(t) = \boldsymbol{z}_i(t) + H_i\boldsymbol{y}_i(t), \end{cases} \tag{8}$$

where $\hat{\boldsymbol{x}}_i(t)$ is the estimated system state vector and $\boldsymbol{z}_i(t) \in \mathbb{R}^3$ is the internal state vector. The UIO parameters $F_i, \hat{K}_i, H_i \in \mathbb{R}^{3\times 3}$ should satisfy

$$T_i\bar{M}_i = \not{0}^{3\times 2}, \tag{9a}$$
$$T_i = \mathrm{I}^3 - H_i, \tag{9b}$$
$$\hat{K}_i = K_{i1} + K_{i2}, \tag{9c}$$
$$F_i = T_iA_{ki} - K_{i1}, \tag{9d}$$
$$K_{i2} = F_iH_i, \tag{9e}$$

where K_{i1} should be appropriately chosen to make the eigenvalues of F_i all lie within the open left half-plane utilizing (9d). Given (7) and (8), the analytical expression of the residual vector $\boldsymbol{r}_i(t)$ is obtained as

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

where $\boldsymbol{\sigma}_{2i}(0) = \boldsymbol{x}_i(0) - \hat{\boldsymbol{x}}_i(0) + H_i\boldsymbol{\rho}_i(0)$ and $\boldsymbol{\sigma}_{3i}(t) = \int_0^t e^{-F_i\tau}(T_i\boldsymbol{\omega}_i(\tau) + (T_i\boldsymbol{b}_i\boldsymbol{k}_i^{\mathrm{T}} - \hat{K}_i)\boldsymbol{\rho}_i^d(\tau))d\tau$. As matrix F_i is Hurwitz stable, there exist positive scalars κ and μ such that $\|e^{F_it}\| \le \kappa e^{-\mu t}, \forall t \ge 0$, with which one obtains that

$$|\boldsymbol{r}_i(t)| \le \bar{\boldsymbol{r}}_i(t) = \kappa e^{-\mu t}(\bar{\boldsymbol{\sigma}}_{2i}(0) + \bar{\boldsymbol{\sigma}}_{3i}(t)) + |T_i|\bar{\boldsymbol{\rho}}_i \tag{10}$$

always hold in the absence of attacks, where $|\boldsymbol{\sigma}_{2i}(0)| \le \bar{\boldsymbol{\sigma}}_{2i}(0) = (\mathrm{I}^3 + |H_i|)\bar{\boldsymbol{\rho}}_i$ and $|\boldsymbol{\sigma}_{3i}(t)| \le \bar{\boldsymbol{\sigma}}_{3i}(t) = \int_0^t |e^{-F_i\tau}|(|T_i|\bar{\boldsymbol{\omega}}_i + |T_i\boldsymbol{b}_i\boldsymbol{k}_i^{\mathrm{T}} - \hat{K}_i|\bar{\boldsymbol{\rho}}_i)$. Once (10) is violated, it is considered that the integrity of $\boldsymbol{y}_i(t)$ is corrupted and controller i is considered as compromised.

B. Problem Formulation

The UIO-based locator can largely resist the naive attacker that arbitrarily designs the bias vector, but merely has limited performance when facing the intelligent attacker that launches the stealthy deception attacks [12]. In this work, we aim to propose a novel PDDL framework against the stealthy deception attacks that can be easily integrated into the original supervisory layers.

The controller firmware manipulation means that the attacker can tamper with the control command $V_{si}(t)$, local measurements $I_{si}(t), V_i(t)$, current measurement to the neighboring controllers $I_{si}^{r,c}(t)$, and output vector to the upper host $\boldsymbol{y}_i(t)$. Given the closed-loop primary controller (4), the modification on $V_{si}(t)$ will not affect the steady-state PCC voltage once the tampered $V_{si}(t)$ can be reached by buck converter i. Hence, this paper considers the worst case where the attacker may tamper with the following four variables

$$I_{si}(t) \to I_{si}(t) + \Delta I_{si}^{a}(t), V_i(t) \to V_i(t) + \Delta V_i^{a}(t), \quad (11)$$

$$I_{si}^{r,c}(t) \to I_{si}^{r,c}(t) + \Delta I_{si}^{r,a}(t), \boldsymbol{y}_i(t) \to \boldsymbol{y}_i(t) + \Delta \boldsymbol{y}_i^{a}(t), \quad (12)$$

where $\Delta I_{si}^{a}(t), \Delta V_i^{a}(t), \Delta I_{si}^{r,a}(t)$, and $\Delta \boldsymbol{y}_i^{a}(t)$ denote the injected biases designed by the attacker. The following knowledge is required to design the bias vectors: 1) the converter electrical parameters R_{si}, L_{si}, C_{si}; 2) the resistances of the power lines connected to neighboring DERs R_{ij}; 3) the equivalent impedance load Z_{Li}; 4) the PCG vector $\boldsymbol{k}_i$.

Remark 1: The first two knowledge is about the electrical parameters and is almost time-invariant, and thus can be obtained from the insider [45]. The third knowledge is related to the ZIP load and is forecast based on historical load profiles [46]. The last knowledge $\boldsymbol{k}_i$ is designed by the system operator and can vary once the controller is reloaded. Hence, $\boldsymbol{k}_i$ is estimated on-line based on (4) after collecting three sets of linear independent output vectors $\boldsymbol{y}_i(t)$. We note that the estimation of $\boldsymbol{k}_i$ cannot be completed immediately as the collection of data should at least wait for the occurrence of a daily operation in the DCmG such as the load switch.

Based on the above capabilities, the ZTS attack and Stuxnet-like attack can be designed.

1) ZTS Attack [26]: ($\Delta I_{si}^{a}(t) = 0, \Delta V_i^{a}(t) = 0, \Delta I_{si}^{r,a}(t) \neq 0, \Delta \boldsymbol{y}_i^{a}(t) \neq \nVdash^3$) In this case, the attacker merely manipulates the output vector to upper host i and the current measurement to neighboring controllers. In particular, $\Delta \boldsymbol{y}_i^{a}(t)$ and $\Delta I_{si}^{r,a}(t), t \geq T_a$ are constructed as

$$\begin{cases} \Delta \dot{\boldsymbol{y}}_i^{a}(t) = A_{ki} \Delta \boldsymbol{y}_i^{a}(t) + \bar{M}_i \bar{\boldsymbol{d}}_i^{a}(t), \Delta \boldsymbol{y}_i^{a}(T_a) = \nVdash^3 \\ \Delta I_{si}^{r,a}(t) = [0, 1, 0] * \Delta \boldsymbol{y}_i^{a}(t). \end{cases} \quad (13)$$

which mimics the dynamics of DER (7) to deceive the UIO-based locator. Here, T_a denotes the activation time of the attack, and $\bar{\boldsymbol{d}}_i^{a}(t)$ signifies the faked unknown input vector by the attacker.

2) Stuxnet-Like Attack [27], [28]: ($\Delta I_{si}^{a}(t) \neq 0, \Delta V_i^{a}(t) \neq 0, \Delta I_{si}^{r,a}(t) \neq 0, \Delta \boldsymbol{y}_i^{a}(t) \neq \nVdash^3$) In this case, the attacker simultaneously manipulates the local measurements $I_{si}(t), V_i(t)$, the communicated one $I_{si}^{r,c}$, and the communicated output vector $\boldsymbol{y}_i(t)$. As the preparation step, the attacker will record the normal output vector $\boldsymbol{y}_i(t)$ for $t \in [T_s, T_s + T_{re}]$, where T_s and T_{re} are the start time and length of the record period. When manipulating the local measurements, the historically recorded normal output vector is replayed to upper host i to conceal the attack impact resulted from the corrupted local measurements. That is,

$$\begin{cases} \Delta \boldsymbol{y}_i^{a}(t) = \boldsymbol{y}_i(t - \psi_{re}) - \boldsymbol{y}_i(t), t \geq T_a \\ \Delta V_i^{a}(t) = [1, 0, 0] * \Delta \boldsymbol{y}_i^{a}(t) \\ \Delta I_{si}^{a}(t) = \Delta I_{si}^{r,a}(t) = [0, 1, 0] * \Delta \boldsymbol{y}_i^{a}(t), \end{cases} \quad (14)$$

where ψ_{re} denotes the time shift caused by the replay attack.

Both the ZTS attack [26] and Stuxnet-like attack [27], [28], which are two well-known stealthy deception attacks, can bypass the UIO-based locator as either the carefully faked measurements or the replayed normal measurements conform the dynamics of DER (7). To defend against the stealthy deception attacks, the following problems are formulated: 1) How to design the detection indicators for each DER to perceive the anomalies caused by the stealthy deception attacks? 2) How to proactively locate the compromised controllers with limited transient fluctuations emerging on voltages and currents? 3) How to integrate the detection and localization functionalities such that they can be easily deployed in upper hosts?

IV. Attack Detection Phase

In this section, two detection indicators are designed to quantify the present system states' deviations from voltage balancing and current sharing. Different from the previous sections, we adopt the discrete-time forms to demonstrate the derivations of the two indicators, which can be directly used in the digital signal based upper host, as the discrete-time and continuous-time forms of the involved DAC estimator are totally different. In particular, the variable with superscript $(\cdot)^d$ is used to signify its discrete-time form such as $V_i^d(n) = V_i(nT_{sam})$, where T_{sam} is the sampling period.

A. VBD and CSD

1) VBD: According to Definition 1, the VBD can be quantified as the deviation of the average PCC voltage (APV) $\overline{V}^d(n) = \sum_{i=1}^{N} V_i^d(n)$ from the operating point V_{op}. Since upper host $i \in \mathscr{A}$ merely knows the PCC voltages of partial DERs, the APV cannot be directly calculated and the second-order DAC observer is required to estimate the APV. According to [47], the dynamics of the DAC observer follow

$$\begin{cases} \widehat{V}_i^d(n+1) = \widehat{V}_i^d(n) + \sum_{j \in \mathscr{N}_i^{u,c}} a_{ij}^{u,c} \left(\widehat{V}_j^{du,c}(n) - \widehat{V}_i^d(n) \right) + U_i^d(n+1) \\ U_i^d(n+1) = U_i^d(n) + \sum_{j \in \mathscr{N}_i^{u,c}} a_{ij}^{u,c} \left(U_j^{du,c}(n) - U_i^d(n) \right) + \Delta V_i^{d(2)}(n), \end{cases}$$

where $\widehat{V}_i^d(n)$ is the estimated APV, $U_i^d(n)$ is the internal state, $\Delta V_i^{d(2)}(n) = \Delta V_i^{d(1)}(n) - \Delta V_i^{d(1)}(n-1)$ and $\Delta V_i^{d(1)}(n) = V_i^d(n) - V_i^d(n-1)$ are the second-order and first-order differences of $V_i^d(n)$, respectively, and $\widehat{V}_j^{du,c}(n), U_j^{du,c}(n)$ are the information received from upper host j. Here, the communication network among upper hosts is denoted by a WUG $\mathscr{G}_c^u = \{\mathscr{A}, \mathscr{E}_c^u\}$, where set $\mathscr{E}_c^u$ collects all communication links and the weight of $\{i, j\}$ is $a_{ij}^{u,c}$. The set of neighbors of upper host i is denoted by $\mathscr{N}_i^{u,c}$. The following Assumption are made for $\mathscr{G}_c^u$ and $\Delta V_i^{d(2)}(n)$.

Assumption 2: The WUG $\mathcal{G}_c^u$ is connected and the weights satisfy $a_{ii}^{u,c} = 1 - \sum_{j\in\mathcal{N}_i^{u,c}} a_{ij}^{u,c} \geq \alpha$, $a_{ij}^{u,c} \in \{0\} \cup [\alpha, 1]$, where $\alpha > 0$ is a constant. Moreover, $\Delta V_i^{d(2)}(n)$ is relatively bounded and we have $\max_{n\geq 0} \Delta V_i^{d(2)}(n) - \min_{n\geq 0} \Delta V_i^{d(2)}(n) \leq \theta T_{sam}$, where $\theta > 0$ is a constant.

The convergence of $\widehat{V}_i^d(n)$ to $\overline{V}^d(n)$ is guaranteed via the following result.

Lemma 1 [47, Th. 4.1.]: Let δ be a positive constant and $h = \frac{\delta\alpha^{N(N+1)+2}}{32\theta(N-1)^2}$.[3] When Assumption 2 and $T_{\text{sam}} \in (0, h]$ are both satisfied, the DAC observer can finally achieve $|\overline{V}^d(n) - \widehat{V}_i^d(n)| \leq \delta$ for $n \to \infty$ with the initial states $\widehat{V}_i^d(0) = V_i^d(0)$ and $U_i^d(0) = \Delta V_i^{d(1)}(0)$.

We note that the assumption for $\Delta V_i^{(2)}(n)$ is reasonable as the APV will either be constant or grow like a ramp signal when single or multiple communication links are compromised, respectively [26]. Moreover, from the expression of h, it can be inferred that the steady-state APV deviation (APVD), defined as

$$\widehat{V}_i^{d,err}(\infty) = V_{op} - \widehat{V}_i^d(\infty), \tag{15}$$

can be infinitely small if T_{sam} is small enough. Nevertheless, $\widehat{V}_i^{d,err}(n)$ cannot be directly utilized for the anomaly detection as the daily operations in DCmGs such as the load switches and plugging-in/out of DERs will also result in non-trivial transient values of $\widehat{V}_i^{d,err}(n)$. Fortunately, under the daily operations, we observe that the APVD will finally converge to zero while the ZTS or replay attacks can induce non-zero steady-state APVD [26]. To reduce the false alarms resulted from daily operations, based on the STW technology, the detection indicator for VBD is derived as

$$\mathscr{D}_i^V(n) = \frac{1}{L_{stw}^v} \sum_{l=n-L_{stw}^v-1}^{n} \left|\widehat{V}_i^{d,err}(l)\right|, n \geq L_{stw}^v, \tag{16}$$

where $L_{stw}^v \in \mathbb{Z}$ is the length of the STW.

2) CSD: According to Definition 2, the CSD can be quantified as

$$I_{si}^{d,err}(n) = \sum_{j\in\mathcal{N}_i^{u,c}} \left|I_{sj}^{du,c}(n) - I_{si}^d(n)\right|, \tag{17}$$

where $I_{sj}^{du,c}(n)$ is the current measurement communicated from upper host j and $I_{si}^d(n)$ denotes the current measurement received from controller i. Similar to the derivation of the detection indicator for VBD, the detection indicator for CSD is calculated as

$$\mathscr{D}_i^I(n) = \frac{1}{L_{stw}^i} \sum_{l=n-L_{stw}^i-1}^{n} |I_{si}^{d,err}(l)|, n \geq L_{stw}^i, \tag{18}$$

where $L_{stw}^i \in \mathbb{Z}$ is the length of the STW.

Remark 2: The STW lengths L_{stw}^v, L_{stw}^i should be appropriately chosen to satisfy the two conditions: 1) To avoid unacceptable detection delay and computation burden, the STW length cannot be too large; 2) To make the responses of daily operations distinguishable from those of attacks, the STW length cannot be too small. The larger STW length can better reduce the number of false alarms resulted from daily operations.

B. Setting of Detection Thresholds

In this subsection, we investigate the setting of the detection thresholds for $\mathscr{D}_i^V(n)$ and $\mathscr{D}_i^I(n)$ $(n \geq 0)$, which are denoted by $\bar{\mathscr{D}}_i^V$ and $\bar{\mathscr{D}}_i^I$, respectively. In particular, the thresholds are set to tolerate the set of the most frequent daily operations $\mathscr{O}(n) = \{_1(n), \ldots, _{|\mathscr{O}(n)|}(n)\}$, where $_1(n)$ denotes the occurrence of a daily operation at time n. Hence, we have

$$\bar{\mathscr{D}}_i^V = \max_{n\geq L_{stw}^v, l(0)\in\mathscr{O}(0)} \mathscr{D}_{i|_l(0)}^V(n), \tag{19}$$

$$\bar{\mathscr{D}}_i^I = \max_{n\geq L_{stw}^i, l(0)\in\mathscr{O}(0)} \mathscr{D}_{i|_l(0)}^I(n), \tag{20}$$

where $\mathscr{D}_{i|_l(0)}^V(n)$ and $\mathscr{D}_{i|_l(0)}^V(n)$ denote the responses of VBD and CSD to daily operation $_l(0)$, respectively.[4] Under any single daily operation $_l(n) \in \mathscr{O}(n), \forall n \geq 0$, the detection indicators satisfy

$$\mathscr{D}_i^V(n) \leq \bar{\mathscr{D}}_i^V, \mathscr{D}_i^I(n) \leq \bar{\mathscr{D}}_i^I. \tag{21}$$

Once any condition in (21) is violated, it is considered that there exist anomalies in the DCmG and the enabled warning signal $\varrho_i^{u,c} = 1$ is transmitted to the neighboring upper hosts.

Remark 3: Since the compromised controller can only fake the information communicated to the local upper host and neighboring controllers, it is difficult for the attacker to anticipate and eliminate the VBDs and CSDs seen from all upper hosts. Considering the practical situation that the attacker does not have enough resources to compromise all controllers, the derived detection indicators can effectively reflect the adverse impact caused by the attacker. The false alarm and missed alarm are two metrics regarding the accuracy of the detection method, which are closely related to the detection thresholds. The larger detection thresholds can tolerate the larger fluctuations caused by daily operations, implying the fewer false alarms caused by them. But the larger detection thresholds will result in more missed alarms, i.e., only the stealthy deception attacks with large enough attack vectors could be detected. The smaller detection thresholds have the opposite results. Hence, the detection thresholds should be appropriately chosen to minimize the number of missed alarms while guaranteeing the small number of false alarms. The proposed detection scheme can work in DCmGs with large scales if only the APV can be successfully estimated (i.e., the WUG $\mathcal{G}_c^u$ satisfies Assumption 2.).

V. Attack Localization Phase

In this section, we introduce the localization of the stealthy deception attacks based on PCG perturbation. Once $\varrho_i = 1$ or $\varrho_j^{u,c} = 1, \forall j \in \mathcal{N}_i^{u,c}$, upper host i will determine the PCG perturbation magnitude, after which the perturbed PCG vector is coded and sent to controller i. The low-cost coding scheme is adopted to multiply the perturbed PCG vector by a coding matrix such that it can be hidden from the attacker when

[3]The value of B in [47] is set to 1 as $\mathcal{G}_c^u$ is always connected.

[4]The response data can be obtained from the historical or simulated data.

the attacker does not know the exact coding matrix [48]. The coding matrix is integrated into the control code, and thus controller i can obtain the original perturbed PCG vector from the coded one. Moreover, according to Remark 1, the attacker needs to collect some information that is different from the current steady state to complete the estimation of $\boldsymbol{k}_i$, and thus it is reasonable to have the following Assumption.

Assumption 3: The attacker cannot construe the coded command as the PCG perturbation, and cannot estimate the perturbed PCG vector immediately.

Hence, the attacker will not adjust the attack strategy immediately when the PCG perturbation occurs, under which the stealthy deception attacks based on the antiquated PCG vector are likely to be located by the updated UIO-based locator. In the following subsections, we will first introduce two metrics that quantify the locatability of attacks and the induced transient fluctuations on system states under PCG perturbation, and then design the optimal perturbation magnitude to balance the trade-off between them.

A. Locatability of Attacks

The locatability of attacks is quantified as the residual increment under PCG perturbation. Let $\boldsymbol{k}_i^p$ be the PCG vector after perturbation, with which the UIO parameters in (8) are updated. Then, according to our previous work [12], the residual increments under the two stealthy deception attacks (13) and (14) are calculated as follows.

Lemma 2: Given Assumption 3, when the attack vector $\Delta \boldsymbol{y}_i^a(t)$ is constructed as (13), the residual increment $\forall t \geq T_a$ is

$$\Delta \boldsymbol{r}_i^{att1}(t) = \int_{T_a}^{t} e^{F_i^p(t-\tau)} T_i^p \left(A_{ki} - A_{ki}^p\right) \Delta \boldsymbol{y}_i^a(\tau) d\tau. \quad (22)$$

When the attack vector $\Delta \boldsymbol{y}_i^a(t)$ is constructed as (14), the residual increment $\forall t \in [T_a, T_a + T_{re}]$ is

$$\Delta \boldsymbol{r}_i^{att2}(t) = \int_{T_a}^{t} e^{F_i^p(t-\tau)} T_i^p \left(A_{ki} - A_{ki}^p\right) \boldsymbol{x}_i(\tau - \psi_{re}) d\tau + \\ + \boldsymbol{f}\left(\boldsymbol{\epsilon}_i^p(T_a), \boldsymbol{\epsilon}_i(T_a), \boldsymbol{\omega}_i(t), \boldsymbol{\rho}_i(t)\right), \quad (23)$$

where $\boldsymbol{\epsilon}_i^p(t) = \boldsymbol{x}_i(t - \psi_{re}) - \hat{\boldsymbol{x}}_i^p(t)$ and $\boldsymbol{\epsilon}_i(t) = \boldsymbol{x}_i(t - \psi_{re}) - \hat{\boldsymbol{x}}_i(t)$ denote the state estimation errors with and without PCG perturbation, respectively, and function vector $\boldsymbol{f}(\cdot)$ denotes the neglectable impact caused by the initial state estimation errors and system noises.

B. Perturbation Magnitude Optimization

Although the ranges on PCGs (5) can guarantee the asymptotic voltage stability in DCmGs, some useless transient fluctuations on system states will inevitably emerge. We use the PFI variation after PCG perturbation to quantify the transient fluctuations of system states, and intuitively the smaller PFI variation means the smaller transient fluctuation. Since the steady states after PCG perturbation can be attained within several seconds, the ZIP loads during the short period can be assumed invariant. This implies that the steady-state PCC voltages, source currents, and PCIs before and after PCG perturbation are the same. Let V_{si}^{sb} and V_{si}^{sa} be the steady-state PCIs before and after PCG perturbation, respectively, $\boldsymbol{k}_i^p = [k_{[i1]}^p, k_{[i2]}^p, k_{[i3]}^p]^{\mathrm{T}}$, and V_i^s and I_{si}^s be the invariant steady-state PCC voltage and source current, respectively. Then, we have

$$V_{si}^{sb} = V_{si}^{sa} \quad (24)$$

$$\Downarrow$$

$$k_{[i1]} V_i^s + k_{[i2]} I_{si}^s + k_{[i3]} v_i^{sb} = k_{[i1]}^p V_i^s + k_{[i2]}^p I_{si}^s + k_{[i3]}^p v_i^{sa} \quad (25)$$

where v_i^{sb} and v_i^{sa} signify the steady-state integrals of the PCC voltage tracking errors before and after PCG perturbation, respectively. The intuition for the decrease of PCI variation is to make the PCI after PCG perturbation approach V_{si}^{sa} as much as possible, under which we have

$$\left(k_{[i1]} - k_{[i1]}^p\right) V_i^s + \left(k_{[i2]} - k_{[i2]}^p\right) I_{si}^s = 0, \quad (26)$$

$$k_{[i3]} - k_{[i3]}^p = 0. \quad (27)$$

Intuitively, if (26) and (27) are satisfied, (25) can hold at the time when the PCG perturbation occurs, under which the PCI variation is minimized. However, there exists a nontrivial trade-off between the maximization of the attack locatability and the minimization of the PCI variation. By substituting (26) and (27) into (25), we have $v_i^{sb} = v_i^{sa}$, which implies that the steady-state output vector is not altered by the PCG perturbation. When the attacker simply replays the steady-state output vector before the PCG perturbation, the updated UIO-based locator after the PCG perturbation would still be insensitive to the replayed output vector as it is indistinguishable from the actual output vector.

Therefore, to maximize the locatability of the stealthy deception attacks and limit the transient fluctuations on PCC voltages and currents simultaneously, the realization degree of (27) is appropriately relaxed as it merely affects the integral of the PCC voltage tracking error. The optimization problem is formulated as

$$\min_{\boldsymbol{k}_i^p} \ -P_i^{att} + \omega_i P_i^{tsi} \quad (28)$$

$$\text{s.t.} \ \left(k_{[i3]} - k_{[i3]}^p\right)^2 \leq \zeta_i, \quad (29)$$

$$\begin{cases} \underline{k}_{[i1]} \leq k_{[i1]} < 1 \\ \underline{k}_{[i2]} \leq k_{[i2]} < R_{fi} \\ 0 < k_{[i3]} < \frac{1}{L_{fi}} \left(k_{[i1]} - 1\right)\left(k_{[i2]} - R_{fi}\right), \end{cases} \quad (30)$$

where P_i^{att} measures the residual increments $\|\Delta \boldsymbol{r}_i^{att1}\|_2$, $\|\Delta \boldsymbol{r}_i^{att2}\|_2$ and satisfies

$$P_i^{att} = \frac{\left\| T_i^p \left(A_{ki} - A_{ki}^p\right) \Delta \boldsymbol{y}_i^{sv} \right\|_2}{\left\| \Delta \boldsymbol{y}_i^{sv} \right\|_2} + \frac{\left\| T_i^p \left(A_{ki} - A_{ki}^p\right) \boldsymbol{x}_i^{sb} \right\|_2}{\left\| \boldsymbol{x}_i^{sb} \right\|_2}, \quad (31)$$

P_i^{tsi} measures the extent to which (26) is achieved, i.e.,

$$P_i^{tsi} = \left[\left(k_{[i1]} - k_{[i1]}^p\right) V_i^s + \left(k_{[i2]} - k_{[i2]}^p\right) I_{si}^s \right]^2, \quad (32)$$

and $\omega_i > 0$ denotes the parameter weight that balances the locatability of attacks and the induced transient fluctuations on voltages and currents. We note that in P_i^{att} the steady-state

self-constructed attack vector $\Delta \boldsymbol{y}_i^{sv}$ and steady-state state vector before PCG perturbation $\boldsymbol{x}_i^{sb} = [V_i^s, I_{si}^s, v_i^{sb}]^{\mathrm{T}}$ are used as alternatives for $\Delta \boldsymbol{y}_i^a(\infty)$ and $\boldsymbol{x}_i(t - \psi_{re})$, respectively, which are actually inaccessible to the system operator. In particular, $\Delta \boldsymbol{y}_i^{sv}$ is constructed from (13) with a predetermined constant unknown input vector $\boldsymbol{d}_i^v$, where the larger absolute value of element means that it is much more vulnerable to the attacker. Moreover, inequality constraint (29) requires that the realization degree of (27) should be larger than $\zeta_i > 0$, and inequality constraints (30) describe a subspace of the space defined by (5), which guarantees the asymptotic voltage stability after PCG perturbation. Here, $\underline{k}_{[i1]}$ and $\underline{k}_{[i2]}$ are properly chosen by the system operator to make the local optimum bounded.

Since the optimization problem (28) with conditions (29)-(30) is non-convex, finding the global minimum is time-consuming. In this study, we use the standard *fmincon* solver from MATLAB equipped with the interior-point algorithm to obtain the local minimum, and the initial point is chosen as the original PCG vector.

Remark 4: The idea of achieving attack localization by proactively perturbing the control gains could be applicable to microgrids that adopt different primary control strategies like droop methods [49], [50]. But many efforts are still required before completing the application. Two primary issues are listed: 1) Due to the changes of the system model and control strategy, the new perturbation manner that does not destroy the system stability should be investigated. 2) When new localization technologies different from UIO-based locators are deployed, then the enhancement of the localization capability under perturbation should also be analyzed. Besides perturbing control gains, there exist many other similar methods that can achieve attack localization like adding probe signals to control commands [51] and injecting watermarking signals into measurements [28]. The choose of the attack localization method should be determined considering both the system model and the control strategy and the detailed investigation is left for our future work.

VI. PDDL Framework

As shown in Fig. 3, the PDDL framework combines the attack detection and localization functionalities. The localization phase will only be activated once any anomaly is detected, which can largely reduce the transient fluctuations caused by periodical PCG perturbation [12]. The PDDL framework can be easily integrated into the upper hosts, without introducing any extra device or requiring any modification on the communication architecture. Considering the possibility of the intelligent attacker, who merely causes small deviations on the control objectives, the induced VBD and CSD may not exceed the detection thresholds. To address the issue, the detection indicators are also compared with half of the detection thresholds. Once

$$\mathscr{D}_i^V(n) > \frac{\bar{\mathscr{D}}_i^V}{2} \text{ or } \mathscr{D}_i^I(n) > \frac{\bar{\mathscr{D}}_i^I}{2} \tag{33}$$

is successively satisfied for N^d sampling points, the localization phase will be activated to locate the intelligent attacker.

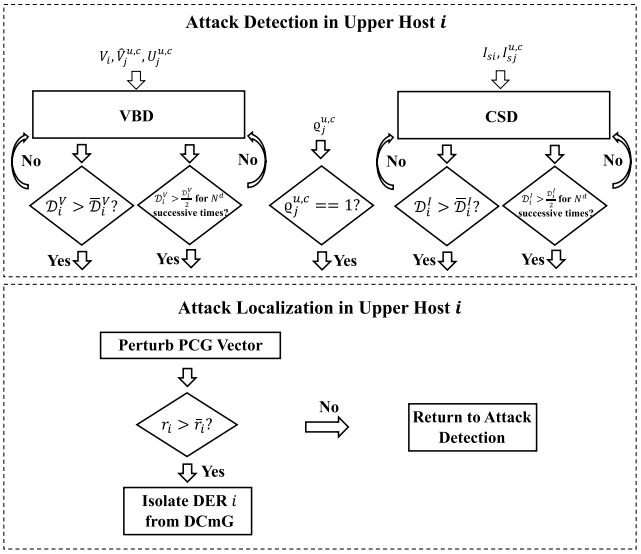


Fig. 3. The overview of the PDDL framework in upper host i.

Actually, there would always be some undetectable attacks and the above mentioned strategy is to limit the impact that the undetectable attacks can cause.

The implementation details of PDDL framework are demonstrated in Algorithm 1. After updating the information from the neighboring upper hosts $\forall j \in \mathcal{N}_i^{u,c}$ and controller i, upper host i first checks the warning signal $\varrho_j^{u,c}$. If $\varrho_j^{u,c}$ from any neighboring upper host is enabled, then the localization phase will be activated. Otherwise, the two detection indicators $\mathscr{D}_i^V$, $\mathscr{D}_i^I$ are calculated. The counting variable N^n is updated when (33) holds. If (21) is violated or N^n is equal to N^d, then the localization phase will be activated and the warning signals $\varrho_i^{u,c}$, ϱ_i will be enabled. Once the localization phase is activated, upper host i will determine $\boldsymbol{k}_i^p$ by solving (28)-(30). The coded PCG perturbation $\Theta_i \boldsymbol{k}_i^p$ is transmitted to controller i, after which the UIO parameters in (8) are updated. Here, $\Theta_i \in \mathbb{R}^{3\times 3}$ is the invertible coding matrix. If (10) is violated, then controller i is considered to be compromised and DER i will be isolated.

A. Commercial Security Solutions

Based on the IEC 62351 standard of security recommendations [4], there already exist some commercial security solutions like DNP3 security authentication (DNP3-SA) [52], DNPSec [53], IEC/TS 60870-5-7 [54], and IEC 61850-90-5 [55], [56] that address the cyber security issues in power systems. The DNP3 protocol is especially tailored for the applications in power-related SCADA systems, and two well-known ones to secure DNP3 are DNP3-SA and DNPSec [57]. DNP3-SA provides authentication and message integrity checking capabilities based on challenge-response Hash-based message authentication code (HMAC) and SHA-2 hashing. DNPSec employs triple data encryption standard (3-DES) and HMAC SHA-1 to provide authentication, protection of message confidentiality and integrity capabilities. IEC/TS 60870-5-7 are security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351-5 standard) that are used for telecontrol applications. Similar to DNP3-SA,

Algorithm 1 PDDL Framework in Upper Host $i \in \mathscr{A}$

Input: The information from the neighboring upper hosts $\forall j \in \mathscr{N}_i^{u,c}$, i.e., $\hat{V}_j^{u,c}(t), U_j^{u,c}(t), I_{tj}^{u,c}(t), \varrho_j^{u,c}$, the information from controller i, i.e., $\boldsymbol{y}_i(t)$, the coding matrix $\Theta_i \in \mathbb{R}^{3\times 3}$, and the counting variable $N^n = 0$.

Output: Detection Phase

if $\varrho_j^{u,c} == 1$ **then**
  Goto the Localization Phase;
end if
Calculate the detection indicators $\mathscr{D}_i^V$ and $\mathscr{D}_i^I$;
if (33) is satisfied **then**
  $N^n = N^n + 1$;
else
  $N^n = 0$;
end if
if (21) is violated or N^n is equal to N^d **then**
  Set $\varrho_i = 1$ and $\varrho_i^{u,c} = 1$;
  Goto the Localization Phase;
else
  Return to step 4;
end if

Output: Localization Phase

  Determine $\boldsymbol{k}_i^p$ by solving (28)-(30);
  Send the coded PCG perturbation $\Theta_i \boldsymbol{k}_i^p$ to controller i;
  Update the UIO parameters in (8);
  if (10) is violated **then**
    Isolate DER i from the DCmG;
  else
    Return to step 4;
  end if

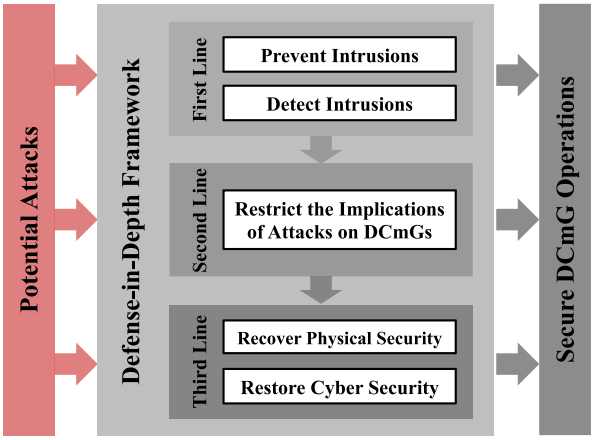


Fig. 4. The defense-in-depth security framework.

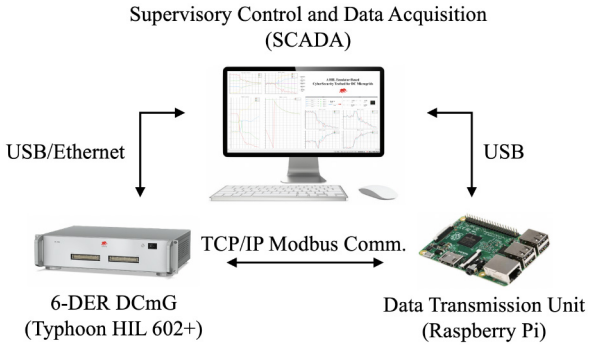


Fig. 5. The overview of the HIL testbed.

IEC/TS 60870-5-7 uses challenge-response HMAC mechanism to achieve the capabilities of authentication and message integrity checking. IEC 61850-90-5 uses a security mechanism based on group domain of interpretation (GDOI) to guarantee the confidentially and integrity of messages. In particular, the confidentiality is achieved by implementing the concept of perfect-forward security and encryption key rotation between publishers and subscribers. The message integrity is protected via digital signatures with asymmetric cryptography.

However, there are still some flaws against these security protocols. The availability of messages is not protected against DoS attacks. For DNP3-SA and IEC/TS 60870-5-7 protocols, the confidentiality of messages (except the key update message) is not guaranteed [58]. By using formal modeling and analysis methods, Amoah *et al.* revealed a previously unidentified flaw in the DNP3-SA protocol [59]. The attacker can replay a previously authenticated command to an outstation with arbitrary parameters. Indeed, it is difficult to thoroughly eliminate the cyber vulnerabilities of DCmGs relying merely on the security technologies from the information technology (IT) domain [60]. For instance, the standard perimeter-hardening techniques such as firewalls cannot prevent the exploitations of zero-day vulnerabilities.

B. Defense-in-Depth Security Framework

Considering the cyber-physical feature of DCmGs, additional security methods dedicated for DCmGs should be designed and implemented by twining the efforts from both IT and power domains. Toward this end, Li *et al.* proposed a defense-in-depth security framework, which includes three lines of defense as shown in Fig. 4 [60]. The first line of defense aims at preventing and detecting cyber intrusions to protect DCmGs from being maliciously affected. The second line of defense is to restrict the implications of attacks on DCmGs once the intrusion into the cyber system is successful. The third line of defense is to restore cyber security while recovering physical functionalities, if DCmGs are inevitably affected by attacks. The mentioned commercial secure protocols, which provide authentication, confidentiality protection, and integrity checking capabilities by adopting the security methods from the IT domain, belong to the first line of defense. Once the attacker has successfully intruded into the cyber system, the proposed PDDL framework, which belongs to the second line of defense, aims at isolating the compromised controllers from DCmGs to restrict the attack implications by twining the cyber and physical features of DCmGs. Hence, the combination of the commercial security solutions and PDDL framework has great importance in deeply improving the cyber

TABLE II
DIFFERENCES BETWEEN THE COMMERCIAL SECURITY SOLUTIONS AND PDDL FRAMEWORK

Security Methods	First Line of Defense				Second Line of Defense
	Authentication	Confidentiality	Integrity	Availability	Restriction of Attack Implications
DNP3-SA	Yes	No*	Yes	No	No
DNP3Sec	Yes	Yes	Yes	No	No
IEC/TS 60870-5-7	Yes	No*	Yes	No	No
IEC 61850-90-5	No	Yes	Yes	No	No
PDDL	No	No	No	No	**Yes**

* Yes for key update messages

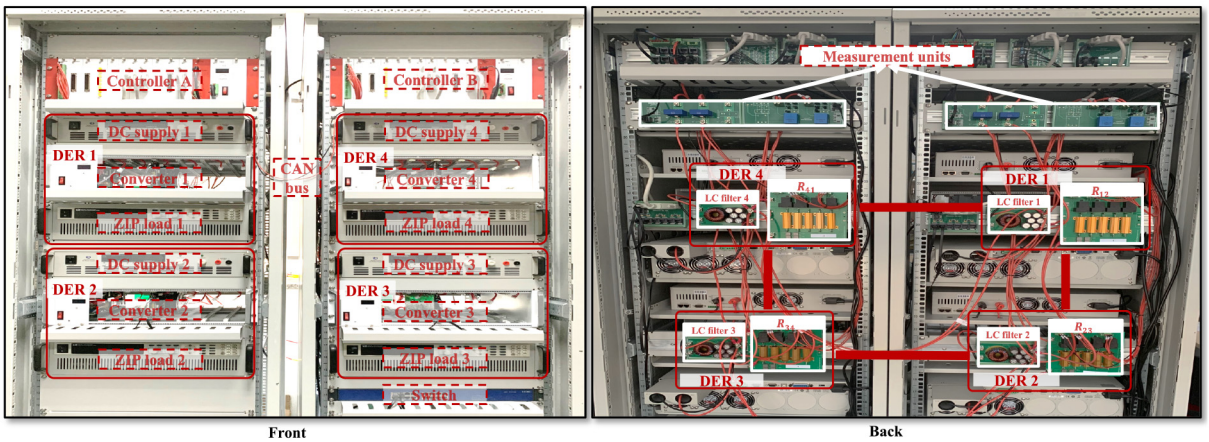


Fig. 6. This figure shows the overview of the full-hardware testbed, which includes the front and back views. The testbed contains 4 DERs and each DER comprises the DC supply, buck converter, and ZIP load. Moreover, controller A regulates the output voltages of converters 1 and 2, and the other converters are regulated by controller B. The data interaction between controllers is accomplished through the CAN bus, and the upper host gets access to the controllers through the switch.

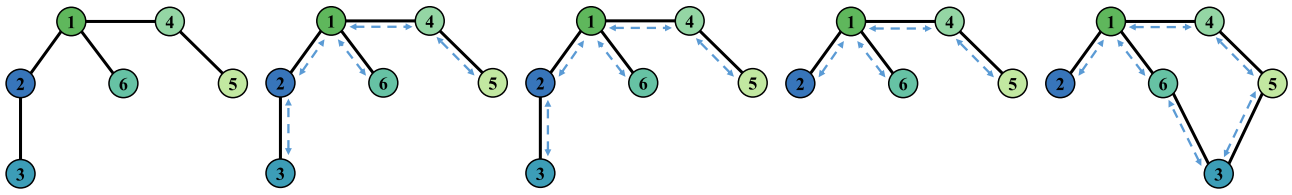


Fig. 7. This figure shows the evolution of DCmG under daily operations.

security of DCmGs. Table II lists the differences between the commercial security solutions and PDDL framework.

VII. SIMULATION AND EXPERIMENTAL RESULTS

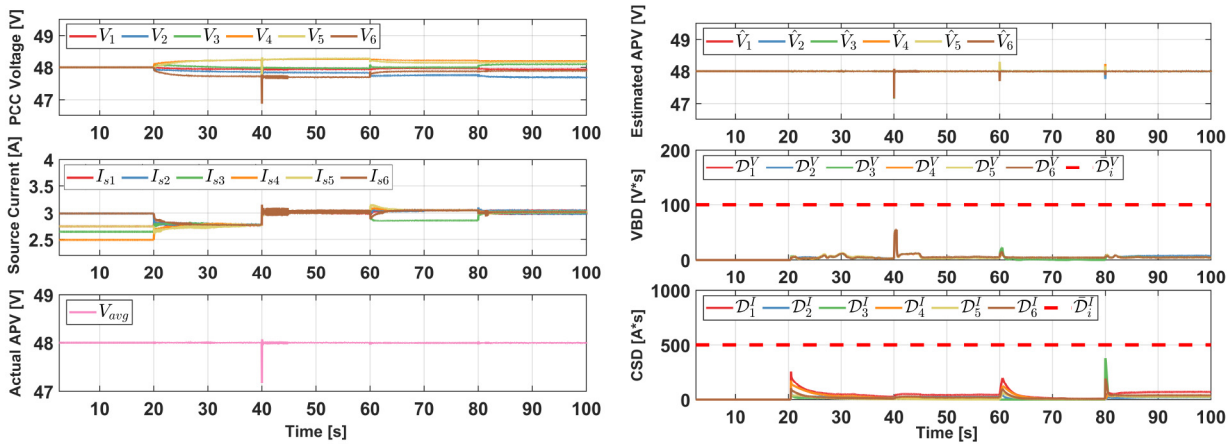
In this section, we demonstrate the setting of detection thresholds and validate the effectiveness of the PDDL framework through HIL-based simulations and full-hardware experimental studies. Furthermore, the computation time of solving the optimization problem (28)-(30) tested and comparative studies are conducted. To implement the UIO-based locator in the discrete-time signal based upper host, the continuous-time form (8) is transformed to the following discrete-time form

$$\text{UIO}_i^d \begin{cases} z_i^d(n+1) = F_i^d z_i^d(n) + \hat{K}_i^d y_i^d(n) \\ \hat{x}_i^d(n) = z_i^d(n) + H_i^d y_i^d(n), \end{cases} \tag{34}$$

where $F_i^d, \hat{K}_i^d, H_i^d$ are the discrete-time UIO parameters. The discrete-time system matrices are set to $A_{ki}^d = e^{A_{ki}T_{sam}}$, $\bar{M}_i^d = (A_{ki})^{-1}(A_{ki}^d - \mathrm{I}^3)\bar{M}_i$ and $T_{sam} = 1/2000$.

A. Setting of Detection Thresholds

In this subsection, we demonstrate the setting of detection thresholds $\bar{\mathscr{D}}_i^V$ and $\bar{\mathscr{D}}_i^I$ through HIL-based simulations. In the HIL testbed, we establish the 6-DER DCmG with a typical radial topology and widely used electrical parameters as listed in Table III. We collect the responses of the VBD and CSD indicators to three representative daily operations, i.e., the load switch, plugging-out and plugging-in of DERs. Concretely, the adopted actions that promote the DCmG evolution are summarized as follows: at $t = 0$s, the physical couplings among DERs are established and the primary controllers are activated; at $t = 20$s, the communication network $\mathscr{G}_c^r$ among real-time controllers is established; at $t = 40$s, the current loads $I_{Li}, \forall i \in \mathscr{A}$



(a) System states (b) Detection indicators

Fig. 8. This figure shows the variations of system states (including PCC voltages, source currents, and the actual APV) and detection indicators (including the estimated APV, VBD, and CSD) under the DCmG evolution.

TABLE III
ELECTRICAL SETUP OF DER i AND LINE PARAMETERS IN THE HIL TESTBED

Parameter	Symbol	Value
Output capacitance	C_{fi}	1.8mF
Inductance	L_{fi}	2.2mH
Inductor + switch loss resistance	R_{fi}	0.2Ω
Switching frequency	f_{sw}	10kHz
Power line resistance	R_{ij}	1Ω

are increased by 10%; at $t = 60$s, DER 3 is plugged out from the DCmG; at $t = 80$s, DER 3 is plugged into the DCmG. For clarity, a graphical illustration of the DCmG evolution is provided in Fig. 7.

The simulation results are shown in Fig. 8. It is revealed that the setup of communication network $\mathscr{G}_c^r$ and the occurrence of the three daily operations will both cause non-trivial fluctuations on the VBD and CSD indicators. To better differentiate the impact caused by daily operations from that by attacks, the length of time windows L_{stw}^v and L_{stw}^i is set as 1000. Under this setting, the fluctuations caused by daily operations can be totally tolerated by detection thresholds

$$\bar{\mathscr{D}}_i^V = 100, \bar{\mathscr{D}}_i^I = 500, \forall i \in \mathscr{A}.$$

B. Effectiveness Validation on HIL Testbed

In this subsection, we validate the effectiveness of the PDDL framework against the two stealthy deception attacks defined in the attack model through HIL-based simulations. The overview of the HIL testbed is shown in Fig. 5. Specifically, the SCADA center runs a dedicated software for the Typhoon HIL 602+ emulator, which is specialized in the ultra-low-latency, ultra-high-fidelity, real-time emulation of power electronics enabled microgrids [61], 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. The 6-DER DCmG with a radial network topology [62] and widely used electrical parameters as listed in the supplementary material is established in the HIL testbed. DER 3 is assumed to be compromised for demonstration. Given that the original PCGs are $\boldsymbol{k}_i = [0.85, 0.01, 2]^{\mathrm{T}}, \forall i \in \mathscr{A}$, the lower bounds $\underline{k}_{[i1]}$ and $\underline{k}_{[i2]}$ are set as 0.5 and -0.5, respectively, to make the optimum bounded. The parameters involved in optimization problem (28)-(30) are chosen as $\omega_i = 10000$ and $\zeta_i = 1$. The optimal perturbed PCGs are designed as $\boldsymbol{k}_i^p = [0.8795, -0.5, 1]^{\mathrm{T}}, \forall i \in \mathscr{A}$ based on the system states at $t = 40.49$s, and the ignorable fluctuations caused by the PCG perturbation are reflected in Fig. 13.

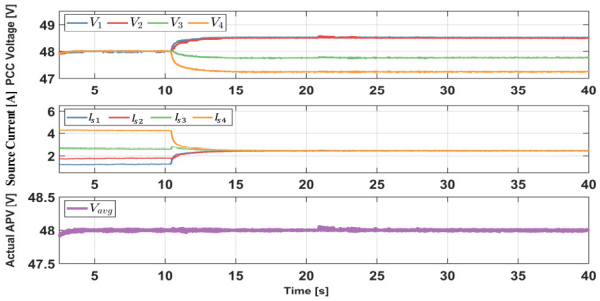


Fig. 9. This figure shows the transient fluctuations caused by the PCG perturbation at $t = 20.85$s in the full-hardware testbed, where the optimal perturbed PCGs are designed as $\boldsymbol{k}_i^p = [0.2259, -0.5, 1]^{\mathrm{T}}, \forall i \in \mathscr{A}$.

TABLE IV
ELECTRICAL SETUP OF DER i AND LINE PARAMETERS IN THE FULL-PHYSICAL TESTBED

Parameter	Symbol	Value
Output capacitance	C_{fi}	0.492mF
Inductance	L_{fi}	0.5mH
Inductor + switch loss resistance	R_{fi}	0.05Ω
Switching frequency	f_{sw}	10kHz
Power line resistance	R_{ij}	1Ω

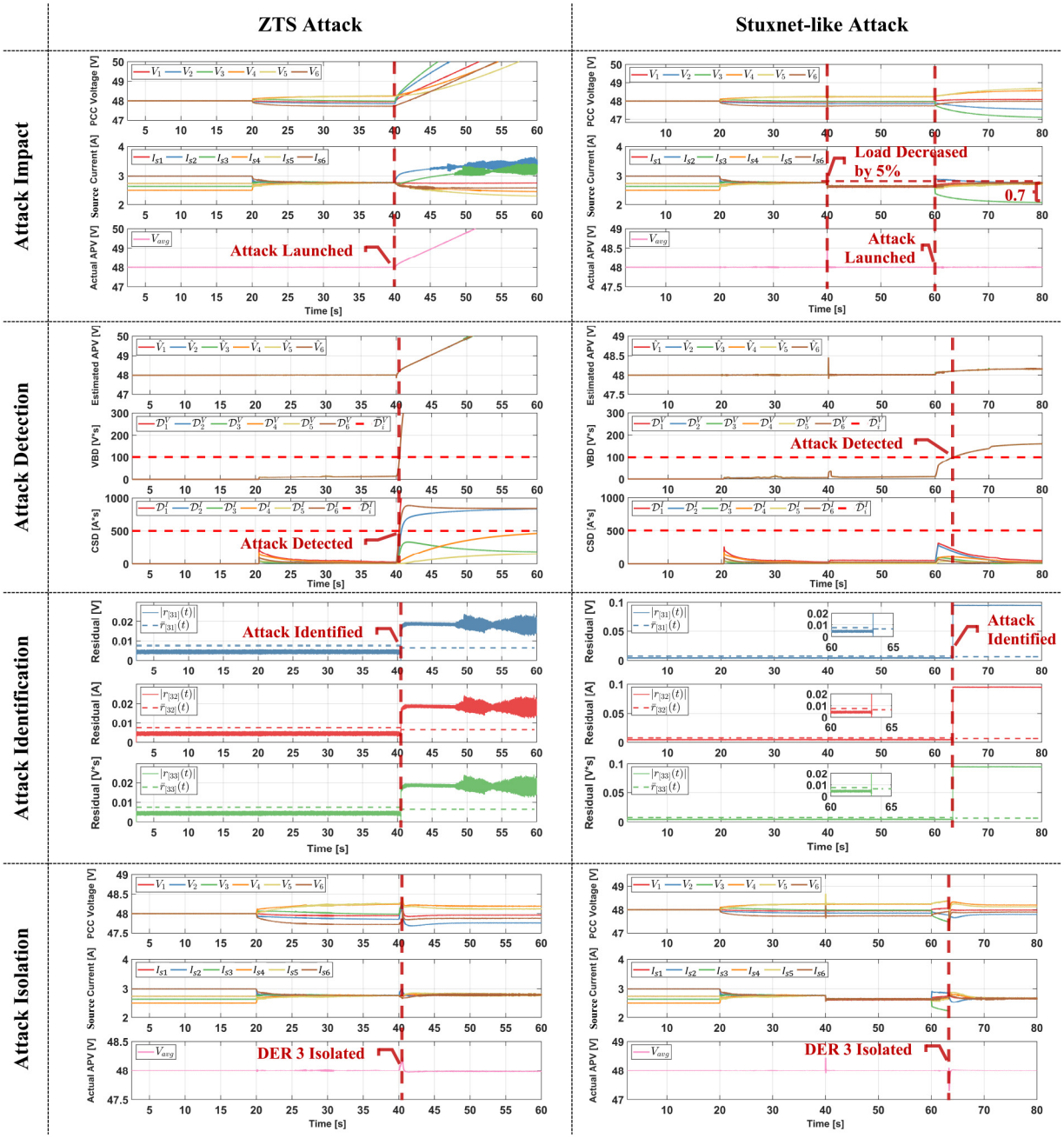


Fig. 10. This figure shows the HIL-based simulation results that validate the effectiveness of the PDDL framework against the ZTS attack and Stuxnet-like attack. The figures in the first row depict the attack impact caused by attacks. The figures in the second row depict the VBD and CSD that perceive the existence of attacks. The figures in the third row depict the residuals that locate the compromised DER 3. The figures in the fourth row depict the elimination of attack impact after isolating DER 3.

1) Effectiveness Against the ZTS Attack: In this case, the attacker designs the injected bias vector based on (13), where the fake unknown input vector is $\bar{\boldsymbol{d}}_3^a = [0.5, 0.5]^{\mathrm{T}}$ and $T_a = 40$s. The biases are injected into the measurements transmitted to upper host 3 and neighboring controller 2. As shown in (1, 1) and (2, 1) of Fig. 10, voltage balancing and current sharing are violated and the proposed VBD and CSD indicators immediately exceed the predetermined thresholds. The attack is first detected by DER 1 at $t = 40.49$s, after which the optimal perturbed PCGs are designed as $\boldsymbol{k}_i^p = [0.8795, -0.5, 1]^{\mathrm{T}}, \forall i \in \mathscr{A}$. According to (3, 1) of Fig. 10, the residual vector $\boldsymbol{r}_3(t)$ increases significantly and the attack is located in DER 3 at almost the time when the PCG perturbation occurs. After DER 3 is isolated from the DCmG, voltage balancing and current sharing are reestablished among the remaining DERs as illustrated in (4, 1) of Fig. 10.

2) Effectiveness Against the Stuxnet-Like Attack: In this case, the attacker injects constant biases $\Delta I_{s3}^a = 0.7$A and $\Delta I_{s3}^{r,a} = 0.7$A into the local current measurement $I_{s3}(t)$ and the communicated one $I_{s3}^{r,c}(t)$, respectively, at $T_a = 60$s. At the same time, the recorded data at $t \in [25, 35]$s is replayed to upper host 3 to cover the attack impact. We note that

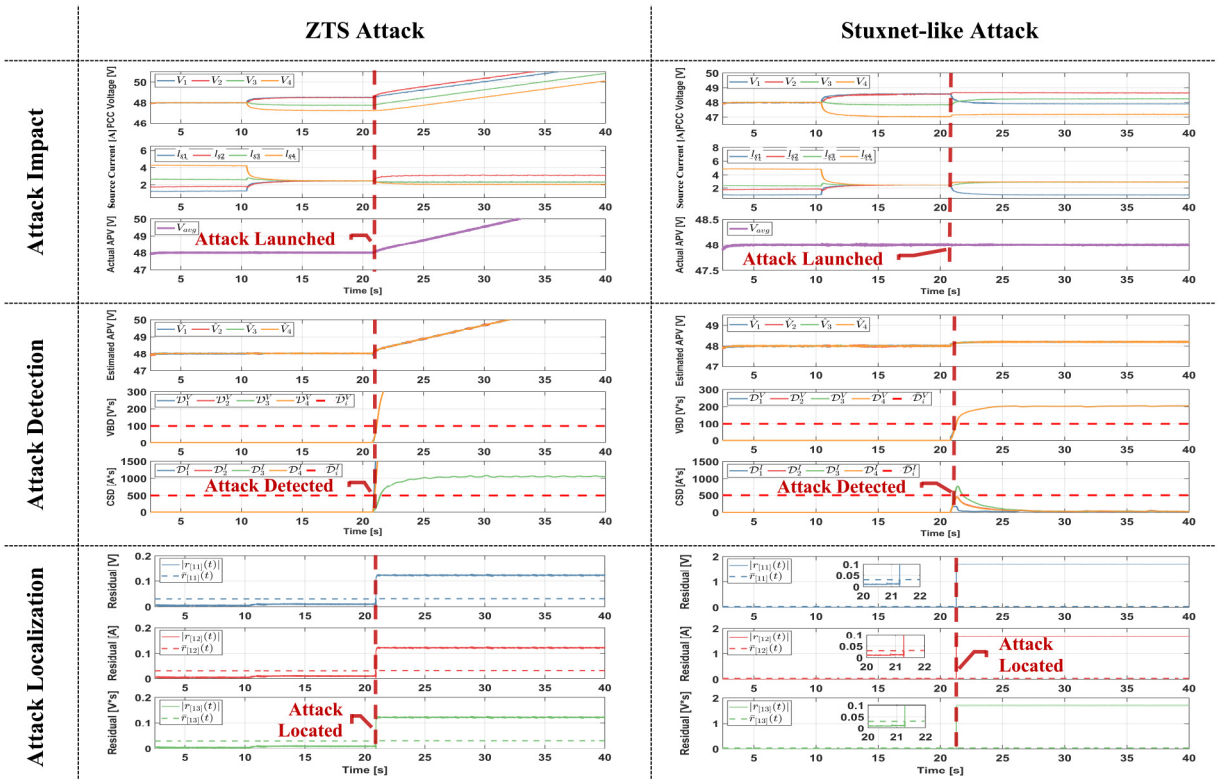


Fig. 11. This figure shows the full-hardware experimental results that validate the effectiveness of the PDDL framework against the ZTS attack and Stuxnet-like attack. The figures in the first row depict the attack impact caused by attacks. The figures in the second row depict the VBD and CSD that perceive the existence of attacks. The figures in the third row depict the residuals that locate the malicious DER 1.

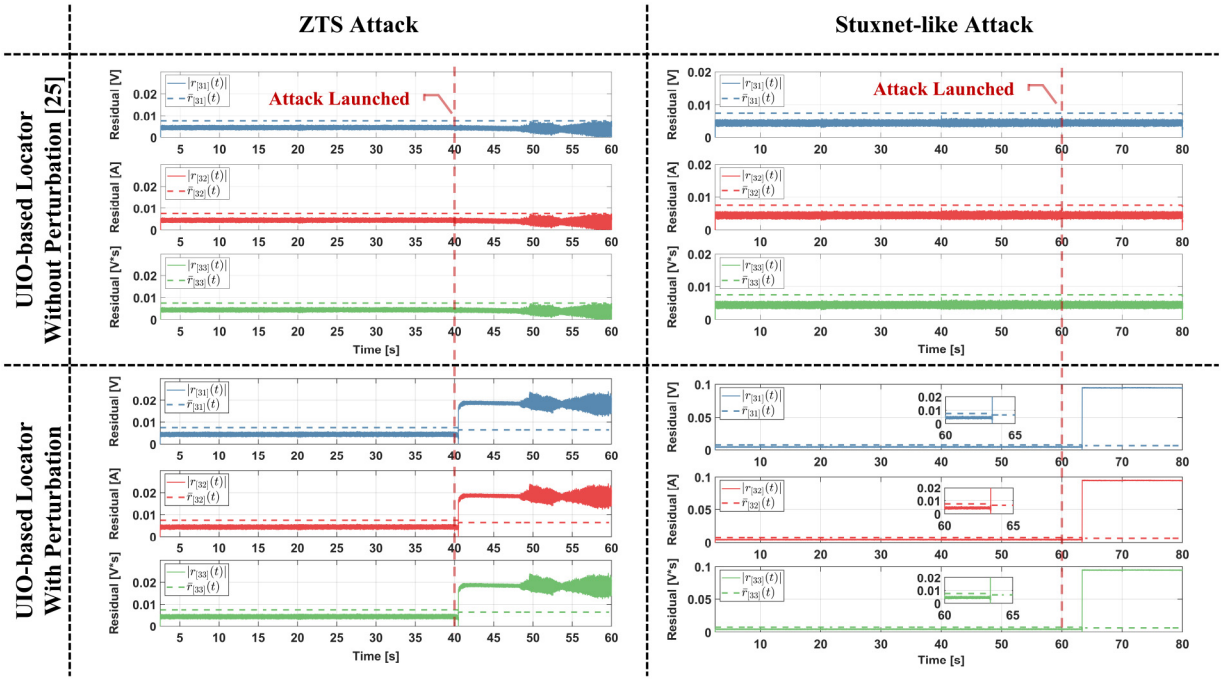
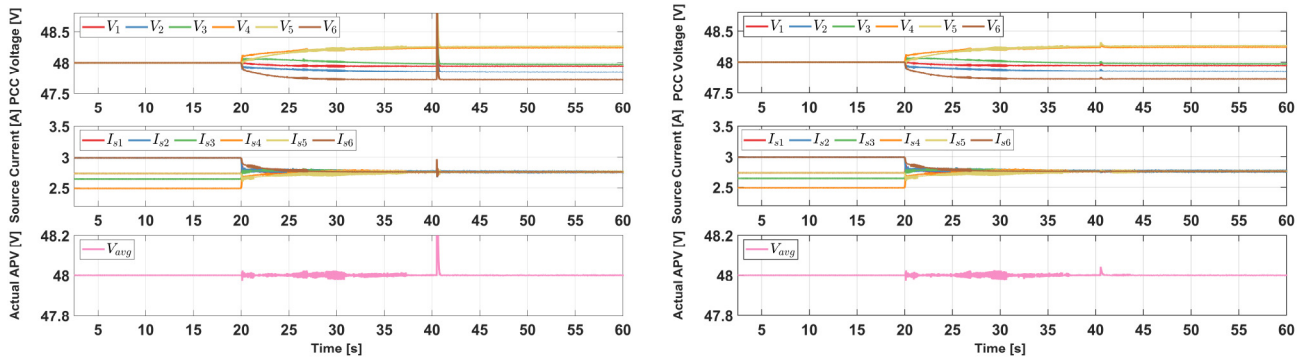


Fig. 12. This figure compares the defensive capability of the UIO-based locator [25] against the stealthy deception attacks with that of the proposed UIO-based locator with PCG perturbation.

the compromised current measurement to the neighboring controllers is consistent with the current component in the replayed output vector to upper host 3 as indicated by (2, 2) of Fig. 10. Moreover, the results in (1, 2) of Fig. 10 indicate that the compromised DER 3 can deceive other DERs to undertake more loads for it and voltage balancing can still be achieved. Nevertheless, from the point view of upper host 3, voltage balancing is violated as the replayed voltage component is



(a) Empirically chosen PCG perturbation [12]

(b) PCG perturbation by solving problem (28)-(30).

Fig. 13. This figure compares the fluctuations of the empirically chosen PCG perturbation [12] with those of the carefully designed PCG perturbation by solving problem (28)-(30).

unequal to the actual PCC voltage. The attack is detected by the VBD indicator at $t = 63.35$s, after which the optimal perturbed PCGs are designed as $\boldsymbol{k}_i^p = [0.877, -0.5, 1]^{\mathrm{T}}, \forall i \in \mathscr{A}$. According to $(3, 2)$ and $(4, 2)$ of Fig. 10, the compromised DER 3 can be successfully located by the UIO-based locator and the control objectives will recover after isolating DER 3.

C. Effectiveness Validation on Full-Hardware Testbed

In this subsection, we validate the effectiveness of the PDDL framework against the two stealthy deception attacks through full-hardware experimental studies. The overview of the full-hardware testbed is shown in Fig. 6, where the 4-DER with a ring topology is established and the electrical parameters are shown in Table IV. DER 1 is considered to be compromised for demonstration. Considering that the original PCGs are $\boldsymbol{k}_i = [0.2, 0, 2]^{\mathrm{T}}, \forall i \in \mathscr{A}$, the lower bounds $\underline{\boldsymbol{k}}_{[i1]}$ and $\underline{\boldsymbol{k}}_{[i2]}$ are set as 0.2 and -0.5, respectively. The parameters involved in (28)-(30) are chosen as $\omega_i = 10000$ and $\zeta_i = 1$. According to Fig. 9, where the optimal perturbed PCGs are designed as $\boldsymbol{k}_i^p = [0.2259, -0.5, 1]^{\mathrm{T}}, \forall i \in \mathscr{A}$ based on the system states at $t = 20.85$s, the induced transient fluctuations on PCC voltages and currents are trivial.

1) Effectiveness Against the ZTS-Attack: In this case, the attack vector is designed according to (13) with $\tilde{\boldsymbol{d}}_1^a = [1, 1]^{\mathrm{T}}$ and $T_a = 20.85$s. The attack vector is injected into the measurements transmitted to upper host 1 and neighboring controller 2 simultaneously. The results shown in the first column of Fig. 11 are similar to those resulted from the HIL testbed, implying that the proposed PDDL framework can effectively defend against attack strategy I in the full-hardware testbed. We note that after the attack is detected, the designed optimal perturbed PCGs are $\boldsymbol{k}_i^p = [0.2259, -0.5, 1]^{\mathrm{T}}, \forall i \in \mathscr{A}$.

2) Effectiveness Against the Stuxnet-Like Attack: In this case, the attacker injects constant biases $\Delta I_{s1}^a = 2$A and $\Delta I_{s1}^{r,a} = 2$A into the local current measurement $I_{s3}(t)$ and the communicated one $I_{s3}^{r,c}(t)$, respectively, at $T_a = 20.85$s. To cover the attack impact, the historically recorded steady-state data is replayed to upper host 1. Here, the compromised current measurement to the neighboring controllers is consistent with the current component replayed to upper host 1, under which the CSD indicator can finally converge to zero as shown in $(2, 2)$ of Fig. 11. Nevertheless, voltage balancing seen from upper host 1 is violated due to the inconsistency between the replayed voltage component and the actual PCC voltage. According to $(2, 2)$ of Fig. 11, the attack is first perceived by DER 3 at $t = 21.14$s, after which the optimal perturbed PCGs are designed as $\boldsymbol{k}_i^p = [0.2259, -0.5, 1]^{\mathrm{T}}, \forall i \in \mathscr{A}$. Finally, the compromised DER 1 is accurately located when the PCG perturbation occurs as shown in $(3, 2)$ of Fig. 11.

TABLE V
COMPUTATION TIME (MILLISECOND)

	Avg.	Max.		Avg.	Max.
$\underline{k}_{[i1]} = -1,$ $\underline{k}_{[i2]} = -1$	37	33	$\underline{k}_{[i1]} = 0.5,$ $\underline{k}_{[i2]} = -0.5,$	33	21
$\underline{k}_{[i1]} = 0,$ $\underline{k}_{[i2]} = 0$	22	10	$\underline{k}_{[i1]} = -0.5,$ $\underline{k}_{[i2]} = 0.1,$	14	12

D. Computation Time Test

In this subsection, we test the computation time of solving the optimization problem (28)-(30) with varying parameters $\underline{k}_{[i1]}, \underline{k}_{[i2]}$. The test is conducted on a host equipped with Intel Core i9-10850K CPU @ 3.60GHz and 32.0 GB RAM. In each case with fixed parameters, the local optimum to the problem is solved for 200 times using *fmincon* from MATLAB, and the average and maximal computation time are recorded in Table V. The results indicate that the computation time is smaller than 50ms, and the online implementation of the PDDL framework is promising.

E. Comparative Studies

In the HIL testbed, we have compared the PDDL framework with the two alternative methods from [12], [25] to reflect the superior defense capability against the stealthy deception attacks and the significantly reduced fluctuations caused by PCG perturbation. According to Fig. 12, the ZTS attack and Stuxnet-like attack can easily bypass the UIO-based locator proposed in [25]. After integrating the PCG perturbation, the two stealthy deception attacks can be successfully located within an acceptable time delay (less than 3.5s). As shown

in Fig. 13, the empirically chosen PCG perturbation [12] will induce non-neglectable fluctuations on PCC voltages and source currents. By solving problem (28)-(30), the fluctuations of the designed PCG perturbation can be ignorable (reduced significantly).

VIII. Conclusion

In this paper, we proposed a PDDL framework against the stealthy deception attacks in DCmGs, where the attack detection is achieved by observing the VBD and CSD and the attack localization is accomplished through the enhanced UIO-based locators under PCG perturbation. Once any anomaly is perceived, the optimal PCG perturbation will be activated to locate the compromised DERs. Through extensive HIL-based simulations and systematic full-hardware experimental studies, it is validated that the proposed PDDL framework can effectively perceive and mitigate the impact caused by the ZTS attack and Stuxnet-like attack. In our future works, we will investigate the applicability of the PDDL framework to AC microgrids.

References

[1] H. Lotfi and A. Khodaei, "AC versus DC microgrid planning," *IEEE Trans. Smart Grid*, vol. 8, no. 1, pp. 296–304, Jan. 2017.

[2] Z. Cheng and M.-Y. Chow, "Resilient collaborative distributed energy management system framework for cyber-physical DC microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 4637–4649, Nov. 2020.

[3] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab, and A. Abusorrah, "Distributed control and communication strategies in networked microgrids," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2586–2633, 4th Quart., 2020.

[4] S. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5643–5654, Sep. 2020.

[5] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011.

[6] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, Apr. 2011.

[7] *Analysis of the Cyber Attack on the Ukrainian Power Grid*, vol. 388, Electr. Inf. Sharing Anal. Center (E-ISAC), Washington, DC, USA, 2016.

[8] 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 Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1543–1551, Feb. 2019.

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

[10] C. Deng, F. Guo, C. Wen, D. Yue, and Y. Wang, "Distributed resilient secondary control for DC microgrids against heterogeneous communication delays and DoS attacks," *IEEE Trans. Ind. Electron.*, vol. 69, no. 11, pp. 11560–11568, Nov. 2022.

[11] S. Zuo and D. Yue, "Resilient containment of multigroup systems against unknown unbounded FDI attacks," *IEEE Trans. Ind. Electron.*, vol. 69, no. 3, pp. 2864–2873, Mar. 2022.

[12] M. Liu, C. Zhao, Z. Zhang, R. Deng, P. Cheng, and J. Chen, "Converter-based moving target defense against deception attacks in DC microgrids," *IEEE Trans. Smart Grid*, early access, Nov. 19, 2021, doi: 10.1109/TSG.2021.3129195.

[13] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. Annu. Allerton Conf. Commun. Control Comput. (Allerton)*, 2009, pp. 911–918.

[14] J. Yan, F. Guo, and C. Wen, "Attack detection and isolation for distributed load shedding algorithm in microgrid systems," *IEEE J. Emerg. Sel. Topics Ind. Electron.*, vol. 1, no. 1, pp. 102–110, Jul. 2020.

[15] J. Zhang, L. Guo, and J. Ye, "Cyber-attack detection for photovoltaic farms based on power-electronics-enabled harmonic state space modeling," *IEEE Trans. Smart Grid*, early access, Oct. 19, 2021, doi: 10.1109/TSG.2021.3121009.

[16] S. Sahoo, J. C.-H. Peng, S. Mishra, and T. Dragičević, "Distributed screening of hijacking attacks in DC microgrids," *IEEE Trans. Power Electron.*, vol. 35, no. 7, pp. 7574–7582, Jul. 2020.

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

[18] D. Shi, P. Lin, Y. Wang, C.-C. Chu, Y. Xu, and P. Wang, "Deception attack detection of isolated DC microgrids under consensus-based distributed voltage control architecture," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 1, pp. 155–167, Mar. 2021.

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

[20] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, "Detection and mitigation of data manipulation attacks in AC microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2588–2603, May 2020.

[21] Z. Yang, L. He, P. Cheng, J. Chen, D. K. Yau, and L. Du, "PLC-sleuth: Detecting and Localizing PLC intrusions using control invariants," in *Proc. Int. Symp. Res. Attacks Intrusions Defenses*, Oct. 2020, pp. 333–348.

[22] Z. Yang, L. He, H. Yu, C. Zhao, P. Cheng, and J. Chen, "Detecting PLC intrusions using control invariants," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9934–9947, Jun. 2022.

[23] S. Zhao, Q. Yang, P. Cheng, R. Deng, and J. Xia, "Adaptive resilient control for variable-speed wind turbines against false data injection attacks," *IEEE Trans. Sustain. Energy*, vol. 13, no. 2, pp. 971–985, Apr. 2022.

[24] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3690–3701, Sep. 2020.

[25] 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 Trans. Autom. Control*, vol. 65, no. 9, pp. 3800–3815, Sep. 2020.

[26] M. Liu, C. Zhao, R. Deng, P. Cheng, and J. Chen, "False data injection attacks and the distributed countermeasure in DC microgrids," *IEEE Trans. Control Netw. Syst.*, early access, Jun. 10, 2022, doi: 10.1109/TCNS.2022.3181483.

[27] J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, "Moving target defense approach to detecting Stuxnet-like attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 291–300, Jan. 2020.

[28] 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.

[29] 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 Trans. Inf. Forensics Security*, vol. 15, pp. 2320–2335, 2020.

[30] M. Liu, C. Zhao, Z. Zhang, and R. Deng, "Explicit analysis on effectiveness and hiddenness of moving target defense in AC power systems," *IEEE Trans. Power Syst.*, early access, Feb. 24, 2022, doi: 10.1109/TPWRS.2022.3152801.

[31] T. V. Vu, B. L. Nguyen, Z. Cheng, M.-Y. Chow, and B. Zhang, "Cyber-physical Microgrids: Toward future resilient communities," *IEEE Ind. Electron. Mag.*, vol. 14, no. 3, pp. 4–17, Sep. 2020.

[32] L. Obregon, *Secure Architecture for Industrial Control Systems*, vol. 2, SANS Inst., Bethesda, MD, USA, 2015.

[33] 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 Trans. Power Syst.*, vol. 34, no. 3, pp. 1780–1800, May 2019.

[34] 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 Trans. Control Syst. Technol.*, vol. 24, no. 6, pp. 1965–1979, Nov. 2016.

[35] M. S. Sadabadi, Q. Shafiee, and A. Karimi, "Plug-and-play robust voltage control of DC microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6886–6896, Nov. 2018.

[36] T. L. Nguyen, J. M. Guerrero, and G. Griepentrog, "A self-sustained and flexible control strategy for islanded DC nanogrids without communication links," *IEEE J. Emerg. Select. Topics Power Electron.*, vol. 8, no. 1, pp. 877–892, Mar. 2020.

[37] 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, Sep. 2018.

[38] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.
[39] T. Nelso and M. Chaffin, *Common Cybersecurity Vulnerabilities in Industrial Control Systems*, Dept. Homeland Security, Nat. Cyber Security Division, Washington, DC, USA, 2011.
[40] L. Garcia, F. Brasser, M. H. Cintuglu, A.-R. Sadeghi, O. A. Mohammed, and S. A. Zonouz, "Hey, my Malware knows physics! Attacking PLCs with physical model aware Rootkit," in *Proc. Netw. Distrib. System Security (NDSS) Symp.*, 2017, pp. 1–15.
[41] S. P. Skorobogatov, "Semi-invasive attacks: A new approach to hardware security analysis," Comput. Lab., Univ. Cambridge, Cambridge, U.K., Rep. UCAM-CL-TR-630, 2005.
[42] Z. Basnight, J. Butts, J. Lopez, Jr., and T. Dube, "Firmware modification attacks on programmable logic controllers," *Int. J. Crit. Infrastruct. Protect.*, vol. 6, no. 2, pp. 76–84, 2013.
[43] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[44] J. Chen, R. J. Patton, and H.-Y. Zhang, "Design of unknown input observers and robust fault detection filters," *Int. J. Control*, vol. 63, no. 1, pp. 85–105, 1996.
[45] J. Hunker and C. Probst, "Insiders and insider threats—An overview of definitions and mitigation techniques," *J. Wireless Mobile Netw. Ubiquitous Comput. Dependable Appl.*, vol. 2, no. 1, pp. 4–27, 2011.
[46] N. Amjady, "Short-term bus load forecasting of power systems by a new hybrid method," *IEEE Trans. Power Syst.*, vol. 22, no. 1, pp. 333–341, Feb. 2007.
[47] M. Zhu and S. Martínez, "Discrete-time dynamic average consensus," *Automatica*, vol. 46, no. 2, pp. 322–329, 2010.
[48] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 106–117, Mar. 2017.
[49] F. Katiraei and M. R. Iravani, "Power management strategies for a microgrid with multiple distributed generation units," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1821–1831, Nov. 2006.
[50] C. K. Sao and P. W. Lehn, "Control and power management of converter fed microgrids," *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 1088–1098, Aug. 2008.
[51] Y. Li, P. Zhang, L. Zhang, and B. Wang, "Active synchronous detection of deception attacks in microgrid control systems," *IEEE Trans. Smart Grid*, vol. 8, no. 1, pp. 373–375, Jan. 2017.
[52] G. Gilchrist, "Secure authentication for DNP3," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2008, pp. 1–3.
[53] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, "DNPSec: Distributed network protocol version 3 (DNP3) security framework," in *Advances in Computer, Information, and Systems Sciences, and Engineering*. Dordrecht, The Netherlands: Springer, 2007, pp. 227–234.
[54] R. Schlegel, S. Obermeier, and J. Schneider, "A security evaluation of IEC 62351," *J. Inf. Security Appl.*, vol. 34, pp. 197–204, Jun. 2017.
[55] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks," in *Proc. IEEE Power Energy Soc. General Meeting (PESGM)*, 2016, pp. 1–5.
[56] I. Ali, M. A. Aftab, and S. S. Hussain, "Performance comparison of IEC 61850-90-5 and IEEE C37.118.2 based wide area PMU communication networks," *J. Modern Power Syst. Clean Energy*, vol. 4, no. 3, pp. 487–495, 2016.
[57] A. Volkova, M. Niedermeier, R. Basmadjian, and H. de Meer, "Security challenges in control network protocols: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 619–639, 1st Quart., 2019.
[58] C. Rosborough, C. Gordon, and B. Waldron, "All about eve: Comparing DNP3 secure authentication with standard security technologies for SCADA communications," in *Proc. Aust. Inf. Security Conf.*, vol. 161, 2019, pp. 1–11.
[59] R. Amoah, S. Camtepe, and E. Foo, "Formal modelling and analysis of DNP3 secure authentication," *J. Netw. Comput. Appl.*, vol. 59, pp. 345–360, Jan. 2016.
[60] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.
[61] P. Maloney, "Building a better microgrid with hardware in the loop," Microgrid Knowl. Westborough, MA, USA, White Paper, 1996.
[62] S. Papathanassiou, N. Hatziargyriou, and K. Strunz, "A benchmark low voltage microgrid network," in *Proc. CIGRE Symp. Power Syst. Dispersed Gener.*, 2005, pp. 1–8.

Mengxiang Liu (Student Member, IEEE) 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 (Member, IEEE) 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, where she worked as a Postdoctoral Fellow with the College of Control Science and Engineering from 2018 to 2021, and a Postdoctoral Fellow with the ECE Department, University of Victoria from 2019 to 2020. She is currently an Associate Researcher with 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.

Jinhui Xia (Member, IEEE) received the B.Eng., M.Eng., and Ph.D. degrees in electrical engineering from the Dalian University of Technology, Dalian, China, in 2014, 2017, and 2020, respectively. Since September 2020, he has been a Postdoctoral Fellow with the Department of Control Science and Engineering, Zhejiang University, Hangzhou, China. From January 2018 to January 2019, he was a visiting Ph.D. student with the Electric Power and Energy Systems Group, Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, Canada. His research interests include fault diagnosis and robust control strategies for grid-connected power converters and permanent magnet synchronous machines. He contributes regularly as a reviewer for various international journals and conferences.

Ruilong Deng (Senior Member, IEEE) 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. He is currently 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. His research interests include cybersecurity, smart grid, and wireless networking. He serves/served as an Associate Editor 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 a Guest Editor for IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, IEEE TRANSACTIONS ON CLOUD COMPUTING, and *IET Cyber-Physical Systems: Theory & Applications*.

Peng Cheng (Member, IEEE) received the B.Sc. and Ph.D. degrees in control science and engineering from Zhejiang University, Hangzhou, 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. His research interests include networked sensing and control, cyber–physical systems, and control system security. 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 an Associate Editor for IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS, *Wireless Networks*, and *International Journal of Communication Systems*. He also serves/served as a Guest Editor for IEEE TRANSACTIONS ON AUTOMATIC CONTROL and IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORKS.

Jiming Chen (Fellow, IEEE) 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 with the University of Waterloo from 2008 to 2010. He is currently a Professor with the College of Control Science and Engineering, Zhejiang University. His research interests include the Internet of Things, sensor networks, networked control, and control system security. He serves/served as an Associate Editor for *ACM Transactions on Embedded Computing Systems*, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE NETWORK, IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS, and IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. 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.