



This is a repository copy of *Detection-triggered recursive impact mitigation against secondary false data injection attacks in cyber-physical microgrids*.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/219419/>

Version: Accepted Version

---

**Article:**

Liu, M. [orcid.org/0000-0002-2663-4787](https://orcid.org/0000-0002-2663-4787), Zhang, X. [orcid.org/0000-0002-6063-959X](https://orcid.org/0000-0002-6063-959X), Zhang, R. et al. (3 more authors) (2025) Detection-triggered recursive impact mitigation against secondary false data injection attacks in cyber-physical microgrids. *IEEE Transactions on Smart Grid*, 16 (2). pp. 1744-1761. ISSN 1949-3053

<https://doi.org/10.1109/tsg.2024.3493754>

---

© 2024 The Authors. Except as otherwise noted, this author-accepted version of a journal article published in *IEEE Transactions on Smart Grid* is made available via the University of Sheffield Research Publications and Copyright Policy under the terms of the Creative Commons Attribution 4.0 International License (CC-BY 4.0), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>

**Reuse**

This article is distributed under the terms of the Creative Commons Attribution (CC BY) licence. This licence allows you to distribute, remix, tweak, and build upon the work, even commercially, as long as you credit the authors for the original work. More information and the full terms of the licence here:

<https://creativecommons.org/licenses/>

**Takedown**

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing [eprints@whiterose.ac.uk](mailto:eprints@whiterose.ac.uk) including the URL of the record and the reason for the withdrawal request.



[eprints@whiterose.ac.uk](mailto:eprints@whiterose.ac.uk)  
<https://eprints.whiterose.ac.uk/>

# Detection-Triggered Recursive Impact Mitigation against Secondary False Data Injection Attacks in Cyber-Physical Microgrids

Mengxiang Liu, Xin Zhang, Rui Zhang, Zhuoran Zhou, Zhenyong Zhang, and Ruilong Deng

**Abstract**—The cybersecurity of microgrid has received widespread attentions due to the frequently reported attack accidents against distributed energy resource (DER) manufactures. Numerous impact mitigation schemes have been proposed to reduce or eliminate the impacts of false data injection attacks (FDIAs). Nevertheless, the existing methods either requires at least one neighboring trustworthy agent or may bring in unacceptable cost burdens. This paper aims to propose a detection-triggered recursive impact mitigation scheme that can timely and precisely counter the secondary FDIAs (SFDIAs) against the communication links among DERs. Once triggering attack alarms, the power line current readings will be utilised to observe the voltage bias injections through the physical interconnections among DERs, based on which the current bias injections can be recursively reconstructed from the residuals generated by unknown input observers (UIOs). The attack impacts are eliminated by subtracting the reconstructed bias from the incoming compromised data. The proposed mitigation method can work even in the worst case where all communication links are under SFDIAs and only require extra current sensors. The bias reconstruction performance under initial errors and system noises is theoretically analysed and the reconstruction error is proved to be bounded regardless of the electrical parameters. To avoid deploying current sensors on all power lines, a cost-effective deployment strategy is presented to secure a spanning tree set of communication links that can guarantee the secondary control performance. Extensive validation studies are conducted in MATLAB/SIMULINK and cyber-physical microgrid testbeds to validate the proposed method’s effectiveness against single/multiple and continuous/discrete SFDIAs.

**Index Terms**—False data injection attack, cyber-physical microgrid, recursive impact mitigation, bias injection reconstruction, unknown input observer

## I. INTRODUCTION

The recent cyberattack accidents against distributed energy resource (DER) manufactures like Vestas [1] and EnerCon [2] imply that the widely penetrated DERs have been frequently targeted by adversaries. The information forensics of

M. Liu, Z. Zhou, and X. Zhang are with the School of Electronic and Electrical Engineering, University of Sheffield, Sheffield, UK (e-mails: {mengxiang.liu, zzhou106, xin.zhang1}@sheffield.ac.uk).

R. Zhang is with the National Energy System Operator NESO, Wokingham, United Kingdom (e-mail: rui.zhang@nationalenergyso.com).

Z. Zhang and R. Deng are with the State Key Laboratory of Industrial Control Technology and the College of Control Science and Engineering, Zhejiang University, Hangzhou, China (e-mails: {dengruilong, zhangzhenyong}@zju.edu.cn).

This work was supported by the UK Research and Innovation Future Leaders Fellowship ‘Digitalisation of Electrical Power and Energy Systems Operation (DEEPS)’ under Grant MR/W011360/2 (Corresponding author: Xin Zhang).

these accidents further verified that the adversary’s attempt is shifting from stealing sensitive data for ransom to interrupting DERs’ normal operations. As one of the widely adopted forms that integrate DERs in the power grid, the cyber-physical microgrid has integrated massive advanced information and communications technologies like TCP/IP communication and CAN/Profinet to meet DERs’ control and dispatch requirements. It is thus vital to foresee the potential cybersecurity issues in microgrids and take necessary cybersecurity enhancement strategies [3].

According to the hierarchical control framework of cyber-physical microgrid as shown in Fig. 1, where the primary controller regulates the local DER states and the secondary controller coordinates DERs to achieve global objectives like load sharing [4], five typical false data injection attacks (FDIAs) against the two controllers by exploiting protocol vulnerabilities [5], firmware rootkit [6], and sensor spoofing tools [7] can be identified. These secondary and primary FDIAs (SFDIA and PFDIA) can disrupt the normal behaviours of DERs, initiate protective actions, and potentially lead to cascading failures. As a result, it is necessary to make appropriate cyber-resilient prevention, detection, mitigation, and recovery strategies [8]–[10]. This paper mainly focuses on the during-attack impact mitigation phase that is used to reduce or eliminate the attack impacts with sufficient time to make the cyber recovery plan.

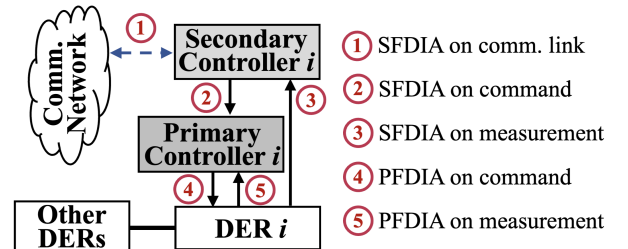


Fig. 1: This figure illustrates the locations of five typical FDIAs against primary and secondary controllers in the cyber-physical microgrid.

Numerous literature has emerged in the topic of designing cyber-resilient impact mitigation strategies for the microgrid under FDIAs, which can be generally classified as model-based and data-driven according to the principles of adopted methods. Focusing on the SFDIA on control commands (②), Zuo *et al.* [11] proposed a resilient cooperative secondary controller that can mitigate the impacts of bounded and

unbounded bias injections in an adaptive manner. Given the SFDIAs (②) in energy storage dominated microrgrids [12] and networked AC/DC microgrids [13], Wang and Deng *et al.* designed distributed resilient secondary controllers by introducing adaptive techniques to maintain the overall control objectives. To infer the bias injected into the communication links, Jin *et al.* [14] aimed to analyse the impacts of SFDIAs (①) on voltages to obtain the exact bias expression. But this method has limitations in handling the case where multiple SFDIAs with general bias types exist. In response to the SFDIAs on communication links (①) and control commands (②), Sahoo *et al.* proposed to reconstruct an detection-triggered secondary control error signal using the trustworthy agents' information [15], [16]. This mitigation strategy requires that at least one of the neighboring links/agents should be trustworthy to guarantee the credibility of reconstructed signals.

Considering the PFDIA on the control command (④), Sadabadi *et al.* [17] introduced a resilient voltage tracking and current sharing primary controller to mitigate the potential adverse impacts. When the secondary communication links (①), control commands (②), and measurements (③) are all subject to unbounded FDIAs, Zuo *et al.* [18] introduced a hidden secure communication network where the transmitted data was immune to malicious modifications to correct the hazardous control actions. With the provision of an internet-of-things (IoT) based digital twin that interacts with the microgrid control system, Saad *et al.* [19] developed practical resilient control algorithms by replacing the malicious data with those received from the Luenberger observer based IoT shadow. The hidden network and digital twin based mitigation strategies can effectively maintain the microgrid control performance even under hybrid SFDIAs (①, ③) and PFDIAs (⑤), but the associated extra costs may be unacceptable for the system operator.

The data-driven methods in mitigating FDIAs' impacts within microgrids have been investigated recently. By training an artificial neural network (ANN) with the inputs of DC-DC converters' output voltages and currents, Habibi *et al.* [20] proposed a novel data-driven method to mitigate the impacts of the SFDIA compromising the parallel converters' point of common coupling (PCC) voltage readings (③). To enable its decentralized implementation, Habibi *et al.* [21] successfully designed an ANN to recover the converter's legitimate output current under FDIAs using the inputs of renewable source's output current and primary voltage control signal. To alleviate the necessity of multiple training processes for a well-tuned deep neural network based estimator, which was used to recover the sum of communicated signals using the local measurements, Xia *et al.* [22] designed a representation subspace distance based transfer learning model.

A tabulated illustration of the reviewed impact mitigation methods against SFDIAs is provided in TABLE I. First of all, the investigation of the impact mitigation schemes [11]–[13] against the SFDIA on control commands (②) has been well developed. Nevertheless, existing impact mitigation schemes against the SFDIA on communication links (①) either have assumptions on the number of compromised links [14]–[16] or may bring in unacceptable cost burdens for the system operator

TABLE I: Comparisons between the proposed impact mitigation method and the existing ones against SFDIAs

Category	Literature	SFDIA Types			Extra Cost
		①	②	③	
Model-based	[11]–[13]	✗	✓	✗	No
	[14]	✓ <sup>◦</sup>	✗	✗	No
	[15], [16]	✓ <sup>*</sup>	✓	✗	Blockchain
	[18]	✓	✓	✓	Hidden layer
	[19]	✓	✗	✓	Digital twin
Data-driven	[20], [21]	✗	✗	✓	No
	[22]	✓	✗	✗	No
<b>Model-based Our work</b>		<b>✓</b>	<b>✗</b>	<b>✗</b>	<b>Current sensor</b>

<sup>◦</sup> The number of SFDIA is limited by 1.

<sup>\*</sup> There should be at least one trustworthy neighboring agent.

[18], [19]. While the data-driven mitigation methods [20]–[22] have not incorporated the physical knowledge, under which the reconstructed data may not comply with the underlying physical dynamics and thus the reconstructed data can oppositely exacerbate the attack impacts.

Towards this end, this paper aims to design an effective and cost-efficient impact mitigation scheme against the SFDIA on communication links (①) based on the unknown input observer (UIO), which has been proved effective in detecting random [23] and stealthy [24]–[26] FDIAs. As shown in Fig. 2, the impact mitigation scheme will only be activated after UIOs have perceived anomalous behaviours. We propose a novel idea to firstly observe the voltage bias injection through incorporating the physical interconnection among DERs, i.e., utilising the power line current to observe the voltage of interconnected DER. Based on the observed voltage bias injection, the current bias injections could then be recursively reconstructed from the UIO's detection residuals. Finally, the reconstructed biases are subtracted from the compromised communicated data to mitigate the attack impacts. The main contributions of this paper are:

- We propose an innovative detection-triggered recursive impact mitigation scheme against the SFDIA on communication links (①), which is effective even when all communication links are compromised, and this scheme only requires to install additional current sensors on power lines.
- We derive the explicit relations between UIO residuals and bias injections, based on which a recursive bias reconstruction scheme is intuitively established. Moreover, we prove that the reconstruction error is bounded by a term related solely to the system noise bounds.
- We present a cost-effective deployment strategy for current sensors based on existing measuring infrastructure, securing a spanning tree set of communication links that can guarantee the secondary control performance.
- We conduct extensive validation studies in MATLAB/SIMULINK and cyber-physical microgrid testbeds to illustrate the proposed method's effectiveness against various SFDIAs in the presence of load variations, DERs plugging-in, and voltage fluctuations.

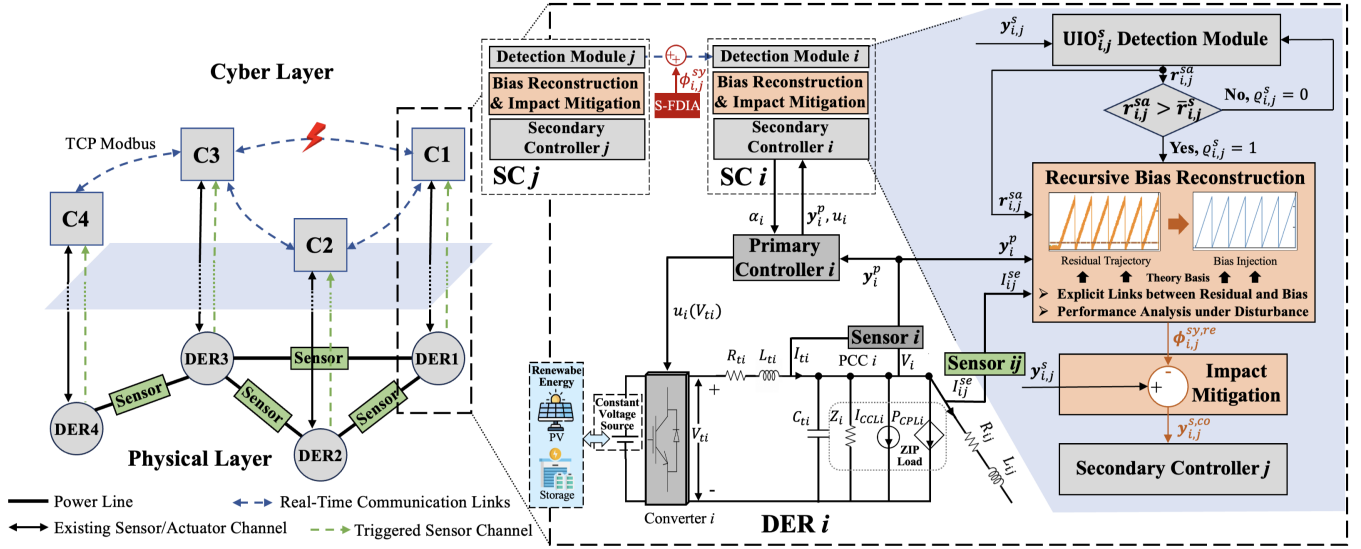


Fig. 2: The left part depicts the architecture of cyber-physical microgrid, the middle part illustrates the specific cyber-physical couplings and exposed attack surfaces to SFDIAs, and the right part details the detection-triggered recursive bias reconstruction and impact mitigation schemes and their integration with the original secondary controller.

## II. CYBER-PHYSICAL MICROGRID SYSTEM MODEL

As shown in Fig. 2, we consider an isolated DC microgrid consisting of  $N \geq 2$  DERs, where renewable energy resources (RESs) including photovoltaic (PV) cells are operated with sufficient storage units to eliminate the intermittent power generation resulting from weather variations and therefore can be simplified as a constant voltage source [27], [28]. The DC-DC converter is commanded to supply the local ZIP load through an RLC filter. The electrical network that physically connects the DERs is denoted by a weighted cyber bi-directional graph  $\mathcal{G}_{el} = \{\mathcal{A}, \mathcal{E}_{el}\}$ , where the set  $\mathcal{A}$  collects all the DER nodes and the set  $\mathcal{E}_{el}$  includes the power lines that connect the DERs with the set of weights as the corresponding line conductance, that is,  $\frac{1}{R_{ij}}, \forall (i, j) \in \mathcal{E}_{el}$ .<sup>1</sup> The set that contains the physical neighbours of the DER  $i \in \mathcal{A}$  in graph  $\mathcal{G}_{el}$  is represented by  $\mathcal{N}_i^{el}$ . The communication network that transmits data between DERs is also indicated by a weighted bidirectional graph  $\mathcal{G}_c = \{\mathcal{A}, \mathcal{E}_c\}$ , where the set  $\mathcal{E}_c$  gathers all communication links with the weights designed as  $a_{ij}^c, \forall (i, j) \in \mathcal{E}_c$ . The cyber neighbors of DER  $i \in \mathcal{A}$  in graph  $\mathcal{G}_c$  are collected in the set  $\mathcal{N}_i^c$ . We assume that the electrical and communication cyber-physical graphs share the same topology are both connected, which establish the sufficient conditions for achieving stable control [29].

Since the microgrid is operated close to the nominal reference point of common coupling (PCC) voltage  $V_{ref,i}$ , the constant power load (CPL)  $P_{CPL,i}$  is linearised around this nominal operating point as

$$I_{CPL,i} = -\frac{P_{CPL,i}}{V_{ref,i}^2} V_i + 2\frac{P_{CPL,i}}{V_{ref,i}}, \quad (1)$$

where the former part is a negative impedance related to the actual PCC voltage  $V_i$  and the latter part is a constant

<sup>1</sup>The inductive part, i.e.,  $L_{ij}$  as shown in Fig. 2, is omitted as it is usually far smaller than the resistive part.

current. Under linearisation (1), the original ZIP load can be characterised by the equivalent constant impedance ( $Z_{Li}$ ) and current ( $I_{Li}$ ) loads as follows:

$$\frac{1}{Z_{Li}} = \frac{1}{Z_i} - \frac{P_{CPL,i}}{V_{ref,i}^2}, \quad (2)$$

$$I_{Li} = I_{CCL,i} + 2\frac{P_{CPL,i}}{V_{ref,i}}, \quad (3)$$

where  $Z_i$  and  $I_{CCL,i}$  denote the original constant impedance and current parts of the ZIP load, respectively. Based on the linearised ZIP load (2)-(3), the dynamics of the RLC filter inside DER  $i$  can be obtained after utilising the Kirchhoff voltage and current laws and incorporating the quasi-stationary line approximation ( $L_{ij} \approx 0$ ), i.e.,

$$\begin{cases} \frac{dV_i}{dt} = \frac{1}{C_{ti}} I_{ti} + \sum_{j \in \mathcal{N}_i^{el}} \frac{1}{C_{ti} R_{ij}} (V_j - V_i) - \frac{1}{C_{ti}} (I_{Li} + \frac{V_i}{Z_{Li}}) \\ \frac{dI_{ti}}{dt} = -\frac{1}{L_{ti}} V_i - \frac{R_{ti}}{L_{ti}} I_{ti} + \frac{1}{L_{ti}} V_{ti} \end{cases}, \quad (4)$$

where  $V_{ti}$  denotes the converter's output voltage,  $I_{ti}$  represents the output current from the renewable source, and  $R_{ti}$ ,  $L_{ti}$ , and  $C_{ti}$  are the RLC filter parameters. Denote the system state by  $\mathbf{x}_i = [V_i, I_{ti}]^T$ , the system dynamics (4) can be rewritten as

$$\dot{\mathbf{x}}_i(t) = \mathbf{A}_{ii} \mathbf{x}_i(t) + \mathbf{b}_i u_i(t) + \mathbf{m}_i d_i(t), \quad (5)$$

where  $\mathbf{x}_i$  is the updated system state, and  $\mathbf{A}_{ii}$ ,  $\mathbf{b}_i$ , and  $\mathbf{m}_i$  denote the system matrix, primary input vector, and unknown input vector, respectively, as detailed in Appendix A. The primary input  $u_i(t) = V_{ti}(t)$  represents the voltage regulation command to the DC-DC converter and the unknown input  $d_i(t) = I_{Li} + \sum_{j \in \mathcal{N}_i^{el}} -\frac{1}{R_{ij}} V_j(t)$  includes the current load as well as the physical couplings with neighboring DERs.

To be compatible with the digital signal based processor, the dynamical model (5) is discretized with sampling time  $T_{samp}$  and is blended with fully measured system states along with bounded process and measurement noises as the following

state-space model:

$$\begin{cases} \mathbf{x}_i(k+1) = A_{ii}^d \mathbf{x}_i(k) + \mathbf{b}_i^d u_i(k) + \mathbf{m}_i^d d_i(k) + \boldsymbol{\omega}_i(k) \\ \mathbf{y}_i(k) = \mathbf{x}_i(k) + \boldsymbol{\rho}_i(k) \end{cases}, \quad (6)$$

where system parameters  $A_{ii}^d$ ,  $\mathbf{b}_i^d$ , and  $\mathbf{m}_i^d$  are derived from the original parameters in (5) with sampling time  $T_{samp}$  and their relations are detailed in appendix A. The system states are fully measured as local output vector  $\mathbf{y}_i(k)$ , and bounded process and measurement noises satisfy  $|\boldsymbol{\omega}_i(k)| \leq \bar{\boldsymbol{\omega}}_i$  and  $|\boldsymbol{\rho}_i(k)| \leq \bar{\boldsymbol{\rho}}_i$ , respectively.

To achieve the reference PCC voltage tracking, the primary control input  $u_i(k)$  is calculated based on the general Proportion-Integral control algorithm as follows

$$u_i(k) = (\mathbf{g}_i^P)^T \mathbf{y}_i^p(k) + g_i^I \sum_{l=0}^k (V_{ref,i} + \alpha_i(l) - \boldsymbol{\kappa}^T \mathbf{y}_i^p(l)), \quad (7)$$

where  $\mathbf{g}_i^P$  and  $g_i^I$  contain proportional and integral control gains, respectively,  $\mathbf{y}_i^p(k)$  is the local outputs available to the primary controller that will be equal to  $\mathbf{y}_i(k)$  in the normal case, and  $\alpha_i(k)$  denotes the secondary control input that is computed utilising the data transmitted over the communication network. To satisfy the hard real-time requirement of primary control, field-level communication protocols like CAN and Profinet are usually adopted to establish the sensor channel. Constant vector  $\boldsymbol{\kappa} = [1, 0]^T$  is used to extract the PCC voltage information for the calculation of accumulated voltage tracking errors.

The distributed secondary controller is deployed on top of the primary controller to regulate the voltage tracking objective in a coordinated manner to achieve the overall control objectives in the microgrid including voltage balancing and current sharing. TCP Modbus communication protocol is recommended to accomplish the data exchange between DERs. In the essential principle of consensus control, the secondary control input is calculated as

$$\alpha_i(k) = \boldsymbol{\iota}^T \sum_{l=0}^k \sum_{j \in \mathcal{N}_i^c} a_{ij} \left( \frac{\mathbf{y}_{i,j}^s(l)}{I_{ij}^s} - \frac{\mathbf{y}_i^p(l)}{I_{ii}^s} \right), \quad (8)$$

where  $\mathbf{y}_{i,j}^s(k)$  denotes the output vector of DER  $j \in \mathcal{N}_i^c$  transmitted over link  $(i, j) \in \mathcal{E}_c$  that will be equal to  $\mathbf{y}_j^p(k)$  in the normal case,  $I_{ij}^s > 0$  and  $I_{ii}^s > 0$  are the rated output currents corresponding to DERs  $j$  and  $i$ , respectively, and constant vector  $\boldsymbol{\iota} = [0, 1]^T$  is applied to obtain the accumulated current sharing errors.

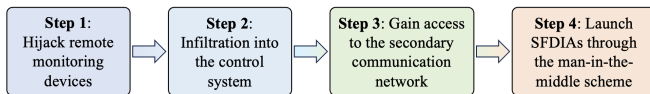


Fig. 3: This figure illustrates a practical attack path consisting of four key steps for launching the SFDIA in microgrids.

### A. Cyber Attack Model

For the data interaction required by secondary control, the TCP Modbus communication protocol has been widely

recommended owing to its open standard and easy-to-use characteristic that facilitate the interoperability among devices from different manufacturers [10]. The insufficient security mechanisms of Modbus in data encryption, node authentication, and key management have exposed the secondary communication network to various cyber attacks like FDIAs [26], which can be launched through the well-known man-in-the-middle attack scheme once the adversary gains access to the network [30]. According to the recently disclosed attack incident against solar power facilities in Japan, the malicious adversary hijacked 800 SolarView Compact remote monitoring devices by exploiting a known flaw that was not patched to engage in bank account thefts [31]. Utilising the hijacked remote monitoring device as a springboard, the adversary could further infiltrate into the control system and severely affect the operation of solar facilities. Inspired by this, a practical attack path which demonstrates the steps of launching the SFDIA in microgrids is shown in Fig. 3. The first step is to hijack remote monitoring devices by exploiting zero-day or disclosed flaws. By conducting infiltration from hijacked remote monitoring devices into the control system, the adversary makes lateral movements to the monitoring host of DER in step 2, after which the adversary would be able to access the secondary control's communication network in step 3. Finally, in step 4, the adversary can launch SFDIAs through the man-in-the-middle scheme, where the malicious entity is inserted between the two legal communication DERs to modify the transmitted data packets while deceiving the two DERs via ARP spoofing [30].

In DER  $i$ , the SFDIA that target at its secondary communication links is modelled as

$$\text{SFDIA : } \mathbf{y}_{i,j}^s(k) = \mathbf{y}_j^p(k) + \boldsymbol{\phi}_{i,j}^{sy}(k), \quad (9)$$

where  $\boldsymbol{\phi}_{i,j}^{sy}$  denotes the bias vector injected into neighboring DER  $j$ 's transmitted output vector. The design of  $\boldsymbol{\phi}_{i,j}^{sy}, \forall i, j \in \mathcal{A}$  against multiple communication links can be implemented in the either independent or conspiring manner to incur hazardous consequences including voltage instability [32] and economic loss [26]. Moreover, we consider the worst case where the adversary's resources are not restricted and arbitrary number of communication links can be compromised.

### B. Unknown Input Observer based Attack Detection

The UIO is originally designed to estimate system states in the presence of the unknown inputs resulted from uncertain system parameters and unexpected component failures, under which performance guaranteed controllers can be designed to tolerate these uncertainties [33]. Recently, the potential application of UIO to detecting FDIAs in large-scale interconnected systems like microgrids has been well investigated [23]. The basic idea is to use the estimated system states to measure if the trajectory of received data satisfy DER system dynamics (6). Specifically, the  $\text{UIO}_{i,j}^s$  designed for the DER  $j$ 's data communicated through the communication link is represented as

$$\begin{aligned} \text{UIO}_{i,j}^s : \\ \begin{cases} \mathbf{z}_{i,j}^s(k+1) = F_j^s \mathbf{z}_{i,j}^s(k) + T_j^s \mathbf{b}_j^d u_{i,j}^s(k) + \hat{K}_j^s \mathbf{y}_{i,j}^s(k) \\ \hat{\mathbf{x}}_{i,j}^s(k) = \mathbf{z}_{i,j}^s(k) + H_j^s \mathbf{y}_{i,j}^s(k) \end{cases}, \quad (10) \end{aligned}$$



where  $\mathbf{z}_{i,j}^s$  is UIO $_{i,j}^s$ 's internal state vector,  $\hat{\mathbf{x}}_{i,j}^s$  is the estimated DER  $j$ 's state vector, and  $\mathbf{u}_{i,j}^s = \mathbf{u}_j$  is the communicated DER  $j$ 's control command. The UIO matrix  $F_j^s$  is designed to be stable, i.e., the real parts of its eigenvalues need to satisfy  $|\lambda_i^e(F_j^s)| < 1, \forall i \in \{1, 2\}$ , to converge the state estimation error and matrix  $T_j^s$  is designed according to  $T_j^s \mathbf{m}_j^d = \mathbb{0}^{2 \times 1}$  to eliminate the impacts of unknown inputs. The principles of choosing UIO matrices  $F_j^s, T_j^s, \hat{K}_j^s, H_j^s$  should satisfy

$$T_j^s = \mathbf{I}^2 - H_j^s \quad (11)$$

$$T_j^s \mathbf{m}_j^d = \mathbb{0}^{2 \times 1} \quad (12)$$

$$\hat{K}_j^s = K_{j1}^s + K_{j2}^s \quad (13)$$

$$F_j^s = T_j^s A_{jj}^d - K_{j1}^s \quad (14)$$

$$K_{j2}^s = F_j^s H_j^s \quad (15)$$

to eliminate the impact of unknown inputs and initial estimation errors on the state estimation accuracy. The detection residual is derived by comparing the estimated state vector with the actual measurement output vector as

$$\mathbf{r}_{i,j}^s(k) = \mathbf{y}_{i,j}^s(k) - \hat{\mathbf{x}}_{i,j}^s(k) \quad (16)$$

and in the normal operation its analytical expression can be obtained considering (6) and (10):

$$\begin{aligned} \mathbf{r}_{i,j}^s(k) &= (F_j^s)^k (\mathbf{r}_{i,j}^s(0) - T_j^s \boldsymbol{\rho}_j(0)) + T_j^s \boldsymbol{\rho}_j(k) \\ &\quad \sum_{l=0}^{k-1} (F_j^s)^{k-1-l} (T_j^s \boldsymbol{\omega}_j(l) - \hat{K}_j^s \boldsymbol{\rho}_j(l)), \end{aligned} \quad (17)$$

where  $\mathbf{r}_{i,j}^s(0)$  is the initial residual vector and will be equal to zero after strategically choosing the initial UIO state vector as  $\mathbf{z}_{i,j}^s(0) = T_j^s \mathbf{y}_{i,j}^s(0)$ . Given the bounded system noises, the upper bounded of  $|\mathbf{r}_{i,j}^s|$  can be thus calculated as

$$\begin{aligned} |\mathbf{r}_{i,j}^s(k)| &\leq \bar{r}_{i,j}^s(k) = \nu_j^s (\zeta_j^s)^k |T_j^s| \bar{\boldsymbol{\rho}}_j + |T_j^s| \bar{\boldsymbol{\rho}}_j \\ &\quad \sum_{l=0}^{k-1} \nu_j^s (\zeta_j^s)^{k-1-l} (|T_j^s| \bar{\boldsymbol{\omega}}_j + |\hat{K}_j^s| \bar{\boldsymbol{\rho}}_j), \end{aligned} \quad (18)$$

where positive scalars  $\nu_j^s$  and  $0 < \zeta_j^s < 1$  are chosen such that  $\|(F_j^s)^k\| \leq \nu_j^s (\zeta_j^s)^k$ .

Once either of the following conditions is satisfied, attack alarms will be triggered for the corresponding voltage or current data

$$r_{i,j}^{s,V}(k) > \bar{r}_{i,j}^{s,V}(k) \quad \text{or} \quad r_{i,j}^{s,I}(k) > \bar{r}_{i,j}^{s,I}(k), \quad (19)$$

where  $\mathbf{r}_{i,j}^s = [r_{i,j}^{s,V}, r_{i,j}^{s,I}]^T$  and  $\bar{\mathbf{r}}_{i,j}^s = [\bar{r}_{i,j}^{s,V}, \bar{r}_{i,j}^{s,I}]^T$ . The attack alarm  $\varrho_{i,j}^s = 1$  indicate that the neighboring communicated measurement output  $\mathbf{y}_{i,j}^s$  are encountering SFDIAs.

### III. MOTIVATING EXAMPLE AND PROBLEM FORMULATION

It is far from sufficient for the cyber-resilient operation of microgrids to perceive the existence, type, and location of unpredictable attack events. It is equivalently important to adopt appropriate countermeasure actions to mitigate and even eliminate the adversarial impacts of attacks after successfully detecting them. The detectability of UIOs against both the random [23] and stealthy [24]–[26] FDIA in microgrids has been thoroughly investigated. It has been well known to

utilise the residuals generated by UIOs (17) to validate the adherence of the received signal's trajectory to the underlying DER dynamics. *However, a hidden and usually ignored fact underlying the generated residuals is that they also synthesize the bias injection information.* Hence, in addition to attack detection, another functionality of UIOs' residuals can be explored to reconstruct the injected biases, which will be then used to recover the legitimate data for the mitigation of attack impacts.

To intuitively reflect the relations between UIOs' residuals and the SFDIA biases, three motivating examples are provided. The four-node DC microgrid with the cyber and physical typologies shown in Fig. 2 is established, where the communication link between DERs 1 and 2 is subject to SFDIAs and three representative types of bias injections (Step, Ramp, and Sine) into the neighboring output vector, i.e.,  $\boldsymbol{\phi}_{2,1}^{sy} = [\phi_{2,1,V}^{sy}, \phi_{2,1,I}^{sy}]^T$ , are considered. When picturing the bias injections and corresponding residuals in Fig. 4, an intuitive observation is that the residual trajectory can reflect many features of the injected biases like their steady-state values and changing patterns. Specifically, under the step bias injection case in sub-figure (a), the steady-state bias injections will result in steady-state increment on the corresponding residuals. Moreover, when the bias injections possess changing patterns like ramp and sine signals in sub-figures (b) and (c), the same patterns can be observed from the resulted residuals. In addition to that, there are explicit theoretical links between residuals and the associated biases as reflected in (6) and (10), which provide theory basis for the forthcoming reconstruction of SFDIA biases.

Therefore, based on the attack alarms triggered by UIOs, this paper aims to propose a post-detection bias injection reconstruction and impact mitigation scheme based on the residuals generated by UIOs. Three essential problems need to be sorted out: 1) Investigation of the analytical relations between residuals and the corresponding bias injections, based on which an computation-friendly and cost-efficient bias injection reconstruction scheme will be designed. 2) Analysis of the impact of initially estimated inaccurate bias injections on the subsequently reconstructed bias injections since it is hard to know the exact bias injections at the alarm flagging time. 3) Performance analysis of proposed bias reconstruction scheme in the presence of bounded system noises as small fluctuations can still significantly diverge the reconstructed biases from real ones. 4) Cost-effective deployment of current sensors that can ensure the secondary control performance under SFDIAs with minimal number of required sensors.

### IV. DETECTION-TRIGGERED BIAS RECONSTRUCTION AND IMPACT MITIGATION

This section introduces the theoretical links between UIO residuals and SFDIA bias injections, based on which the bias reconstruction and impact mitigation scheme are detailed along with rigorous performance analysis. The working flow of the proposed scheme is shown in Fig. 5, where the attack alarming trigger generated by (19) will activate the voltage bias observation action (25) and current bias reconstruction

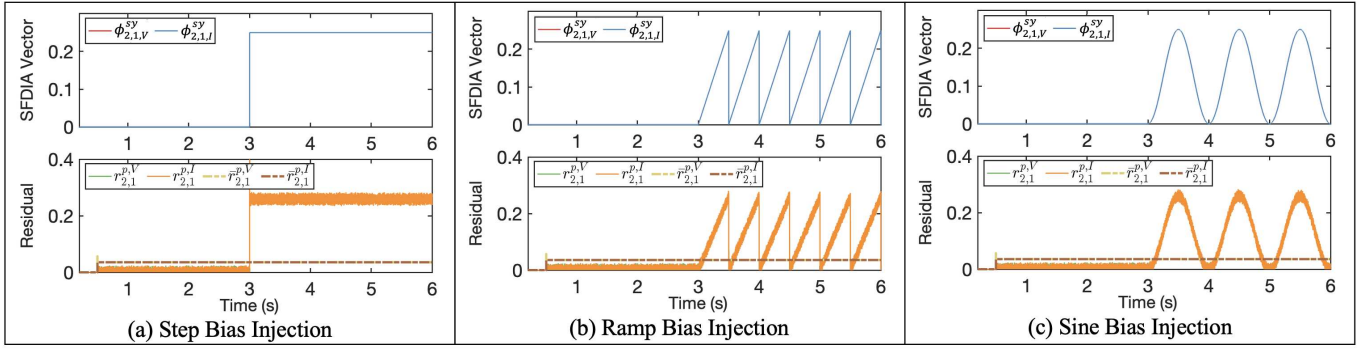


Fig. 4: Motivating examples indicating the relations of UIOs' residuals and Step, Ramp, and Sine bias injections.

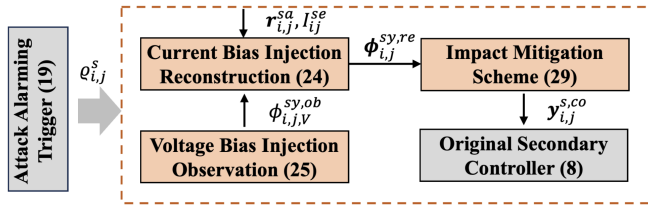


Fig. 5: This figure elaborates the working flow of the detection-triggered bias reconstruction and impact mitigation scheme.

function (24). Then, the reconstructed bias SFDIA vector  $\phi_{i,j}^{sy, re}$  will be fed back to the impact mitigation scheme (29) to eliminate the attack impact on the secondary controller (8).

#### A. Explicit Relations between Residuals and SFDIA Biases

The explicit relations between residual  $r_{i,j}^{sa}$  and bias injection  $\phi_{i,j}^{sy}$  can be derived from the DER dynamics (6), SFDIA model (9), and UIO dynamics (10). According to the bias injection forms (9) and UIO<sup>s</sup><sub>*i,j*</sub> (10), the residual under attacks  $r_{i,j}^{sa}(k+1)$  can be calculated:

$$\begin{aligned} r_{i,j}^{sa}(k+1) &= \mathbf{y}_{i,j}^s(k+1) - \hat{\mathbf{x}}_{i,j}^s(k+1) \\ &= T_j^s \mathbf{y}_{i,j}^s(k+1) - \mathbf{z}_{i,j}^s(k+1) \\ &= T_j^s A_{jj}^d \mathbf{y}_j(k+1) - F_j^s \mathbf{z}_{i,j}^s(k) + \\ &\quad - T_j^s \mathbf{b}_j^d u_{i,j}^s(k) - \hat{K}_j^s \mathbf{y}_{i,j}^s(k) + T_j^s \phi_{i,j}^{sy}(k+1). \end{aligned} \quad (20)$$

The DER *j*'s dynamics similar as (6) can be used to expand  $\mathbf{y}_j(k+1)$  and along with (12), the above expression (20) is transformed to

$$\begin{aligned} r_{i,j}^{sa}(k+1) &= T_j^s A_{jj}^d \mathbf{x}_j(k) + (F_j^s H_j^s - \hat{K}_j^s) \mathbf{y}_{i,j}^s(k) + \\ &\quad - F_j^s \hat{\mathbf{x}}_{i,j}^s(k) + T_j^s \phi_{i,j}^{sy}(k+1) + \\ &\quad + T_j^s \boldsymbol{\rho}_j(k+1) + T_j^s \boldsymbol{\omega}_j(k). \end{aligned} \quad (21)$$

Bearing in mind that the aim is to express  $r_{i,j}^{sa}(k+1)$  in terms of its previous form  $r_{i,j}^{sa}(k)$ , the forthcoming step is to equalise  $\mathbf{x}_j(k)$  as

$$\mathbf{x}_j(k) = \mathbf{y}_{i,j}^s(k) - \phi_{i,j}^{sy}(k) - \boldsymbol{\rho}_j(k). \quad (22)$$

Substituting (22) into (21) and considering the dependencies of UIO parameters (13)-(15), we have

$$\begin{aligned} r_{i,j}^{sa}(k+1) &= F_j^s r_{i,j}^{sa}(k) + T_j^s \phi_{i,j}^{sy}(k+1) + \\ &\quad - T_j^s A_{jj}^d \phi_{i,j}^{sy}(k) + \chi_{i,j}^s(k), \end{aligned} \quad (23)$$

where  $\chi_{i,j}^s(k) = T_j^s \boldsymbol{\rho}_j(k+1) - T_j^s A_{jj}^d \boldsymbol{\rho}_j(k) + T_j^s \boldsymbol{\omega}_j(k)$  collects the noise related term. Equation (23) implies that the residual under SFDIAs is related to the previous residual, plus the difference of SFDIA bias injection between the existing and previous states observed with the UIO internal parameters. These explicit relations would be the basis of inferring bias vector  $\phi_{i,j}^s$  from detection residuals. Another observation from (23) is that, in ideal cases, it can determine only one bias entry of  $\phi_{i,j}^s$  as matrix  $T_j^s$  does not possess full-column rank. Thus, extra legitimate information is necessary for the bias injection reconstruction.

#### B. Physical-Interconnection-Aware Bias Reconstruction

After detecting the SFDIA (9) through UIO alarming conditions (19) at time instant  $k_{i,j}^{sa}$ , the bias injected into the neighboring current measurement, i.e.,  $\phi_{i,j}^{sy, re}(k+1)$ ,  $k \geq k_{i,j}^{sa}$ , can be reconstructed through the residual  $r_{i,j}^{sa}$  and observed voltage bias injection  $\phi_{i,j}^{sy, ob}$  as

$$\begin{aligned} \phi_{i,j}^{sy, re}(k+1) &= (\tilde{\mathbf{t}}_{j2}^s)^T \left( T_j^s A_{jj}^d \phi_{i,j}^{sy, re}(k) - \mathbf{t}_{j1}^s \phi_{i,j}^{sy, ob}(k+1) + \right. \\ &\quad \left. + \psi_{i,j}^{sa}(k) \right), k \geq k_{i,j}^{sa}, \end{aligned} \quad (24)$$

where  $\phi_{i,j}^{sy, re}(k) = [\phi_{i,j}^{sy, ob}(k), \phi_{i,j}^{sy, re}(k)]^T$  includes the previous reconstructed current bias injection,  $\psi_{i,j}^{sa}(k) = r_{i,j}^{sa}(k+1) - F_j^s r_{i,j}^{sa}(k)$  represents the residual discrepancy term under attacks,  $T_j^s = [\mathbf{t}_{j1}^s, \mathbf{t}_{j2}^s]$ , and  $\tilde{\mathbf{t}}_{j2}^s = \frac{\mathbf{t}_{j2}^s}{(\mathbf{t}_{j2}^s)^T \mathbf{t}_{j2}^s}$ .

The voltage injection bias  $\phi_{i,j}^{sy, V}$  is hard to be inferred through the information obtained from existing measuring facilities, but can be observed from extra sensor readings based on the physical couplings between DERs. This idea is made feasible as the electrical and communication graphs share the same topology, and thus the electrical coupling between DERs can be utilised to observe the legitimate voltage information transmitted through the corresponding communication link. After installing current sensors on the power lines interconnecting DERs, from which the power line current is securely

measured as  $I_{ij}^{se}$ , the voltage bias injection can be accurately observed when DER  $i$ 's local sensor channels are free from attacks, i.e.,

$$\begin{aligned} \phi_{i,j,V}^{sy,ob}(k) &= \boldsymbol{\kappa}^T \mathbf{y}_{i,j}^s(k) - \underbrace{(\boldsymbol{\kappa}^T \mathbf{y}_i^p(k) - R_{ij} I_{ij}^{se}(k))}_{V_{i,j}^{ob}(k)} \\ &\approx \phi_{i,j,V}^{sy}(k), k \geq k_{i,j}^{sa}, \end{aligned} \quad (25)$$

because the inductive part of DC power line is negligible, i.e.,  $L_{ij} \approx 0$ , where  $V_{i,j}^{ob}$  is the DER  $j$ 's PCC voltage observed by DER  $i$  through the power line coupling. The observation  $\phi_{i,j,V}^{sy,ob}(k)$  can be available at the alarming time instant  $k_{i,j}^{sa}$  as only local information is required, but the reconstruction scheme (24) will be activated in the next time instant  $k_{i,j}^{sa} + 1$  to make the reconstructed bias accurate enough, because the scheme needs to incorporate the bias information at the previous time instant. Benefiting from the development of non-contact measuring technologies like the hall effect current sensor, which operates through generating hall voltage proportional to the current and magnetic field and has been widely adopted in commercial solar inverters [34], [35], the power line current can be measured without breaking the original circuit connection.

### C. Theoretical Performance Analysis

Although the reconstruction scheme (24) is derived from the theoretical links between residuals and bias injections (23), the accuracy of reconstructed bias can be still affected by the initial reconstruction error and system noise. It is necessary to theoretically analyse the reconstruction performance when suffering from these unknown disturbances.

**Proposition 1:** Under the bias reconstruction scheme (24), when the bias observations are accurate as claimed in (25), the steady-state current bias reconstruction error, denoted by  $\varphi_{i,j,I}^{sy}(k) = \phi_{i,j,I}^{sy}(k) - \phi_{i,j,I}^{sy,re}(k)$ , will be bounded by

$$|\varphi_{i,j,I}^{sy}(\infty)| \leq \frac{(|\tilde{\mathbf{t}}_{j2}^s|)^T \bar{\boldsymbol{\chi}}_{i,j}^s}{1 - \eta_j^s}, \quad (26)$$

if the eigenvalue of the reconstruction dynamics (24), i.e.,  $\eta_j^s$ , satisfies

$$|\eta_j^s| = |(\tilde{\mathbf{t}}_{j2}^s)^T T_j^s A_{jj}^d \boldsymbol{\iota}| < 1, \quad (27)$$

where  $|\boldsymbol{\chi}_{i,j}^s(k)| \leq \bar{\boldsymbol{\chi}}_{i,j}^s = (|T_j^s| |\bar{\boldsymbol{\rho}}_j + |T_j^s A_{jj}^d| |\bar{\boldsymbol{\rho}}_j + |T_j^s| |\bar{\boldsymbol{\omega}}_j|)$  denotes the bound of the noise-related term in (23).

The proof of Proposition 1 is conducted in a straightforward manner through calculating the expressions of  $\varphi_{i,j,I}^{sy}$  considering initial reconstruction errors and system noises, whose details are provided in Appendix B. The establishment of (27) is critical in obtaining an accurate enough bias reconstruction result, under which the steady-state bounded reconstruction error (26) determined by the system noises' bounds can be guaranteed. Specifically, the impact of initial error on the steady-state bias reconstruction's accuracy can be eliminated by the stable eigenvalue  $\eta_j^s$  as the associated reconstruction error term will decay asymptotically to zero with time. While

the system noises can persistently affect the reconstruction accuracy, the accumulated reconstruction error by system noises is proved to be bounded by a known threshold under stable eigenvalue  $\eta_j^s$ . In the forthcoming part, we will analytically analyse the establishment of (27) under different RLC filter parameters by adopting appropriate approximations.

**Proposition 2:** When the products of sampling time  $T_{samp}$  and matrix  $A_{jj}$ 's entries, denoted by  $a_{jj}^{rc}, \forall r, c \in \{1, 2\}$ , satisfy  $|a_{jj}^{rc} T_{samp}| < 1$ , then  $\eta_j^s$  can be approximated as

$$\eta_j^s \approx \eta_j^{s,appr} = 1 + a_{jj}^{22} T_{samp}, \quad (28)$$

under which (27) will definitely hold since  $a_{jj}^{22} < 0$ .

The proof of Proposition 2 is proceed with the Taylor expansion of matrix exponential  $e^{A_{jj} T_{samp}}$  and the condition  $|a_{jj}^{rc} T_{samp}| < 1, \forall r, c \in \{1, 2\}$ , whose details are elaborated in Appendix C. Equation (28) means that the eigenvalue  $\eta_j^s$  is mainly determined by  $A_{jj}$ 's entry  $a_{jj}^{22}$  and the sampling time  $T_{samp}$ , while it is weakly associated with  $A_{jj}$ 's other entries and is irrelevant with the UIO matrix  $T_j^s$ . Moreover, the assumption of  $|a_{jj}^{rc} T_{samp}| < 1$  is reasonable because setting  $T_{samp}$  the same as the switching frequency of converters, e.g., 1kHz, can easily make it hold. Since numerous approximations have been adopted in the proof, the accuracy of approximation (28) and the establishment of condition (27) under various RLC filter parameters are validated through extensive numerical results in Section VI.

1) *Impact Mitigation:* The reconstructed bias vector  $\phi_{i,j}^{sy,re}$  is subtracted from the received compromised data  $\mathbf{y}_{i,j}^s$ , i.e.,

$$\mathbf{y}_{i,j}^{s,co}(k) = \mathbf{y}_{i,j}^s(k) - \phi_{i,j}^{sy,re}(k), k \geq k_{i,j}^{sa} + 1, \quad (29)$$

which is then used as corrected data to calculate the legitimate secondary control input as in (8). Since the reconstructed bias  $\phi_{i,j}^{sy,re}$  can approach the actual bias  $\phi_{i,j}^{sy}$  with a bounded error which is determined by the bounds of system noises, the adverse attack impact can be effectively eliminated by the mitigation action (29).

The implementation details of the proposed detection-triggered impact mitigation scheme is provided in Algorithm 1. In steps 1-8, the detection residual  $r_{i,j}^s$  and residual bound  $\mathbf{r}_{i,j}$  are calculated to check the establishment of conditions (19). The alarm signal  $\varrho_{i,j}^s$  will be flagged to trigger the bias reconstruction phase once any anomaly is perceived. Steps 9-20 elaborate the bias reconstruction process and impact mitigation action. If  $\varrho_{i,j}^s$  is flagged and there exists current sensor on power line ( $i, j$ ), the power line current will first be utilised to observe the voltage bias injection  $\phi_{i,j,V}^{sy,ob}$  through (25). Then, the current bias injection  $\phi_{i,j,I}^{sy,re}$  can be accurately reconstructed from the residuals under attacks  $r_{i,j}^{sa}$  and  $\phi_{i,j,V}^{sy,ob}$  according to (24). If there exists no current sensor within DER  $i$  for power line ( $i, j$ ), then the reconstructed bias will be set as  $\phi_{i,j}^{sy,re} = \mathbf{y}_{i,j}^s - \mathbf{y}_i$  such that the data received from DER  $j$  is unused. Finally,  $\phi_{i,j,I}^{sy,re}$  will be subtracted from the compromised data  $\mathbf{y}_{i,j}^s$  to eliminate the attack impacts on the secondary controller. Under the activated mitigation action, the safety criteria that implies the completion of attack impact



elimination is

$$\tilde{\alpha}_i(k) = \sum_{j \in \mathcal{N}_i^c} \left| \frac{\mathbf{y}_{i,j}^{s,co}(k)}{I_{ij}^s} - \frac{\mathbf{y}_i^p(k)}{I_{ti}^s} \right| \leq \tau, \quad (30)$$

where threshold  $\tau > 0$  is used to judge the accomplishment of load sharing from DER  $i$ 's view. The satisfaction of (30) does not mean that the mitigation actions can be deactivated as the SFDIA will exist all the time, and thus appropriate cyber recovery schedule should be made to remove the intruder from the communication network [36], which still requires substantial efforts and are as our future works.

---

**Algorithm 1** Detection-Triggered Impact Mitigation under  $\phi_{i,j}^{sy}$

---

**Input:** DER parameters  $A_{jj}^d, \mathbf{m}_j^d,$  and  $\mathbf{b}_j^d$ ; UIO $_{i,j}^s$  parameters  $F_j^s, T_j^s, H_j^s, \hat{K}_j^s$ ; Communicated DER  $j$ 's output  $\mathbf{y}_{i,j}^s$  and converter command  $u_{i,j}^s$ ; Residual bound parameters  $\nu_j^s, \zeta_j^s$ ; Secure power line current measurements  $I_{ij}^{se}$ .

**Output:** Detection residual  $\mathbf{r}_{i,j}^s$  and corresponding bound  $\bar{\mathbf{r}}_{i,j}^s$ ; Attack alarm flag  $\varrho_{i,j}^s$ ; Reconstructed current bias injection  $\phi_{i,j}^{sy, re}$ .

- 1: **Detection Phase**
  - 2: Calculate the detection residual  $\mathbf{r}_{i,j}^s$  according to (10)-(16)
  - 3: Calculate the residual bound  $\bar{\mathbf{r}}_{i,j}^s$  according to (18)
  - 4: **if** Either of (19) is satisfied **then**
  - 5:     Flag the alarm signal  $\varrho_{i,j}^s = 1$
  - 6: **else**
  - 7:     Reset the alarm signal  $\varrho_{i,j}^s = 0$
  - 8: **end if**
  - 9: **Bias Reconstruction and Impact Mitigation Phase**
  - 10: **if** The alarm signal  $\varrho_{i,j}^s$  is flagged **then**
  - 11:     **if** Current sensor has been deployed in DER  $i$  for power line  $(i, j)$  **then**
  - 12:         Observe the voltage bias injection through (25)
  - 13:         Reconstruct the current bias injection through (24)
  - 14:     **else**
  - 15:         Set  $\phi_{i,j}^{sy, re} = \mathbf{y}_{i,j}^s - \mathbf{y}_i$ ;      $\triangleright$  Discard the data received from DER  $j$
  - 16:     **end if**
  - 17: **else**
  - 18:     Reset the current bias injection as zero
  - 19: **end if**
  - 20: Eliminate the SFDIA's impacts on secondary controllers through (29)
- 

## V. COST-EFFECTIVE CURRENT SENSOR DEPLOYMENT

Given the high budget of deploying local current sensors on all power lines, a cost-effective deployment strategy is necessary to facilitate the proposed method's practical application. This section will first introduce a useful method that utilises the output current  $I_{ti}$  and PCC voltage  $V_i$  to estimate the sum of power line currents outputted from DER  $i$ , denoted by  $I_{i,se}^{sum} = \sum_{j \in \mathcal{N}_i^{el}} I_{ij}^{se}$ , which can help avoid the deployment of redundant current sensors. Based on this, a cost-effective sensor deployment scheme will be then presented to keep only the necessary current sensors required by the secondary control performance.

### A. Estimation of Power Line Current Sum

According to the circuit of DER  $i$ , the relationships between the original measurements for primary control, i.e.,  $I_{ti}, V_i$ , and  $I_{i,se}^{sum}$  can be written as

$$I_{i,se}^{sum}(k) = I_{ti}(k) - \frac{C_{ti}}{T_{samp}}(V_i(k) - V_i(k-1)) - \hat{I}_{Li}^{sum}(k), \quad (31)$$

where  $\hat{I}_{Li}^{sum}$  denotes the sum estimation of currents flowing over the ZIP load obtained either from historical load data [37], [38] or via load forecasting methods [39], [40]. In the ideal case, the estimated sum of load currents should satisfy  $\hat{I}_{Li}^{sum} = I_{Li} + \frac{V_i}{Z_{Li}}$ . Although there can be some errors between the sum estimation and actual one due to the elusive load usage behaviours, these load estimation errors can be kept below a certain threshold from the long term such that the resulted mitigation actions would still be able to significantly decrease the attack impact as validated in Section VI-B.

The utilisation of (31) can decrease the number of extra current sensors required by the proposed mitigation scheme. In particular, since the sum of currents outputted from DER  $i$  is known, it is not necessary to measure all power line currents and one redundant current sensor can be removed. For example, if DER  $i$  has only one power line connecting it to other DERs, then the estimated current sum can be directly regarded as its power line current.

### B. Cost-Effective Deployment Strategy of Current Sensors

Besides integrating the estimated sum of power line currents (31), the deep analysis of secondary control's objective can further decrease the number of deployed current sensors. The secondary controller (8) is designed to achieve load sharing among DERs through an essential consensus principle, and one of its sufficient condition is to have a connected communication graph [29]. However, in practice, more dense communication network may be developed to guarantee the efficient and robust collaboration of DERs in microgrids. The dense communication network means that the corresponding graph would be still connected even though one or more edges are removed, under which load sharing can be still achieved, but in a slower convergence rate. Therefore, from a cost-effective perspective, the extra current sensors can be strategically deployed on the power lines that makes the "secured" communication links form a spanning tree, i.e., a connected sub-graph possessing the least number of edges. Here, the "secured" communication link means that the legitimate data transmitted over it can be reconstructed by the proposed scheme. A cost-effective deployment strategy of current sensors will be presented in the subsequent part.

The deployment of current sensors consists of two phases as shown in Algorithm 2. *Phase 1*: Selecting a spanning tree sub-graph  $\mathcal{G}'_c = \{\mathcal{A}, \mathcal{E}'_c\}$  of  $\mathcal{G}_c$  that connects DER nodes with the least number of edges and forms no circle. The selection is started from removing edges from the original edge set  $\mathcal{E}_c$ , where the removed edges and associated nodes are collected in  $\mathcal{E}_c^{rm}$  and  $\mathcal{A}^{rm}$ , respectively. The removed edge should be a part of a cycle that is found through depth-first-search based function, i.e., *findcycle*, which has linear time and space complexity with respect to the size of searched graph. In step

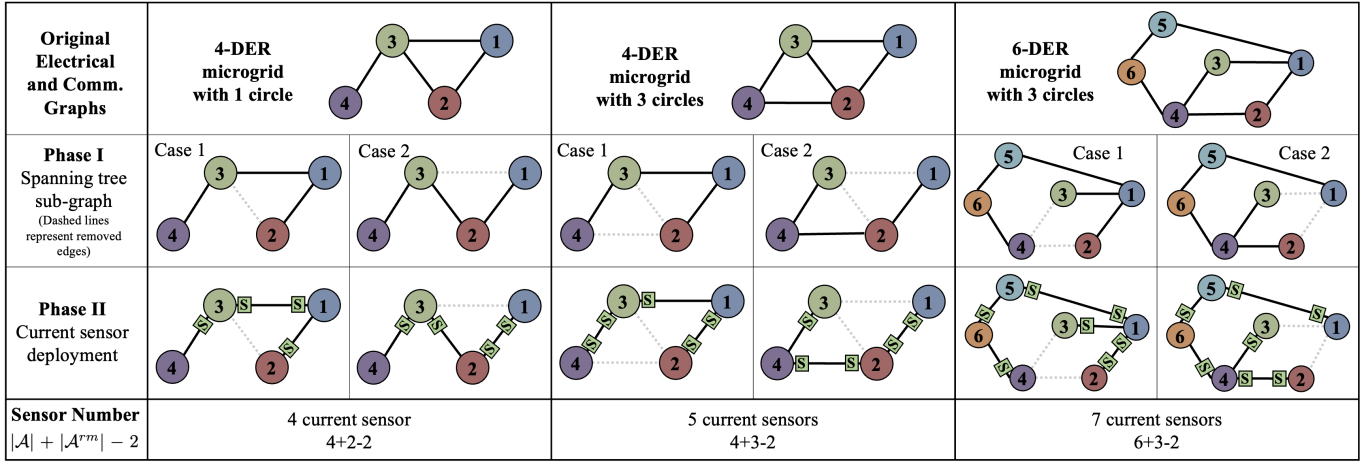


Fig. 6: This figure demonstrates the cost-effective deployment of current sensors on power lines under electrical and communication graphs with various size and density. It is clear that as the increase of network size and density, the number of deployed sensors will grow accordingly.

3, the edge set returned by  $findcycle$  is recorded as  $\mathcal{E}_c^{cy}$ . In steps 5-11, for each edge  $(i, j)$  in  $\mathcal{E}_c^{cy}$ , it will be used to update  $\mathcal{E}_c^{rm}$  and  $\mathcal{A}^{rm}$  if nodes  $i$  or  $j$  has been covered by the removed node sets. Otherwise, through steps 12-16, the edge of  $\mathcal{E}_c^{cy}$  covering the highest connectivity node will be chosen to update  $\mathcal{E}_c^{rm}$  and  $\mathcal{A}^{rm}$ . Then, the spanning tree sub-graph can be obtained as  $\{\mathcal{A}, \mathcal{E}_c / \mathcal{E}_c^{rm}\}$  as in step 17. The reason for removing the edge within cycle  $\mathcal{E}_c^{cy}$  that has overlap with the removed node set  $\mathcal{A}^{rm}$  is to keep the size of  $\mathcal{A}^{rm}$  as small as possible. Since the electrical and communication graphs have the same topology, the resulted spanning tree edge set  $\mathcal{E}_c / \mathcal{E}_c^{rm}$  can be mapped into the electrical graph equally. Therefore, the smaller  $\mathcal{A}^{rm}$  means that the mapped spanning tree sub-graph can cover more DER nodes that have complete adjacent physical couplings, under which more redundant current sensors can be removed based on the estimated sum of power line currents (31) in the next phase. Moreover, when there exists no overlap between  $\mathcal{E}_c^{cy}$  and  $\mathcal{A}^{rm}$ , the edge covering the highest connectivity node will be used to update the removed edge and node sets, which can maximise the overlap possibility in the subsequent cycle traversal.

*Phase II:* Deploying current sensors on power lines based on the obtained spanning tree edge set  $\mathcal{E}_c / \mathcal{E}_c^{rm}$  and (31). In step 21, the sensor deployment positions, which are recorded as directed edges since the current sensor is deployed by each local DER and its readings will not be shared with the neighbouring DER, are initialised as  $\mathcal{E}'_{el}$  that contains all spanning tree edges in  $\mathcal{E}_c / \mathcal{E}_c^{rm}$ . Through steps 22-26, if all adjacent physical couplings of DER  $i$  are included in  $\mathcal{E}'_{el}$ , then there is one redundant sensor deployment according to (31) and one arbitrary adjacent edge can be removed. In general, the number of deployed current sensors is calculated as  $|\mathcal{A}| + |\mathcal{A}^{rm}| - 2$ , which is proportional to the network size and density since  $|\mathcal{A}^{rm}|$  will increase as the number of included circles.

Demonstrative examples are given in Fig. 6 to illustrate the results of Algorithm 2. For a 4-DER microgrid with 1 circle, 4 current sensors are needed to ensure load sharing under worst-case SFDIAs. When the number of circles grows

to 3, one more current sensor is needed to maintain the control performance. Under the same number of circles, if the number of nodes increases to 6, two more current sensors are required to cover the extended network size. Therefore, when the electrical and communication networks' size and density grow, the required security investment will also increase with a linear rate. Moreover, it is noted that Algorithm 2 may output multiple sensor deployment solutions, implying that other considerations like the criticality of communication link and DER node can be incorporated to further optimise the result. Future efforts are still needed to conduct insightful analysis towards this direction.

Compared with the hidden secure network [18] and digital twin [19], the proposed bias reconstruction scheme (24) does not need to run the extra hardware along with the original system. Moreover, the cost of installing current sensors, whose number grows linearly with respect to the network size and density, would be much cheaper than developing a standalone communication network or digital system. While the detection-triggered bias reconstruction scheme (24) can also avoid the limitation of requiring at least one trustworthy communication link between DERs to guarantee the resilient control performance as in [15]. Hence, the primary difference of the proposed detection-triggered bias reconstruction and impact mitigation scheme from existing literature is that it can effectively improve the impact mitigation performance in a cost-efficient manner.

It has great importance to discuss the adaptability of the proposed mitigation method to other types of FDIAs besides ① as demonstrated by Fig. 1. Since this paper focuses on reconstructing the bias injections on the interaction links between DERs, a natural consideration is to apply it to the cases with corrupted local measurements. When the local measurements sent to secondary controller are compromised under SFDIA ③, the proposed bias reconstruction scheme can be seamlessly used to reconstruct the legacy current measurement once one of its neighboring DERs can accurately estimate its PCC voltage through the physical interconnection. For the scenario where the local measurements received by primary

**Algorithm 2** Cost-Effective Current Sensor Deployment

---

**Input:** Electrical graph  $\mathcal{G}_{el}$ , Communication graph  $\mathcal{G}_c$   
**Output:** Spanning tree edge set  $\mathcal{E}_c/\mathcal{E}_c^{rm}$ , Current sensor positions  $\mathcal{E}'_{el}$

- 1: **Phase I: Select Spanning Tree Edge Set**
- 2: Set empty removed edge and node sets  $\mathcal{E}_c^{rm}, \mathcal{A}^{rm}$ ;
- 3:  $\mathcal{E}_c^{cy} = \text{findcycle}(\{\mathcal{A}, \mathcal{E}_c\})$ ;
- 4: **while**  $\mathcal{E}_c^{cy}$  is not empty **do**
- 5:   **for** Edge  $(i, j) \in \mathcal{E}_c^{cy}$  **do**
- 6:     **if**  $i \in \mathcal{A}^{rm}$  or  $j \in \mathcal{A}^{rm}$  **then**
- 7:       Update removed edge set  $\mathcal{E}_c^{rm} = \mathcal{E}_c^{rm} \cup (i, j)$ ;
- 8:       Update removed node set  $\mathcal{A}^{rm} = \mathcal{A}^{rm} \cup \{i, j\}$ ;
- 9:       Break;
- 10:    **end if**
- 11:   **end for**
- 12:   **if** There is no overlap between  $\mathcal{E}_c^{cy}$  and  $\mathcal{A}^{rm}$  **then**
- 13:     Choose  $(i, j) \in \mathcal{E}_c^{cy}$  that covers the highest connectivity node;
- 14:     Update removed edge set  $\mathcal{E}_c^{rm} = \mathcal{E}_c^{rm} \cup (i, j)$ ;
- 15:     Update removed node set  $\mathcal{A}^{rm} = \mathcal{A}^{rm} \cup \{i, j\}$ ;
- 16:    **end if**
- 17:     $\mathcal{E}_c^{cy} = \text{findcycle}(\{\mathcal{A}, \mathcal{E}_c/\mathcal{E}_c^{rm}\})$ ;
- 18: **end while**
- 19: Obtain the spanning tree sub-graph  $\{\mathcal{A}, \mathcal{E}_c/\mathcal{E}_c^{rm}\}$ ;
- 20: **Phase II: Deploy Current Sensors on Power Lines**
- 21: Let  $\mathcal{E}'_{el}$  cover all spanning tree edge set  $\mathcal{E}_c/\mathcal{E}_c^{rm}$ ;
- 22: **for**  $i \in \mathcal{A}$  **do**
- 23:   **if** All adjacent edges of node  $i$  are included in  $\mathcal{E}'_{el}$  **then**
- 24:     Remove one arbitrary adjacent edge from  $\mathcal{E}'_{el}$ ;
- 25:   **end if**
- 26: **end for**

---

controller are corrupted by PFDIA ⑤, the voltage estimation transmitted through the secondary communication network may not satisfy the primary control's real-time requirement. The proposed reconstruction scheme will be thus not able to reconstruct the legacy current and voltage measurements from the residual of one UIO due to the insufficient observability. Further improvements are required to make the bias injections on both current and voltage measurements observable from the UIO residuals. Moreover, the investigation of mitigation strategies under corrupted control commands, i.e., FDIAs ② and ④, has been well addressed by existing literature [11]–[13], [17]. But they all require the sensor channels to be free from attacks, and thus the reconstructed legal measurement from the proposed method can be a useful complement for them when both actuator and sensor channels are subject to bias injections.

## VI. SIMULATION STUDIES AND EXPERIMENTAL VALIDATIONS

This section first verifies the reconstruction stability under varying electrical parameters, and then validates the proposed detection-triggered impact scheme's effectiveness in Matlab/Simulink and cyber-physical microgrid testbeds. Specifically, a 16-DER microgrid is established in Matlab/Simulink

to demonstrate the proposed method's applicability to large-scale systems considering load variations, DERs plugging-in, and security budget limitation. Based on OPAL-RT simulator, raspberry pi, and EXata network modeling software, a cyber-physical 6-DER microgrid is setup to test the proposed method's performance in the presence of practical communication protocols and realistic attack events.

### A. Reconstruction Stability under Varying Parameters

As claimed in Propositions 1-2, the stability of bias reconstruction scheme (24) is determined by the reconstruction dynamics' eigenvalue  $\eta_j^s$ , which can be approximated as  $\eta_j^{s,appr}$  that is mainly related to the RLC resistive ( $R_{ti}$ ) and inductive ( $L_{ti}$ ) parameters as well as sampling time  $T_{samp}$ . Inspired by this, we first show that  $|\eta_j^s|$  under varying RLC capacitive parameter  $C_{ti}$  can be regarded as constant and is less than 1. Then, the variation of  $|\eta_j^s| < 1$  under varying  $R_{ti}, L_{ti}$ , and  $T_{samp}$  is demonstrated and explained with the approximation (28) from Proposition 2.

1) *Constant and Stable  $\eta_j^s$  under Varying  $C_{ti}$ :* By keeping  $R_{ti}, L_{ti}$ , and  $T_{samp}$  invariant as  $0.2, 1e-3$ , and  $5e-4$ , respectively, and perturbing  $C_{ti}$  within  $[1e-3, 10e-3]F$ , the values of  $\eta_j^s$  and  $\eta_j^{s,appr}$  are shown in the left part of Fig. 7. Clearly,  $\eta_j^s$  changes slowly around  $0.9 < 1$  and the variation range is smaller than  $2e-3$ . Moreover, the corresponding approximation error  $|\eta_j^s - \eta_j^{s,appr}|$  is bounded by  $5e-3$ , indicating that the approximation (28) is accurate enough.

2) *Stable  $\eta_j^s$  under Varying  $R_{ti}, L_{ti}$ , and  $T_{samp}$ :* The results of  $\eta_j^s$  and  $\eta_j^{s,appr}$  when varying  $R_{ti}$  and  $L_{ti}$  within  $[0.1, 1]\Omega$  and  $[1e-3, 10e-3]H$ , choosing  $T_{samp}$  from  $\{2.5e-4, 5e-4, 1e-3\}s$ , and keeping  $C_{ti}$  as  $2.2e-3$  are pictured in the right part of Fig. 7. The first observation is that  $|\eta_j^s|$  is always smaller than 1 regardless of the changes of  $R_{ti}, L_{ti}$ , and  $T_{samp}$ , indicating that the reconstruction scheme (24) is always stable under initial errors and system noises. Moreover, the approximation error  $|\eta_j^s - \eta_j^{s,appr}|$  is positively associated with  $L_{ti}$  and  $T_{samp}$  while is negatively related to  $R_{ti}$ . This phenomenon matches the description of Proposition 2, where the approximation can be more accurate with smaller  $|a_{jj}^{rc} T_{samp}|$  that can be caused by the decrease of  $L_{ti}, T_{samp}$  and increase of  $R_{ti}$ . The unacceptable approximation error usually occurs with large  $L_{ti}$  and small  $R_{ti}$ , under which the  $|\eta_j^s|$  will be far smaller than 1. Hence, the stability of the reconstruction scheme (24) is verified through theoretical analysis and numerical results.

### B. Applicability to the 16-DER Microgrid in Matlab/Simulink

This subsection demonstrates the reconstruction accuracy and mitigation performance when all communication links are affected by SFDIAs (9) in the 16-DER microgrid with a mesh topology as shown in Fig. 8. The RLC filter parameters are set as  $R_{ti} = 0.2\Omega, L_{ti} = 1e-3H$ , and  $C_{ti} = 0.5e-3F$ , the equivalent resistive loads are  $Z_{Li} = 10\Omega, \forall i \in \{1, \dots, 16\}$ , and the power lines' impedance are  $R_{ij} = 1.5\Omega, L_{ij} = 1.8e-6H, \forall (i, j) \in \mathcal{E}_{el}$ . The reference PCC voltages of DERs are set around 40V such that their average is equal to it. The communication network topology is considered to

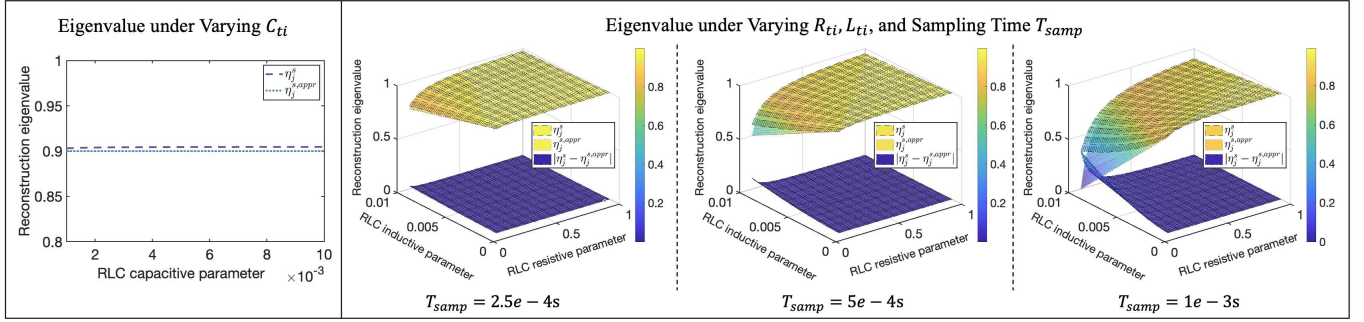


Fig. 7: In this figure, the left part shows that the  $\eta_j^s$  under varying  $C_{ti}$  is stable and can be regarded as constant, under which the approximation error  $|\eta_j^s - \eta_j^{s,appr}|$  is negligible. The right part verifies that  $\eta_j^s < 1$  is always stable under varying  $R_{ti}, L_{ti}$ , and  $T_{samp}$ , and that the approximation  $\eta_j^{s,appr}$  is accurate at most of the time except when  $\eta_j^s$  is far away from 1.

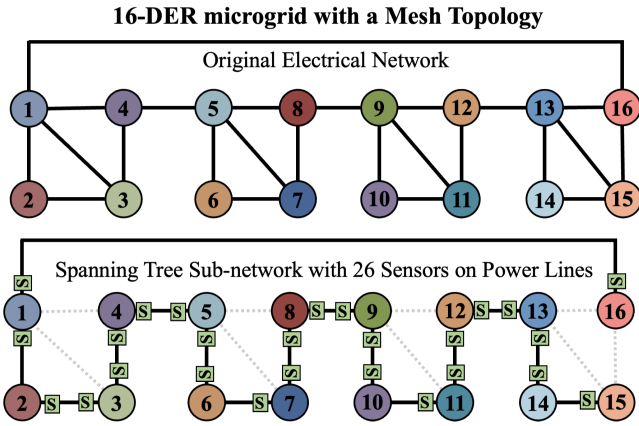


Fig. 8: This figure shows the original electrical network of the 16-DER microgrid, and then the secured spanning tree sub-network after deploying 26 sensors on power lines, where dashed lines represent the removed edges that do not require to deploy sensors.

be the same as the electrical network topology. The sampling time is  $T_{samp} = 1e - 3s$ , under which the stability condition (27) is satisfied. The event timeline is summarised as follows:

- The primary controllers are activated at  $t = 0s$ , where DERs 10 and 14 are not physically connected to other DERs.
- The secondary controllers are started at  $t = 1s$ , after which the UIO-based detectors are activated at  $t = 1.5s$ .
- DERs 10 and 14 are plugged into the microgrid to obtain the topology as shown in Fig. 8 at  $t = 3s$ .
- Variations occur on the equivalent current loads of DERs 1, 2, 5, 6, 9, 10, 13, 14 at  $t = 5s$ .
- SFDIAs that have continuous and discrete bias injections in the form of sine and triangle signals against all communication links are launched at  $t = 7s$ .

1) *Bias Reconstruction Accuracy*: The detection-triggered bias reconstruction results are shown in Fig. 9. We choose to demonstrate the bias reconstruction accuracy for the SFDIAs on communication links (2, 1), (6, 7), (10, 11), (14, 15) since they include the four types of bias injections and their reconstruction processes need to utilise the estimated sum of power line currents (31). According to the pictured results, it is clear that daily operations before  $t = 7s$  including load variation and DERs plugging-in will not falsely flag the

attack alarm and trigger the bias reconstruction scheme. When the SFDIAs are launched at  $t = 7s$ , the bias reconstruction scheme can be immediately triggered to accurately reconstruct both continuous and discrete bias injections with the steady-state reconstruction error smaller than 0.05 under 1% load estimation error. Due to the injected bias's sudden change at  $t = 7s$ , there will be a non-trivial initial reconstruction error that can reach 0.5. Under stable eigenvalue  $\eta_j^s$ , the initial reconstruction error will decay asymptotically to zero as time and eventually the reconstruction error can be bounded by a threshold determined by system noises and load estimation errors. For the discrete bias injections on links (10, 11), (14, 15), the detection residual can be occasionally lower than the threshold when the bias injections are small, which can result in unexpected missed alarms. To avoid this issue, the flagged attack alarm will be kept until the received data is validated as normal for  $N_{att} = 10$  sampling times.

When the load estimation error is increased from 1% to 10% and 20%, respectively, the bias reconstructed accuracy will be affected accordingly. The intuitive observation is the larger load estimation error can result in higher bias reconstruction error. Moreover, the same level of load estimation error may affect the reconstruction error differently when the DER's physical coupling varies. For example, the 10% load estimation error in DER 2 can increase the reconstruction error close to 0.5, while the same level of load estimation error in DERs 6, 10, 14 will only make the reconstruction error close to 0.2. It can be observed from Fig. 8 that DER 1 has 4 physical neighbors while DERs 6, 10, 14 only have 2 physical neighbors. It is noted that the load estimation error's impact on reconstruction error is very similar to that of system noise, and therefore deeper theoretical analysis can be conducted following the procedure in Proposition 1, which are left as our future works.

2) *Mitigation Performance*: The impact mitigation performance of utilising the reconstructed biases from the previous part under different levels of load estimation errors are demonstrated in Fig. 10. In the absence of mitigation strategies, the voltage and current states will be significantly affected by the injected SFDIA biases, under which the load sharing objective can never be achieved. To secure a spanning tree sub-network of the original communication network, 26 current sensors



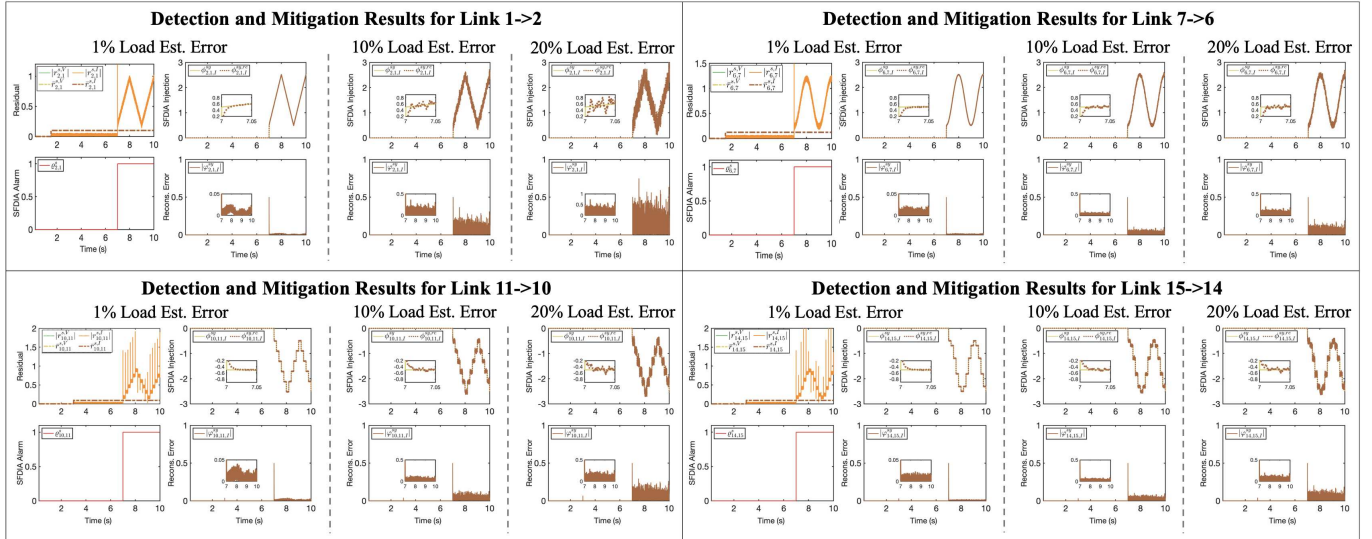


Fig. 9: This figure shows the detection and bias reconstruction results for the SFDIAs on links (2, 1), (6, 7), (10, 11), (14, 15), which includes both continuous and discrete bias injections in the forms of sine and triangle signals. Moreover, the demonstrated reconstruction processes all rely on the estimated load profile since there are reduced sensors deployed on the corresponding power lines as shown in Fig. 8. Hence, the impacts of different levels of load estimation errors on the reconstruction error are also showcased.

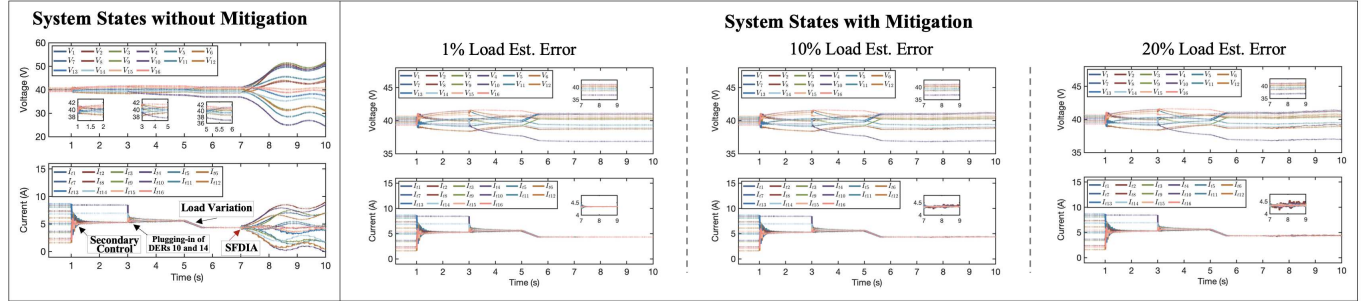


Fig. 10: This figure shows the voltage and current states of the 16-DER microgrid without and with impact mitigation strategies when all communication links are subject to SFDIAs. Moreover, the impact mitigation performance under different levels of load estimation errors are also validated.

should be deployed on power lines and Fig. 8 shows one feasible solution. According to Algorithm 1, if the detector perceives anomaly on the communication link and the corresponding power line's current cannot be sensed or estimated, then the communication link will be switched off. Otherwise, the bias reconstruction and impact mitigation scheme will be triggered. The results indicate that the reconstructed biases can effectively eliminate the attack impacts and reestablish the load sharing objective under 1% load estimation error. As the increase of load estimation error from 1% to 10%, 20%, there will appear obvious fluctuations on voltages and currents. For example, the steady-state currents will deviate from the expected sharing value with the error bounded by 0.5A. Although the mitigation performance can be slightly affected by the load estimation error, it is still able to significantly decrease the attack impact from 5A load sharing error to 0.5A load sharing error.

When the number of current sensors is too limited to form a spanning tree sub-graph for the 16-DER microgrid, the original microgrid can be partitioned into smaller clusters such that load sharing can be still achieved within these clusters under the worst-case SFDIA case. As shown in Fig. 11, if the 16-DER microgrid is partitioned into 4 clusters, then the number of sensors required for securing each cluster would only be 7,

5, 5, 3. After detecting SFDIAs, the power lines without current sensors including (4, 5), (8, 9), (12, 13), (13, 16), (15, 16) will be proactively cut off. The mitigation results indicate that load sharing objective can be successfully achieved within clusters based on the proposed method. The system operator needs to design appropriate partition mechanisms for microgrids to achieve the maximum social profit subject to the security budget for current sensors, which still requires future efforts and is as one of our future works.

### C. Experimental Validations in a cyber-physical 6-DER Microgrid Testbed

This subsection validates the proposed method's robustness against load variations and RES voltage fluctuations, the proposed method's superiority compared with the most related slope-based bias reconstruction method [14], and the proposed method's effectiveness against multiple discrete SFDIAs as well as its lightweight computation burden in a cyber-physical microgrid testbed that is setup in the Control and Power Systems (CAPS) Laboratory at the University of Sheffield.

Before showcasing the results, we will briefly introduce the cyber-physical microgrid testbed. As shown in Fig. 12, the testbed includes three key components, i.e., OPAL-RT OP5600



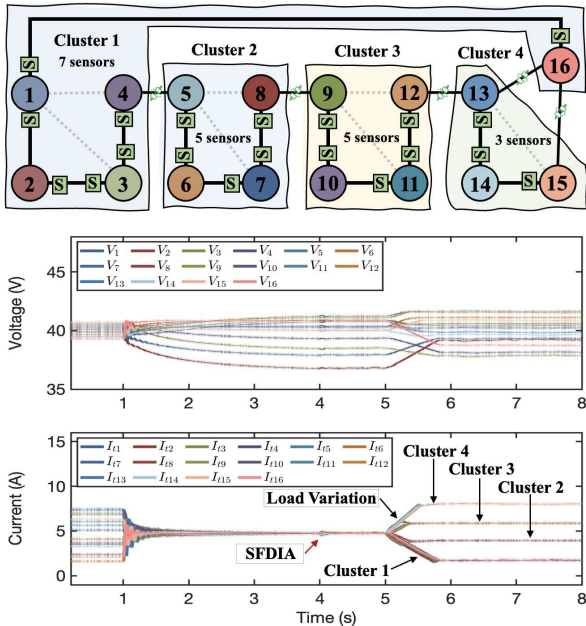
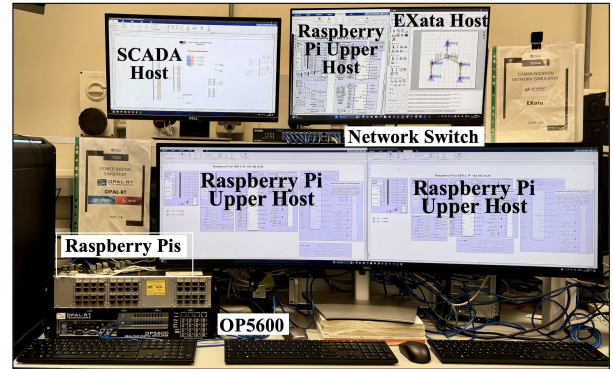


Fig. 11: This figure showcases a feasible partition scheme for the 16-DER microgrid to achieve the load sharing objective within partitioned clusters after proactively cutting off power lines (4, 5), (8, 9), (12, 13), (13, 16), (15, 16) when the number of current sensors is extremely limited.

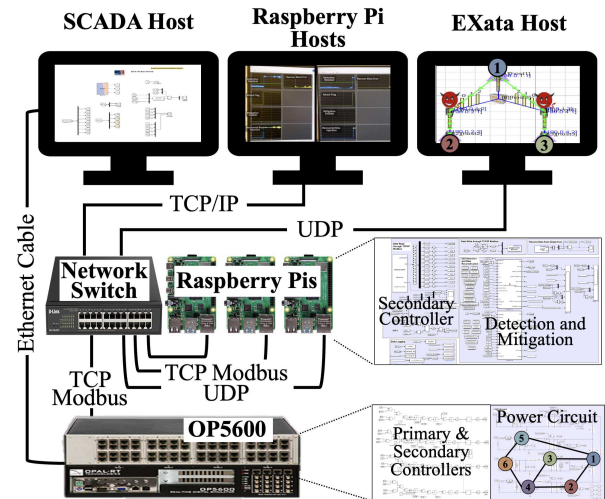
simulator, raspberry Pis, and EXata network modelling software. The 6-DER microgrid with the topology as shown in the last column of Fig. 6 is established and simulated in OPAL-RT OP5600 simulator, where the electrical parameters are set the same as in [26] and additional current sensors are deployed following the cost-effective strategy presented in Algorithm 2. Besides simulating the power circuit, OP5600 also implements primary controllers and half of secondary controllers. The remaining secondary controllers and proposed detection-triggered mitigation method are embedded into 3 raspberry Pis, which interact with OP5600 through TCP Modbus every 10ms. Two UDP data flows between raspberry pis are mapped into EXata via external node emulation mode, and realistic data modification events can be introduced against mapped data flows utilising the advanced cyber library provided by EXata. Three upper hosts are needed to run in parallel with the testbed to monitor and record the real-time data from OP5600 and raspberry Pis through Ethernet cables. In the experiments conducted within the cyber-physical microgrid testbed, the secondary controllers are activated at  $t = 2s$ , followed by the initialisation of UIO-based detectors at  $t = 4s$ .

1) *Robustness under Load Variation and RES Voltage Fluctuation:* Two daily events including current load increase within all DERs and 10% RES voltage fluctuations in DER 2 are introduced within  $t \in [6, 8]s$  and  $t \in [10, 14]s$ , respectively. As shown in Fig. 13, the introduced events will result in changes on PCC voltages and output currents, and slightly alter the residuals of three UIOs deployed in raspberry pis, denoted by  $r_{1,2}^s, r_{3,1}^s, r_{2,1}^s$ , which are still bounded by the appropriately chosen detection thresholds.

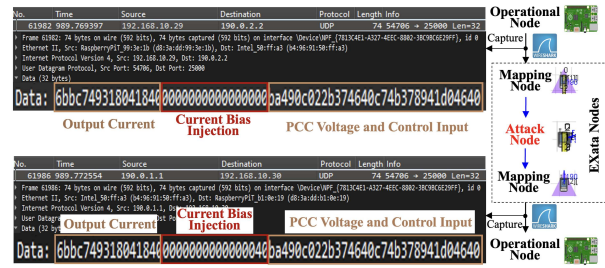
2) *Superiority compared with the Slope-based Bias Reconstruction Method [14]:* The slope-based method [14] was proposed to reconstruct the injected bias by observing the



(a) Overview of cyber-physical microgrid testbed



(b) Illustration of cyber-physical components and connections in the testbed



(c) Demonstration of SFDIA implementation in EXata

Fig. 12: Sub-figures (a) and (b) show the setup of a cyber-physical 6-DER microgrid in CAPS lab, where the microgrid circuit, primary controllers, and three secondary controllers are implemented in OPAL-RT OP5600 simulator, the remaining three secondary controllers and proposed detection-triggered mitigation schemes are run in raspberry Pis, and the data interaction between raspberry Pis are accomplished in EXata network modeling software. Sub-figure (c) demonstrates the SFDIA implementation in EXata. In particular, by interfacing operational nodes, i.e., raspberry Pis, with EXata nodes, the real-time data flows between operational nodes will be mapped into EXata. Through utilising the data modification function provided by EXata's cyber libraries, arbitrary bias injections can be introduced into DER's current measurements.

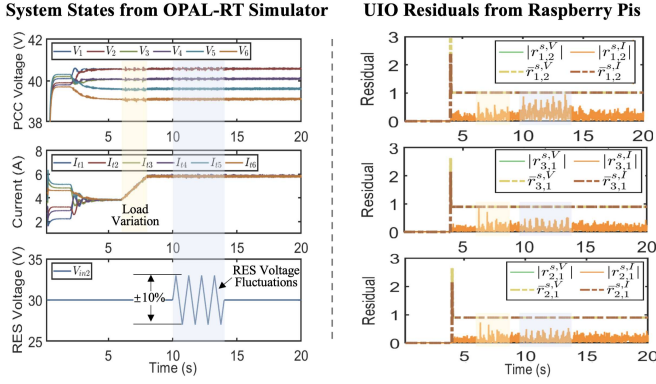


Fig. 13: This figure demonstrates the robustness of UIO residuals under load variations and RES voltage fluctuations.

resulted voltage changing slope, which was designed to be effective only for single constant injection. Therefore, this study chooses to compare the reconstruction and mitigation performance of our and slope-based methods when communication link (2,1) is subject to step and sine bias injections at  $t = 10s$ . The time window during which the voltage changing slope is observed is selected as 50 time steps to eliminate the impacts of voltage harmonics. According to the first two rows' results of Fig. 14, in the presence of step bias injection, the slope-based method can accurately reconstruct the constant bias injection after approximately 5s' observation, with the reconstruction error smaller than 0.2. After integrating the reconstructed bias, load sharing can be reestablished among DERs but the PCC voltages will have about 2V deviations from normal values. For the same step bias injection, our method is able to accurately reconstruct the bias injection immediately when attack alarm is flagged, with almost the same level of steady-state reconstruction error. The induced attack impact can be completely eliminated. Hence, our method can accurately reconstruct the constant bias injection much quicker than the slope-based method, and therefore achieve more comprehensive mitigation performance. Under sine bias injection, the slope-based method is not able to accurately reconstruct the injected bias as the resulted voltage changing slope varies too fast, and the adopted imprecise bias reconstruction is likely to destabilise the microgrid. On the contrary, our method can accurately reconstruct the time-varying sine bias injection and thoroughly eliminate the attack impact. Therefore, our method effectively supplements the slope-based method's limitation in addressing the non-constant bias injection and thus has wider application scenarios.

3) *Effectiveness against Multiple Discrete SFDIAs and Lightweight Computation Burden:* Besides the single continuous bias injection, the effectiveness of the proposed method against multiple discrete bias injections are also validated as shown in the last row of Fig. 14. When discrete sine and rectangle biases are injected into links (2,1) and (3,1), respectively, they can be reconstructed timely and accurately from the residuals generated by  $UIO_{2,1}^s$  and  $UIO_{3,1}^s$  that are deployed in raspberry pis 2 and 3. The discrete bias injection will not affect the reconstruction accuracy and the steady-state reconstruction errors can be always bounded by 0.3.

Moreover, the computation time of the proposed detection-triggered mitigation scheme in 3 raspberry Pis are recorded and shown in Fig. 15. In most cases, the computation time after activating UIOs will not exceed 0.005ms, and the computation time can increase to 0.1ms rarely, which, however, is still far smaller than the communication time step 10ms and thus is negligible. In light of these results, it is reasonable to claim that the proposed detection-triggered impact mitigation scheme is lightweight enough to run in parallel with the secondary controllers.

## VII. CONCLUSION

This paper proposed a novel detection-triggered recursive impact mitigation scheme against the SFDIA on communication links in cyber-physical microgrids, which overcomes the limitation of SFDIA detection and mitigation which requires at least one trustworthy neighboring link and only needs to install extra current sensors. With awareness of the physical interconnections among DERs, the voltage bias injection is observed from the power line current readings, based on which a recursive bias reconstruction scheme can be established to accurately obtain the current bias injection. The attack impact is eliminated by subtracting the reconstructed bias from the compromised communication data. To reduce the cost of deploying current sensors on power lines, a cost-effective deployment strategy is presented to secure a spanning tree subset of communication links that guarantees the secondary control performance. Extensive simulation studies and experimental validations were conducted to verify the correctness of the derived theoretical results, and to validate the effectiveness of the proposed method against single/multiple and continuous/discrete SFDIAs in the presence of load variations, DERs plugging-in, and RES voltage fluctuations. Future works include investigating the optimal current sensor deployment considering economic dispatch [41], [42], applying the proposed defence method to load frequency [43] and wind turbine [44] control, and integrating with advanced data-driven methods [45] to be prepared for wider cyber contingencies such as time delay and denial-of-service.

## ACKNOWLEDGEMENT

The authors would like to thank OPAL-RT for the collaboration between the University of Sheffield and OPAL-RT with real-time simulation solutions and software license support.

## APPENDIX

### A. DER System Parameters

$$A_{ii} = \begin{bmatrix} -\frac{1}{Z_{Li}C_{ti}} - \sum_{j \in \mathcal{N}_i^{el}} \frac{1}{C_{ti}R_{ij}} & \frac{1}{C_{ti}} \\ -\frac{1}{L_{ti}} & -\frac{R_{ti}}{L_{ti}} \end{bmatrix}, \mathbf{b}_i = \begin{bmatrix} 0 \\ \frac{1}{L_{ti}} \end{bmatrix} \\ \mathbf{m}_i = \begin{bmatrix} -\frac{1}{C_{ti}} \\ 0 \end{bmatrix} \quad (32)$$

$$A_{ii}^d = e^{A_{ii}T_{samp}}, Y_{ii}^d = (A_{ii})^{-1}(A_{ii}^d - I^2), \\ \mathbf{b}_i^d = Y_{ii}^d \mathbf{b}_i, \mathbf{m}_i^d = Y_{ii}^d \mathbf{m}_i. \quad (33)$$

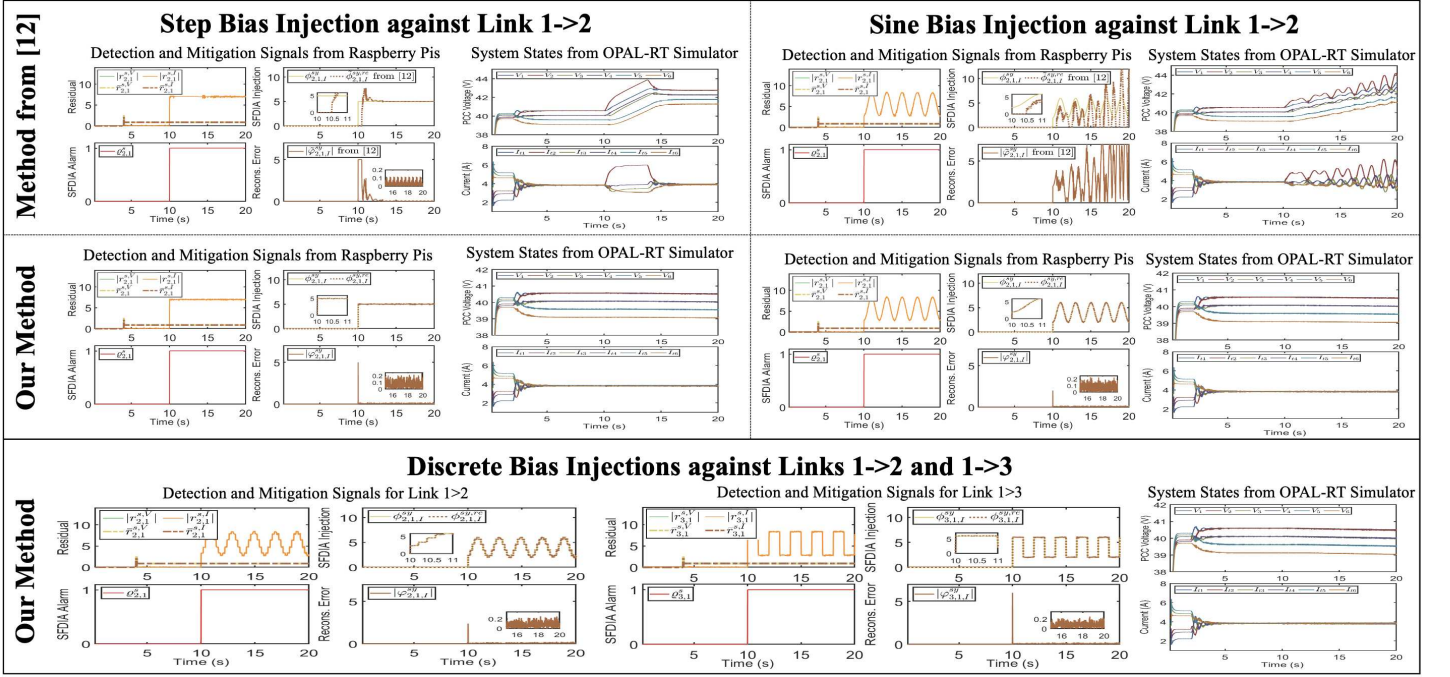


Fig. 14: The figure demonstrates the superiority of the proposed method compared with the slope-based bias reconstruction method from [14] (the first two rows) and its effectiveness against multiple discrete SFDIAs (the last row) based on the cyber-physical microgrid testbed.

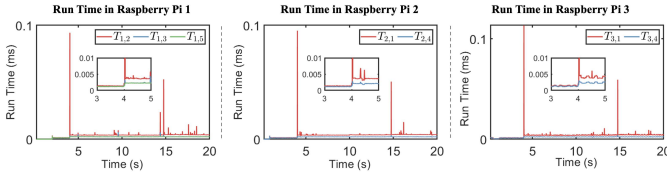


Fig. 15: This figure shows the computation time of the proposed detection-triggered impact mitigation scheme in raspberry pi.

### B. Proof of Proposition 1

**Proof:** Rewriting the reconstruction dynamics (24) for  $k \geq k_{i,j}^{sa}$  utilising its eigenvalue  $\eta_j^s$  as

$$\begin{aligned} \phi_{i,j,I}^{sy,rc}(k+1) &= \eta_j^s \phi_{i,j,I}^{sy,rc}(k) + (\tilde{\mathbf{t}}_{j2}^s)^T T_j^s A_{jj}^d \boldsymbol{\kappa} \phi_{i,j,V}^{sy,ob}(k) \\ &+ (\tilde{\mathbf{t}}_{j2}^s)^T \left( -\mathbf{t}_{j1}^s \phi_{i,j,V}^{sy,ob}(k+1) + \boldsymbol{\psi}_{i,j}^{sa}(k) \right). \end{aligned} \quad (34)$$

Following the same procedure, the original residual dynamics (23) for  $k \geq k_{i,j}^{sa}$  can be reformulated as

$$\begin{aligned} \phi_{i,j,I}^{sy}(k+1) &= \eta_j^s \phi_{i,j,I}^{sy}(k) + (\tilde{\mathbf{t}}_{j2}^s)^T T_j^s A_{jj}^d \boldsymbol{\kappa} \phi_{i,j,V}^{sy}(k) \\ &+ (\tilde{\mathbf{t}}_{j2}^s)^T \left( -\mathbf{t}_{j1}^s \phi_{i,j,V}^{sy}(k+1) + \boldsymbol{\psi}_{i,j}^{sa}(k) + \boldsymbol{\chi}_{i,j}(k) \right). \end{aligned} \quad (35)$$

Thus, the dynamics of reconstruction error for  $k > k_{i,j}^{sa}$  can be obtained by subtracting (34) from (35) as

$$\begin{aligned} \hat{\phi}_{i,j,I}^{sy,err}(k+1) &= \eta_j^s \hat{\phi}_{i,j,I}^{sy,err}(k) + (\tilde{\mathbf{t}}_{j2}^s)^T T_j^s A_{jj}^d \boldsymbol{\kappa} \hat{\phi}_{i,j,V}^{sy,err}(k) \\ &+ (\tilde{\mathbf{t}}_{j2}^s)^T \left( -\mathbf{t}_{j1}^s \hat{\phi}_{i,j,V}^{sy,err}(k+1) + \boldsymbol{\chi}_{i,j}(k) \right) \end{aligned} \quad (36)$$

where the voltage bias's estimation error  $\hat{\phi}_{i,j,V}^{sy,err}(k) = \phi_{i,j,V}^{sy}(k) - \phi_{i,j,V}^{sy,ob}(k)$  can be approximated as zero for  $k \geq k_{i,j}^{sa}$ . Thus, by direct calculation, the steady-state current bias reconstruction error after setting the initial bias injection values as

zeros can be obtained as

$$\begin{aligned} \phi_{i,j,I}^{sy}(\infty) &= (\eta_j^s)^\infty \left( \phi_{i,j,I}^{sy}(k_{i,j}^{sa}) \right) + \\ &+ \sum_{l=0}^{\infty} (\eta_j^s)^l (\tilde{\mathbf{t}}_{j2}^s)^T \boldsymbol{\chi}_{i,j}(l + k_{i,j}^{sa}). \end{aligned} \quad (37)$$

Since  $|\eta_j^s| < 1$  and  $|\boldsymbol{\chi}_{i,j}^s(k)| \leq \bar{\boldsymbol{\chi}}_{i,j}$ , the bound of  $|\phi_{i,j,I}^{sy}(\infty)|$  can be calculated as

$$|\phi_{i,j,I}^{sy}(\infty)| \leq \sum_{l=0}^{\infty} (\eta_j^s)^l (|\tilde{\mathbf{t}}_{j2}^s|)^T \bar{\boldsymbol{\chi}}_{i,j} = \frac{(|\tilde{\mathbf{t}}_{j2}^s|)^T \bar{\boldsymbol{\chi}}_{i,j}}{1 - \eta_j^s}, \quad (38)$$

which completes the proof.  $\blacksquare$

### C. Proof of Proposition 2

**Proof:** According to (12), we know that  $\mathbf{t}_{j1}^s = \zeta_j^{md} \mathbf{t}_{j2}^s$ , where  $\zeta_j^{md} = -\frac{m_{j2}^d}{m_{j1}^d}$  with  $\mathbf{m}_j^d = [m_{j1}^d, m_{j2}^d]^T$ . Thus, we have

$$\begin{aligned} \eta_j^s &= (\tilde{\mathbf{t}}_{j2}^s)^T T_j^s A_{jj}^d \boldsymbol{\kappa} = [(\tilde{\mathbf{t}}_{j2}^s)^T \mathbf{t}_{j1}^s, 1] A_{jj}^d \boldsymbol{\kappa} \\ &= [\zeta_j^{md}, 1] A_{jj}^d \boldsymbol{\kappa}, \end{aligned} \quad (39)$$

which implies that  $\eta_j^s$  is irrelevant with the UIO matrix  $T_j^s$  but is entirely determined by discrete-time system parameters  $A_{jj}^d$  and  $\mathbf{m}_j^d$ . According to (33), the derivation of  $A_{jj}^d$  and  $\mathbf{m}_j^d$  from  $A_{jj}$  and  $\mathbf{m}_j$  is closely related to the intractable matrix exponential term  $e^{A_{jj} T_{samp}}$ . To obtain the insight behind (39), the second-degree Taylor expansion for the approximation of  $e^{A_{jj} T_{samp}}$  is used for the subsequent analysis, i.e.,

$$e^{A_{jj} T_{samp}} = \sum_{l=0}^{\infty} \frac{1}{l!} (A_{jj} T_{samp})^l \approx \mathbf{I} + A_{jj} T_{samp} + \frac{1}{2} (A_{jj} T_{samp})^2, \quad (40)$$

where the higher-degree Taylor expansion term  $\sum_{l=3}^{\infty} \frac{1}{l!} (A_{jj} T_{samp})^l$  is sufficiently small since



$|a_{jj}^{rc}T_{samp}| < 1, \forall r, c \in \{1, 2\}$ . Based on (33) and (40), (39) can be approximated as

$$\eta_j^s \approx 1 + a_{jj}^{22}T_{samp} + \frac{1}{2}((a_{jj}^{22})^2 + a_{jj}^{12}a_{jj}^{21})T_{samp}^2 + \frac{a_{jj}^{12}a_{jj}^{21}T_{samp}^2(2 + (a_{jj}^{11} + a_{jj}^{22})T_{samp})}{2(2 + a_{jj}^{11}T_{samp})}. \quad (41)$$

Since  $a_{jj}^{11} \approx a_{jj}^{22}$ , we have  $\frac{2 + (a_{jj}^{11} + a_{jj}^{22})T_{samp}}{2 + a_{jj}^{11}T_{samp}} \approx 1$ , under which (41) can be further approximated as

$$\eta_j^s \approx 1 + a_{jj}^{22}T_{samp} + \frac{1}{2}(a_{jj}^{22}T_{samp})^2. \quad (42)$$

The last term in (42) is significantly smaller than the previous term due to  $|a_{jj}^{22}T_{samp}| \ll 1$ , and thus (28) can be obtained after ignoring the last term. With  $a_{jj}^{22} < 0$ , it can be easily inferred that (27) always holds, which completes the proof.

## REFERENCES

- [1] Vestas Wind Systems A/S, “Third update on cyber incident,” (Accessed: 2023). [Online]. Available: <https://www.vestas.com/en/media/company-news/2021/third-update-on-cyber-incident-c3466518>
- [2] Reuters, “Satellite outage knocks out thousands of enercn’s wind turbines,” (Accessed: 2023). [Online]. Available: <https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercn-wind-turbines-2022-02-28/>
- [3] Y. Xu, “A review of cyber security risks of power systems: from static to dynamic false data attacks,” *Protection and Control of Modern Power Systems*, vol. 5, no. 1, p. 19, 2020.
- [4] H. Yang, S. Li, Q. Li, and W. Chen, “Hierarchical distributed control for decentralized battery energy storage system based on consensus algorithm with pinning node,” *Protection and control of modern power systems*, vol. 3, pp. 1–9, 2018.
- [5] S. M. S. Hussain, T. S. Ustun, and A. Kalam, “A review of iec 62351 security mechanisms for iec 61850 message exchanges,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5643–5654, 2020.
- [6] 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 *NDSS*, 2017, pp. 1–15.
- [7] A. Barua *et al.*, “Hall spoofing: A non-invasive dos attack on grid-tied solar inverter,” in *USENIX Security*, 2020, pp. 1273–1290.
- [8] S. Peng, M. Liu, L. Chai, and R. Deng, “Dst-gnn: A dynamic spatiotemporal graph neural network for cyberattack detection in grid-tied photovoltaic systems,” *IEEE Transactions on Smart Grid*, pp. 1–1, 2024.
- [9] M. Liu, X. Zhang, H. Zhu, Z. Zhang, and R. Deng, “Physics-aware watermarking embedded in unknown input observers for false data injection attack detection in cyber-physical microgrids,” *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 7824–7840, 2024.
- [10] M. Liu, F. Teng, Z. Zhang, P. Ge, M. Sun, R. Deng, P. Cheng, and J. Chen, “Enhancing cyber-resiliency of der-based smart grid: A survey,” *IEEE Transactions on Smart Grid*, pp. 1–1, 2024.
- [11] S. Zuo, T. Altun, F. L. Lewis, and A. Davoudi, “Distributed resilient secondary control of dc microgrids against unbounded attacks,” *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3850–3859, 2020.
- [12] C. Deng, Y. Wang, C. Wen, Y. Xu, and P. Lin, “Distributed resilient control for energy storage systems in cyber-physical microgrids,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1331–1341, 2021.
- [13] Y. Wang, S. Mondal, C. Deng, K. Satpathi, Y. Xu, and S. Dasgupta, “Cyber-resilient cooperative control of bidirectional interlinking converters in networked ac/dc microgrids,” *IEEE Transactions on Industrial Electronics*, vol. 68, no. 10, pp. 9707–9718, 2021.
- [14] Z. Jin *et al.*, “Distributed data recovery against false data injection attacks in dc microgrids,” in *SmartGridComm*. IEEE, 2022, pp. 265–270.
- [15] S. Sahoo, T. Dragičević, and F. Blaabjerg, “Multilayer resilience paradigm against cyber attacks in dc microgrids,” *IEEE Transactions on Power Electronics*, vol. 36, no. 3, pp. 2522–2532, 2020.
- [16] S. Rath, L. D. Nguyen, S. Sahoo, and P. Popovski, “Self-healing secure blockchain framework in microgrids,” *IEEE Transactions on Smart Grid*, 2023.
- [17] M. S. Sadabadi, N. Mijatovic, J.-F. Tréguët, and T. Dragičević, “Distributed control of parallel dc–dc converters under fdi attacks on actuators,” *IEEE Transactions on Industrial Electronics*, vol. 69, no. 10, pp. 10 478–10 488, 2022.
- [18] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, “Resilient networked ac microgrids under unbounded cyber attacks,” *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3785–3794, 2020.
- [19] A. Saad *et al.*, “On the implementation of iot-based digital twin for networked microgrids resiliency against cyber attacks,” *IEEE transactions on smart grid*, vol. 11, no. 6, pp. 5138–5150, 2020.
- [20] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, “False data injection cyber-attacks mitigation in parallel dc/dc converters based on artificial neural networks,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 2, pp. 717–721, 2020.
- [21] M. R. Habibi *et al.*, “Decentralized coordinated cyberattack detection and mitigation strategy in dc microgrids based on artificial neural networks,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4629–4638, 2021.
- [22] Y. Xia, Y. Xu, S. Mondal, and A. K. Gupta, “A transfer learning-based method for cyber-attack tolerance in distributed control of microgrids,” *IEEE Transactions on Smart Grid*, pp. 1–1, 2023.
- [23] A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, and G. Ferrari-Trecate, “Distributed cyber-attack detection in the secondary control of dc microgrids,” in *IEEE European Control Conference (ECC)*, 2018, pp. 344–349.
- [24] A. J. Gallo *et al.*, “A distributed cyber-attack detection scheme with application to DC microgrids,” *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3800–3815, 2020.
- [25] M. Liu *et al.*, “Converter-based moving target defense against deception attacks in dc microgrids,” *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 3984–3996, 2022.
- [26] M. Liu, C. Zhao, J. Xia, R. Deng, P. Cheng, and J. Chen, “Pddl: Proactive distributed detection and localization against stealthy deception attacks in dc microgrids,” *IEEE Transactions on Smart Grid*, vol. 14, no. 1, pp. 714–731, 2023.
- [27] Y. Yu, G.-P. Liu, Y. Huang, and J. M. Guerrero, “Coordinated predictive secondary control for dc microgrids based on high-order fully actuated system approaches,” *IEEE Transactions on Smart Grid*, 2023.
- [28] R. Han, M. Tucci, A. Martinelli, J. M. Guerrero, and G. Ferrari-Trecate, “Stability analysis of primary plug-and-play and secondary leader-based controllers for DC microgrid clusters,” *IEEE Transactions on Power Systems*, vol. 34, no. 3, pp. 1780–1800, 2018.
- [29] M. Tucci, L. Meng, J. M. Guerrero, and G. Ferrari-Trecate, “Stable current sharing and voltage balancing in DC microgrids: A consensus-based secondary control layer,” *Automatica*, vol. 95, pp. 1–13, 2018.
- [30] H. Pu, L. He, P. Cheng, J. Chen, and Y. Sun, “Cormand2: A deception attack against industrial robots,” *Engineering*, vol. 32, pp. 186–201, 2024.
- [31] C. Brumfield, “Hijack of monitoring devices highlights cyber threat to solar power infrastructure,” Accessed: 2024, <https://www.csoonline.com/article/2119281/hijack-of-monitoring-devices-highlights-cyber-threat-to-solar-power-infrastructure.html>.
- [32] M. Liu, Z. Jin, J. Xia, M. Sun, R. Deng, and P. Cheng, “Demo abstract: A hil emulator-based cyber security testbed for DC microgrids,” in *IEEE INFOCOM 2021*, 2021, pp. 1–2.
- [33] J. Chen, R. J. Patton, and H.-Y. Zhang, “Design of unknown input observers and robust fault detection filters,” *International Journal of Control*, vol. 63, no. 1, pp. 85–105, 1996.
- [34] T. Instruments, “10kw 3-level 3-phase grid tie inverter reference design for solar string inverts (rev. a),” Accessed: 2024, [Online]. Available: <http://www.ti.com/lit/pdf/tidue53>.
- [35] Microchip, “Grid-connected solar microinverter reference design,” Accessed: 2024, [Online]. Available: <https://www.microchip.com/content/dam/mchp/documents/OTH/ApplicationNotes/ApplicationNotes/01444A.pdf>.
- [36] M. Liu, Z. Chu, and F. Teng, “Cyber recovery from dynamic load altering attacks: Linking electricity, transportation, and cyber networks,” *arXiv preprint arXiv:2309.03380*, 2023.
- [37] K. Lai and L. Zhang, “Sizing and siting of energy storage systems in a military-based vehicle-to-grid microgrid,” *IEEE Transactions on Industry Applications*, vol. 57, no. 3, pp. 1909–1919, 2021.
- [38] V. Vossos, K. Garbesi, and H. Shen, “Energy savings from direct-dc in us residential buildings,” *Energy and Buildings*, vol. 68, pp. 223–231, 2014.

- [39] R. Trivedi, S. Patra, and S. Khadem, "A data-driven short-term pv generation and load forecasting approach for microgrid applications," *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, vol. 3, no. 4, pp. 911–919, 2022.
- [40] M. Sun, T. Zhang, Y. Wang, G. Strbac, and C. Kang, "Using bayesian deep learning to capture uncertainty for residential net load forecasting," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 188–201, 2019.
- [41] B. Hu, H. Wang, and S. Yao, "Optimal economic operation of isolated community microgrid incorporating temperature controlling devices," *Protection and Control of Modern Power Systems*, vol. 2, no. 1, pp. 1–11, 2017.
- [42] H. Li, A. T. Eseye, J. Zhang, and D. Zheng, "Optimal energy management for industrial microgrids with high-penetration renewables," *Protection and Control of Modern Power Systems*, vol. 2, no. 2, pp. 1–14, 2017.
- [43] Z. Zhang, R. Deng, and D. K. Y. Yau, "Vulnerability of the load frequency control against the network parameter attack," *IEEE Transactions on Smart Grid*, pp. 1–1, 2023.
- [44] S. Zhao *et al.*, "Dual-triggered adaptive torque control strategy for variable-speed wind turbine against denial-of-service attacks," *IEEE Transactions on Smart Grid*, 2022.
- [45] Z. Zhang, M. Liu, M. Sun, R. Deng, P. Cheng, D. Niyato, M.-Y. Chow, and J. Chen, "Vulnerability of machine learning approaches applied in iot-based smart grid: A review," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 18951–18975, 2024.



**Rui Zhang** received the Ph.D. degrees in electrical and electronic engineering from the esteemed University of Manchester in 2012. He is currently a Technical Policy Manager, playing a vital role in shaping policies and strategies for the National Energy System Operator, U.K. With a strong background in power system control and operation, His research interests encompass a wide range of areas, including zero-carbon operation and whole energy system operation optimization.



**Zhuoran Zhou** (Student Member, IEEE) received the B.Sc. degree from the School of Mechanical Engineering and Automatic Control, Wuhan University, Wuhan, China, in 2020, and the M.Sc. degrees from School of Mechanical Engineering, Cranfield University, Cranfield, UK, in 2021. He is currently a Ph.D. Student with the Department of Automatic Control and System Engineering, University of Sheffield, U.K. His research interests include cyber-physical power systems, DC-microgrid modelling, and attack detection.



**Mengxiang Liu** (Member, IEEE) received the B.Sc. degree in Automation from Tongji University, Shanghai, in 2017 and the Ph.D. degree in Cyberspace Security from Zhejiang University, Hangzhou, in 2022. He is currently a Research Associate in Power Systems Engineering with the Department of Automatic Control and Systems Engineering, University of Sheffield, Sheffield, UK. His research interests include cyber resiliency, smart grid, active defense, and cyber-physical co-simulation.



**Zhenyong Zhang** (Member, IEEE) received the bachelor's degree from Central South University, Changsha, China, in 2015, and the Ph.D. degree from Zhejiang University, Hangzhou, China, in 2020. He is currently a Research Fellow with the College of Control Science and Engineering, Zhejiang University, Hangzhou, China. His research interests include cyber-physical system security, applied cryptography, machine learning security, and metaverse security.



**Xin Zhang** (Senior Member, IEEE) received the B.Eng. degree in automation and control systems from Shandong University, Jinan, China, in 2007, and the M.Sc. and Ph.D. degrees in electrical power engineering from The University of Manchester, Manchester, U.K., in 2007 and 2010, respectively. From 2011 to 2019, he was with National Grid Electricity System Operator, Wokingham, U.K. From 2019 to 2021, he was a Senior Lecturer with Cranfield University, U.K. From 2021 to 2023, he was an Associate Professor with Brunel University London, U.K. Currently, he is a Professor of control and power systems with the University of Sheffield, U.K. His research interests include power system control and operation, cyber-physical power systems modelling and digital simulation, and grid-integrated transport electrification. In 2022, he was a recipient of U.K. Research and Innovation (UKRI) Future Leaders Fellowship and U.K. Engineering and Physical Sciences Research Council (EPSRC) New Investigator Award.



**Ruilong Deng** (Senior Member, IEEE) received the B.Sc. and Ph.D. degrees both in Control Science and Engineering from Zhejiang University, Hangzhou, Zhejiang, China, in 2009 and 2014, respectively. He was a Research Fellow with Nanyang Technological University, Singapore, from 2014 to 2015; an AITF Postdoctoral Fellow with the University of Alberta, Edmonton, AB, Canada, from 2015 to 2018; and an Assistant Professor with Nanyang Technological University, from 2018 to 2019. Currently, he is a Professor with the College of Control Science and Engineering, Zhejiang University. His research interests include smart grid, cyber security, and control systems. Dr. Deng 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 Cloud Computing*, *IEEE Transactions on Emerging Topics in Computing*, *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, and *IET Cyber-Physical Systems: Theory & Applications*. He also serves/served as a Symposium Chair for *IEEE SmartGridComm*, *IEEE ICPS*, and *IEEE GLOBECOM*.