Cyber-Resilient Adaptive Control of Grid-Following Inverter-Based Resources Against Measurement Manipulation

Jamali, Mahmood ; Sadabadi, Mahdieh S.; Oshnoei, Arman

Published in:
25th IEEE International Conference on Industrial Technology

Publication date:
2024

Cyber-Resilient Adaptive Control of Grid-Following Inverter-Based Resources Against Measurement Manipulation

Mahmood Jamali
Dept. of Automatic Control and Systems Engineering
University of Sheffield
Sheffield, United Kingdom
mahmood.jamali@sheffield.ac.uk

Mahdieh S. Sadabadi
Dept. of Electrical and Electronic Engineering
University of Manchester
Manchester, United Kingdom
mahdieh.sadabadi@manchester.ac.uk

Arman Oshnoei
Dept. of Energy
Aalborg University
Aalborg, Denmark
aros@energy.aau.dk

***Abstract*—The cyber vulnerability of smart inverters is exacerbated by the widespread adoption of data transfer and communication platforms. This paper proposes a novel resilient adaptive vector current control scheme designed for three-phase grid-following (GFL) inverter-based resources (IBRs) at the device level of modernized power grids. While effective upper-layer control strategies exist, malicious attackers can still exploit susceptibilities in the primary control of GFL IBRs. The control objective is to substantially mitigate the destructive impacts of sensor attacks while ensuring that the system's outputs (or current signals) track the desired references. The proposed adaptive control scheme is structured based on a state estimator and an attack estimator, which rectifies the manipulated measurements, thereby enhancing resilient performance against time-invariant and uniform-bounded sensor attacks. Lyapunov theory delivers a rigorous theoretical analysis and asymptotic stability. Comparative simulation results further illustrate the resilience and efficiency of the proposed adaptive control methodology.**

***Index Terms*—False data injection (FDI) sensor attacks, state estimator and attack estimator, three-phase grid-following (GFL) inverter-based resources (IBRs), resilient adaptive control scheme.**

I. INTRODUCTION

The conventional power grids have rapidly evolved into modernized power systems, utilizing renewable energy resources and innovations, in response to the global energy crisis and climate change concerns. The increased utilization of renewable energy resources underscores the pivotal role of advanced power electronics in effectively managing the diversity of generation sources and loads [1]. Grid-following (GFL) inverter-based resources (IBRs) serve as controllable interfaces within modernized power grids, including microgrids, to establish a link between the cyber network and physical devices. In particular, three-phase GFL IBRs facilitate the seamless integration of renewable energy resources, along with remote and dynamic control capabilities. The implementation of modernized power systems with the pervasive fusion of information technologies is commonly referred to as cyber-physical systems (CPSs)-based power grids. These advancements make a significant contribution to improving the flexibility and overall performance of power systems [2].

The computational system of CPS-based microgrids is responsible for a variety of functions in highly sensitive environments, relying extensively on the efficient collection, processing, and transmission of data. This integration of devices with information technologies creates a broad cyberattack surface that could potentially be targeted by serious threats, posing risks to the confidentiality and integrity of data in microgrids. In cases where such cyberattacks are executed stealthily or intentionally designed with authorized access, the security protocols in place might fail to identify them [3]. As a result, data corruption, involving alterations to control commands and measured data, has the potential to push microgrids into unstable and unsafe operational states. The recovery process following such cyberattacks may be protracted or even unachievable. This may result in equipment damage, broad-scale blackouts, and considerable economic losses [4].

To minimize concerns regarding malicious attacks and ensure safe operations, cybersecurity must be given a top priority in modernized power grids. Recent investigations have highlighted resilient and cybersecurity-related issues and challenges in identifying attacks in CPS-based microgrids, as detailed in [5]–[7] and references therein. The authors in [8] propose a detection scheme that combines the Kalman filter and the adaptive cumulative sum method to identify spoofed sensor data in grid-connected IBRs. A technique of dynamic watermarking is suggested in [9] to differentiate between malicious attacks and sensor unreliability in grid-tied IBRs.

All the developed techniques have a common objective, which is to enhance the level of security against cyber threats. However, depending solely on these identification methods may be inadequate and ineffectual if a sophisticated threat actor can circumvent the established identification protocols. With this critical consideration, it becomes imperative to concentrate on mitigation control schemes for smart inverters to reduce the impact of cyberattacks. From a control standpoint, designing resilient control techniques for GFL IBRs in CPS-based microgrids is challenging due to the need for swift response times, normally from 0.5 to 5 ms—as stipulated by IEEE Std 1547.P10-2018 [10].

The focus of research on mitigating strategies for CPS-based microgrids against attacks predominantly centers on the islanded operation mode. Recent studies addressing this topic can be found in [11]–[13]. The ultimate control objective of interest in these methods is to design a system-level resilient control framework to mitigate the adverse effects of cyber-attacks on higher-level control layers. Nevertheless, primary control (or device-level control) in both operation modes of

CPS-based microgrids remains vulnerable to exploitation by malware through firmware updates, as emphasized in [14]. Therefore, giving precedence to improving resilience and cybersecurity at the individual device is indispensable. This approach, consequently, ensures that the operation of modernized power grids with IBRs remains safe and secure, thus reducing the susceptibility to strategically launched cyberattacks.

While studies in [15], [16] have addressed the challenges of control design for GFL IBRs in the presence of faulty sensors, further investigations are required in scenarios where an attacker manipulates the data from the sensors and inputs fabricated measurement signals to the controller. Motivated by the concerns detailed above and existing gaps in the literature, this paper presents a resilient adaptive control scheme specifically crafted for GFL IBRs. The main goal is to derive the system's outputs (or current signals of IBRs) to the reference values, even in the presence of manipulated measurements due to sensor attacks. The proposed methodology aims to fortify the resilience of primary controls against manipulated measurement signals, which could go undetected to operators and affect the direct-quadrature (dq) frame output signals of GFL IBRs. As a result, false data injection (FDI) attacks compromise the available sensor measurement signals to maximally degrade the feedback control efficacy. In the event of sensor attacks, a disparity emerges between the actual and measured IBR output signals, leading to imprecise control commands and incorrect switching sequences. Hence, this study, inspired by the findings in [17], introduces an adaptive control structure to guarantee the accurate execution of switching and modulation processes. To achieve this, a state estimator and an attack estimator are augmented with an integral component to complement the state feedback controller. This estimator-based control framework not only boosts resilience but also certifies stability in the face of sensor data integrity attacks. The paper's main contributions are summarized as follows.

- It proposes a novel resilient vector current control strategy for GFL IBRs by employing a state estimator and an attack estimator, which form restorative control signals integrated into the state control feedback, that can mitigate the effect of FDI time-invariant and uniform-bounded sensor attacks.
- It develops a control scheme to enhance sensor-attack resilience in the primary control of GFL IBRs and establishes a reliable operation. The proposed controller guarantees reference tracking even in the face of FDI sensor attacks capable of manipulating all available measurements.
- It presents a theoretical stability analysis using Lyapunov theory and LaSalle's invariance principle to rigorously support the proof of asymptotic stability of the closed-loop control system.

MATLAB simulation results verify the effectiveness of the proposed resilient adaptive vector current control scheme.

The remainder of the paper is organized as follows. Section II provides the mathematical model of a GFL IBR utilizing the LCL filter in a state-space form. Section III presents the proposed resilient vector current control scheme and delves into the analysis of the stability. Section IV validates the effectiveness of the proposed control scheme by providing the simulation results. Section V concludes the paper.

The notation employed throughout this paper is fairly standard. In this context, $\mathbb{R}$ represents the set of real numbers, $\mathbb{R}^n$ denotes column vectors of size n, and $\mathbb{R}^{n\times m}$ signifies real matrices with dimensions $n\times m$. The operator $\|.\|$ corresponds to the standard Euclidean norm. For a symmetric matrix $\mathcal{A}$, the notation $\mathcal{A} > 0$ and $\mathcal{A} \leq 0$ are shown to respectively indicate positive definiteness and negative semi-definiteness. The symbol $\mathbf{0}_n$ indicates an $n \times n$ matrix of zeros.

II. Mathematical Model of System Under Study

Considering Fig. 1, the mathematical representation of the state-space model for a GFL IBR (equipped) with an LCL filter in the dq reference frame is provided as follows [16].

$$\dot{x} = Ax + Bu \tag{1a}$$

$$y = Cx \tag{1b}$$

where $x = [i_{1d} \;\; i_{1q} \;\; i_{2d} \;\; i_{2q} \;\; v_{cfd} \;\; v_{cfq}]^T \in \mathbb{R}^6$ is the state vector, the input vector is defined as $u = [m_d \;\; m_q]^T \in \mathbb{R}^2$, the output vector is characterized as $y = [i_{2d} \;\; i_{2q}]^T \in \mathbb{R}^2$, and the state matrices are specified as

$$A = \begin{bmatrix} -\frac{R_{t_1}}{L_{f_1}} & \omega & \frac{R_f}{L_{f_1}} & 0 & -\frac{1}{L_{f_1}} & 0 \\ -\omega & \frac{R_{t_1}}{L_{f_1}} & 0 & \frac{R_f}{L_{f_1}} & 0 & -\frac{1}{L_{f_1}} \\ \frac{R_f}{L_{f_2}} & 0 & -\frac{R_{t_2}}{L_{f_2}} & \omega & \frac{1}{L_{f_2}} & 0 \\ 0 & \frac{R_f}{L_{f_1}} & -\omega & \frac{R_{t_2}}{L_{f_2}} & 0 & \frac{1}{L_{f_2}} \\ \frac{1}{C_f} & 0 & -\frac{1}{C_f} & 0 & 0 & \omega \\ 0 & \frac{1}{C_f} & 0 & -\frac{1}{C_f} & -\omega & 0 \end{bmatrix} \tag{2a}$$

$$B = \begin{bmatrix} \frac{V_{dc}}{2L_{f_1}} & 0 \\ 0 & \frac{V_{dc}}{2L_{f_1}} \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \; C = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{2b}$$

In this representation, in compliance with Fig. 1, i_{d1} and i_{q1} denote the dq components of the inverter current phasor $\overrightarrow{i_1}$, representing i_{1a}, i_{1b}, and i_{1c}; i_{d2} and i_{q2} refer to the dq components of the current phasor $\overrightarrow{i_2}$, indicating i_{2a}, i_{2b}, and i_{2c}; v_{cfd} and v_{cfq} correspond to the dq components of the RC filter voltage; m_d and m_q stand for the modulation indices governing the switching operation of the GFL IBR in the dq framework. In (2a), $R_{t_1} \triangleq R_{f_1} + R_f$ and $R_{t_2} \triangleq R_{f_2} + R_f$. Here, L_{f_1}/R_{f_1} is the inductance/resistance for the IBR side of the LCL filter, while L_{f_2}/R_{f_2} denotes the inductance/resistance for the grid side of the LCL filter. Furthermore, C_f expresses the shunt capacitance of the LCL filter. The control input u is utilized to ensure stability and

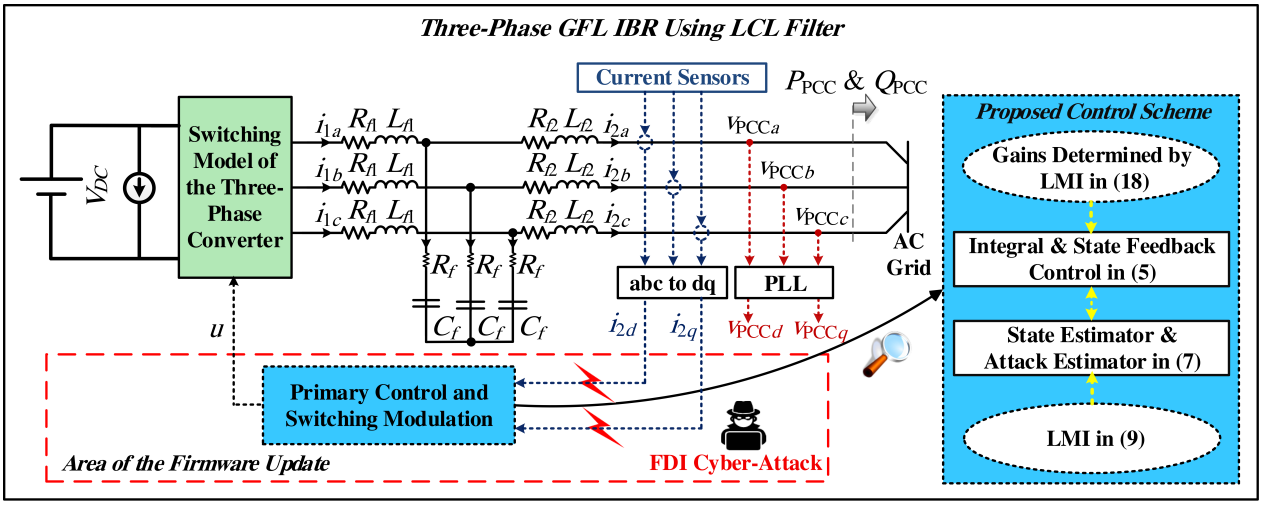

Fig. 1. Block diagram of a GFL IBR using LCL filter outfitted with the proposed control scheme under FDI sensor attacks.

achieve rapid and seamless reference tracking performance, specifically, ensuring that i_{2d} and i_{2q} respectively converge to $i_{2\text{d-ref}}$ and $i_{2\text{q-ref}}$ in the steady-state. Here, $i_{2\text{d-ref}}$ and $i_{2\text{q-ref}}$ represent the reference values for i_{2d} and i_{2q}, respectively. Worth noting that the reference signals, $i_{2\text{d-ref}}$ and $i_{2\text{q-ref}}$, are derived from the desired values for the active power ($P_{\text{PCC-ref}}$) and reactive power ($Q_{\text{PCC-ref}}$) injected into the point of common coupling (PCC) along with V_{PCCd} which is the d component of the PCC voltage.

A. Sensor Data Manipulation

In the context of GFL IBR, the system's output variables often include the current signals of IBRs. When inverters rely on external measurement units or sensors to access data, malicious actors could exploit various methods to perform FDI attacks, which creates a bias on reported measurements, to manipulate the data transmitted to the controller [18]. Modifications to the measured data can directly influence inverter dynamics, potentially resulting in undesirable impacts on the system performance and unpredictable consequences.

In the event of sensor attacks, the integrity of the output signal y is compromised, which subsequently modifies the dynamics of the IBR described in (1b). The dynamics of a GFL IBR (equipped) with an LCL filter in the presence of FDI attacks on the outgoing measured data can be reformulated as follows.

$$\begin{aligned} \dot{x} &= Ax + Bu, \\ y &= C(\underbrace{x + \delta_{\mathbf{x}}(t)}_{\tilde{x}}), \end{aligned} \tag{3}$$

where $\tilde{x} \in \mathbb{R}^6$ is the manipulate sensor measurement and $\delta_{\mathbf{x}}(t) \in \mathbb{R}^6$ is the FDI attack vector manipulating sensor measurements in the primary control of GFL IBRs.

Any form of falsification injected into the measurements is intended to externally manipulate and distort them, leading to the production of imprecise control signals. This, in turn, results in inaccurate modulation indices and switching signals, ultimately causing a disruption in the proper operation of the IBR. Hence, the adoption of a resilient control strategy becomes essential for effectively mitigating the impacts of cyber-attacks. The following section provides a detailed explanation of the proposed cyber-resilient control scheme. It illustrates the controller's capacity to achieve offset-free current tracking performance and maintain the stability of GFL IBRs, even when confronted with data integrity sensor cyberattacks.

Cyberattack tactics have frequently evolved. Adversaries aim to design strategic cyberattacks, referred to as stealthy attacks, to evade existing IBRs' cyber-defense mechanisms while having an adverse impact on the stability and performance of the IBRs. Any sudden and unauthorized changes in the measurements or behavior of devices can be simply identified by cyber-defense mechanisms or bad-data detectors. As a result, attackers typically refrain from injecting unbounded signals into sensor measurements in order to preserve the attribute of stealth. Moreover, time-invariant false data can be designed to emulate authentic system states in the dq framework. Given the constant and time-invariant characteristics of the dq framework, such attacks are less likely to stand out as suspicious. Therefore, this paper makes the following assumption regarding FDI attacks on sensor measurements.

Assumption 1. It is assumed that any FDI attacks manipulating sensor measurements in (3) are both "*uniform-bounded*" and "*time-invariant*", where, $\delta_{\mathbf{x}}(t) \equiv \delta_{\mathbf{x}}$ and $\|\delta_{\mathbf{x}}\|$ is finite. Besides, the system dynamics (1) are externally influenced by altering the measured data through firmware updates.

III. Resilient Adaptive Control Scheme

This section discusses the development of a resilient adaptive control scheme designed to address reference tracking current control for GFL IBRs in the face of FDI sensor attacks. The analysis demonstrates that the proposed control strategy is resilient against uniform-bounded and time-invariant FDI

sensor attacks. Thus, the output of the system in (1b) remains bounded and tracks the reference values regardless of the existence of FDI cyberattacks on sensors.

In the conventional design of vector current control for GFL IBRs, the vector controller includes a state feedback controller and an integrator whose dynamics are given as follows:

$$u = K_{\mathbf{x}} x + K_{\mathbf{z}} z \tag{4a}$$

$$\dot{z} = -Cx + y^* \tag{4b}$$

where $z \in \mathbb{R}^2$ denotes the state of the integrator, while $K_{\mathbf{x}} \in \mathbb{R}^{2\times 6}$ is the feedback gain matrix. Additionally, $K_{\mathbf{z}} \in \mathbb{R}^{2\times 2}$ represents a integrator gain matrix and $y^* = [i_{\text{2d-ref}} \;\; i_{\text{2q-ref}}]^T \in \mathbb{R}^2$ is the dq reference signal vector. The gain matrices $K_{\mathbf{x}}$ and $K_{\mathbf{z}}$ are designed so that the closed-loop system becomes stable. Note that the integrator is incorporated into the original state feedback controller to attain precise (offset-free) current reference tracking. The conventional vector current controller presented in (4) is highly effective in terms of tracking and achieving the desired performance. However, it is vulnerable to FDI sensor attacks since it relies on compromised states for generating control commands. In what follows, a state estimator and an attack estimator are introduced and integrated into the original controller to address this deficiency. The inclusion of restorative control signals through the estimation process bolsters the resilience of GFL IBRs equipped with the proposed resilient control scheme.

We modify the control command u in (4a) and the integrator dynamics in (4b) by developing an adaptive control scheme. The proposed adaptive current controller includes restorative control signals $\xi_{\mathbf{x}}$ and $\xi_{\mathbf{z}}$ in the presence of FDI sensor attacks as follows.

$$u = -K_{\mathbf{x}}\tilde{x} - K_{\mathbf{z}} z + \underbrace{K_{\mathbf{x}}\hat{\delta}_{\mathbf{x}}}_{\xi_{\mathbf{x}}} \tag{5a}$$

$$\dot{z} = -C\tilde{x} + y^* + \underbrace{C\hat{\delta}_{\mathbf{x}}}_{\xi_{\mathbf{z}}} \tag{5b}$$

where $\hat{\delta}_{\mathbf{x}} \in \mathbb{R}^6$ represents the estimated sensor attack, which will be introduced in (7a).

Let us denote the augmented state vector and state feedback matrix as $X = [x^T \;\; z^T]^T$ and $K = [K_{\mathbf{x}} \; K_{\mathbf{z}}]$. The overall dynamics of the closed-loop GFL IBRs in (1) with the adaptive current controller in (5), and in the presence of sensor attacks, can be written as follows:

$$\dot{X} = A_a X - (B_a K - C_a)\left(\tilde{X} - \hat{\Delta}\right) + r \tag{6}$$

where $A_a = \begin{bmatrix} A & \mathbf{0}_{6\times 2} \\ \mathbf{0}_{2\times 6} & \mathbf{0}_{2\times 2} \end{bmatrix}$; $B_a = \begin{bmatrix} B \\ \mathbf{0}_{2\times 2} \end{bmatrix}$; $C_a = \begin{bmatrix} \mathbf{0}_{6\times 6} & \mathbf{0}_{6\times 2} \\ -C & \mathbf{0}_{2\times 2} \end{bmatrix}$; $\hat{\Delta}(t) = [\hat{\delta}_{\mathbf{x}}^T \;\; \mathbf{0}_{1\times 2}]^T$ is the estimation of the augmented sensor attack vector Δ; $\tilde{X}(t) = [\tilde{x}^T \;\; z^T]^T \in \mathbb{R}^8$ is the manipulated state vector and $r = \begin{bmatrix} \mathbf{0}_{6\times 1} \\ y^* \end{bmatrix}$. The following estimators are designed to establish the restorative control signals to achieve stabilization and current reference tracking in the presence of FDI sensor attacks.

$$\dot{\hat{\Delta}}(t) = -\beta A_a^T P\left(\tilde{X}(t) - \hat{X}(t) - \hat{\Delta}(t)\right) \tag{7a}$$

$$\dot{\hat{X}}(t) = A_r \hat{X}(t) + (\beta A_a^T P + H)\left(\tilde{X}(t) - \hat{X}(t) - \hat{\Delta}(t)\right) + r \tag{7b}$$

where $\hat{X}(t) = [\hat{x}^T \;\; \hat{z}^T]^T \in \mathbb{R}^8$ is the estimation of the manipulated state variables. Additionally, $\beta \in \mathbb{R}$ denotes a positive tuning gain and $H \in \mathbb{R}^{8\times 8}$ serves as the gain matrix for the state estimator. The estimator gain H is chosen so that $G := (A_r - H)$ is a Hurwitz matrix, where

$$A_r = \begin{bmatrix} A - BK_{\mathbf{x}} & -BK_{\mathbf{z}} \\ -C & \mathbf{0}_2 \end{bmatrix}. \tag{8}$$

In accordance with the converse Lyapunov theory [19], this selection enables the control designer to find a positive-definite matrix $P \in \mathbb{R}^{8\times 8}$ that satisfies the following inequality.

$$G^T P + P^T G + \alpha P < 0 \tag{9}$$

where $\alpha \in \mathbb{R}$ is a non-negative constant.

The main theoretical results of this paper are given in the following theorem. It shows that the GFL IBR equipped with the proposed controller in (5) remains stable and the output signals of the IBR (1b) can successfully track the desired reference current values even when subjected to FDI sensor attacks. Before proceeding with the analysis, let us define the error vectors as $e \triangleq \tilde{X}(t) - \hat{X}(t) - \hat{\Delta}(t)$ and $\tilde{\Delta} \triangleq \Delta - \hat{\Delta}$. According to Assumption 1, from (7) one can yield

$$\dot{\tilde{\Delta}} = \beta A_a^T P e. \tag{10}$$

By referring to (6) and using (7), one can derive the following results for the state error dynamics.

$$\begin{aligned} \dot{e} &= A_a X - (B_a K - C_a)\left(\tilde{X} - \hat{\Delta}\right) \\ &= -A_r \hat{X} - (\beta A_a^T P + H)e + \beta A_a^T P e. \end{aligned} \tag{11}$$

Next, by adding and subtracting $A_r\hat{\Delta}$ to and from (11), one can obtain

$$\begin{aligned} \dot{e} &= (A_a - B_a K + C_a)\,\tilde{X} + B_a K\hat{\Delta} - C_a\hat{\Delta} \\ &= -A_r\hat{X} - He + A_r\hat{\Delta} - A_r\hat{\Delta}. \end{aligned} \tag{12}$$

Recall that $A_r = A_a - B_a K + C_a$ as derived in (8). From (6), by rearranging (12), the following compact form for the state error dynamics is obtained:

$$\dot{e} = Ge - A_a\tilde{\Delta}. \tag{13}$$

Theorem 1. *Consider the GFL IBR system given by* (3)*, subject to uniform-bounded and time-invariant sensor attacks satisfying Assumption 1. With the proposed adaptive current*

vector controller in (5) *and utilizing the state estimator and attack estimator in* (7)*, the error dynamics* $\dot{e}$ *and* $\dot{\tilde{\Delta}}$ *in* (10) *and* (13) *are uniformly bounded for all initial conditions. Furthermore, the GFL IBR current outputs successfully track the dq reference values in the presence of FDI sensor attacks, i.e.* $\lim_{t\to\infty}(y - y^*) = \mathbf{0}_{2\times 1}$.

Proof. In order to prove the asymptotic stability of the origin in the error dynamics defined in (10) and (13), the following quadratic Lyapunov function candidate is considered.

$$V(e, \tilde{\Delta}) = e^T P e + \beta^{-1} \tilde{\Delta}^T \tilde{\Delta} \tag{14}$$

where $P > 0$ satisfies (9). It is apparent that $V(0, 0) = 0$, $V(e, \tilde{\Delta}) > 0$ and $V(e, \tilde{\Delta})$ ensures radially unbounded behavior. The time derivative of (14) along the error dynamics in (10) and (13) is derived as follows.

$$\begin{aligned} \dot{V}(e, \tilde{\Delta}) &= 2e^T P \left(Ge - A_a \tilde{\Delta} \right) + 2\tilde{\Delta} A_a^T P e \\ &= e^T \left(G^T P + PG \right) e \\ &= -\alpha e^T P e \leq 0. \end{aligned} \tag{15}$$

Thereby, the error dynamics in (10) and (13) are uniformly bounded for all initial conditions.
Now, to demonstrate that $\lim_{t\to\infty}(y - y^*) = \mathbf{0}_{2\times 1}$, it is required to take the second derivative of the Lyapunov candidate in (14) which is as follows.

$$\ddot{V}(e, \tilde{\Delta}) = -2\alpha e^T P \left(Ge - A_a \tilde{\Delta} \right). \tag{16}$$

Note that since the set of $(e, \tilde{\Delta})$ is bounded for all $t \geq 0$, (16) is also guaranteed to be bounded. Consequently, $\dot{V}(e, \tilde{\Delta})$ is uniformly continuous with respect to t. By using Barbalat's lemma [19], $\lim_{t\to\infty} \dot{V}(e, \tilde{\Delta}) = 0$ and $e(t)$ converges to 0 as $t \to \infty$. To advance with the proof, let us establish the zero-dissipation set as

$$\Lambda := \left\{ (e, \tilde{\Delta}) \in \mathbb{R}^8 \times \mathbb{R}^8 \mid \dot{V}(e, \tilde{\Delta}) = 0 \right\}, \tag{17}$$

and $\Gamma \subseteq \Lambda$, which is the largest invariant set in Λ. It can be deduced from (10) that $A_a \tilde{\Delta} = 0$, leading to $\tilde{\Delta} = 0$. As a result, the largest invariant set of Λ is the origin, i.e. $(e, \tilde{\Delta}) \to \Gamma = \{(0, 0)\}$ as $t \to \infty$. This implies that $\lim_{t\to\infty}(X - \hat{X}) = \mathbf{0}_8$, indicating the convergence of the estimated states to the authentic system states. According to (5b), it can be concluded that $\lim_{t\to\infty}(y - y^*) = \mathbf{0}_{2\times 1}$. This completes the proof. ■

IV. Simulation Results

For illustration purposes, this section provides comparative simulation results for the proposed resilient adaptive vector current control scheme. In order to evaluate the effectiveness of the controller, numerical simulations are conducted using MATLAB/Simulink. Additionally, this section includes simulation results for the conventional PI current controller applied to GFL IBRs, vividly showing its failure while under FDI sensor attacks. In this regard, a three-phase GFL IBR using an LCL filter, as depicted in Fig. 1, is considered and its parameters are detailed as follows: $L_{f_1}/R_{f_1} = L_{f_2}/R_{f_2} = 1.1\ mH/0.01\ \Omega$, $C_f/R_f = 15.4\ \mu F/2.08\ \Omega$ and $V_{DC} = 400\ V$. To devise appropriate restorative control signals, the parameters for the estimators in (7) are configured as $\beta = 500$ and $H = 600 \times \mathbf{I}_{8\times 8}$ (identity matrix). The matrix P is obtained by solving the linear matrix inequality (LMI) problem in (9). The state feedback matrices $K_{\mathbf{x}}$ and $K_{\mathbf{z}}$ are outlined by solving the following LMI problem.

$$Q(A_a + C_a)^T + (A_a + C_a)Q - K^T B_a^T - B_a K + \gamma Q \leq 0 \tag{18}$$

where $Q > 0 \in \mathbb{R}^{8\times 8}$ and $\gamma \in \mathbb{R}$ is a positive constant.

A uniform-bounded and time-invariant FDI attack, consistent with Assumption 1, is launched to manipulate the data integrity of sensor measurements. The FDI sensor attack vector, representing the characteristics of a potential sensor attack in the dq framework, is designated as $\delta_{\mathbf{x}} = \begin{bmatrix} 0 & 0 & 2 & 3 & 0 & 0 \end{bmatrix}^T$. It is assumed that the attack targets the current sensor measurements of the GFL IBR at t=3 s and persists until the end of the simulation time. To attain the desired active and reactive power levels, abrupt load changes occur at t = 1 s and t = 2 s, correspondingly. The simulation results for the key signals of interest, which include the actual current signals in the dq-frame (i_{2d} and i_{2q}), active power (P_{PCC}), and reactive power (Q_{PPC}) of the GFL IBR, are shown in Fig. 2. As evident from this figure, the GFL IBR, equipped with the proposed adaptive current control scheme, demonstrates resilience against FDI sensor attacks and effectively recovers the desired performance in the face of FDI sensor attacks. The signals swiftly return to their reference values within a brief time frame, specifically in less than 0.1 s. The state estimator and attack estimator signals are also depicted in Fig. 3, affirming the successful estimation process.

Fig. 4 depicts the simulation results for the conventional PI current controller. As observed from this figure, this controller effectively achieves reference tracking before the occurrence of the FDI sensor attack. However, following the cyber intrusion, the signals of interest struggle to return promptly to their reference values. Therefore, the capacity for tracking references is compromised.

V. Conclusion

This paper has developed and investigated a resilient adaptive control framework for the vector current control of the grid-following inverter-based resources in the presence of manipulated measurements resulting from cyber-attacks. The attackers are assumed to infiltrate sensor measurements and affect the controller by injecting false data. The proposed adaptive control scheme comprises a state estimator and an attack estimator, designed to mitigate the effects of uniform-bounded and time-invariant sensor attacks. A thorough Lyapunov stability certificate has also been derived. Simulation results have verified the cyber-resilience of the proposed current control framework. The future research direction will focus on (i) extending the proposed control scheme to address false data injection attacks on both control inputs and sensors in

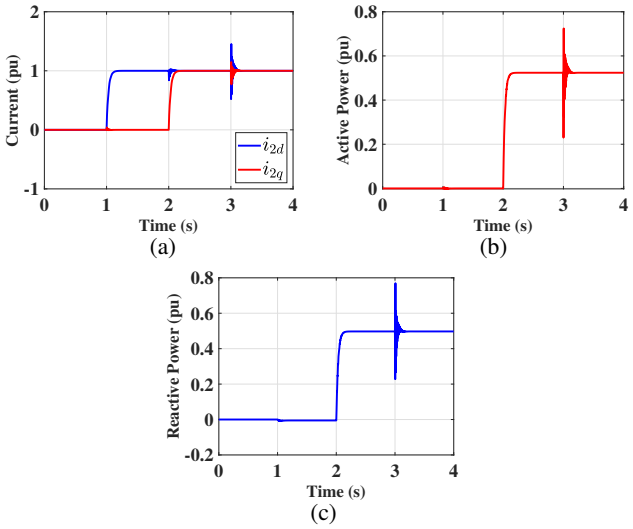

Fig. 2. Performance of the proposed resilient adaptive current control scheme: (a) actual current signals i_{2d} and i_{2q}, (b) active power (P_{PCC}) and (c) reactive power (Q_{PCC}) of GFL IBR.

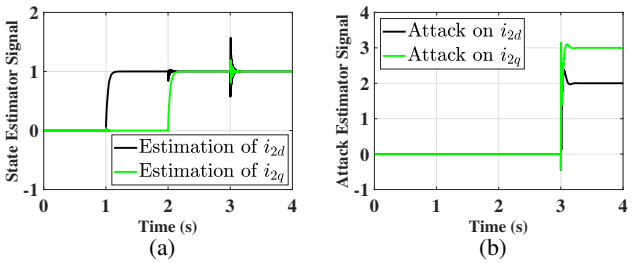

Fig. 3. Estimated signals of interest by estimators in (7): (a) currents (i_{2d} and i_{2q}) and (b) attacks affecting them.

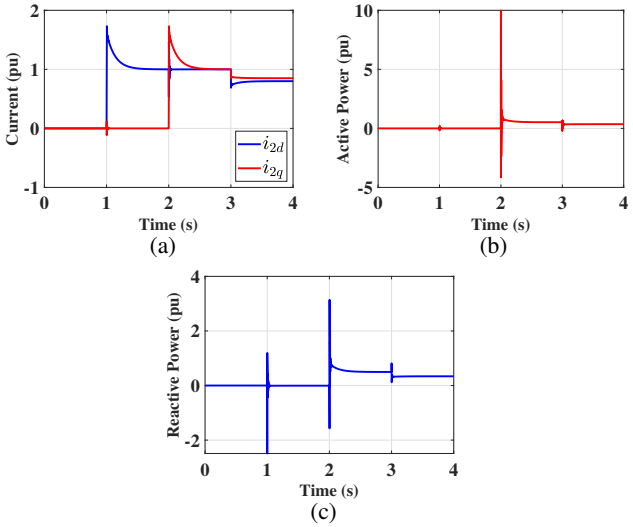

Fig. 4. Performance of the PI controller configured with control gains $K_P = 5$ and $K_I = 25$: (a) actual current signals i_{2d} and i_{2q}, (b) active power (P_{PCC}) and (c) reactive power (Q_{PCC}) of GFL IBR.

grid-following inverter-based resources and (ii) experimental validation of the proposed control methodology.

REFERENCES

[1] T. O. Olowu, S. Dharmasena, H. Jafari, and A. Sarwat, "Investigation of false data injection attacks on smart inverter settings," in *2020 IEEE CyberPELS (CyberPELS)*. IEEE, 2020, pp. 1–6.

[2] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy," *IEEE Access*, vol. 10, pp. 35 846–35 875, 2022.

[3] S. K. Mazumder, A. Kulkarni, S. Sahoo, F. Blaabjerg, H. A. Mantooth, J. C. Balda, Y. Zhao, J. A. Ramos-Ruiz, P. N. Enjeti, P. Kumar *et al.*, "A review of current research trends in power-electronic innovations in cyber–physical systems," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5146–5163, 2021.

[4] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151 019–151 064, 2020.

[5] H. Goyel and K. S. Swarup, "Data integrity attack detection using ensemble-based learning for cyber–physical power systems," *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1198–1209, 2022.

[6] A. Kavousi-Fard, W. Su, and T. Jin, "A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 650–658, 2020.

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

[8] J. Zhang, M. D. R. Greidanus, S. K. Mazumder, J. Ye, W. Song, and H. A. Mantooth, "Model-based detection scheme for spoofed sensor data in grid-connected inverters," *IEEE Transactions on Industrial Electronics*, vol. 71, no. 3, pp. 3224–3228, 2023.

[9] W.-H. Ko, J. A. Ramos-Ruiz, T. Huang, J. Kim, H. Ibrahim, P. N. Enjeti, P. Kumar, and L. Xie, "Robust dynamic watermarking for cyber-physical security of inverter-based resources in power distribution systems," *IEEE Transactions on Industrial Electronics (Early Access)*, 2023.

[10] IEEE Standards Coordinating Committee 21, "1547-2018 - IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," IEEE Std 1547, Tech. Rep., 2018.

[11] M. S. Sadabadi, N. Mijatovic, J.-F. Trégouët, and T. Dragičević, "Distributed control of parallel DC–DC converters under FDI attacks on actuators," *IEEE Transactions on Industrial Electronics*, vol. 69, no. 10, pp. 10 478–10 488, 2021.

[12] 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 Transactions on Industrial Electronics*, vol. 71, no. 1, pp. 4719–4730, 2023.

[13] M. Jamali and M. S. Sadabadi, "Resilient angle stabilization in converter-interfaced microgrids," in *2023 European Control Conference (ECC)*. IEEE, 2023, pp. 1–6.

[14] M. G. Angle, S. Madnick, J. L. Kirtley, and S. Khan, "Identifying and anticipating cyberattacks that could cause physical damage to industrial control systems," *IEEE Power and Energy Technology Systems Journal*, vol. 6, no. 4, pp. 172–182, 2019.

[15] S. Saha, M. Haque, C. Tan, M. A. Mahmud, M. Arif, S. Lyden, and N. Mendis, "Diagnosis and mitigation of voltage and current sensors malfunctioning in a grid-connected PV system," *International Journal of Electrical Power & Energy Systems*, vol. 115, p. 105381, 2020.

[16] M. Davari, M. P. Aghababa, F. Blaabjerg, and M. Saif, "An innovative, adaptive faulty signal rectifier along with a switching controller for reliable primary control of GC-VSIs in CPS-based modernized microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 7, pp. 8370–8387, 2020.

[17] E. Arabi, T. Yucelen, and W. M. Haddad, "Mitigating the effects of sensor uncertainties in networked multi-agent systems," *Journal of Dynamic Systems, Measurement, and Control*, vol. 139, no. 4, p. 041003, 2017.

[18] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, vol. 38, no. 2, pp. 2364–2383, 2022.

[19] H. K. Khalil, *Nonlinear systems*. 3rd ed. London, U.K.: Prentice-Hall, 2002.