Innovative Observer-Based Framework for Attack Reconstruction and Mitigation in AC Microgrids

Hamidreza Shafei
Faculty of Engineering and Information Technology
University of Technology Sydney, Australia
Hamidreza.shafei@student.uts.edu.au

Subrata K. Sarker
Faculty of Engineering and Information Technology
University of Technology Sydney, Australia
Subratakumar.sarker@student.uts.edu.au

Li Li
Faculty of Engineering and Information Technology
University of Technology Sydney, Australia
Li.Li@uts.edu.au

Ricardo P. Aguilera
Faculty of Engineering and Information Technology
University of Technology Sydney, Australia
raguilera@ieee.org

Hassan Haes Alhelou
School of Engineering
Massachusetts Institute of Technology (MIT), USA
alhelou@mit.edu

***Abstract*—In this article, an observer-based technique is proposed to address false data injection attacks (FDIAs) in ac microgrids (MGs). To achieve this, unknown input observers (UIOs) are developed in each distributed generation (DG) unit according to the number of its neighbors to estimate the states of the neighboring DGs. The equations of each DG are augmented by considering attack signals in the voltage and current channels, which serve as communication links between the neighboring DGs. The proposed method is then utilized to detect the FDIAs by estimating the states of all neighboring units. After reconstructing the attacks, their destructive impacts are mitigated by purifying the contaminated signals. Simulation results demonstrate the effectiveness of the proposed scheme in providing accurate frequency and voltage regulation, as well as active and reactive power sharing among DGs.**

***Index Terms*—AC microgrids, Unknown input observer, Cyber-attack detection, False data injection attack**

I. Introduction

Owing to the escalating energy demands, microgrids (MGs) are gaining attention for their advantages, including reduced pollution, high power quality, enhanced reliability and efficiency, and rapid installation. These systems must function securely amid diverse conditions like equipment failures, weather fluctuations, and cyber-attacks, which pose risks to their resilience and dependability. Cyber-attacks, particularly, are highly damaging due to their intentional harm. Consequently, there has been a growing emphasis on devising protocols to safeguard MGs against cyber threats in recent years.

With the latest advancements in control and communication systems, MGs have become increasingly distributed, rendering them susceptible to various types of cyber-attacks. Scholarly works suggest two main strategies for enhancing the cyber-security of MGs: (a). detecting and mitigating attacks through cleaning polluted signals [1] [2], and (b). establishing a robust control protocol to ensure resilience [3]. In the former category, various methods are explored to address this challenging issue, including signal-based techniques [4], model-based schemes [5] [6], and data-based methods [7]. Extensive research on cybersecurity strategies for MGs is available in [8].

Detection of attacks using signal-based methods involves monitoring the signals from cyber links. Conversely, model-based detection schemes require mathematical system modeling [9]. When an accurate system model is unavailable, data-based detection methods are useful, as they leverage historical data to infer the system's model [10]. Nevertheless, these methods face challenges due to their high computational complexity, which makes them unsuitable for large-scale distributed systems. Among these approaches, various research efforts have explored attack detection using model-based schemes on ac MGs. Common methods in this area include sliding mode observers [11], Kalman filter [12], and observer-based detection methods [13].

Abianeh et al. [11] developed a cyber-resilient distributed control system by combining multi-objective sliding mode control (SMC) with communication link quality observation to enhance the reliability of ac MGs against various types of false data injection attacks (FDIAs). Due to the inherent robustness of SMC, the proposed method shows satisfactory performance in the face of parameter uncertainty. In a different study, Shi et al. [14] introduced an observer-based resilient distributed control approach for ac MGs to estimate and mitigate FDIAs without requiring attack information. However, this method is susceptible to cyber-attacks and time delays and necessitates an additional distributed term. To improve the speed of voltage and frequency convergence in ac MGs, Lu et al. [15] proposed an observer-based finite-time stability control method incorporating confidence and trust factors. A limitation of this method is its inability to fully eliminate certain types of attacks. Additionally, a distributed resilient observer-based decentralized adaptive control approach was proposed for ac MGs to counter denial of service attacks [16]. A review of the literature highlights several research gaps that need addressing to enhance the resilience of ac MGs against cyber threats. This work aims to address these challenges by developing an unified attack detection and mitigation protocols using a UIO to reconstruct attack signals without needing additional information, thereby protecting ac MGs from FDIAs.

Due to the advantages of model-based methods, each DG incorporates a series of UIOs. A significant benefit of the UIO approach for state estimation is its ability to estimate states even in the presence of unknown inputs. These UIOs allow adjacent units to detect attacks in transmitted data by augmenting each DG's equations with manipulated signals. To clean the transmitted data after attack reconstruction, a mitigation strategy is employed. The main advantage of this proposed method is its capacity to locally cleanse corrupted signals. Unlike [17], we develop observer-based framework for ac MGs that carefully considers their dynamics characteristics. The main contributions of this paper are:

1) Robust State Estimation with UIOs: Each DG incorporates a series of UIOs to estimate states, even in the presence of unknown inputs, leveraging the advantages of model-based methods.
2) Effective Attack Detection and Mitigation: UIOs enable adjacent units to detect attacks in transmitted data by augmenting each DG's equations with manipulated signals. After attack reconstruction, a mitigation strategy is employed to cleanse the transmitted data, ensuring its reliability.
3) Localised Signal Cleansing: The proposed method's main advantage is its capacity to locally cleanse corrupted signals, enhancing the security and resilience of the ac MG against cyberattacks and maintaining system stability.

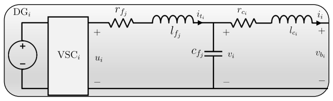


Fig. 1: The schematic of *i*-th inverter-based DG

This paper is organized as follows: Section II addresses the problem definition, including physical modeling, observer design, and countermeasures against attacks. Section III examines the control strategy, focusing on both secondary and primary control systems. Section IV provides simulation results, illustrating the effectiveness of the proposed approach in dealing with FDIAs within ac MGs. The paper concludes with Section V, which summarizes the findings of the study.

II. Problem Formulation

A. AC MG modeling

This section discusses the dynamic model of the considered ac MG, as shown in Fig. 1. The model includes a dc voltage source, a voltage source converter (VSC) operating as a pulse width modulation inverter, an LC filter, and an output connector linked to a three-phase series RLC load. Each DG is connected to its neighboring DGs via resistive and inductive power lines.

Assuming continuous mode and employing Kirchhoff's principles, the mathematical representation of the *i*-th inverter-based DG in abc-frame is established as:

$$\begin{aligned}
\dot{i}_{t_{abc_i}} &= \frac{1}{l_{f_i}}(u_{abc_i} - v_{abc_i} - r_{f_i} i_{t_{abc_i}}),\\
\dot{v}_{abc_i} &= \frac{1}{c_{f_i}}(i_{t_{abc_i}} - i_{abc_i}),\\
\dot{i}_{abc_i} &= \frac{1}{l_{c_i}}(v_{abc_i} - v_{b_{abc_i}} - r_{c_i} i_{abc_i}),
\end{aligned} \tag{1}$$

where $i_{t_{abc_i}}$, v_{abc_i}, and i_{abc_i} represent the generated current, inverter output voltage, and inverter output current, respectively, all of which are measurable. Consequently, the output vector for DG$_i$ in abc-frame is expressed as $y_{abc_i} = [i_{t_{abc_i}},\ v_{abc_i},\ i_{abc_i}]^T$. Additionally, l_{f_i}, r_{f_i}, c_{f_i}, and l_{c_i}, r_{c_i} denote the filter inductance, resistance, shunt capacitor, and the inductance and resistance of the output connector, respectively. In (1), u_{abc_i} and $v_{b_{abc_i}}$ denote the output voltage of the *i*-th VSC and the *i*-th bus voltage, respectively.

By applying the Clarke-Park transformation, each equation from (1) can be converted to the rotating $dq0$-frame as follows:

$$\begin{aligned}
\dot{i}_{t_{d_i}} &= \frac{1}{l_{f_i}}(u_{d_i} - v_{d_i} - r_{f_i} i_{t_{d_i}}) + \omega_0 i_{t_{q_i}}, \\
\dot{i}_{t_{q_i}} &= \frac{1}{l_{f_i}}(u_{q_i} - v_{q_i} - r_{f_i} i_{t_{q_i}}) - \omega_0 i_{t_{d_i}}, \\
\dot{v}_{d_i} &= \frac{1}{c_{f_i}}(i_{t_{d_i}} - i_{d_i}) + \omega_0 v_{q_i}, \\
\dot{v}_{q_i} &= \frac{1}{c_{f_i}}(i_{t_{q_i}} - i_{q_i}) - \omega_0 v_{d_i}, \\
\dot{i}_{d_i} &= \frac{1}{l_{c_i}}(v_{d_i} - v_{b_{d_i}} - r_{c_i} i_{d_i}) + \omega_0 i_{q_i}, \\
\dot{i}_{q_i} &= \frac{1}{l_{c_i}}(v_{q_i} - v_{b_{q_i}} - r_{c_i} i_{q_i}) - \omega_0 i_{d_i}.
\end{aligned} \tag{2}$$

Each DG is assumed to be connected to its neighboring units through an undirected communication network without self-loops. The dynamic equations of the *i*-th DG can be expressed in state-space form as follows:

$$\begin{aligned}
\dot{x}_i(t) &= A_i x_i(t) + E_i d_i(t), \\
y_i(t) &= C_i x_i(t).
\end{aligned} \tag{3}$$

Here, $x_i(t) = [i_{t_{d_i}}, i_{t_{q_i}}, v_{d_i}, v_{q_i}, i_{d_i}, i_{q_i}]^T \in \mathbb{R}^n$ and $y_i(t) \in \mathbb{R}^r$ represent the system state and system measurement. It is worth mentioning that $y_i(t) = x_i(t)$, $n = r$. In this equation, $A_i \in \mathbb{R}^{n \times n}$, $E_i \in \mathbb{R}^{n \times m}$, and $C_i \in \mathbb{R}^{r \times n}$ represent the system, input, and output matrices, respectively. It is assumed that all exogenous inputs in DG$_i$ [i.e., $E_i d_i(t)$] are unknown to its neighboring DGs, where E_i is a full column rank matrix. Following [18], it is assumed that the frequency is controlled in an open loop by equipping each DG with an internal oscillator, which provides Park's transformation angle $\theta(t) = \int_{t_0}^{t} \omega_0 d\tau$, where $\omega_0 = 2\pi f_0$, and f_0 represents the nominal frequency.

Remark 1: The output voltage of each VSC (i.e., u_{d_i} and u_{q_i}), as well as the bus voltage of each DG (i.e., $v_{b_{d_i}}$ and $v_{b_{q_i}}$), are unknown to their neighboring DGs. Therefore, $d_i(t) = [u_{d_i}, u_{q_i}, v_{b_{d_i}}, v_{b_{q_i}}]^T$.

The next section develops the UIO to estimate the states of all neighboring units, even in the presence of unknown inputs. The structure of this methodology is illustrated in Fig. 2.

B. UIO design

This section discusses a bank of UIOs designed to estimate the states of all neighboring units for attack detection purposes. This scheme enables the reconstruction of potential cyberattacks in the communication channels within a finite time. It is assumed that cyberattacks target the sensor channels and are generally formulated as:

$$\tilde{y}_i(t) = y_i(t) + D_i a_i(t), \tag{4}$$

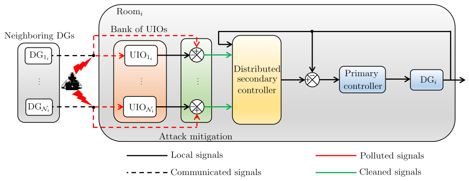


Fig. 2: The proposed attack detection/mitigation scheme

where $\tilde{y}_i(t)$ represents the disrupted output signals and $D_i \in \mathbb{R}^{r \times \alpha}$ denotes the attack matrices. Additionally, $a_i(t) \in \mathbb{R}^{\alpha}$ represents the FDIA signals, which compromise data integrity by altering the communicated signals through the injection of false data into the communication channels.

Remark 2: Thanks to *Remark 1* and the consideration of all inputs of a DG as unknown inputs, the potential for new cyber-attacks resulting from signal transmission of those inputs is eliminated, thereby enhancing the reliability of the proposed technique.

In this sequence, the equations for each DG have been augmented by incorporating intruder signals as follows:

$$\begin{aligned}
\dot{z}_i(t) &= \bar{A}_i z_i(t) + \bar{E}_i d_i(t), \\
\tilde{y}_i(t) &= \bar{C}_i z_i(t).
\end{aligned} \tag{5}$$

where $\bar{A}_i \in \mathbb{R}^{(n+\alpha)\times(n+\alpha)}$, $\bar{E}_i \in \mathbb{R}^{(n+\alpha)\times m}$, and $\bar{C}_i \in \mathbb{R}^{r\times(n+\alpha)}$ represent the augmented matrices of appropriate sizes. Additionally, $z_i(t) = [x_i, a_i]^T$ is the augmented state vector, where the FDIA signal a_i is assumed to be a constant scalar. The augmented system matrices are defined as follows:

$$\begin{aligned}
\bar{A}_i &= \left[\begin{array}{c|c} A_i & \mathbf{0}_{n\times\alpha} \\ \hline \mathbf{0}_{\alpha\times n} & \mathbf{0}_{\alpha\times\alpha} \end{array}\right], \bar{E}_i = \left[\begin{array}{c} E_i \\ \hline \mathbf{0}_{\alpha\times m} \end{array}\right], \\
\bar{C}_i &= \left[\begin{array}{c|c} C_i & D_i \end{array}\right].
\end{aligned} \tag{6}$$

For attack detection, the following full-order UIO is described to estimate the augmented states [19].

$$\begin{aligned}
\dot{g}_i(t) &= F_i g_i(t) + K_i \tilde{y}_i(t), \\
\hat{z}_i(t) &= g_i(t) + H_i \tilde{y}_i(t).
\end{aligned} \tag{7}$$

Matrices $F_i \in \mathbb{R}^{(n+\alpha)\times(n+\alpha)}$, $H_i \in \mathbb{R}^{(n+\alpha)\times r}$, and $K_i \in \mathbb{R}^{(n+\alpha)\times r}$, all appropriately sized, need to be determined. Additionally, $\hat{z}_i = [\hat{x}_i, \hat{a}_i]^T$ represents the estimation of the augmented states. Letting $K_i = K_{1i} + K_{2i}$, the estimation error of the UIO for the system (5) [i.e., $\mathcal{E}_i(t) = z_i(t) - \hat{z}_i(t)$] satisfies the following:

$$\begin{aligned}
\dot{\mathcal{E}}_i(t) = &\left(\bar{A}_i - H_i\bar{C}_i\bar{A}_i - K_{1i}\bar{C}_i\right)\mathcal{E}_i(t) \\
&- \left[F_i - \left(\bar{A}_i - H_i\bar{C}_i\bar{A}_i - K_{1i}\bar{C}_i\right)\right] g_i(t) \\
&- \left[K_{2i} - \left(\bar{A}_i - H_i\bar{C}_i\bar{A}_i - K_{1i}\bar{C}_i\right) H_i\right] \tilde{y}_i(t) \\
&-(H_i\bar{C}_i - I_{(n+\alpha)})\bar{E}_i d_i(t).
\end{aligned} \tag{8}$$

If the following relations are met, the estimation error tend towards zero asymptotically ($\dot{\mathcal{E}}_i(t) = F_i \mathcal{E}_i(t)$).

$$\begin{aligned} 0 &= (H_i \bar{C}_i - I_{(n+\alpha)}) \bar{E}_i, \\ F_i &= \bar{A}_i - H_i \bar{C}_i \bar{A}_i - K_{1i} \bar{C}_i, \\ K_{2i} &= F_i H_i, \\ K_i &= K_{1i} + K_{2i}. \end{aligned} \tag{9}$$

The solution to the above equation provides an estimate of the actual state values, provided that the following conditions are met.

Condition 1: $rank(\bar{C}_i \bar{E}_i) = rank(\bar{E}_i)$, which implies that this method is applicable when the number of outputs is greater than the number of unknown inputs.

Condition 2: The pair $(\bar{C}_i, \bar{A}_i - H_i \bar{C}_i \bar{A}_i)$ is detectable.

In [19], the proof of the necessary and sufficient conditions for (7) is provided. It is important to note that, based on the idea presented in *Remark 2*, detection does not require additional transmission, which helps to prevent new cyber-attacks. Once an attack is detected, the harmful effects of FDIAs can be mitigated by purifying the compromised signals through subtracting the estimated attack signals from them.

III. Control system design

In this section, the design of the control systems, including both primary and secondary controllers, is discussed. The goal is to ensure the overall stability of the ac MG by providing accurate voltage and frequency regulation, as well as proportional active and reactive power sharing among DGs. To achieve this, two cascade PI controllers are implemented in the primary control, along with a distributed secondary controller.

A. Distributed secondary control

Following [5], this section discusses a distributed secondary control based on a leader-followers approach to achieve control objectives in ac MGs. In this structure, one DG is designated as the "leader," serving as the autonomous and intelligent reference DG, while all other DGs are considered "followers" of the reference DG. Given the distributed nature of the secondary controller, each DG communicates only with its adjacent units. The control architecture of an autonomous MG is illustrated in Fig. 3. The droop control scheme is used to calculate the reference voltage and frequency for each DG to meet the desired objectives [5]. For this purpose, we have:

$$\begin{aligned} \omega_i^\star &= \omega_n - m_{P_i} P_i + \delta\omega_i, \\ v_{d_i}^\star &= v_{d_{ref}} - n_{Q_i} Q_i + \delta v_i. \end{aligned} \tag{10}$$

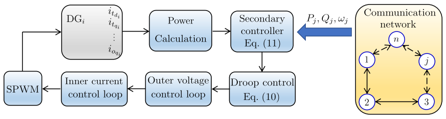


Fig. 3: Control structure of the considered ac MG

Here, ω_n and $v_{d_{ref}}$ represent the reference frequency and d-component voltage for the entire MG. Additionally, P_i and Q_i denote the measured active and reactive powers, while m_{P_i} and n_{Q_i} are the droop coefficients. Furthermore, $\delta\omega_i$ and δv_i are correction terms used to determine the accurate reference voltage and frequency for each DG. These corrections are calculated within the distributed secondary control system as outlined in [5]:

$$\begin{aligned} \delta\dot{\omega}_i = K_1 \Big(& \textstyle\sum_{j \in \mathcal{N}_i} a_{ij} \left(\omega_j - \omega_i\right) + g_i \left(\omega_n - \omega_i\right) \\ & + \textstyle\sum_{j \in \mathcal{N}_i} a_{ij} \left(m_{P_j} P_j - m_{P_i} P_i\right) \Big), \\ \delta\dot{v}_i = K_2 \Big(& \textstyle\sum_{j \in \mathcal{N}_i} a_{ij} \left(n_{Q_j} Q_j - n_{Q_i} Q_i\right) \Big). \end{aligned} \tag{11}$$

where $a_{ij} = 1$ when the i-th DG is a neighbour of DG j; otherwise, $a_{ij} = 0$. Additionally, K_1 and K_2 denote the constant gains of the secondary controller. In (11), $\mathcal{N}_i$ denotes the set of incident power lines connecting DG$_i$ to its neighbors. Further analysis of this consensus-based secondary controller can be found in [5].

B. Primary control design

In this paper, we develop two cascade PI controllers for the d and q components of each DG to ensure the stability of the entire MG. Considering the d component of the generated current and inverter output voltage [i.e., the first and third relations in (2)], the following two transfer functions are derived for the *i*-th DG are represented. It is important to note that the same procedure is applied to the q component. Thus, we have:

$$\begin{aligned} \frac{i_{t_{d_i}}(s)}{\frac{1}{l_{f_i}}\left(u_{d_i}(s) - v_{d_i}(s)\right) + \omega_0 i_{t_{q_i}}(s)} &= \frac{1}{s + \frac{r_{f_i}}{l_{f_i}}}, \\ \frac{v_{d_i}(s)}{\frac{1}{c_{f_i}}\left(i_{t_{d_i}}(s) - i_{d_i}(s)\right) + \omega_0 v_{q_i}(s)} &= \frac{1}{s}. \end{aligned} \tag{12}$$

Considering the reference voltage and frequency magnitudes calculated by the secondary control system for each DG, the primary control is designed to ensure the stability of the entire system. The schematic of this primary control system is illustrated in Fig. 4. The following provides the gains of these controllers:

$$\begin{aligned} k_{p_{v_d}} &= 2\zeta(\omega_n/10) \quad & k_{i_{v_d}} &= (\omega_n/10)^2, \\ k_{p_{i_d}} &= 2\zeta\omega_n - \frac{r_{f_i}}{l_{f_i}} \quad & k_{i_{i_d}} &= \omega_n^2. \end{aligned} \tag{13}$$

where $k_{p_{v_d}}$, $k_{i_{v_d}}$, $k_{p_{i_d}}$, and $k_{i_{i_d}}$ represent the designed proportional and integral gains for the d component of the inner current and outer voltage control loops. It

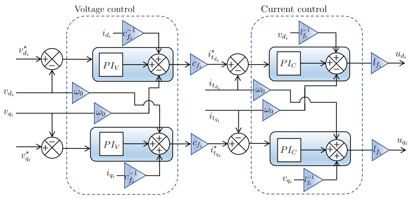


Fig. 4: Block diagram of the primary control

TABLE I: Simulation parameters

Parameter	Value	Parameter	Value
l_{f_i}	$20\ mH$	l_{c_i}	$0.35\ mH$
r_{f_i}	$0.1\ \Omega$	r_{line}	$0.15\ \Omega$
c_{f_i}	$0.15\ mF$	l_{line}	$35\ mH$
r_{c_i}	$0.005\ \Omega$	$Load$	$5\ kW$+ $1.2\ kVar$

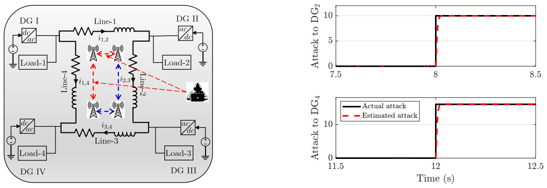
will be demonstrated that the designed control systems, which include both primary and secondary controls, as well as the proposed attack detection and mitigation schemes, achieve the following objectives [5].

$$\begin{aligned}&\lim_{t\to\infty}||\omega_i(t)-\omega_n||=0\ \ \forall\, i,\\&\lim_{t\to\infty}||m_{P_i}P_i-m_{P_j}P_j||=0\ \ \forall\, i,j\\&\lim_{t\to\infty}||n_{Q_i}Q_i-n_{Q_j}Q_j||=0\ \ \forall\, i,j.\end{aligned}\tag{14}$$

The effectiveness of this technique in ensuring the safe operation of ac MGs in the presence of FDIAs is demonstrated in the next section.

IV. Simulation Results

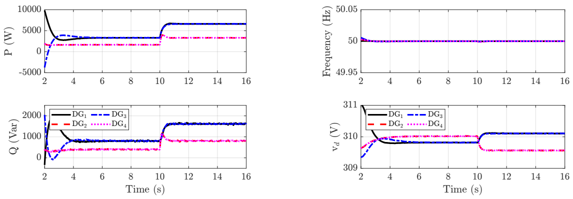
In this section, we evaluate the effectiveness of the proposed scheme against FDIAs using an ac MG consisting of four DGs interconnected by resistive-inductive power lines. The diagram of this MG is shown in Fig. 5(a). It is assumed that the capacity of the odd-numbered DGs (i.e., DG_1 and DG_3) is twice that of the even-numbered DGs (i.e., DG_2 and DG_4). Table I lists all the parameter values for the considered MG.



(a) (b)

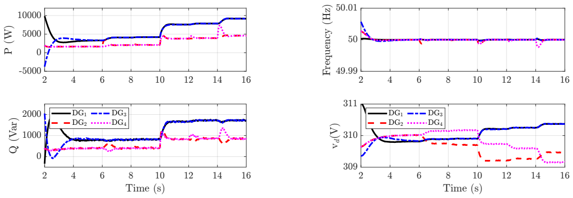
Fig. 5: **(a).** Schematic of the under-study ac MG, **(b).** FDIA detection with the proposed UIO strategy.

To demonstrate the effectiveness of the designed primary and distributed secondary control systems in providing stability for the considered MG and achieving the desired objectives (i.e., accurate voltage and frequency regulation, and equitable active and reactive power sharing), Fig. 6(a) shows the active and reactive powers, while Fig. 6(b) illustrates the frequency and d component for all DGs in the absence of any cyber-attacks. Moreover, at $t = 10s$, the load is increased by $5\ kW$+ $1.2\ kVar$. As shown, the desired objectives for the ac MG are met. However, as indicated in Fig. 7, these objectives are not achieved when the microgrid is subjected to cyber-attacks without any mitigation measures. In this simulation, constant FDIAs are applied to both the current and voltage channels of DG_2 and DG_4. In this regard, a constant FDIA at $t = 6s$, and a constant FDIA at $t = 14s$ are applied to the current channels of DG_1 and DG_4, respectively. Moreover, a constant FDIA at $t = 8s$, and a constant FDIA at $t = 12s$ are applied to the voltage channels of DG_1 and DG_4, respectively. The results highlight that voltage regulation and accurate active/reactive power sharing are compromised, underscoring the critical need for effective attack detection and mitigation protocols.



(a) (b)

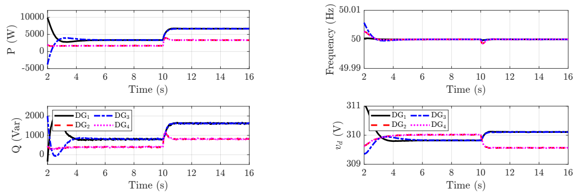
Fig. 6: **(a).** The value of active/reactive power, and **(b).** voltage/frequency for all DGs in the absence of FDIAs.



(a) (b)

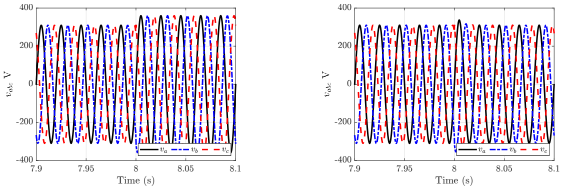
Fig. 7: **(a).** The value of active/reactive power, **(b).** voltage and frequency for all DGs when the compromised MG has no attack detection/mitigation mechanism.

After observing the impact of FDIAs on the ac MG in the absence of a detection mechanism, the proposed strategy is applied to reconstruct the attack signals and eliminate the effects of attacks. As shown in Fig. 8, which presents the active/reactive powers, as well as the frequency and d component of the voltage for all DGs, the proposed UIO-based scheme effectively detects and mitigates FDIAs. This demonstrates that the method can effectively address FDIAs. Also, Fig. 9 illustrates the three-phase voltage of DG_1 both with and without the proposed scheme. It is clear that the scheme rapidly mitigates the destructive effects of cyberattacks.



(a) (b)

Fig. 8: **(a).** The value of active and reactive power, and **(b).** voltage and frequency for all DGs against constant FDIAs with the proposed attack mitigation mechanism.



(a) (b)

Fig. 9: The three-phase voltage of DG_1 under constant FDIA **(a).** without and **(b).** with the proposed scheme.

Additionally, Fig. 5(b) illustrates the actual profile of cyber-attacks alongside their estimated counterparts, confirming the effectiveness of our proposed local observer for attack detection.

V. Conclusion and Future Works

In this study, we developed an observer-driven strategy to address cyber threats in ac MGs. Each DG is equipped with a set of UIOs to monitor the conditions of neighboring units. By incorporating attack signals into the DG equations, our observer system can detect and construct constant FDIAs. Detected attacks are then neutralized by subtracting them from the corrupted signals. Additionally, we established a decentralized secondary control framework to determine reference voltage and frequency levels, ensuring precise frequency regulation and equitable distribution of active and reactive power among DGs. Simulations results validate the effectiveness of this approach in protecting ac MGs against constant FDIAs.

References

[1] Zhou, Q., Shahidehpour, M., Alabdulwahab, A. Abusorrah, A., 2020. A cyber-attack resilient distributed control strategy in islanded microgrids. IEEE Tran Smart Grid, 11, pp.3690-3701.

[2] Mustafa, A., Poudel, B., Bidram, A. and Modares, H., 2019. Detection and mitigation of data manipulation attacks in AC microgrids. IEEE Trans on Smart Grid, 11(3), pp.2588-2603.

[3] Sahoo, S., Yang, Y. and Blaabjerg, F., 2020. Resilient synchronization strategy for AC microgrids under cyber attacks. IEEE Transactions on Power Electronics, 36(1), pp.73-77.

[4] Mustafa, A., Poudel, B., Bidram, A. and Modares, H., 2019. Detection and mitigation of data manipulation attacks in AC microgrids. IEEE Tran on Smart Grid, 11(3), pp.2588-2603.

[5] Rath, S., Pal, D., Sharma, P.S. and Panigrahi, B.K., 2020. A cyber-secure distributed control architecture for autonomous AC microgrid. IEEE Systems Journal, 15(3), pp.3324-3335.

[6] Mahvash, H., Taher, S.A. and Guerrero, J.M., 2024. Detecting and mitigating cyber-attacks in AC microgrid composed of marine current turbine DFIGs to improve energy management system. e-Prime-Advances in Electrical Engineering, Electronics and Energy, p.100464.

[7] Mohiuddin, S.M., Qi, J., Fung, S., Huang, Y. and Tang, Y., 2021, October. Deep learning based multi-label attack detection for distributed control of AC microgrids. In IEEE Inter Conf on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (pp. 233-238). IEEE.

[8] Shafei, H., Li, L. and Aguilera, R.P., 2023. A Comprehensive Review on Cyber-Attack Detection and Control of Microgrid Systems. Power Systems Cybersecurity: Methods, Concepts, and Best Practices, pp.1-45.

[9] Alhelou, H.H. and Cuffe, P., 2021. A dynamic-state-estimator-based tolerance control method against cyberattack and erroneous measured data for power systems. IEEE Transactions on Industrial Informatics, 18(7), pp.4990-4999.

[10] Tan, S., Xie, P., Guerrero, J.M. and Vasquez, J.C., 2022. False data injection cyber-attacks detection for multiple dc microgrid clusters. Applied Energy, 310, p.118425.

[11] Abianeh, A.J., Mardani, M.M., Ferdowsi, F., Gottumukkala, R. and Dragičević, T., 2021. Cyber-resilient sliding-mode consensus secondary control scheme for islanded AC microgrids. IEEE Transactions on Power Electronics, 37(5), pp.6074-6089.

[12] Sargolzaei, A., Yazdani, K., Abbaspour, A., Crane III, C.D. and Dixon, W.E., 2019. Detection and mitigation of false data injection attacks in networked control systems. IEEE Transactions on Industrial Informatics, 16(6), pp.4281-4292.

[13] Yan, J., Guo, F. and Wen, C., 2020. Attack detection and isolation for distributed load shedding algorithm in microgrid systems. IEEE J. of Emer and Sele Top in Indus. Elec, 1(1), pp.102-110.

[14] Shi, M., Chen, X., Shahidehpour, M., Zhou, Q. and Wen, J., 2021. Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded AC microgrids. IEEE Tran on Smart Grid, 12(3), pp.1953-1963.

[15] Lu, R., Wang, J. and Wang, Z., 2020. Distributed observer-based finite-time control of AC microgrid under attack. IEEE Transactions on Smart Grid, 12(1), pp.157-168.

[16] Deng, C., Wen, C., Zou, Y., Wang, W. and Li, X., 2020. A hierarchical security control framework of nonlinear CPSs against DoS attacks with application to power sharing of AC microgrids. IEEE Trans on Cybernetics, 52(6), pp.5255-5266.

[17] Shafei, H., Li, L. and Aguilera, R.P., 2023, June. Observer-based Attack Detection and Mitigation in DC Microgrid Systems. In 2023 IEEE 14th International Symposium on Power Electronics for Distributed Generation Systems (pp. 959-964). IEEE.

[18] Cucuzzella, M., Incremona, G.P. and Ferrara, A., 2017. Decentralized sliding mode control of islanded AC microgrids with arbitrary topology. IEEE Tran on Indu Elec, 64(8), pp.6706-6713.

[19] Chen, J., Patton, R.J. and Zhang, H.Y., 1996. Design of unknown input observers and robust fault detection filters. International Journal of control, 63(1), pp.85-105.