
Article:
Liu, M., Zhang, X. orcid.org/0000-0002-6063-959X, Zhao, C. et al. (1 more author) (2025) Matrix coding enabled impact mitigation against primary false data injection attacks in cyber-physical microgrids. IEEE Transactions on Power Systems. pp. 1-16. ISSN 0885-8950

https://doi.org/10.1109/tpwrs.2025.3528322

Matrix Coding Enabled Impact Mitigation against Primary False Data Injection Attacks in Cyber-Physical Microgrids

Mengxiang Liu, *Member, IEEE*, Xin Zhang, *Senior Member, IEEE*, Chengcheng Zhao, *Member, IEEE*, and Ruilong Deng, *Senior Member, IEEE*

***Abstract*—The impact mitigation against false data injection attacks (FDIAs) has become a prevailing topic in enhancing the cyber resilience of microgrids. In particular, the primary FDIA (PFDIA) injecting biases into the sensor channel of the primary controller can fake the real physical states and result in devastating control commands to the power conversion device. Nevertheless, existing impact mitigation schemes cannot handle the PFDIA due to the primary control's strict real-time requirement. Therefore, this paper proposes a time- and cost-efficient impact mitigation scheme against the PFDIA by alternately encoding the transmitted measurement with an invertible coding matrix. Specifically, when the PFDIA is detected by unknown input observers (UIOs), two additional half-downsampled UIOs, which only require simple multiplication, addition, and subtraction operations within each control cycle, will be triggered to obtain the residuals under encoded and unencoded data. The complete bias vector can be then reconstructed recursively from these two residuals, and the bias will be removed from the compromised data to eliminate the malicious attack impact. Based on the theoretical analysis of reconstruction performance, the coding matrix is optimised to minimise the system noises' impact on reconstruction accuracy subject to the reconstruction stability and the encoding's hiddenness from the adversary. Finally, extensive experimental studies are conducted to validate the effectiveness, superiority, robustness, and lightweightness of the proposed impact mitigation scheme.**

***Index Terms*—Power system security, communication system security, false data injection attack, attack mitigation, unknown input observer, microgrid**

I. Introduction

The Solarwind hack event disclosed in 2020 has been verified to affect thousands of enterprises and government agencies worldwide including the U.S. Department of Energy [1], attracting significant attentions on the cybersecurity issue of national critical infrastructure such as the power grid. The recently reported incidents against renewable energy companies including Enercon [2] and Vestas [3] imply that the massively penetrated distributed energy resources (DERs) are becoming the adversary's new targets under the rapid decarbonisation and digitalisation. Microgrids, which can manage the DERs in a local distribution area autonomously, have been widely implemented to integrate the massively penetrated DERs. It is thus necessary to analyse the potential cyber threats in microgrids and develop appropriate defense strategies to counter against them.

Focusing on cyber threats in operational technology, special attention is being paid to false data injection attacks (FDIAs) targeting the hierarchical control framework of microgrids [4], [5]. As shown in Fig. 1, the primary controller is responsible for the regulation of local states, whose references can be adjusted by the secondary controller to achieve global objectives such as load sharing [6]. Considering the cyber vulnerabilities from TCP/IP communication [7], supply chain [1], and field bus communication [8], five typical FDIAs against the primary and secondary controllers are demonstrated. These FDIAs can easily disrupt the control performance, induce voltage instability, and trigger protective isolation, finally resulting in cascading failure and power outage [9], [10]. Therefore, numerous defense strategies, including protection, detection, mitigation, and recovery, are needed to enhance the cyber resilience of microgrid under FDIAs [11]. This paper mainly focuses on the during-attack impact mitigation phase, which is usually activated after detecting anomaly to stabilise the system for the following-up recovery planning.

In full recognition of the vulnerabilities of standard TCP/IP based communication protocols [7], which are widely utilised in the information exchange between secondary controllers, many impact mitigation schemes have been proposed against the secondary FDIA (SFDIA) that tampers with communication data (①). Based on the realisation that the norm of the total disagreement in a DER will deviate from the norm of disagreements among neighbors during the SFDIA, Abhinav *et al.* devised trust-based cooperative controllers to mitigate the adverse impact on achieving consensus [12]. On perceiving that the received data is compromised, an event-driven attack-resilient controller was designed to replace it with the neighboring trustworthy signal to guarantee the synchronisation under up to $N-1$ attacked units [13]. By adaptively decreasing the weight of the communication link when it is subject to attacks, a resilience-enhanced secondary

This work was supported in part by the UK Research and Innovation Future Leaders Fellowship 'Digitalisation of Electrical Power and Energy Systems Operation (DEEPS)' under Grant MR/W011360/2; in part by the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant under Agreement MSCA-2023-PF-101149984; in part by the UK Engineering and Physical Sciences Research Council (EPSRC) New Investigator Award under Grant EP/W028905/1; in part by the Royal Society International Exchanges under Grant IEC\NSFC\242449. (Corresponding Author: Xin Zhang)

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

C. Zhao 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: {chengchengzhao, dengruilong}@zju.edu.cn).

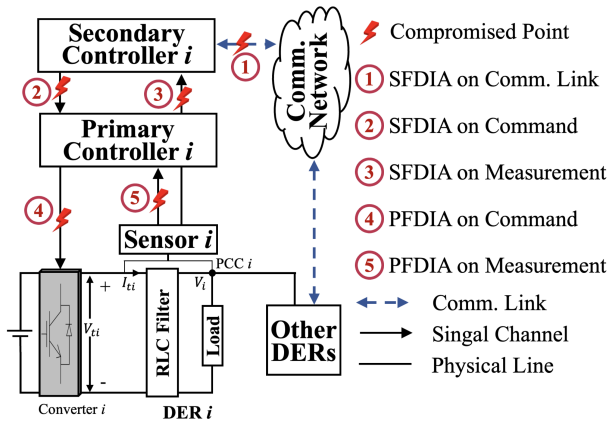


Fig. 1: This figure illustrates the five typical FDIAs against primary and secondary controllers in microgrids.

controller was presented to reduce the harmful consequence resulting from corrupted signals [14]. To address the instability induced by attacks, Leng *et al.* provided an optimal design framework for power electronic systems and extended the modeling prophecies to decipher the sensitivity analysis with respect to multi-valued cyber attacks [15]. In recognition of the power line interconnections between DERs, Liu *et al.* designed a detection-triggered recursive bias reconstruction scheme through strategically deploying current sensors on power lines [16].

Having equivalent severity with the corruption of communicated signal, the hijacking of controller has also been paid particular attention, especially with the increasingly disclosed supply chain vulnerabilities against critical infrastructure like the Solarwind [1]. Numerous impact mitigation approaches against the FDIAs on commands ②, ④, where ④ is one of the primary FDIAs (PFDIA). In utilisation of the adaptive control principle, resilient secondary cooperative controllers were developed to correct the actions of contaminated commands assuming that the secondary communication is attack-free [17]–[20]. By adopting the high-order differentiator [21] and sliding mode observer [22], Jiang *et al.* designed resilient secondary control algorithms to compensate for the adverse impacts induced by the SFDIAs against leader and follower nodes. Integrating the design of primary and secondary controllers into a framework, resilient cooperative control schemes with Lyapunov-based stability analysis was proposed to counter against the distorted secondary and primary control commands [23], [24]. With the introduction of a secure hidden layer enabled by advanced software-defined networking and blockchain technologies, resilient secondary controllers based on the virtual states that interact with the vulnerable communication network were provided to mitigate the impacts of both corrupted communication signals and distorted control commands [25]–[27].

With the adoption of industrial internet-of-things technologies, applications that connect field devices to the cloud have rapidly emerged, thereby exposing microgrid's unencrypted real-time sensor channels to potential FDIAs (③, ⑤) [28]. Utilising the DC-DC converter's voltage and current states as inputs, Habibi *et al.* trained an artificial neural network (ANN) to predict the parallel converter's point of common coupling (PCC) voltage reading such that the disruptive control action resulting from the SFDIA on PCC voltages (③) could be corrected [29]. Besides the centralised implementation, a fully decentralised ANN was then devised to recover the converter's legitimate output current by utilising only the local renewable source's current and voltage control error [30]. Considering the non-linearity resulting from the unknown constant power load (CPL), Cecilia *et al.* implemented a high-order sliding-mode observer to estimate the system states and CPL, which were then used for impact mitigation through reconstructing the attack signal which was injected into the local current measurement [31]. To address the aforementioned method's limitations in practical implementations including the high sensitivity to model uncertainty and measurement noise as well as the nonadjustable convergence rate, a novel observer consisting of the interconnection of three subsystems was designed to achieve reliable and rapid estimation of bias injections [32].

This paper mainly concerns about the impact mitigation method against the PFDIA on measurements (⑤). Although massive effort has been devoted to designing impact mitigation schemes against the SFDIA on communication links (①) and the FDIAs on control commands (②, ④), they are not applicable to handling the compromised primary measurements as the data exchange rate through secondary communication network (second level) cannot meet the strict real-time requirement of primary control (millisecond level). Similarly, the trained ANN networks utilizing local measurements [29], [30] might be also difficult to make predictions in the time scale of milliseconds to satisfy the primary controller's requirement. The recently proposed observer-based impact mitigation schemes [31], [32] can reconstruct the bias injection in a reliable and rapid manner, but the sound performance is built on a strong assumption that the voltage measurement is free from malicious bias injections. To sum up, a rapid and accurate impact mitigation scheme that can counter against the PFDIA tampering with voltage and current measurements simultaneously (⑤) is still lacking.

The unknown input observer (UIO) is an effective tool in estimating the system states in the presence of unknown input terms such as model uncertainty, and its effectiveness of detecting FDIAs has been fully illustrated [33]–[35]. The generated UIO residual not only reflects the measurement's inconsistency with DER dynamics, but also incorporates the information of injected biases, which may provide possible solutions for the bias reconstruction. Nevertheless, each UIO's reconstruction capability is limited and cannot deal with the case where multiple measurements are corrupted. The matrix coding is a lightweight encryption technology that first encodes the transmitted data by multiplying it with an invertible matrix and then decodes the received data by multiplying it with the coding matrix's inverse [36]. Besides ensuring the privacy of transmitted data, the matrix coding can also enable the detectability against stealthy FDIAs since the received data is not corrupted in the way expected by the adversary [37]. Inspired by the proactive perturbation capability of matrix coding, the UIO's limitation in bias reconstruction

may be resolved by encoding the transmitted data alternately. Specifically, after detecting the PFDIA through UIOs [33], the transmitted measurement vector will be encoded with an invertible coding matrix every two sampling periods. Then, two half-downsampled UIOs, which are linear and only require simple multiplication, addition, and subtraction operations within each control cycle, will be triggered to calculate the residuals under encoded and unencoded data. The complete bias vector can be reconstructed recursively from the two independent residuals and will be removed from the compromised data to mitigate the adverse impact. The main contributions of this paper are as follows:

- We propose a rapid and accurate bias reconstruction and impact mitigation scheme against the PFDIA ⑤ by alternately encoding the transmitted measurement vector with an invertible matrix, which is computation-friendly and does not require additional device.
- We theoretically analyse the reconstruction performance and prove that, under continuous bias injections, the steady-state reconstruction error will be bounded when the coding matrix is appropriately chosen.
- We provide an optimal design scheme for the coding matrix such that the system noise's impact on reconstruction accuracy are minimised subject to the reconstruction stability and the encoding's hiddenness from the adversary.
- We conduct extensive experimental studies in cyber-physical co-simulated and full-hardware microgrid testbeds to validate the effectiveness, superiority, robustness, and lightweightness of the proposed impact mitigation scheme.

II. System Model of Cyber-Physical Microgrid

We consider an isolated DC microgrid consisting of $N \geq 2$ DERs, where the DC-DC converter is commanded to supply the local ZIP load through a resistor-inductor-capacitor (RLC) filter as shown in Fig. 2. Let set $\mathcal{A} = \{1, \cdots, N\}$ include the DER nodes, then the cyber communication and physical electrical networks can be represented by weighted bidirectional graphs $\mathcal{G}_c = \{\mathcal{A}, \mathcal{E}_c\}$ and $\mathcal{G}_{el} = \{\mathcal{A}, \mathcal{E}_{el}\}$, respectively. The cyber edge set $\mathcal{E}_c$ consists of the communication links and their edge weights are denoted by $a_{ij}, \forall (i,j) \in \mathcal{E}_c$. Set $\mathcal{N}_i^c$ comprises the cyber neighbors of DER i. The physical edge set $\mathcal{E}_{el}$ collects the power lines and the edge weight is the corresponding line conductance, i.e., $\frac{1}{R_{ij}}, \forall (i,j) \in \mathcal{E}_{el}$. The physical neighbors of DER i are denoted by set $\mathcal{N}_i^{el}$.

Since the microgrid is operated around the nominal reference PCC voltage $V_{ref,i}$, the CPL $P_{CPL,i}$ can be linearised at this nominal point as $I_{CPL,i} = -\frac{P_{CPL,i}}{V_{ref,i}^2} V_i + 2\frac{P_{CPL,i}}{V_{ref,i}}$, where the former term is a negative impedance related to the actual PCC voltage V_i and the latter term is an equivalent constant current. Afterwards, the original ZIP load can be represented as an equivalent of constant impedance (Z_{Li}) and current (I_{Li}) loads, i.e.,

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

$$I_{Li} = I_{CCL,i} + 2\frac{P_{CPL,i}}{V_{ref,i}}, \tag{2}$$

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 (1)-(2), the dynamics of the RLC filter inside DER i can be acquired based on the Kirchhoff voltage and current laws and the quasi-stationary line approximation, i.e., $L_{ij} \approx 0$, as

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

where V_{ti} denotes the converter's regulated voltage, I_{ti} represents the output current from the DER such as renewable sources, and R_{ti}, L_{ti}, and C_{ti} are the RLC filter parameters. Denote the system state by $\boldsymbol{x}_i = [V_i, I_{ti}]^{\mathrm{T}}$, the system dynamics (3) can be rewritten as

$$\dot{\boldsymbol{x}}_i(t) = A_{ii} \boldsymbol{x}_i(t) + \boldsymbol{b}_i u_i(t) + \boldsymbol{m}_i d_i(t), \tag{4}$$

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

In line with the digital signal driven microcontroller, the continuous dynamical model (4) is discretized with sampling time T_{samp} and is augmented with fully measured system states along with bounded process and measurement noises, which is formulated as the regular state-space model:

$$\begin{cases} \boldsymbol{x}_i(k+1) = A_{ii}^d \boldsymbol{x}_i(k) + \boldsymbol{b}_i^d u_i(k) + \boldsymbol{m}_i^d d_i(k) + \boldsymbol{\omega}_i(k) \\ \boldsymbol{y}_i(k+1) = \boldsymbol{x}_i(k+1) + \boldsymbol{\rho}_i(k+1) \end{cases}, \tag{5}$$

where system parameters $A_{ii}^d, \boldsymbol{b}_i^d$, and $\boldsymbol{m}_i^d$ are derived from the original parameters in (4) and their connections are detailed in appendix A. The system states are fully measured as output vector $\boldsymbol{y}_i(k)$, and the 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 accurately track the reference PCC voltage, the primary control input $u_i(k)$ is calculated based on the following Proportional-Integral tracking algorithm as

$$u_i(k) = \left(\boldsymbol{g}_i^P\right)^{\mathrm{T}} \boldsymbol{y}_i^p(k) + g_i^I \sum_{l=0}^{k} \left(V_{ref,i} + \alpha_i(l) - \boldsymbol{\kappa}^{\mathrm{T}} \boldsymbol{y}_i^p(l) \right), \tag{6}$$

where $\boldsymbol{g}_i^P$ and g_i^I are proportional and integral control gains, respectively, $\boldsymbol{y}_i^p(k)$ is the local outputs available to the primary controller that is equal to $\boldsymbol{y}_i(k)$ in the normal case, and $\alpha_i(k)$ denotes the secondary control input that is computed by utilising the data transmitted over the secondary communication network. Constant vector $\boldsymbol{\kappa} = [1, 0]^{\mathrm{T}}$ is to extract the PCC voltage information for the derivation of accumulated voltage tracking errors.

The secondary controller is implemented on top of the

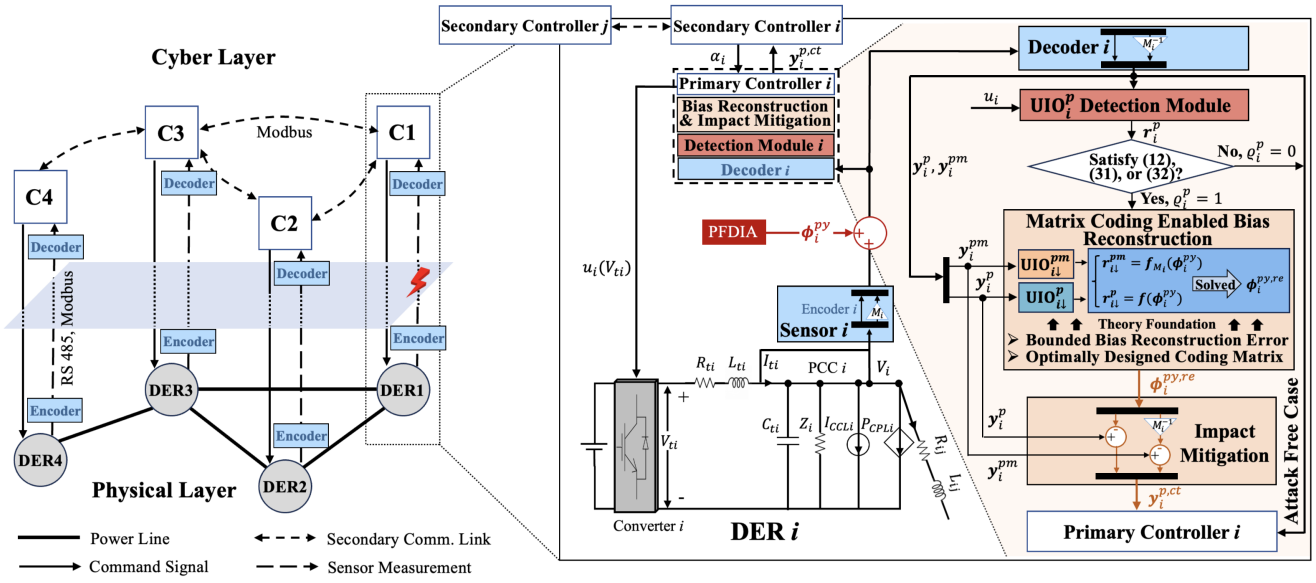


Fig. 2: In this figure, the left part depicts the cyber-physical architecture of microgrid, the middle part shows the detailed cyber-physical couplings and the PFDIA surface, and the right part illustrates the work flow of the proposed bias reconstruction and impact mitigation method based on two half-downsampled UIOs in the presence of alternate matrix coding.

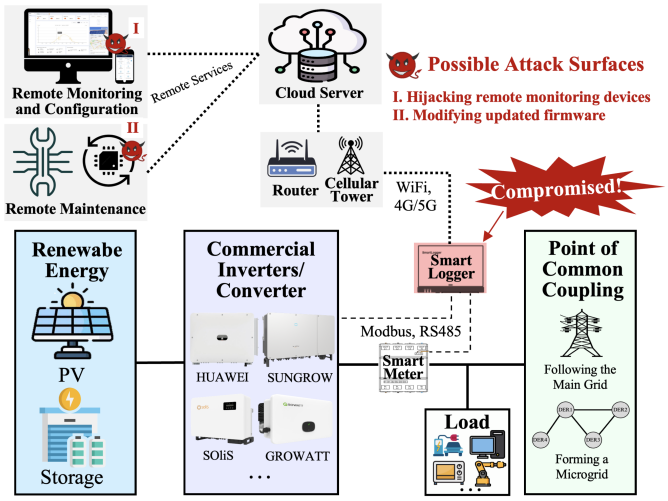
primary controller to regulate the voltage tracking reference utilising the incoming data from neighboring DERs to achieve the microgrid's overall objective such as current sharing [6]. Following the principle of distributed consensus control, the secondary control input is computed as

$$\alpha_i(k) = \boldsymbol{\iota}^{\mathrm{T}} \sum_{l=0}^{k} \sum_{j \in \mathcal{N}_i^c} a_{ij}^c \left(\frac{\boldsymbol{y}_{i,j}^s(l)}{I_{tj}^s} - \frac{\boldsymbol{y}_i^p(l)}{I_{ti}^s} \right), \tag{7}$$

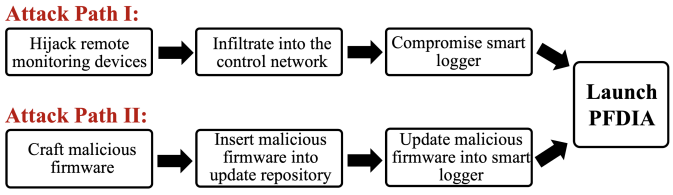
where $\boldsymbol{y}_{i,j}^s(k)$ denotes the output vector of DER $j \in \mathcal{N}_i^c$ transmitted over link $(i,j) \in \mathcal{E}_c$, which is equal to $\boldsymbol{y}_j^p(k)$ in the normal case, $I_{tj}^s > 0$ and $I_{ti}^s > 0$ are the rated output currents corresponding to DERs j and i, respectively, and constant vector $\boldsymbol{\iota} = [0,1]^{\mathrm{T}}$ is to extract the accumulated current discrepancy among DERs.

A. Attack Model

As the integration of standard field-level communication protocols such as RS485 and Modbus into grid-tied DER systems and microgrids, their scalability and interoperability have been greatly enhanced to enable the remote monitoring, configuration, and maintenance services for the massive penetration of renewable energy sources (RESs) as shown in subfigure (a) of Fig. 3. According to the user manuals of four mainstream inverter manufacturers including HUAWEI [38], SUNGROW [39], SOliS [40], and GROWATT [41], the smart meter's reading will be relayed to the inverter device installed near RESs via a smart logger, where the data exchanged is implemented through either RS485 or Modbus communication protocols, to achieve rapid and efficient control functionalities. The smart logger is also connected to the public internet via a router or cellular tower so that the logged data can be conveniently uploaded to the cloud server through advanced internet-of-things technologies such as WiFi and 4G/5G. The implemented architecture can provide the owner with numerous services including remote monitoring and configuration, and remote maintenance to conveniently operate and manage geographically dispersed RESs.



(a) Communication architecture supported by mainstream inverter manufacturers and practical attack surfaces according to recent attack accidents.



(b) Two attack paths by exploiting practical attack surfaces.

Fig. 3: This figure illustrates the communication architecture and protocols supported by four mainstream inverter manufacturers including HUAWEI [38], SUNGROW [39], SOliS [40], and GROWATT [41], two practical attack surfaces disclosed by recent attack incidents, as well as two attack paths by exploiting these practical attack surfaces.

However, the digitalisation of operation and management

process also exposes these critical RESs to numerous cyber threats. Following two practical attack surfaces disclosed by related attack incidents, we present two attack paths as shown in sub-figure (b) of Fig. 3 that may be exploited by the realistic adversary to launch PFDIAs. The most recent incident in 2024 was reported to hijack 800 remote monitoring devices of solar panels and successfully engage in bank account thefts [42]. It was addressed by security experts that the adversary is likely infiltrate into the RES control system through utilising the hijacked device as a springboard, adversely affecting the grid operation. In light of this critical attack surface, attack path I is presented: The adversary would first gain unauthorised access to the cloud server by hijacking remote monitoring devices, followed by lateral movement to infiltrate the field-level control network. By exploiting existing or zero-day cyber flaws, the smart logger could be eventually compromised to manipulate the data flow forwarded to the inverter/converter device. The infamous SolarWinds hack event in 2020 [1] was evidenced to affect thousands of enterprises and government agencies worldwide such as the U.S Department of Energy by inserting malicious code into the updated software, also known as supply chain attacks. Based on this well-known attack surface, attack path II is provided: The adversary would first craft malicious firmware and then insert it into the update repository after passing the integrity check for firmware [43]. Finally, the malicious firmware would be updated into the smart logger such that biases could be injected into the meter readings [44] after receiving remote hacker's commands via the preinstalled backdoor.

After justifying the possibility of launching PFDIAs within realistic communication architecture by exploiting practical attack surfaces, the subsequent will focus on illustrating PFDIA's mathematical model. In this paper, we consider the PFDIA that constantly injects biases into the primary controller's sensor readings. Specifically, in DER i, the PFDIA is modelled as

$$\text{PFDIA}: \quad \boldsymbol{y}_i^p(k) = \boldsymbol{y}_i(k) + \boldsymbol{\phi}_i^{py}(k) \tag{8}$$

where $\boldsymbol{\phi}_i^{py}$ denotes the *continuous* bias vector designed by the adversary to achieve malicious objectives [35]. The impact mitigation scheme in this paper is designed for general attack forms while not having other requirements besides the attack vector's continuity. Moreover, the adversary is assumed to have no knowledge of the DER electrical parameters, controller gains, and deployed mitigation strategies, under which it would be hard for the adversary to design the stealthy PFDIA vector that can bypass the UIO-based detector. It is noted here that the exclusion of stealthy PFDIAs is to ensure that all considered attacks are detectable by the UIO-based detector, while it does not mean that the proposed bias reconstruction scheme is applicable only to the random or naive PFDIAs. By contrary, the stealthy PFDIA vector could be accurately reconstructed once the attack alarm was successfully flagged for it, which, however, requires to improve the detectability of UIO-based detector against stealthy PFDIAs and could be possibly achieved through utilising the idea of moving target defense [34].

Moreover, although the PFDIA and measurement error have very similar impacts when viewed from the primary controller, they have essential differences in origination: 1) The measurement error denotes the measured quantity's deviation from its unknown true value and consists of random and systematical errors [45], where the former reflects unpredictable fluctuations of measurement apparatus's readings, and the latter is usually predictable and may be caused by imperfect calibration of measurement instruments. 2) The PFDIA (8) models the process where the adversary injects biases into transmitted measurements by compromising the smart logger. Their differences in origination make the corresponding countermeasures entirely different. For example, the idea of reconstructing bias injections through introducing matrix coding into the data transmission may not be applicable to the elimination of measurement errors as they already exist before transmitting them to the controller. In this paper, we mainly focus on the bias reconstruction scheme under PFDIAs, assuming that the measurement instrument has been configured properly to avoid systematical errors, and considering that the random measurement error can be modelled as bounded noise [46]. The bias reconstruction scheme will be designed to possess strong robustness against these bounded measurement noises as seen in the subsequent theoretical analysis (Section IV-B) and experimental validation (Section V-A) parts.

B. Unknown Input Observer based Attack Detection

The UIO has shown great potential in detecting FDIAs for large-scale interconnected systems such as microgrids [34], [35]. The essential idea is to use the discrepancy between actual measurements and estimated states to check if the trajectory of received data satisfies DER's physical dynamics (5). Specifically, the UIO_i^p that checks the integrity of local sensor readings is characterised by

$$\text{UIO}_i^p: \begin{cases} \boldsymbol{z}_i^p(k+1) = F_i^p \boldsymbol{z}_i^p(k) + T_i^p \boldsymbol{b}_i^d u_i(k) + \hat{K}_i^p \boldsymbol{y}_i^p(k) \\ \hat{\boldsymbol{x}}_i^p(k+1) = \boldsymbol{z}_i^p(k+1) + H_i^p \boldsymbol{y}_i^p(k+1) \end{cases}, \tag{9}$$

where $\boldsymbol{z}_i^p$ is UIO_i^p's internal state vector and $\hat{\boldsymbol{x}}_i^p$ is the estimated DER i's state vector. The UIO matrix F_i^p is chosen to be stable, i.e., the real parts of its eigenvalues should satisfy $|\lambda_l^{\text{re}}(F_i)| < 1, \forall l \in \{1, 2\}$, to converge the state estimation error and matrix T_i^p is designed satisfying $T_i^p \boldsymbol{m}_i^d = \mathbb{0}^{2\times 1}$ to eliminate the impact of unknown input d_i. The principles of choosing UIO matrices are provided in appendix B. The detection residual is derived by comparing the estimated state vector with the actual measurement vector as $\boldsymbol{r}_i^p(k) = \boldsymbol{y}_i^p(k) - \hat{\boldsymbol{x}}_i^p(k)$. In the normal operation, based on (5) and (9), the residual form can be derived as

$$\begin{aligned} \boldsymbol{r}_i^p(k) = (F_i^p)^k \big(\boldsymbol{r}_i^p(0) - T_i^p \boldsymbol{\rho}_i(0)\big) + T_i^p \boldsymbol{\rho}_i(k) \\ \sum_{l=0}^{k-1} \big(F_i^p\big)^{k-1-l} \big(T_i^p \boldsymbol{\omega}_i(l) - \hat{K}_i^p \boldsymbol{\rho}_i(l)\big), \end{aligned} \tag{10}$$

where the initial residual vector $\boldsymbol{r}_i^p(0) = \mathbb{0}^{2\times 1}$ can be acquired after strategically choosing the initial UIO state vector as $\boldsymbol{z}_i^p(0) = T_i^p \boldsymbol{y}_i^p(0)$. Given the bounded system noises, the upper

bound of $|\boldsymbol{r}_i^p|$ can therefore be calculated as

$$|\boldsymbol{r}_i^p(k)| \leq \bar{\boldsymbol{r}}_i^p(k) = \big(\nu_i^p(\varsigma_i^p)^k + 1\big)|T_i^p|\bar{\boldsymbol{\rho}}_i \\ \sum_{l=0}^{k-1} \nu_i^p(\varsigma_i^p)^{k-1-l}\big(|T_i^p|\bar{\boldsymbol{\omega}}_i + |\hat{K}_i^p|\bar{\boldsymbol{\rho}}_i\big), \quad (11)$$

where positive scalars $\nu_i^p \geq 1$ and $0 < \varsigma_i^p < 1$ are chosen such that $||(F_i^p)^k|| \leq \nu_i^p(\varsigma_i^p)^k$. The derived detection threshold in (11) can tolerate the fluctuations resulting from bounded system noises, and thus effectively avoiding the generation of false attack alarms for them.

Once either of the following conditions is satisfied, attack alarms will be triggered by UIO_i^p for the incoming data

$$r_{i,V}^p(k) > \bar{r}_{i,V}^p(k) \quad \text{or} \quad r_{i,I}^p(k) > \bar{r}_{i,I}^p(k), \quad (12)$$

where the residual elements are decomposed from $\boldsymbol{r}_i^p = [r_{i,V}^p, r_{i,I}^p]^{\mathrm{T}}$ and $\bar{\boldsymbol{r}}_i^p = [\bar{r}_{i,V}^p, \bar{r}_{i,I}^p]^{\mathrm{T}}$. Concurrently, the attack alarm $\varrho_i^p = 1$ will be flagged to indicate that the local measurement output $\boldsymbol{y}_i^p$ are suffering from FDIAs.

III. Motivating Example and Problem Formulation

The residual vector $\boldsymbol{r}_i^p$ generated by UIO_i^p can accurately and rapidly perceive the existence of naive PFDIAs [33]. Furthermore, its extensions for uncovering stealthy PFDIAs through strategically perturbing the converter control gains have been well demonstrated [34], [35]. After knowing the occurrence and location of PFDIAs, the forthcoming step is to adopt appropriate actions to mitigate and eliminate the attack impact. A hidden and often ignored fact is that the derived residual $\boldsymbol{r}_i^p$ not only reflects the inconsistency between the received data and the underlying DER physical dynamics, but also incorporates the information of bias injections, which may provide benefit for the reconstruction of these biases. To avoid confusions from the previous part, variable $\boldsymbol{r}_i^{pa}$ derived from $\boldsymbol{r}_i^p$ is adopted to denote the residual vector under PFDIAs, whose expression can be calculated from (5), (8), and (9) as

$$\boldsymbol{r}_i^{pa}(k+1) = F_i^p\boldsymbol{r}_i^{pa}(k) + T_i^p\boldsymbol{\phi}_i^{py}(k+1) + \\ - T_i^p A_{ii}^d\boldsymbol{\phi}_i^{py}(k) + \boldsymbol{\xi}_i^p(k+1), \quad (13)$$

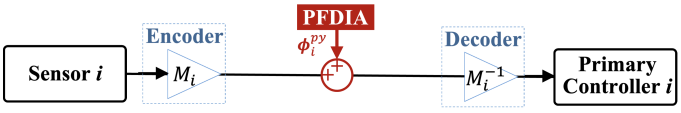
where term $\boldsymbol{\xi}_i^p(k+1) = T_i^p\boldsymbol{\rho}_i(k+1) - T_i^p A_{ii}^d\boldsymbol{\rho}_i(k) + T_i^p\boldsymbol{\omega}_i(k)$ denotes the system noise's impact. After neglecting the noise term, an intuitive bias reconstruction scheme can be derived from (13) as

$$T_i^p\boldsymbol{\phi}_i^{py}(k+1) = T_i^p A_{ii}^d\boldsymbol{\phi}_i^{py}(k) + \boldsymbol{\delta}_{i,r}^{pa}(k+1), \quad (14)$$

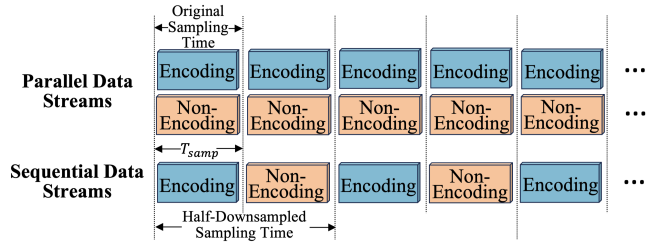
where term $\boldsymbol{\delta}_{i,r}^{pa}(k+1) = \boldsymbol{r}_i^{pa}(k+1) - F_i^p\boldsymbol{r}_i^{pa}(k)$ represents the residual discrepancy from the previous time instant.

The key deficiency of the reconstruction scheme (14) is that it is unable to obtain the complete bias vector $\boldsymbol{\phi}_i^{py}$ as matrix T_i^p is not full-column-rank according to (39), which means that at most one bias entry in $\boldsymbol{\phi}_i^{py}$ can be reconstructed from (14). Therefore, it is necessary to capture another relation between residuals and bias injections such that the complete bias vector can be reconstructed.

The matrix coding scheme provides a convenient way to capture the relation between residuals and bias injections in the presence of data encoding. As shown in sub-figure (a) of Fig. 4, in sensor i, the measurement vector $\boldsymbol{y}_i^p$ is first encoded, i.e., left multiplied by a coding matrix M_i, before being transmitted out. After receiving the encoded data at primary controller i, it is then decoded, i.e., left multiplied by the coding matrix's inverse M_i^{-1}, to obtain the actual measurement vector in normal cases. In the presence of PFDIAs, the encoded data will be contaminated with bias $\boldsymbol{\phi}_i^{py}$, under which the decoded data would be eventually calculated as $\boldsymbol{y}_i^p + M_i^{-1}\boldsymbol{\phi}_i^{py}$, where $M_i^{-1}\boldsymbol{\phi}_i^{py}$ denotes the bias injection after decoding. Therefore, the matrix coding scheme can be utilised to change the way in which the injected bias would contaminate the transmitted measurement vector. The resulting residual generated by UIO could reflect the bias's information after being left multiplied by M_i^{-1}. When integrated with (14), this may endow the ability of reconstructing bias vector $\boldsymbol{\phi}_i^{py}$, provided the coding matrix M_i is appropriately designed.



(a) Illustration of the principle of matrix coding.



(b) Two integration schemes of encoding and non-encoding data streams.

Fig. 4: This figure introduces the principle of matrix coding and two integration schemes (parallel and sequential) of encoding and non-encoding data streams.

It also requires some considerations on the integration scheme of the encoding and non-encoding data streams such that the two mentioned relations between residuals and bias injections can be successfully obtained for bias reconstruction. The intuitive idea is to have the encoding and non-encoding data streams in parallel as illustrated in sub-figure (b) of Fig. 4, which can perfectly capture the two relations in the original sampling rate and requires to establish only one extra UIO. However, the parallel data streams have two practical limitations: 1) The adversary can easily perceive the activation of mitigation strategy after observing the increase of data packet size, and may hesitate to inject bias into the added data segment, which will directly fail the bias reconstruction. 2) The extra data stream may increase the communication burden between sensors and primary controllers, which may result in severe communication latency and unacceptable control performance degradation.

To address the above mentioned limitations, this paper aims to integrate the encoding and non-encoding data streams in a sequential manner as shown in sub-figure (b) of Fig. 4. In particular, encoding and non-encoding data will be transmitted alternately with the original sampling rate such

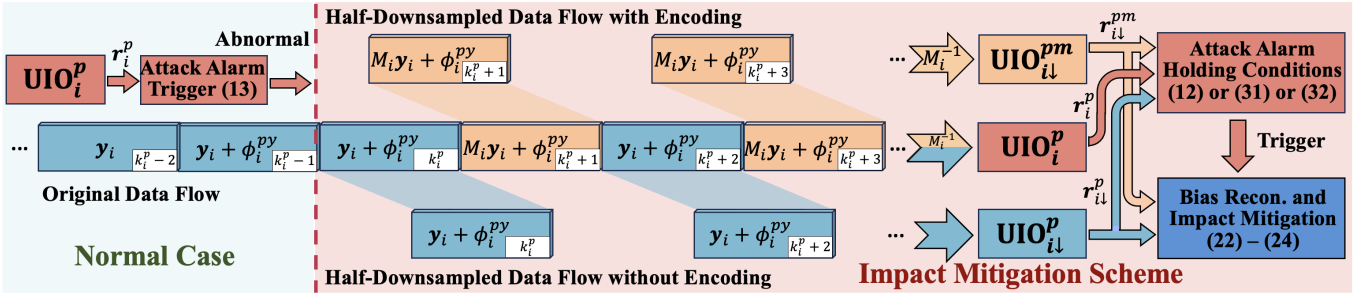


Fig. 5: This figure demonstrates the work flow of the matrix coding enabled impact mitigation scheme, where two half-downsampled $\text{UIO}_{i\downarrow}^{pm}$ and $\text{UIO}_{i\downarrow}^{p}$ are established to reconstruct the complete bias vector and the newly generated residuals $\boldsymbol{r}_{i\downarrow}^{pm}$ and $\boldsymbol{r}_{i\downarrow}^{p}$ are utilised to form the holding conditions (31) and (32) of attack alarm.

that the data stream can be kept unaltered to avoid unrealistic adversary assumptions and unacceptable control performance degradation. Two extra half-downsampled UIOs need to be established to capture the relations between residuals and bias injections, whose computation burden is negligible as only simple operations are involved as validated in Section V-A. Although the two half-downsampled UIOs synthesis the bias information at two consecutive sampling steps, the captured relations are still effective for bias reconstruction since the bias injection is assumed to be continuous and its values at two consecutive sampling steps in the scale of milliseconds can be almost regarded as consistent. In the subsequent sections, this paper will present the mathematical formulation and theoretical analysis of the proposed matrix coding enabled bias reconstruction scheme. The key issues needed to be sorted out include 1) Establishment of the relations between residuals and bias injections captured by half-downsampled UIOs, 2) Theoretical performance analysis of the proposed bias reconstruction scheme after integrating the two captured relations, and 3) Optimal design of coding matrix to ensure the stability of proposed bias reconstruction scheme and guarantee the encoding scheme's hiddenness from the adversary.

IV. Matrix Coding Enabled Bias Reconstruction and Impact Mitigation

This section first introduces the half-downsampled UIOs under alternate matrix coding, then provides the bias reconstruction and impact mitigation scheme, and finally optimally design the coding matrix considering the reconstruction accuracy and the encoding's hiddenness from the adversary. As shown in Fig. 5, after knowing the existence of PFDIA via (12), the measurement vector will be encoded by invertible matrix M_i every two sampling periods such that the bias injections with and without encoding can be synthesised by half-downsampled $\text{UIO}_{i\downarrow}^{p}$ and $\text{UIO}_{i\downarrow}^{pm}$, respectively, which are then utilised to reconstruct the complete bias vector. Before being sent to $\text{UIO}_{i\downarrow}^{p}$ and $\text{UIO}_{i\downarrow}^{pm}$, the encoded data will be decoded by M_i^{-1} to obtain the expected residuals for alarm holding and bias reconstruction. In particular, the newly generated residuals $\boldsymbol{r}_{i\downarrow}^{p}, \boldsymbol{r}_{i\downarrow}^{pm}$ will be incorporated into the holding conditions (31), (32) of attack alarm to eliminate the adverse impacts on attack detectability resulting from matrix coding.

A. Half-Downsampled UIOs under Alternate Matrix Coding

Once the attack alarm is flagged at k_i^p, two half-downsampled $\text{UIO}_{i\downarrow}^{p}$ and $\text{UIO}_{i\downarrow}^{pm}$ with reduced sampling rate $\frac{1}{2T_{samp}}$ will be established. They have the same UIO parameters, but need to be run alternately to synthesise the original and decoded bias injections into residuals. The forms of $\text{UIO}_{i\downarrow}^{p}$ and $\text{UIO}_{i,\downarrow}^{pm}$ for $l \in \{0, 1, 2, \cdots\}$ are written as

$$\text{UIO}_{i\downarrow}^{p}: \begin{cases} \boldsymbol{z}_{i\downarrow}^{p}(k+1) = F_{i\downarrow}^{p}\boldsymbol{z}_{i\downarrow}^{p}(k) + T_{i\downarrow}^{p}\boldsymbol{b}_{i\downarrow}^{d}u_i(k) + \hat{K}_{i\downarrow}^{p}\boldsymbol{y}_i^{p}(k) \\ \hat{\boldsymbol{x}}_{i\downarrow}^{p}(k+1) = \boldsymbol{z}_{i\downarrow}^{p}(k+1) + H_{i\downarrow}^{p}\boldsymbol{y}_i^{p}(k+1), k = k_i^p + 2l \end{cases} \tag{15}$$

and

$$\text{UIO}_{i\downarrow}^{pm}: \begin{cases} \boldsymbol{z}_{i\downarrow}^{pm}(k+1) = F_{i\downarrow}^{p}\boldsymbol{z}_{i\downarrow}^{pm}(k) + T_{i\downarrow}^{p}\boldsymbol{b}_{i\downarrow}^{d}u_i(k) + \hat{K}_{i\downarrow}^{p}\boldsymbol{y}_i^{pm}(k) \\ \hat{\boldsymbol{x}}_{i\downarrow}^{pm}(k+1) = \boldsymbol{z}_{i\downarrow}^{pm}(k+1) + H_{i\downarrow}^{p}\boldsymbol{y}_i^{pm}(k+1), k = k_i^p + 2l + 1 \end{cases}, \tag{16}$$

where the system parameters $A_{ii\downarrow}^{d}, \boldsymbol{m}_{i\downarrow}^{d}, \boldsymbol{b}_{i\downarrow}^{d}$ and UIO parameters $F_{i\downarrow}^{p}, T_{i\downarrow}^{p}, \hat{K}_{i\downarrow}^{p}, H_{i\downarrow}^{p}$ are obtained according to (37) and (38)-(42), respectively, with sampling step $2T_{samp}$. The time axis k of (15) and (16) is in line with sampling step T_{samp} for convenience of the subsequent analysis of bias reconstruction, and the alternate working mechanism of these two UIOs is reflected in the expanded terms of k.

Under the PFDIA (8), the decoded data would be $\boldsymbol{y}_i^{pm} = \boldsymbol{y}_i + M_i^{-1}\boldsymbol{\phi}_i^{py}$. For $\text{UIO}_{i\downarrow}^{p}$, the residual vector under PFDIA $\boldsymbol{r}_{i\downarrow}^{p} = \boldsymbol{y}_i^{p} - \hat{\boldsymbol{x}}_{i\downarrow}^{p}$ can be derived as

$$\begin{aligned} \boldsymbol{r}_{i\downarrow}^{p}(k+2) = {} & F_{i\downarrow}^{p}\boldsymbol{r}_{i\downarrow}^{p}(k) + T_{i\downarrow}^{p}\boldsymbol{\phi}_i^{py}(k+2) + \\ & - T_{i\downarrow}^{p}A_{ii\downarrow}^{d}\boldsymbol{\phi}_i^{py}(k) + \boldsymbol{\xi}_{i\downarrow}^{p}(k+2), k = k_i^p + 2l, \end{aligned} \tag{17}$$

where $\boldsymbol{\xi}_{i\downarrow}^{p}(k+2) = T_{i\downarrow}^{p}\boldsymbol{\rho}_i(k+2) - T_{i\downarrow}^{p}A_{ii\downarrow}^{d}\boldsymbol{\rho}_i(k) + T_{i\downarrow}^{p}\boldsymbol{\omega}_i(k)$ is the system noise related term. For $\text{UIO}_{i\downarrow}^{pm}$, the bias vector that affects the residual will be left multiplied by matrix M_i^{-1}, under which the residual vector $\boldsymbol{r}_{i\downarrow}^{pm} = \boldsymbol{y}_i^{pm} - \hat{\boldsymbol{x}}_{i\downarrow}^{pm}$ satisfies

$$\begin{aligned} \boldsymbol{r}_{i\downarrow}^{pm}(k+2) = {} & F_{i\downarrow}^{p}\boldsymbol{r}_{i\downarrow}^{pm}(k) + T_{i\downarrow}^{p}M_i^{-1}\boldsymbol{\phi}_i^{py}(k+2) + \\ & - T_{i\downarrow}^{p}A_{ii\downarrow}^{d}M_i^{-1}\boldsymbol{\phi}_i^{py}(k) + \boldsymbol{\xi}_{i\downarrow}^{p}(k+2), k = k_i^p + 2l + 1. \end{aligned} \tag{18}$$

B. Bias Reconstruction and Impact Mitigation

The equations (17) and (18) capture the relations between residuals and bias injections at even and odd sampling steps, respectively. To derive the explicit bias reconstruction scheme, the system noise term $\boldsymbol{\epsilon}_{i\downarrow}^{p}$ is ignored first, with its impact on the reconstruction accuracy being then investigated in Proposition

1. Therefore, equations (17) and (18) can be written together at $k = k_i^p + 2l$ as

$$\begin{cases} T_{i\downarrow}^p \boldsymbol{\phi}_i^{py}(k+2) = T_{i\downarrow}^p A_{ii\downarrow}^d \boldsymbol{\phi}_i^{py}(k) + \boldsymbol{\delta}_{i\downarrow,r}^p(k+2) \\ T_{i\downarrow}^p M_i^{-1} \boldsymbol{\phi}_i^{py}(k+3) = T_{i\downarrow}^p A_{ii\downarrow}^d M_i^{-1} \boldsymbol{\phi}_i^{py}(k+1) + \boldsymbol{\delta}_{i\downarrow,r}^{pm}(k+3) \end{cases}, \tag{19}$$

where $\boldsymbol{\delta}_{i\downarrow,r}^p(k+2) = \boldsymbol{r}_{i\downarrow}^p(k+2) - F_{i\downarrow}^p \boldsymbol{r}_{i\downarrow}^p(k)$ and $\boldsymbol{\delta}_{i\downarrow,r}^{pm}(k+3) = \boldsymbol{r}_{i\downarrow}^{pm}(k+3) - F_{i\downarrow}^p \boldsymbol{r}_{i\downarrow}^{pm}(k+1)$. Since the injected bias $\boldsymbol{\phi}_i^{py}$ is assumed to be continuous, the bias injections at sampling steps k and $k+1$ can be regarded as almost the same when T_{samp} is in the scale of milliseconds. To proceed with the subsequent analysis, we define the half-downsampled bias vector as

$$\boldsymbol{\phi}_{i\downarrow}^{py}(k) \equiv \boldsymbol{\phi}_i^{py}(k) \approx \boldsymbol{\phi}_i^{py}(k+1), k = k_i^p + 2l, \tag{20}$$

which indicates that the bias injections within each half-downsampled step are considered to be the same. Substituting (20) into (19), the relations between residuals and bias injections that enable the proposed bias reconstruction scheme can be obtained as

$$\mathcal{T}_{i\downarrow}^{pm} \boldsymbol{\phi}_{i\downarrow}^{py}(k+2) = \mathcal{T}_{\mathcal{A}i\downarrow}^{pm} \boldsymbol{\phi}_{i\downarrow}^{py}(k) + \Delta_{i\downarrow,r}^{pm}(k+3), \tag{21}$$

where $\mathcal{T}_{i\downarrow}^{pm} = [T_{i\downarrow}^p; T_{i\downarrow}^p M_i^{-1}]$, $\mathcal{T}_{\mathcal{A}i\downarrow}^{pm} = [T_{i\downarrow}^p A_{ii\downarrow}^d; T_{i\downarrow}^p A_{ii\downarrow}^d M_i^{-1}]$, and $\Delta_{i\downarrow,r}^{pm}(k+3) = [\boldsymbol{\delta}_{i\downarrow,r}^p(k+2); \boldsymbol{\delta}_{i\downarrow,r}^{pm}(k+3)]$. The bias reconstruction scheme can be thus derived from (21) as

$$\boldsymbol{\phi}_{i\downarrow}^{py,re}(k+2) = \mathcal{T}_{i\downarrow,inv}^{pm} \big(\mathcal{T}_{\mathcal{A}i\downarrow}^{pm} \boldsymbol{\phi}_{i\downarrow}^{py,re}(k) + \Delta_{i\downarrow,r}^{pm}(k+3) \big), \tag{22}$$

where $\boldsymbol{\phi}_{i\downarrow}^{py,re}$ denotes the reconstruction of $\boldsymbol{\phi}_{i\downarrow}^{py}$, and $\mathcal{T}_{i\downarrow,inv}^{pm} = \big((\mathcal{T}_{i\downarrow}^{pm})^{\mathrm{T}} \mathcal{T}_{i\downarrow}^{pm} \big)^{-1} (\mathcal{T}_{i\downarrow}^{pm})^{\mathrm{T}}$. The scheme (22) reconstructs the bias vector every two sampling steps at k, and, at the middle step $k+1$, the reconstructed biases are kept the same as the last reconstructed ones according to (20), i.e.,

$$\begin{cases} \boldsymbol{\phi}_i^{py,re}(k) = \boldsymbol{\phi}_{i\downarrow}^{py,re}(k) \\ \boldsymbol{\phi}_i^{py,re}(k+1) = \boldsymbol{\phi}_{i\downarrow}^{py,re}(k) \end{cases}, k = k_i^p + 2l. \tag{23}$$

The reconstructed bias vector will be removed from the compromised sensor readings to eliminate the PFDIA's impact on primary and secondary controllers, which is formulated as

$$\boldsymbol{y}_i^{p,ct}(k) = \begin{cases} \boldsymbol{y}_i^p(k) - \boldsymbol{\phi}_i^{py,re}(k), k = k_i^p + 2l, \\ \boldsymbol{y}_i^p(k) - M_i^{-1} \boldsymbol{\phi}_i^{py,re}(k), k = k_i^p + 2l + 1, \end{cases}, \tag{24}$$

where $\boldsymbol{y}_i^{p,ct}$ denotes the corrected local measurement vector. The performance of the bias reconstruction scheme (22) can be affected by the initial reconstruction error $\boldsymbol{\varphi}_i^{py,re} = \boldsymbol{\phi}_i^{py} - \boldsymbol{\phi}_i^{py,re}$ and system noises. Theoretical analysis of the reconstruction accuracy under these disturbances is provided as follows.

Proposition 1: Under continuous bias vector $\boldsymbol{\phi}_i^{py}$, small enough sampling step T_{samp} such that (20) holds with negligible approximation errors, and apparent residual alteration $|\boldsymbol{r}_{i\downarrow}^p - \boldsymbol{r}_{i\downarrow}^{pm}|$ resulting from matrix coding, the reconstruction error will be bounded by

$$\big| \boldsymbol{\varphi}_i^{py,re}(\infty) \big| \le \bar{\boldsymbol{\varphi}}_i^{py,re} = \sum_{n=0}^{\infty} \big| \mathcal{T}_{i\downarrow,inv}^{pm} \mathcal{T}_{\mathcal{A}i\downarrow}^{pm} \big|^n \big| \mathcal{T}_{i\downarrow,inv}^{pm} \big| \bar{\Xi}_{i\downarrow}^p \tag{25}$$

regardless of the initial reconstruction errors if matrix $\mathcal{T}_{i\downarrow,inv}^{pm} \mathcal{T}_{\mathcal{A}i\downarrow}^{pm}$ is Schur stable, i.e.,

$$\big| \mathrm{Re}\big(\lambda(\mathcal{T}_{i\downarrow,inv}^{pm} \mathcal{T}_{\mathcal{A}i\downarrow}^{pm}) \big) \big| < 1, \tag{26}$$

where $\bar{\Xi}_{i\downarrow}^p$ is the noise term's bound satisfying $|\Xi_{i\downarrow}^p(k)| \le \bar{\Xi}_{i\downarrow}^p = [\bar{\boldsymbol{\xi}}_{i\downarrow}^p; \bar{\boldsymbol{\xi}}_{i\downarrow}^p]$, $|\bar{\boldsymbol{\xi}}_{i\downarrow}^p(k)| \le \bar{\boldsymbol{\xi}}_{i\downarrow}^p = |T_{i\downarrow}^p| \bar{\boldsymbol{\rho}}_i + |T_{i\downarrow}^p A_{ii\downarrow}^d| \bar{\boldsymbol{\rho}}_i + |T_{i\downarrow}^p| \bar{\boldsymbol{\omega}}_i(k)$, and function $\lambda(\cdot)$ returns the eigenvalues of the input square matrix.

Proof: Considering the system noise related term $\Xi_{i\downarrow}^p(k+3) = [\boldsymbol{\xi}_{i\downarrow}^p(k+2); \boldsymbol{\xi}_{i\downarrow}^p(k+3)]$, the reconstruction dynamics (22) can be rewritten as

$$\begin{aligned} \boldsymbol{\phi}_{i\downarrow}^{py}(k+2) = \mathcal{T}_{i\downarrow,inv}^{pm} \big(\mathcal{T}_{\mathcal{A}i\downarrow}^{pm} \boldsymbol{\phi}_{i\downarrow}^{py}(k) + \Delta_{i\downarrow,r}^{pm}(k+3) + \\ + \Xi_{i\downarrow}^p(k+3) \big). \end{aligned} \tag{27}$$

Defining the downsampled reconstruction error as $\boldsymbol{\varphi}_{i\downarrow}^{py,re} = \boldsymbol{\phi}_{i\downarrow}^{py} - \boldsymbol{\phi}_{i\downarrow}^{py,re}$, and, without loss of generality, assuming that the initial reconstructed bias vector is $\boldsymbol{\phi}_{i\downarrow}^{py,re}(k_i^p) = \mathbb{0}^{2\times 1}$, then by making the difference between equations (22) and (27), the dynamics of the reconstruction error can be obtained as

$$\boldsymbol{\varphi}_{i\downarrow}^{py,re}(k+2) = \mathcal{T}_{i\downarrow,inv}^{pm} \mathcal{T}_{\mathcal{A}i\downarrow}^{pm} \boldsymbol{\varphi}_{i\downarrow}^{py,re}(k) + \mathcal{T}_{i\downarrow,inv}^{pm} \Xi_{i\downarrow}^p(k+3). \tag{28}$$

Through direct calculation from (28), the expression of $\boldsymbol{\varphi}_{i\downarrow}^{py,re}$ can be derived as

$$\begin{aligned} \boldsymbol{\varphi}_{i\downarrow}^{py,re}(k) = \big(\mathcal{T}_{i\downarrow,inv}^{pm} \mathcal{T}_{\mathcal{A}i\downarrow}^{pm} \big)^{(k-k_i^p)/2} \boldsymbol{\varphi}_i^{py}(k_i^p) + \sum_{n=0}^{(k-k_i^p)/2-1} \\ \big(\mathcal{T}_{i\downarrow,inv}^{pm} \mathcal{T}_{\mathcal{A}i\downarrow}^{pm} \big)^n \mathcal{T}_{i\downarrow,inv}^{pm} \Xi_{i\downarrow}^p(k_i^p + 2n + 3), k = k_i^p + 2l. \end{aligned} \tag{29}$$

According to (26), we have $\big(\mathcal{T}_{i\downarrow,inv}^{pm} \mathcal{T}_{\mathcal{A}i\downarrow}^{pm} \big)^{\infty} \to \mathbb{0}^{2\times 2}$, under which the steady-state value of $\boldsymbol{\phi}_{i\downarrow}^{py,re}$ will satisfy

$$\begin{aligned} |\boldsymbol{\varphi}_{i\downarrow}^{py,re}(\infty)| &= \Big| \sum_{n=0}^{\infty} \big(\mathcal{T}_{i\downarrow,inv}^{pm} \mathcal{T}_{\mathcal{A}i\downarrow}^{pm} \big)^n \mathcal{T}_{i\downarrow,inv}^{pm} \Xi_{i\downarrow}^p(k_i^p + 2n + 3) \Big| \\ &\le \sum_{n=0}^{\infty} \big| \mathcal{T}_{i\downarrow,inv}^{pm} \mathcal{T}_{\mathcal{A}i\downarrow}^{pm} \big|^n \big| \mathcal{T}_{i\downarrow,inv}^{pm} \bar{\Xi}_{i\downarrow}^p \big| = \bar{\boldsymbol{\varphi}}_i^{py,re} \end{aligned} \tag{30}$$

Since the bias vector ϕ_i^{py} is continuous and the sampling step T_{samp} is small enough, the bias alteration between two consecutive sampling steps would be negligible, i.e., $\boldsymbol{\varphi}_{i\downarrow}^{py,re} \approx \boldsymbol{\varphi}_i^{py,re}$. Therefore, the result (25) holds and the proof is completed. ■

According to Proposition 1, the reconstruction error in steady state will be bounded by the threshold determined by system noises' bounds once matrix $\mathcal{T}_{i\downarrow,inv}^{pm} \mathcal{T}_{\mathcal{A}i\downarrow}^{pm}$ is designed to be Schur stable. The impact of initial reconstruction error on the steady-state reconstruction error can be entirely eliminated since the impact will decay exponentially with time in the presence of Schur stable $\mathcal{T}_{i\downarrow,inv}^{pm} \mathcal{T}_{\mathcal{A}i\downarrow}^{pm}$. The condition (26) can be easily satisfied through choosing M_i such that $A_{ii\downarrow}^d M_i^{-1} = M_i^{-1} A_{ii\downarrow}^d$, where $\mathcal{T}_{i\downarrow}^{pm} \mathcal{T}_{\mathcal{A}i\downarrow}^{pm} = A_{ii\downarrow}^d$ would be Schur stable naturally. The larger residual alteration $|\boldsymbol{r}_{i\downarrow}^p - \boldsymbol{r}_{i\downarrow}^{pm}|$ resulting from matrix coding makes the two sub-equations in (19) more divergent, such that the bias's information can be reflected more comprehensively. Besides the reconstruction stability and residual alteration, the design of coding matrix also needs to consider the encoding's hiddenness from the adversary and minimise the system noise's impact on reconstruction

accuracy, which will be elaborated in the next subsection.

Nevertheless, as the adoption of matrix coding, the detectability of UIO$_i^p$ may also be affected as half of the received data is affected by original bias injections $\boldsymbol{\phi}_i^{py}$ while the other data is tampered with decoded bias injections $(M_i)^{-1}\boldsymbol{\phi}_i^{py}$. From the perspective of UIO$_i^p$, the received data is discontinuous, under which the alarm signal ϱ_i^p may not be hold via (12). To avoid the adverse impact resulting from the adopted matrix coding, after establishing UIO$_{i\downarrow}^p$ and UIO$_{i\downarrow}^{pm}$, the generated residuals $\boldsymbol{r}_{i\downarrow}^p, \boldsymbol{r}_{i\downarrow}^{pm}$ will also be utilised to hold the alarm signal besides the bias reconstruction (22). Specifically, the detection bounds corresponding to $\boldsymbol{r}_{i\downarrow}^p$ and $\boldsymbol{r}_{i\downarrow}^{pm}$ can be calculated similarly to (11) and are denoted by $\bar{\boldsymbol{r}}_{i\downarrow}^p$ and $\bar{\boldsymbol{r}}_{i\downarrow}^{pm}$, respectively. At $k = k_i^p + 2l$, in addition to condition (12), the subsequent newly incorporated conditions (31) or (32)

$$r_{i\downarrow,V}^{pm}(k-1) > \bar{r}_{i\downarrow,V}^{pm}(k-1) \text{ or } r_{i\downarrow,I}^{pm}(k-1) > \bar{r}_{i\downarrow,I}^{pm}(k-1) \quad (31)$$

$$r_{i\downarrow,V}^{p}(k-2) > \bar{r}_{i\downarrow,V}^{p}(k-2) \text{ or } r_{i\downarrow,I}^{p}(k-2) > \bar{r}_{i\downarrow,I}^{p}(k-2) \quad (32)$$

will also set ϱ_i^p as 1, where $\boldsymbol{r}_{i\downarrow}^{pm} = [r_{i\downarrow,V}^{pm}; r_{i\downarrow,I}^{pm}], \bar{\boldsymbol{r}}_{i\downarrow}^{pm} = [\bar{r}_{i\downarrow,V}^{pm}; \bar{r}_{i\downarrow,I}^{pm}]$ and $\boldsymbol{r}_{i\downarrow}^{p} = [r_{i\downarrow,V}^{p}; r_{i\downarrow,I}^{p}], \bar{\boldsymbol{r}}_{i\downarrow}^{p} = [\bar{r}_{i\downarrow,V}^{p}; \bar{r}_{i\downarrow,I}^{p}]$.

C. Optimisation Problem for Coding Matrix

As mentioned in the previous subsection, the stability condition (22) can be easily satisfied by letting $A_{ii\downarrow}^d M_i^{-1} = M_i^{-1} A_{ii\downarrow}^d$. However, this intuitively designed coding matrix can make it quickly recognisable by the adversary as the transmitted encoded data may deviate a lot from the normal physical states, such as encoding the current measurement as negative. Therefore, it is necessary to make the encoded data indistinguishable from the real physical states. Moreover, the reconstructed bias's fluctuations resulting from system noises and residual alterations caused by matrix coding should also be carefully investigated. Considering the reconstruction stability, encoding's hiddenness from the adversary, system noise's impact, and residual alteration resulting from matrix coding, the design of coding matrix M_i is formulated as a constrained optimisation problem as follows:

$$\min_{M_i} \parallel |\mathcal{T}_{i\downarrow,inv}^{pm}| \bar{\Xi}_{i\downarrow}^{p} \parallel_2 - \alpha_{i\downarrow}^{pm} \Gamma_{i\downarrow}^{pm} \quad (33)$$

$$\text{s.t.} \quad (26),$$

$$|(M_i - \mathrm{I}^2)\boldsymbol{x}_i^{ref}| \le \sigma_i \boldsymbol{x}_i^{ref}, \quad (34)$$

$$-\left(\det(M_i)\right)^2 \le -\mu_i, \quad (35)$$

where the first term in objective function (33) is obtained from (25) to minimise the impact of system noises on the reconstruction accuracy, the second term in (33) consisting of $\Gamma_{i\downarrow}^{pm} = \parallel T_{i\downarrow}^p \left(\mathrm{I}^2 - (M_i)^{-1}\right) \parallel_2 + \parallel T_{i\downarrow}^p A_{ii\downarrow}^d \left(\mathrm{I}^2 - (M_i)^{-1}\right) \parallel_2$ aims to maximise the residual alteration caused by matrix coding, and $\alpha_{i\downarrow}^{pm} > 0$ is the weight parameter. The inequality constraints (34) make the encoded data close to the nominal physical state $\boldsymbol{x}_i^{ref} = [V_{ref,i}, I_{avg,ti}]$ with the deviation rate σ_i smaller than 0.1, such that the adopted matrix coding can be hidden from the adversary. Here, $I_{avg,ti}$ denotes the average output current observed from DER i's historical load profile. The inequality constraint (35) guarantees the invertibility of coding matrix M_i by ensuring its determinant $\det(M_i)$ to be positive via $\mu_i > 0$.

Due to the existence of matrix inverse and eigenvalue calculation in $\mathcal{T}_{i\downarrow,inv}^{pm}$ and (26), respectively, the formulated optimisation problem (33) is essentially nonlinear and nonconvex. The relaxation of the original problem (33) to a linear and convex one whose optimum can be fast obtained by existing solvers would require additional effort and is out of the scope of this paper. In this paper, we utilise the *fconmin* function from Matlab and equip it with interior-point algorithm to find the local minimum around an appropriately chosen initial point. The local minimum may not be as good as the global minimum, but can still perform much better than the intuitively chosen coding matrix through satisfying $A_{ii\downarrow}^d M_i^{-1} = M_i^{-1} A_{ii\downarrow}^d$.

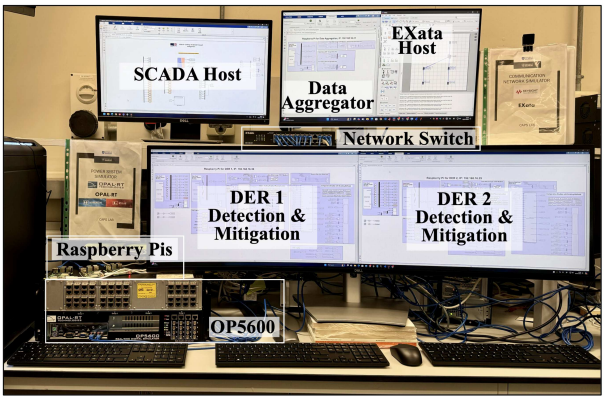
V. Experimental Validations

In this section, extensive experimental studies are conducted in cyber-physical co-simulation platform and full-hardware microgrid testbeds. The experimental results validate the proposed matrix coding enabled impact mitigation scheme's effectiveness, its superiority compared with existing methods, its robustness to daily events, parameter uncertainties, as well as nonlinear CPLs, and its lightweight computation burden.

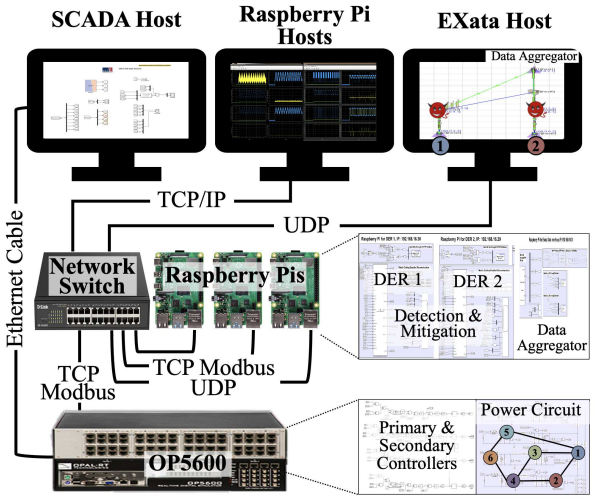
A. Cyber-Phyiscal Co-Simulation Experimental Studies

The co-simulated 6-DER microgrid testbed is established utilising the OPAL-RT real-time digital simulator OP5600, three Raspberry Pis, and the Keysight EXata network simulator as shown in Fig. 6. The power circuit, primary controllers, and secondary controllers are simulated in OP5600, and the Raspberry Pis are run in real time with the simulated microgrid through TCP Modbus based data exchange channels, where the register read/write interval is set as 1ms. Among the three Raspberry Pis, one Raspberry Pi is configured as data aggregator to read data from OP5600, and the aggregated data will be distributed to the other two Raspberry Pis, which are embedded with the detection and mitigation algorithms of DERs 1 and 2, through the mapped UDP data flows in EXata network simulator. After processing the received data, these two Raspberry Pis will write the corrected data back to OP5600 as the inputs of primary and secondary controllers. Under such configuration, based on the advanced cyber library provided by EXata, realistic data modification events can be launched against the transmitted data packets within EXata. The electrical parameters of DER are set the same as those in [35], the nominal reference PCC voltages are $V_{ref,i} = 40\text{V}$, and the CPLs are $P_{CPL,i} = 40\text{W}, \forall i \in \mathcal{A}$. The bound that tolerates measurement noise is set as $\bar{\boldsymbol{\rho}}_i = [0.01, 0.01]^{\mathrm{T}}$. The time of activating secondary controllers and UIO-based detectors is at $t = 2\text{s}$ and $t = 4\text{s}$, respectively. The subsequent part will validate the proposed mitigation scheme's effectiveness, its superiority compared with existing methods, and its robustness under various disturbances.

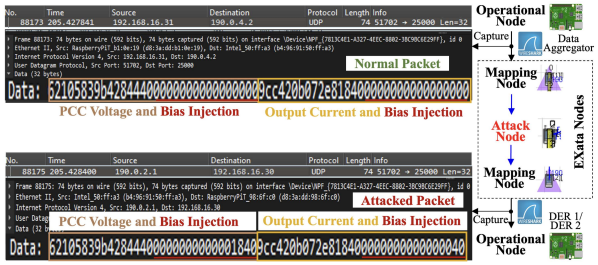
1) Effectiveness against Continuous and Discontinuous PFDIA Bias Injections: This part validates the effectiveness of proposed mitigation scheme against PFDIAs, where the data modification events with continuous and discontinuous bias injections against the data flows of DERs 1 and 2, respectively, are launched in EXata at $t = 6\text{s}$. The results of detection,



(a) Experimental setup



(b) Connection architecture



(c) Realistic data modification event

Fig. 6: This figure shows the cyber-physical co-simulation microgrid testbed as well as the introduced realistic data modification events: 1) Power system simulation consists of the power circuits and controllers of a 6-DER microgrid in the OPAL-RT real-time digital simulator OP5600, 2) Communication simulation includes the communication links of primary control in the Keysight EXata network simulator, 3) UIO-based detection and matrix coding enabled impact mitigation schemes are deployed in two Raspberry Pis, and the third Raspberry Pi runs as a data aggregator to map data flows into the EXata network simulator, and 4) Cyber-physical interface with the data exchange between Raspberry Pis and OP5600 being implemented via TCP Modbus, while the data interaction between EXata and Raspberry Pis is implemented through UDP.

reconstruction, encoding's hiddenness, and mitigation effectiveness are showcased in sub-figures (a)-(d) of Fig. 7 and Fig. 8. In particular, as shown in sub-figure (a), the normally sampled residual $\boldsymbol{r}_i^p, i \in \{1,2\}$ will immediately increase above the detection threshold $\bar{\boldsymbol{r}}_i^p$ when the PFDIAs are introduced, timely triggering the PFDIA alarm. At the same time, the two half-downsampled UIOs will be activated to generate residuals $\boldsymbol{r}_{i\downarrow}^p, \boldsymbol{r}_{i\downarrow}^{pm}$ for bias reconstruction and update them every 2ms. The reconstruction performance under continuous and discontinuous PFDIA injections has slight difference as demonstrated in sub-figure (b). For the continuous bias case in DER 1, the reconstructed biases can quickly track the real biases after non-trivial initial reconstruction errors, where the steady-state reconstruction errors will be eventually bounded by predefined values as stated in Proposition 1. When the bias injections are discontinuous in DER 2, there would emerge non-negligible initial reconstruction errors every time when the biases have step changes. Despite these reconstruction errors, the reconstruction errors can still converge exponentially to zero under moderate changing rate of discontinuous biases (1s in this case). By optimising the coding matrix through (33), the hiddenness of adopted data encoding technology can be effectively preserved from the adversary as validated in sub-figure (c). From the perspective of adversary, the transmitted voltage and current data will approximately have ± 5V and ± 5A variations, respectively, after adopting the encoding scheme, which are indistinguishable from the attack impacts and thus barely raise the alert of adversary. When the mitigation action (24) is enabled at $t = 8$s, the transmitted encoded data will become more stable, further decreasing the possibility of leaking defense-side's information to the adversary and increasing the difficulty of making effective follow-up adversarial movements. In sub-figure (d), the results indicate that the enabled mitigation action (24) can effectively eliminate the attack impacts on system states and rapidly reestablish load sharing in the 6-DER microgrid.

TABLE I: Steady-state voltage and current bias reconstruction errors in the comparative studies with existing literature [16], [31], [32]

Error \ Type	(a) PFDIA against only current			(b) PFDIA against both voltage and current		
	[31], [32]	[16]	**Prop.**	[31], [32]	[16]	**Prop.**
$\lvert\varphi_{1,V}^{py,re}(\infty)\rvert$	0	< 0.2	$<$ **0.4**	> 5	> 2	$<$ **0.4**
$\lvert\varphi_{1,I}^{py,re}(\infty)\rvert$	< 0.4	< 0.4	$<$ **0.1**	> 5	> 10	$<$ **0.1**

2) Comparative Studies with Existing Bias Reconstruction Methods: This part validates the proposed method's superiority compared with existing methods from [16], [31], [32] in the bias reconstruction accuracy, where two PFDIA cases tampering only current measurement and both voltage and current measurements are considered. Although the method from [16] is designed to reconstruct the SFDIA bias, its idea of deploying current sensors on power lines can be seamlessly extended to the PFDIA case. Specifically, the measured power line currents serving as new inputs will alter the $(1,1)$th element of system matrix A_{ii}, under which another UIO can be established to capture a new relation between bias injections and residuals. After combining it with (14), the complete bias vector is able to be reconstructed. According to Fig. 9, when the voltage measurement is free from attack, the method from [31], [32] can accurately reconstruct the bias injected into current measurement by employing adaptive observers, where the resulted steady-state current bias reconstruction error is smaller than 0.4A as presented in TABLE I. However, if both

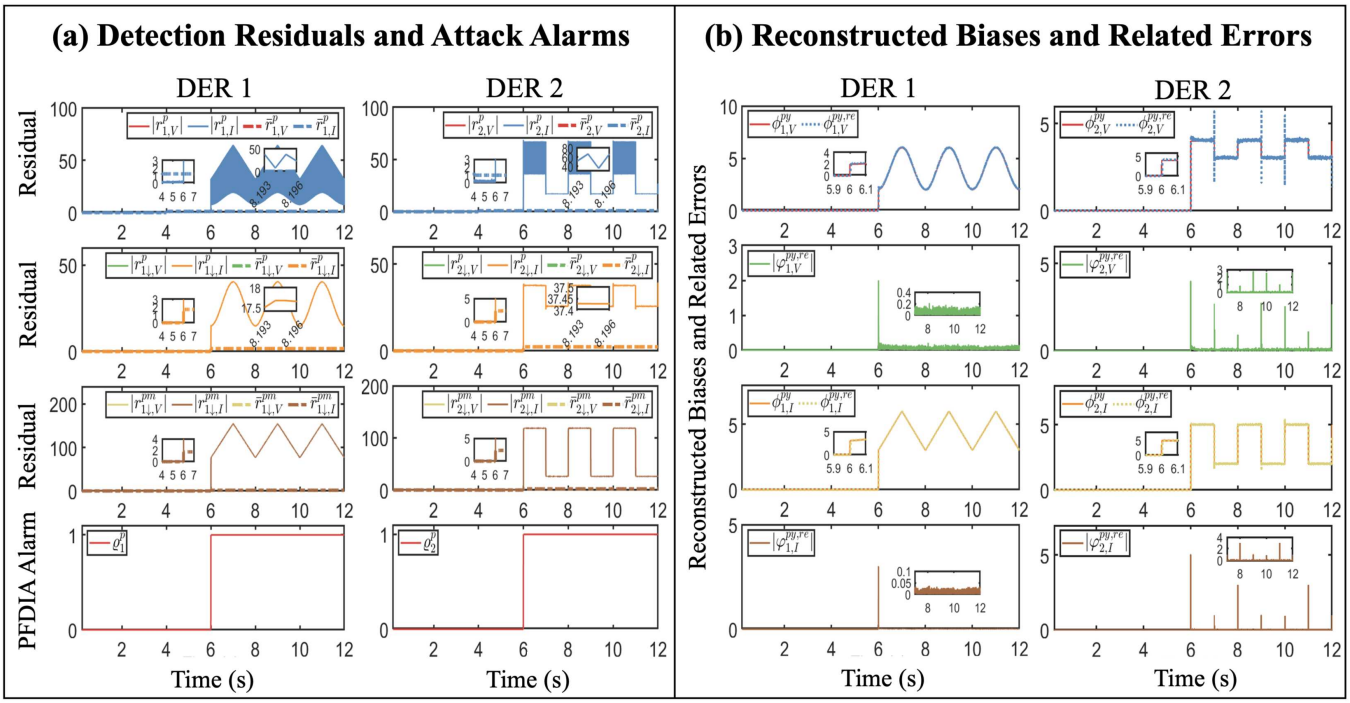


Fig. 7: This figure shows the proposed method's effectiveness against continuous and discontinuous PFDIA bias injections: where the results of detection and reconstruction are presented in sub-figures (a) and (b), respectively.

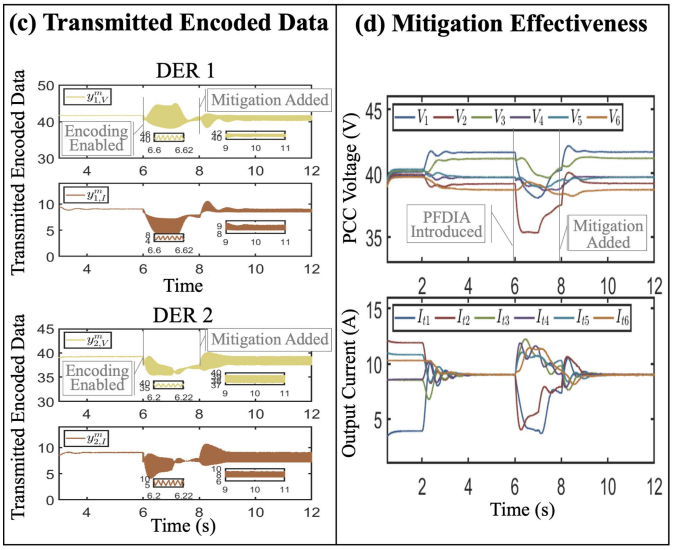


Fig. 8: This figure is the continuation of Fig. 7, jointly validating the proposed method's effectiveness against PFDIAs, where the results of encoding's hiddenness and mitigation effectiveness are presented in sub-figures (c) and (d), respectively.

voltage and current measurements are compromised, the adaptive observer based method is not able to reconstruct either of bias injections as it relies heavily on the attack-free voltage information to estimate the legitimate current measurement. Although the method from [16] can successfully reconstruct the voltage and current biases, the reconstruction errors are not able to converge to zero in steady state under the two PFDIA cases. Moreover, the growth of initial reconstruction error will increase the steady-state reconstruction error correspondingly. It is revealed that the non-zero steady-state reconstruction error is caused by an unstable eigenvalue on unit circle, making the reconstruction scheme extremely sensitive to disturbances such as initial errors and system noises. Hence, the strategy of deploying additional current sensors on power lines is unsuitable for the reconstruction of PFDIA bias injection. Compared with these existing methods as illustrated in Fig. 10, the proposed bias reconstruction scheme can always achieve < 0.4V and < 0.1A steady-state voltage and current bias reconstruction errors under the two PFDIA cases, successfully filling the research gap of impact mitigation scheme that is able to effectively counter against the PFDIA compromising both voltage and current measurements.

3) Robustness to Daily Events, Parameter Uncertainties, and Nonlinear Constant Power Load: As shown in Fig. 11, when DERs 2 and 5 are plugged into the microgrid at $t = 6$s, the UIO parameters will be updated accordingly and the detection residuals can still be bounded by corresponding thresholds. Moreover, the activation of current load variation within $[8, 10]$s will not cause significant fluctuations on the detection residuals. Therefore, the detection residual generated by UIO-based detector has negligible sensitivity to these daily events and will not flag false attack alarms for them. When there exist different levels of uncertainties on the electrical parameters including R_{ti}, L_{ti}, C_{ti}, the detection, reconstruction, and mitigation performance are illustrated in Fig. 12. The existence of parameter uncertainties will increase the detection residual in the normal case and thus may result in false alarms as illustrated in the 30% uncertainty case. Moreover, the inaccurate parameters can induce non-zero steady-state bias reconstruction errors, but the corresponding sensitivities are limited as the 30% uncertainty will only cause < 0.6V and < 0.2A steady-state errors. In such case, the ac-

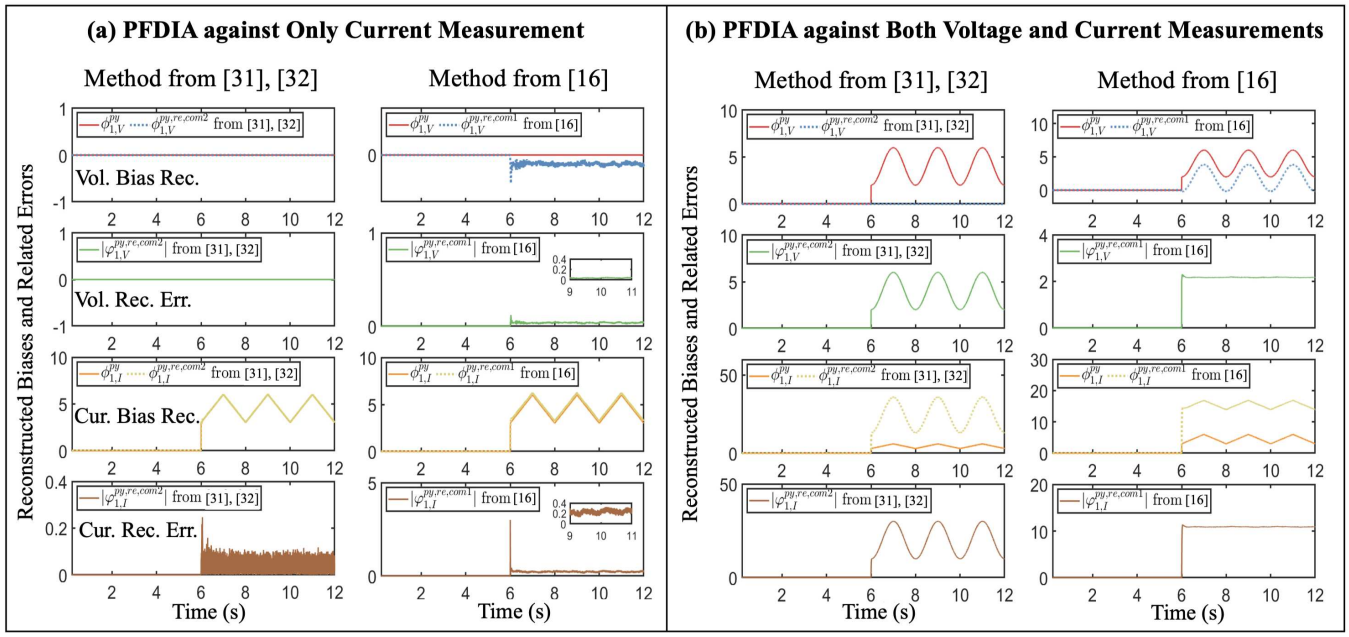


Fig. 9: This figure illustrates the bias reconstruction performance of existing methods from [16], [31], [32], where two PFDIA cases tampering with only current measurement and both voltage and current measurements are demonstrated in sub-figures (a) and (b), respectively.

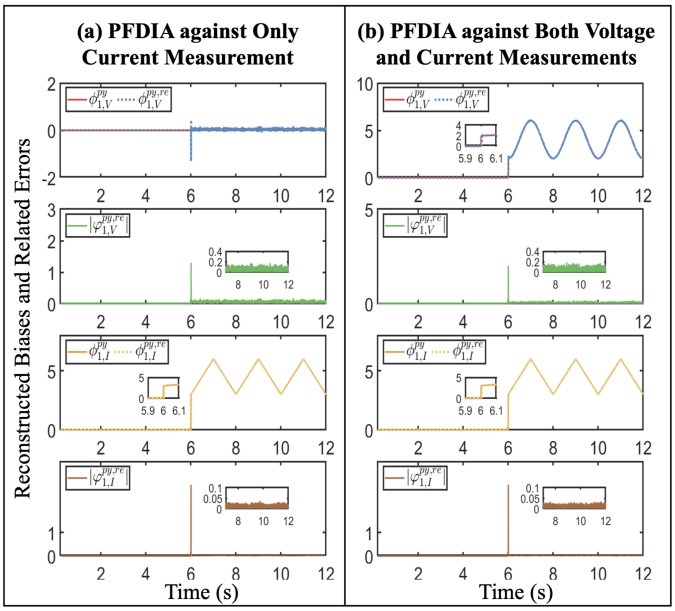


Fig. 10: This figure is the continuation of Fig. 9, illustrating the improved bias reconstruction accuracy of the proposed matrix coding enabled method compared with [16], [31], [32], where the same PFDIA cases tampering with only current measurement and both voltage and current measurements are demonstrated in sub-figures (a) and (b), respectively.

tivated mitigation action (24) can still reestablish load sharing in the microgrid after stimulating some negligible transient fluctuations on the system states. Finally, the reconstruction and mitigation performance under different nonlinear CPLs are validated in Fig. 13. The results indicate that the bias reconstruction accuracy will not be affected by the existence of nonlinear CPLs, verifying the effectiveness of the linearisation scheme (1), (2) in handling the non-linearity resulting from CPLs.

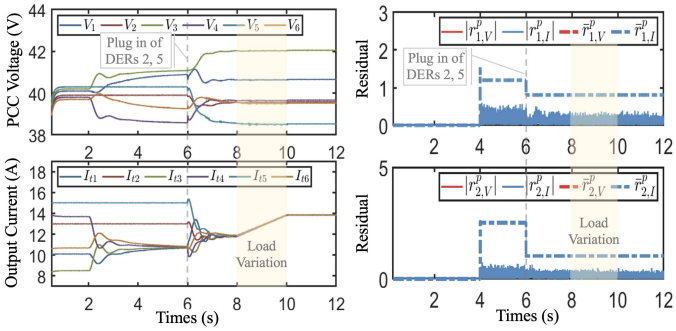


Fig. 11: This figure shows the UIO-based detector's performance when plugging-in of DERs and load variation are introduced at $t = 6$s and within $t \in [8, 10]$s, respectively.

4) Lightweight Computation Burden: The runtime of proposed matrix coding enabled impact mitigation method in two Raspberry Pis equipped with 8GB RAM are demonstrated in Fig. 14. It is clear that the runtime will have a significant increment after activating the UIO-based detector at $t = 4$s, and further increase appears on the runtime when the introduced PFDIAs trigger the bias reconstruction scheme at approximately $t = 6$s. Due to the computational efficiency of the proposed method, the average runtime in the two Raspberry Pis are 0.0042ms and 0.0044ms with the maximal runtime being 0.0797ms and 0.0866ms, respectively, which are significantly lower than the data exchange interval 1ms among OP5600, Raspberry Pis, and EXata. Therefore, the proposed method is lightweight enough to be integrated into the primary control loop that has strict real-time requirement, verifying its applicability to realistic industrial scenarios.

B. Full-Hardware Experimental Studies

This subsection validates the effectiveness of the proposed matrix coding enabled impact mitigation in a full-hardware

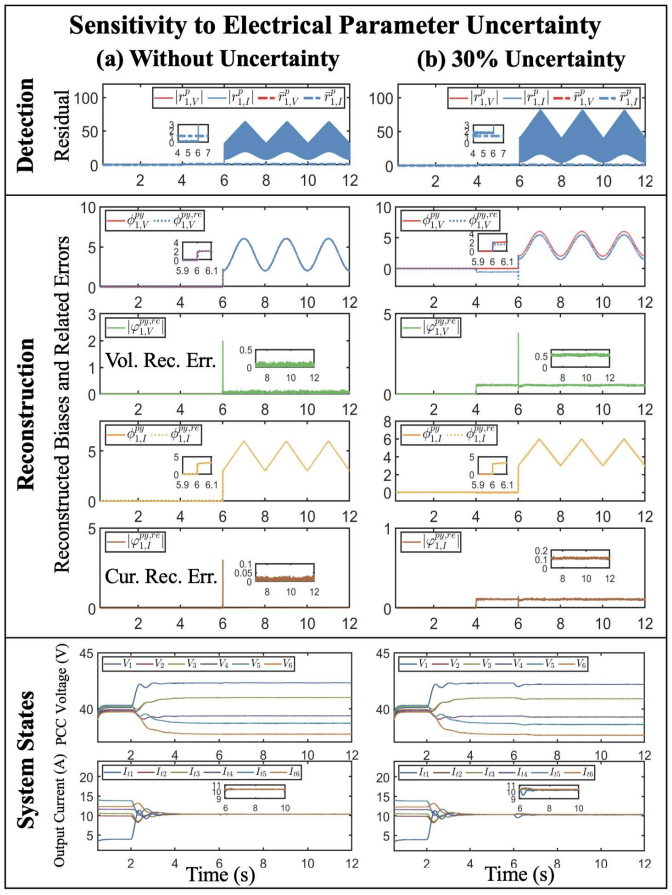


Fig. 12: This figure demonstrates the detection, reconstruction, and mitigation performance under 0 and 30% electrical parameter uncertainties.

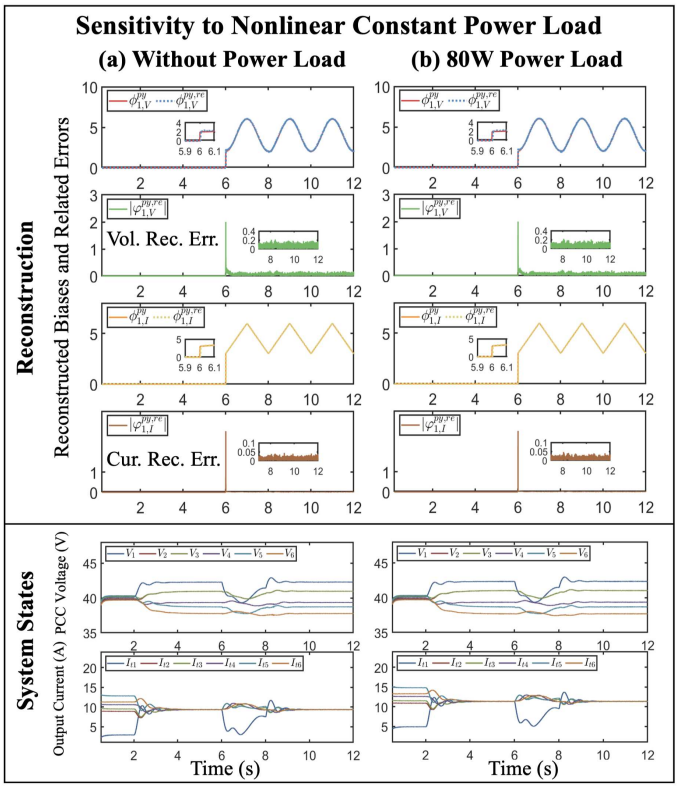


Fig. 13: This figure showcases the reconstruction and mitigation performance under 0W and 80W nonlinear CPLs.

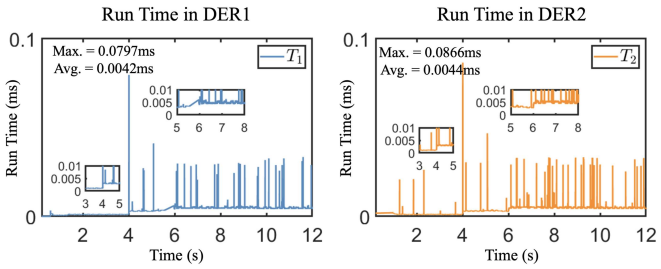


Fig. 14: This figure demonstrates the runtime of the proposed matrix coding enabled mitigation scheme in two Raspberry Pis equipped with 8GB RAM.

microgrid testbed, whose overview and component description are shown in Fig. 15. In particular, the full-hardware testbed has two real-time digital controllers, i.e., RTU-BOX 204[1], which are developed based on TI microcontrollers for the rapid prototype control system and are equipped with rich analog/digital input/out ports. The RTU-BOX 204 is directly compatible with the SIMULINK programming environment, where an integrated development environment, named as Rtu-nit Studio, is provided to compile and download SIMULINK model into the controller as well as collect real-time operating states from the controller. Moreover, four building block half bridge modules[2] are inserted into two racks to function as DC-DC converters, which have active over-voltage and over-current protection mechanisms to guarantee the operator's safety. The circuit within each DER consisting of a DC-DC converter, a DC supply, a ZIP load, and a LC filter is illustrated in Fig. 2, and the 4 DERs are connected through power lines to form a meshed network, where the electrical parameters are explained in [35]. The PCC reference voltages of DERs are set to be equal to 48V, and the equivalent resistive and current loads are configured as 30Ω and 2A, 4A, 6A, 8A, respectively. The detection and mitigation algorithms are embedded into controllers via SIMULINK models, and the execution rate is set as 1ms. In the operation stage, the UIOs are activated at $t = 2.5$s, and the PFDIA against DER 1's measurements is launched at $t = 5$s, whose bias injections include continuous sine and discontinuous triangle signals.

According to the results shown in Fig. 16, the proposed method can accurately track both continuous and discontinuous bias injections and is able to achieve < 0.4V and < 0.05A steady-state voltage and current bias reconstruction errors. After enabling the mitigation action (24) at $t = 7$s, the adversely affected system states can rapidly converge to normal ranges such that load sharing is eventually reestablished in the microgrid. Moreover, the fluctuations of encoded data are within normal ranges, i.e., < 2V for voltage and < 0.5A for current in steady state, which are able to preserve the hiddenness of adopted data encoding technology from the adversary. Thus, the proposed method is verified to be effective in the fully hardware-configured 4-DER microgrid, further proving its practical value in potential industrial scenarios.

[1]https://www.rtunit.com/Home/proDetail?productId=6
[2]https://www.rtunit.com/Home/proDetail?productId=15

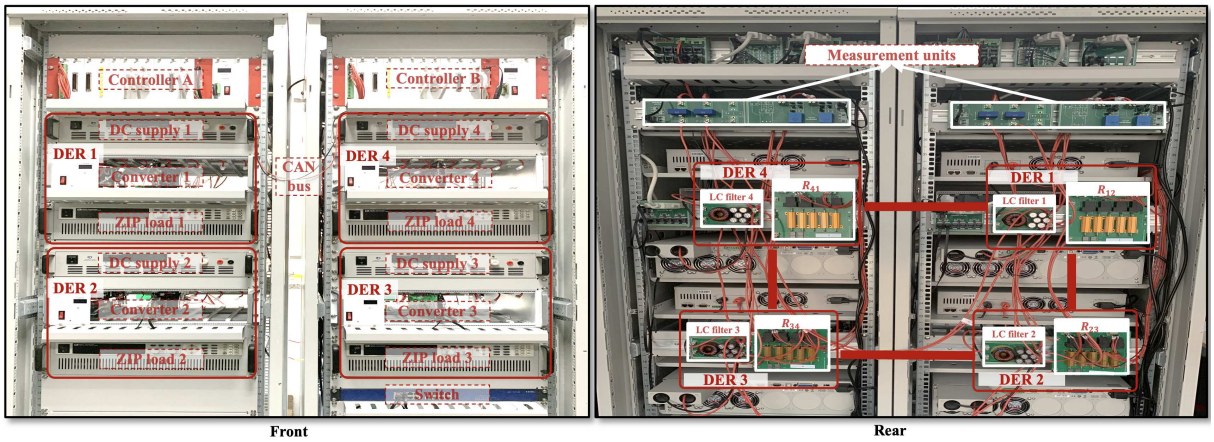


Fig. 15: This figure shows the overview of the 4-DER full-hardware microgrid testbed at Zhejiang University, where the circuit within each DER consists of a DC-DC converter, a DC supply, a ZIP load, and a LC filter. Each controller outputs two asynchronous PWM signals for two converters, and the data exchange between controllers is implemented via CAN bus.

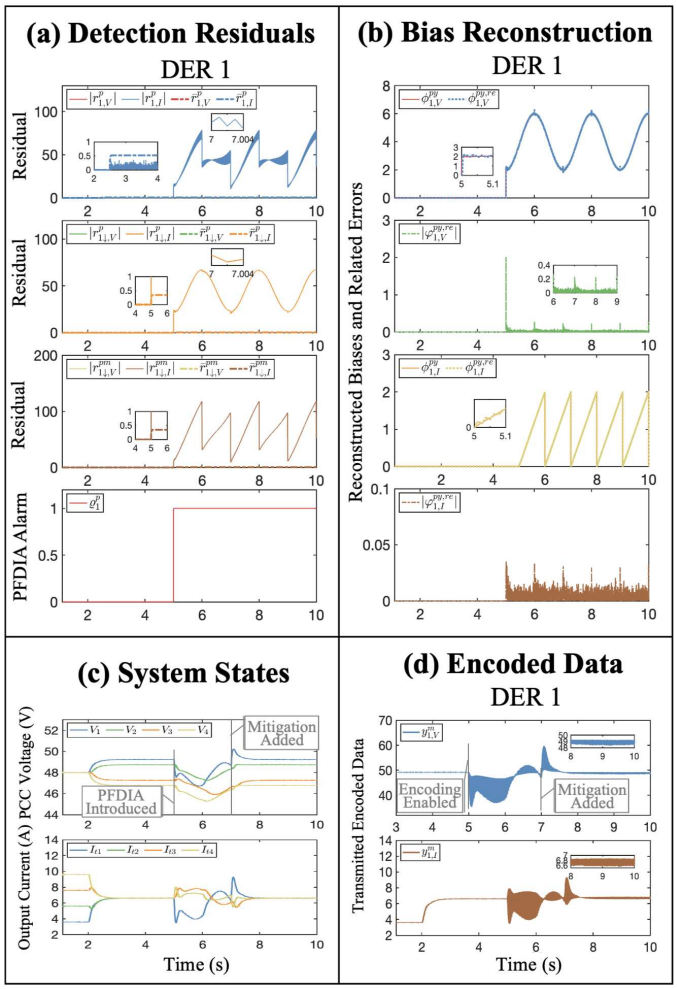


Fig. 16: This figure validates the effectiveness of proposed matrix coding enabled mitigation scheme against PFDIAs in the full-hardware microgrid testbed.

VI. Conclusion

This paper proposed a time-efficient and cost-efficient impact mitigation scheme against the PFDIA in cyber-physical microgrids by alternately encoding the transmitted measurement data. Two half-downsampled UIOs were triggered after detecting anomaly to calculate the residuals under encoded and unencoded data, from which the complete bias vector could be rapidly and accurately reconstructed. Theoretical performance analysis was conducted to endow the optimised coding matrix with minimised impact of system noises on reconstruction accuracy, as well as guaranteed reconstruction stability and encoding's hiddenness. The reconstructed bias was eventually removed from the compromised data to achieve impact mitigation. Finally, through extensive experimental studies carried out in cyber-physical co-simulated and full-hardware microgrid testbeds, the effectiveness, superiority, robustness, and lightweightness of the proposed scheme were clearly validated and demonstrated. Future works include investigating effective countermeasures against gross measurement errors and the denial-of-service attack that blocks data transmission channels.

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

$$A_{ii} = \begin{bmatrix} -\frac{1}{Z_{Li}C_{ti}} & -\sum_{j\in\mathcal{N}_i^{el}} \frac{1}{C_{ti}R_{ij}} & \frac{1}{C_{ti}} \\ & -\frac{1}{L_{ti}} & -\frac{R_{ti}}{L_{ti}} \end{bmatrix}, \boldsymbol{b}_i = \begin{bmatrix} 0 \\ \frac{1}{L_{ti}} \end{bmatrix}$$
$$\boldsymbol{m}_i = \begin{bmatrix} -\frac{1}{C_{ti}} \\ 0 \end{bmatrix} \quad (36)$$

$$A_{ii}^d = e^{A_{ii}T_{samp}}, Y_{ii}^d = (A_{ii})^{-1}(A_{ii}^d - \mathrm{I}^2),$$
$$\boldsymbol{b}_i^d = Y_{ii}^d \boldsymbol{b}_i, \boldsymbol{m}_i^d = Y_{ii}^d \boldsymbol{m}_i. \quad (37)$$

B. Unknown Input Observer Matrices

$$T_i^p = \mathrm{I}^2 - H_i^p \tag{38}$$
$$T_i^p \boldsymbol{m}_i^d = \mathbb{0}^{2\times 1} \tag{39}$$
$$\hat{K}_i^p = K_{i1}^p + K_{i2}^p \tag{40}$$
$$F_i^p = T_i^p A_{ii}^d - K_{i1}^p \tag{41}$$
$$K_{i2}^p = F_i^p H_i^p \tag{42}$$

REFERENCES

[1] R. Walton, "Doe confirms its systems were compromised by solarwinds hack," (Accessed: 2024). [Online]. Available: https://www.utilitydive.com/news/doe-confirms-its-systems-were-compromised-by-solarwinds-hack/592441/

[2] Reuters, "Satellite outage knocks out thousands of enercon's wind turbines," Accessed: 2024, [Online]. [Online]. Available: https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/

[3] A. Durakovic, "Vestas indicates cyber security incident was ransomware attack," Accessed: 2024, [Online]. [Online]. Available: https://www.offshorewind.biz/2021/11/29/vestas-indicates-cyber-security-incident-was-ransomware-attack/

[4] 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. 3, pp. 1–12, 2020.

[5] F. R. Badal, P. Das, S. K. Sarker, and S. K. Das, "A survey on control issues in renewable energy integration and microgrid," *Protection and Control of Modern Power Systems*, vol. 4, no. 1, pp. 1–27, 2019.

[6] 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.

[7] H. Pu, L. He, P. Cheng, M. Sun, and J. Chen, "Security of industrial robots: Vulnerabilities, attacks, and mitigations," *IEEE Netw.*, vol. 37, no. 1, pp. 111–117, 2023.

[8] S. Mehner and H. König, "No need to marry to change your name! attacking profinet io automation networks using dcp," in *Detection of Intrusions and Malware, and Vulnerability Assessment International Conference*. Springer, 2019, pp. 396–414.

[9] J. Liu, X. Lu, and J. Wang, "Resilience analysis of dc microgrids under denial of service threats," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3199–3208, 2019.

[10] J. Zhou, Q. Yang, X. Chen, Y. Chen, and J. Wen, "Resilient distributed control against destabilization attacks in dc microgrids," *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 371–384, 2023.

[11] 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 Trans. Smart Grid*, pp. 1–1, 2024.

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

[13] S. Sahoo, Y. Yang, and F. Blaabjerg, "Resilient synchronization strategy for ac microgrids under cyber attacks," *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 73–77, 2020.

[14] J. Xiao, L. Wang, Z. Qin, and P. Bauer, "A resilience enhanced secondary control for ac micro-grids," *IEEE Trans. Smart Grid*, 2023.

[15] M. Leng, S. Sahoo, and F. Blaabjerg, "Stabilization of dc microgrids under cyber attacks-optimal design and sensitivity analysis," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 113–123, 2024.

[16] M. Liu, X. Zhang, R. Zhang, Z. Zhou, Z. Zhang, and R. Deng, "Detection-triggered recursive impact mitigation against secondary false data injection attacks in cyber-physical microgrids," *IEEE Transactions on Smart Grid*, pp. 1–1, 2024.

[17] S. Zuo, T. Altun, F. L. Lewis, and A. Davoudi, "Distributed resilient secondary control of dc microgrids against unbounded attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3850–3859, 2020.

[18] D. Zhou, Q. Zhang, F. Guo, Z. Lian, J. Qi, and W. Zhou, "Distributed resilient secondary control for islanded dc microgrids considering unbounded fdi attacks," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 160–170, 2024.

[19] C. Deng, Y. Wang, C. Wen, Y. Xu, and P. Lin, "Distributed resilient control for energy storage systems in cyber–physical microgrids," *IEEE Trans. Industr. Inform.*, vol. 17, no. 2, pp. 1331–1341, 2021.

[20] 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 Trans. Ind. Electron.*, vol. 68, no. 10, pp. 9707–9718, 2021.

[21] Y. Jiang, Y. Yang, S.-C. Tan, and S. Y. R. Hui, "A high-order differentiator based distributed secondary control for dc microgrids against false data injection attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 4035–4045, 2022.

[22] Y. Jiang, Y. Yang, S.-C. Tan, and S. Y. Hui, "Distributed sliding mode observer-based secondary control for dc microgrids under cyber-attacks," *IEEE J. Emerg. Sel. Top Circuits Syst.*, vol. 11, no. 1, pp. 144–154, 2020.

[23] S. Tan, P. Xie, J. M. Guerrero, J. C. Vasquez, J. M. Alcala, J. E. M. Carreño, and M. G. Zapata, "Lyapunov-based resilient cooperative control for dc microgrid clusters against false data injection cyber-attacks," *IEEE Trans. Smart Grid*, 2023.

[24] M. S. Sadabadi, N. Mijatovic, J.-F. Trégouët, and T. Dragičević, "Distributed control of parallel dc–dc converters under fdi attacks on actuators," *IEEE Trans. Ind. Electron.*, vol. 69, no. 10, pp. 10 478–10 488, 2022.

[25] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient networked ac microgrids under unbounded cyber attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3785–3794, 2020.

[26] M. Jamali, M. S. Sadabadi, M. Davari, S. Sahoo, and F. Blaabjerg, "Resilient cooperative secondary control of islanded ac microgrids utilizing inverter-based resources against state-dependent false data injection attacks," *IEEE Trans. Ind. Electron.*, 2023.

[27] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, "A fdi attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 1929–1938, 2020.

[28] Z. Song, A. Skuric, and K. Ji, "A recursive watermark method for hard real-time industrial control system cyber-resilience enhancement," *IEEE Trans. Autom. Sci. Eng.*, vol. 17, no. 2, pp. 1030–1043, 2020.

[29] 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," *IIEEE Trans. Circuits Syst. II Express Briefs*, vol. 68, no. 2, pp. 717–721, 2020.

[30] M. R. Habibi, S. Sahoo, S. Rivera, T. Dragičević, and F. Blaabjerg, "Decentralized coordinated cyberattack detection and mitigation strategy in dc microgrids based on artificial neural networks," *IEEE J. Emerg. Sel. Top. Power Electron.*, vol. 9, no. 4, pp. 4629–4638, 2021.

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

[32] A. Cecilia, S. Sahoo, T. Dragičević, R. Costa-Castelló, and F. Blaabjerg, "On addressing the security and stability issues due to false data injection attacks in dc microgrids—an adaptive observer approach," *IEEE Trans. Power Electron.*, vol. 37, no. 3, pp. 2801–2814, 2022.

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

[34] M. Liu, C. Zhao, Z. Zhang, R. Deng, P. Cheng, and J. Chen, "Converter-based moving target defense against deception attacks in dc microgrids," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3984–3996, 2022.

[35] 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 Trans. Smart Grid*, vol. 14, no. 1, pp. 714–731, 2023.

[36] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 106–117, 2016.

[37] C. Liu, R. Deng, W. He, H. Liang, and W. Du, "Optimal coding schemes for detecting false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 738–749, 2022.

[38] HUAWEI, "Sun2000-(50ktl-zhm3, 50ktl-m3) user manual," Accessed: 2024, [Online]. Available: https://download.huawei.com/edownload/e/download.do?actionFlag=download&nid=EDOC1100369104&partNo=6001&mid=SUPE_DOC&_t=20240426103315000.

[39] SUNGROW, "Pv grid-connected inverter user manual sg250hx-us," Accessed: 2024, [Online]. Available: https://info-support.sungrowpower.com/application/pdf/2022/04/25/SG250HX-US-UEN-Ver17-202203.pdf.

[40] SOliS, "User manual for 4g series grid inverter - solis-1p(3.6-5)k-4g-us," Accessed: 2024, [Online]. Available: https://www.solisinverters.com/uploads/file/Solis_Manual_(3,6-5)K_4G_PLUS_LW_USA_03212023.pdf#page=19.10.

[41] GROWATT, "Mid 11-30ktl3-xh user manual," Accessed: 2024, [Online]. Available: https://en.growatt.com/upload/file/MID_11-30KTL3-XH_User_Manual_EN_202405.pdf.
[42] C. Brumfield, "Hijack of monitoring devices highlights cyber threat to solar power infrastructure," (Accessed: 2024). [Online]. Available: https://www.csoonline.com/article/2119281/hijack-of-monitoring-devices-highlights-cyber-threat-to-solar-power-infrastructure.html
[43] J. Johnson, B. Anderson, B. Wright, J. Quiroz, T. Berg, R. Graves, J. Daley, K. Phan, M. Kunz, R. Pratt *et al.*, "Cybersecurity for electric vehicle charging infrastructure." Sandia National Lab, Tech. Rep., 2022.
[44] 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.
[45] J. Taylor, *Introduction to error analysis, the study of uncertainties in physical measurements*. University Science Books, 1997.
[46] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to dc microgrids," *IEEE Trans. Automat. Contr.*, vol. 65, no. 9, pp. 3800–3815, 2020.

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 School of Electrical and Electronic Engineering, University of Sheffield, Sheffield, U.K. His research interests include smart grid, cyber-physical security, and cyber-physical co-simulation.

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. Currently, he is a Professor of Control and Power Systems with the School of Electrical and Electronic Engineering, University of Sheffield, Sheffield, U.K. 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. 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.

Chengcheng Zhao (Member, IEEE) received the B.Sc. degree in measurement and control technology and instruments from Hunan University, Changsha, China, in 2013, and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2018. She was a PostDoctoral Fellow with the College of Control Science and Engineering, Zhejiang University, from 2018 to 2021. She is currently a Researcher with the College of Control Science and Engineering, Zhejiang University. Her research interests include consensus and distributed optimization, and security and privacy in networked systems. She received the IEEE PESGM 2017 Best Conference Papers Award, and one of her papers was shortlisted in the IEEE ICCA 2017 Best Student Paper Award Finalist. She is an Editor of Wireless Networks and IET Cyber-Physical Systems: Theory and Applications.

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.