# A Fully Resilient Cyber-Secure Synchronization Strategy for AC Microgrids

Sadabadi, Mahdieh S.; Sahoo, Subham; Blaabjerg, Frede

*Published in:*
I E E E Transactions on Power Electronics

*DOI (link to publication from Publisher):*
10.1109/TPEL.2021.3091587



*Publication date:*
2021

*Document Version*
Accepted author manuscript, peer reviewed version

# A Fully Resilient Cyber-Secure Synchronization Strategy for AC Microgrids

Mahdieh S. Sadabadi, *Member, IEEE*, Subham Sahoo, *Member, IEEE*, and Frede Blaabjerg, *Fellow, IEEE*

***Abstract*—This letter focuses on resilient synchronization in networked AC microgrids under cyber-attacks, where attackers aim to desynchronize converters by injecting bounded false data to communication and control channels. To this end, a resilient cooperative control framework for the secondary frequency regulation in AC microgrids is developed. The proposed resilient distributed control strategy achieves synchronization regardless of the existence of cyber-attacks. Moreover, it offers the maximum level of resilience, i.e. it guarantees resilient synchronization even if all distributed generation units in microgrids are subject to cyber-attacks. Theoretical analysis and verification case studies are carried out in order to demonstrate the advantages and performance of the proposed resilient cooperative control.**

***Index Terms*—AC microgrids, resilient synchronization, distributed control, false data injection (FDI) cyber-attack, secondary control, attack-resilient control.**

## I. Introduction

MICROGRID technology is becoming ever more reliant on distributed control and communication networks. While distributed control strategies could improve scalability and reliability in microgrids, they pose major cybersecurity challenges. The existence of cyber-attacks in microgrid control systems can easily lead to the loss of synchronization and might result in instability issues.

To deal with cybersecurity issues in AC microgrids, an observer-based attack-resilient distributed control approach for synchronization in islanded microgrids has been proposed [1]. In this work, multiple confidence and trust factors are developed to estimate the effects of cyber-attacks. However, the online calculation of these factors increases the computational burden of this approach. Furthermore, [1] considers only constant and time-independent cyber-attacks and also assumes that more than half of the neighbors of the attacked distributed generation (DG) units should be healthy. Resilient cooperative control strategies have been developed in [2], [3]. In these approaches, the distributed controller is augmented with a hidden layer whose duty is to mitigate the adverse effects of cyber-attacks. However, to provide an attack-resilient feature, they rely on a strong assumption that the hidden layer is not infiltrated by cyber-attacks. An asynchrony index criterion for the detection of stealth attacks has been proposed in [4]. The proposed mitigation platform in [4] guarantees resilient synchronization for up to $N-1$ (in a system with $N$ converters) attacked converters. A resilient distributed secondary control for islanded AC microgrids based on a weighted mean subsequence reduced algorithm has been proposed in [5]. However, the proposed approach requires a specific connectivity level for the connectivity of underlying communication graph. The authors in [6], [7] have established full resilience against data integrity attacks in AC microgrids, where the adversary attempts to increase the total generation cost by manipulating the cost parameters. However to the best of authors' knowledge, the development of a resilient distributed secondary control, which guarantees full resilience in synchronization is still an open question.

This letter introduces a novel resilient secondary frequency control for islanded AC microgrids, which relies on a resilience index. It is shown that increasing the resilience index enhances the resilience of synchronization to false data injection (FDI) cyber-attacks. The proposed resilient distributed control framework offers the maximum level of resilience, i.e. it guarantees resilient synchronization for up to $N$ (out of $N$) attacked DG units.

*Preliminaries:* In graph theory, a graph is called undirected if all edges are bidirectional and no directions are associated with them.

*Notation:* Throughout this letter, $\mathbf{1}_n$ is an $n\times 1$ vector of ones, $\mathbf{0}_n$ is an $n\times 1$ zero vector, $\mathbf{I}_n$ is an $n\times n$ identity matrix, $\mathbf{0}_{n\times m}$ is a zero matrix whose dimension is $n\times m$, and $X^T$ denotes the transpose of matrix $X$. $\mathbb{R}_+$ and $\mathbb{R}_{\geq 0}$ respectively are a set of positive and non-negative real values.

## II. Standard Primary and Secondary Control in Islanded Microgrids

In an AC microgrid with $N$ DG units, two of the key secondary control objectives are frequency synchronization and proportionate active power sharing, which can be mathematically represented as:

$$\lim_{t\to\infty}\omega_i(t)=\omega_0,\ \forall i\in\{1,\dots,N\} \tag{1a}$$

$$\lim_{t\to\infty}m_{P_i}P_i(t)=\lim_{t\to\infty}m_{P_j}P_j(t),\ \forall i,j\in\{1,\dots,N\} \tag{1b}$$

where $\omega_i$ is the angular frequency of DG $i$, $\omega_0$ is nominal reference angular frequency, $P_i$ is the measured active power of DG $i$, and $m_{P_i}$ is the $P$-$\omega$ droop coefficient employed in the active power secondary control layer.

To achieve synchrony in AC microgrids, a hierarchical control strategy consisting of a primary droop and a cooperative secondary control is adopted. This strategy is shown in Fig. 1.

The work was supported by 2020-2021 National Productivity Investment Fund (NPIF).

M. S. Sadabadi is with the Department of Automatic Control and Systems Engineering, University of Sheffield, Sheffield, United Kingdom (e-mail: m.sadabadi@sheffield.ac.uk).

S. Sahoo and F. Blaabjerg are with the Department of Energy Technology, Aalborg University, 9220 Aalborg, Denmark (e-mails: sssa@et.aau.dk; fbl@et.aau.dk).

### A. Primary Frequency Droop Control

Droop control is one of widely-used control strategies for the primary control of islanded AC microgrids. The $P$-$\omega$ droop control mechanism can be written as [1]:

$$\omega_i = \omega_{n_i} - m_{P_i} P_i, \tag{2}$$

where $\omega_{n_i}$ is the set-point of the droop mechanism, which is chosen by a secondary control layer.

### B. Cooperative Secondary Frequency Control

The primary droop control results in a deviation in the frequency of microgrids from their reference setpoints. To address this issue, secondary control strategies are utilized to provide appropriate setpoints $\omega_{n_i} = \int u_{\omega_{n_i}} dt$ for the primary control in (2), where the auxiliary control $u_{\omega_{n_i}} = \dot{\omega}_{n_i}$ is given based on the following cooperative control strategy [8]:

$$u_{\omega_{n_i}} = -K_\omega \Big( \sum_{j \in \mathcal{N}_i} \eta_{ij} \left( \omega_{n_i} - \omega_{n_j} \right) + g_i \left( \omega_i - \omega_0 \right) \Big), \tag{3}$$

where $\mathcal{N}_i$ is the set of neighbors of DG $i$, $g_i \in \mathbb{R}_{\geq 0}$ is a pinning gain, and $K_\omega \in \mathbb{R}_+$ is a coupling gain. Assuming that the associated neighbor-to-neighbor communication digraph $\mathcal{G}$ in (3) contains a spanning tree and $g_i$ is non-zero for at least one DG, it can be shown that $\lim_{t \to \infty} \omega_i(t) = \omega_0$ and the proportional active current sharing in (1b) is guaranteed [8].

Although the distributed cooperative control in (3) guarantees synchronization, it has been shown in [9] that (3) is not resilient against FDI cyber-attacks on control and communication channels. Hence, it mandates the design of a fully resilient cooperative secondary frequency control to guarantee (1) despite the presence of cyber-attacks.

**Remark 1:** Inverter-based DG units have nonlinear dynamics in direct-quadrature $(dq)$ reference frame, which include load characteristics. As fully described in [10], by virtue of an input–output feedback linearization approach, the nonlinear dynamics of DG units can be transformed to linear dynamics. As a result, the secondary frequency control is transformed to a first-order synchronization problem in (3).

## III. Cooperative Resilient Frequency Control

This section discusses the development of a resilient cooperative secondary frequency control for islanded AC microgrids under cyber-attacks. In what follows, it is worth notifying that the communication graph represented by a Laplacian matrix $\mathbb{L}$ is assumed to be connected and undirected. Hence, $\mathbb{L} = \mathbb{L}^T$.

### A. Proposed Attack-Resilient Distributed Control Strategy

To accomplish full resilience for synchrony in AC microgrids under FDI cyber-attacks, the following cooperative frequency control framework is proposed:

$$\begin{aligned}
\dot{\omega}_{n_i} &= -K_\omega \Big( \sum_{j \in \mathcal{N}_i} \eta_{ij} \left( \omega_{n_i} - \omega_{n_j} \right) + g_i \left( \omega_i - \omega_0 \right) \Big) - K(\omega_{n_i} - \rho_i) \\
&\quad + \beta \sum_{j \in \mathcal{N}_i} \eta_{ij} \left( \sigma_i - \sigma_j \right), \\
\tau_\sigma \dot{\sigma}_i &= -\gamma \sigma_i - \beta \sum_{j \in \mathcal{N}_i} \eta_{ij} \left( \omega_{n_i} - \omega_{n_j} \right), \\
\tau_\rho \dot{\rho}_i &= \omega_{n_i} - \rho_i,
\end{aligned} \tag{4}$$

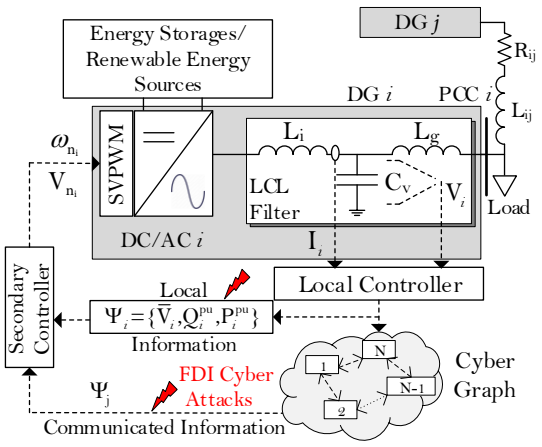


Fig. 1. Single-line diagram of a cyber-physical system consisting of $N$ grid-forming converters in an AC microgrid managed by a cooperative cyber topology – cyber-attacks (in red bolts) launched into communication channels and local control inputs.

where $\sigma_i$ and $\rho_i$ are auxiliary states of the controller of DG $i$, $\tau_\sigma \in \mathbb{R}_+$, $\tau_\rho \in \mathbb{R}_+$, $K \in \mathbb{R}_+$, $\gamma \in \mathbb{R}_+$, and $\beta \in \mathbb{R}_+$, called resilience index, are the control parameters. In the proposed attack-resilient cooperative control, the auxiliary state $\sigma_i$ as well as the resilience index $\beta$ are added to enhance resilience against cyber-attacks, whereas $\rho_i$ is added to prevent unwanted oscillations in the frequency response of DG units. In order to increase the time-constant of the dynamics of the auxiliary states, $\gamma/\tau_\sigma$ is chosen sufficiently high. By doing a steady-state analysis similar to [8], it can be shown that the proposed resilient cooperative control in (4) guarantees the frequency synchronization and proportional active power sharing in (1).

### B. FDI Cyber-attacks Formulation

The proposed distributed control framework in (4) relies on exchanging $\Psi_j = \{\sigma_j, \omega_j, P_j\}$ amongst different converters. Under potential FDI cyber-attacks on the transmitted data and local control inputs, one may obtain:

$$\begin{aligned}
\hat{\omega}_{[i,j]} &= \omega_i + \lambda_{\omega_{[i,j]}} \delta_{\omega_{[i,j]}}, \quad \hat{P}_{[i,j]} = P_i + \lambda_{P_{[i,j]}} \delta_{P_{[i,j]}}, \\
\hat{\sigma}_{[i,j]} &= \sigma_i + \lambda_{\sigma_{[i,j]}} \delta_{\sigma_{[i,j]}}, \quad \hat{u}_{\omega_{[i]}} = u_{\omega_i} + \lambda_{u_{\omega_{[i]}}} \delta_{u_{[i]}},
\end{aligned} \tag{5}$$

for $i \in \{1, \ldots, N\}$ and $j \in \mathcal{N}_i$, where $\hat{\omega}_{[i,j]}$, $\hat{P}_{[i,j]}$, $\hat{\sigma}_{[i,j]}$, and $\hat{u}_{[i]}$ are the disrupted data sent to/received by converter $j$.

In the presence of an attack on the communication of $\omega_i$ ($\sigma_i$, $P_i$) from converter $i$ to converter $j$, $\lambda_{\omega_{[i,j]}} = 1$ ($\lambda_{\sigma_{[i,j]}} = 1$, $\lambda_{P_{[i,j]}} = 1$) and $\lambda_{\omega_{[i,j]}} = 0$ ($\lambda_{\sigma_{[i,j]}} = 0$, $\lambda_{P_{[i,j]}} = 0$) otherwise. Similarly, if there exists an attack on $u_{\omega_i}$, $\lambda_{u_{\omega_{[i]}}} = 1$, otherwise $\lambda_{u_{\omega_{[i]}}} = 0$. It is assumed that $\delta_{\omega_{[i,j]}}$, $\delta_{P_{[i,j]}}$, $\delta_{\sigma_{[i,j]}}$, and $\delta_{u_{\omega_{[i]}}}$ in (5) are unknown but uniformly bounded.

The cyber-attacks in (5) can be represented in a vector form as $\mathbf{d}_{\omega_n} = \left[ d_{\omega_{n_1}}, \ldots, d_{\omega_{n_N}} \right]^T$ and $\mathbf{d}_\sigma = [d_{\sigma_1}, \ldots, d_{\sigma_N}]^T$, where $d_{\omega_{n_i}} = \sum_{j=1}^N \eta_{j,i} (\lambda_{\omega_{[j,i]}} \delta_{\omega_{[j,i]}} + \lambda_{P_{[j,i]}} m_{P_j} \delta_{P_{[j,i]}} + \lambda_{\sigma_{[j,i]}} \delta_{\sigma_{[j,i]}}) + \lambda_{u_{[i]}} \delta_{u_{[i]}}$ and $d_{\sigma_i} = \sum_{j=1}^N \eta_{i,j} (\lambda_{\omega_{[j,i]}} \delta_{\omega_{[j,i]}} + \lambda_{P_{[j,i]}} m_{P_j} \delta_{P_{[j,i]}})$.

### C. Lyapunov-based Stability Analysis

The proposed resilient cooperative control approach in (4) can be rewritten as follows:

$$\begin{aligned}
\dot{\omega}_{n_i} =& -K_\omega\Big(\sum_{j\in\mathcal{N}_i}\eta_{ij}\big(\omega_{n_i}-\omega_{n_j}\big)+g_i\big(\underbrace{\omega_i+m_{P_i}P_i}_{\omega_{n_i}}-\underbrace{(\omega_0+m_{P_i}P_i)}_{\omega_{n_0}}\big)\Big)\\
&-K(\omega_{n_i}-\rho_i)+\beta\sum_{j\in\mathcal{N}_i}\eta_{ij}\left(\sigma_i-\sigma_j\right),\\
\tau_\sigma\dot{\sigma}_i =& -\gamma\sigma_i-\beta\sum_{j\in\mathcal{N}_i}\eta_{ij}\left(\omega_{n_i}-\omega_{n_j}\right),\\
\tau_\rho\dot{\rho}_i =& \ \omega_{n_i}-\rho_i.
\end{aligned} \tag{6}$$

In the proposed distributed control strategy in (4), it is assumed that the pinning gain $g_i$ is non-zero (a positive value) for at least one DG unit. Since the non-zero value of $g_i$ affects the convergence rate of the distributed control strategy in (6) and the speed of frequency synchronization in an islanded AC microgrid, these non-zero values of $g_i$ are chosen to be equal to $\beta$, where $\beta$ is selected to be sufficiently high. The choice of $\beta$ will be discussed in Subsection III-D. A larger value of the non-zero pining gain leads to a more effective communication between the chosen pinned and unpinned DG units; thus, the reference frequency $\omega_0$ can propagate faster in the neighbor-neighbor communication network [9]. In light of this and considering the fact that the time-constant of the auxiliary state dynamics is selected to have a large value, the states of (6) converge to their steady-state values quickly. As a result, $m_{P_i}P_i$ of all DG units converges to a certain common steady value fast. Hence, it is reasonable to assume that $\omega_{n_0}$ is equal for all DG units. It is worth notifying that such an assumption has already been used in previous studies, e.g. for AC microgrids in [2] and for DC microgrids in [11].

The proposed cooperative control can be approximated and represented in a vector form as follows:

$$\begin{aligned}
\dot{\omega}_n &= -K_\omega\left(\mathbb{L}+\mathbb{A}\right)\left(\omega_n-\mathbf{1}_N\omega_{n_0}\right)-K(\omega_n-\rho)+\beta\mathbb{L}\sigma,\\
\tau_\sigma\dot{\sigma} &= -\gamma\sigma-\beta\mathbb{L}\omega_n,\\
\tau_\rho\dot{\rho} &= \omega_n-\rho,
\end{aligned} \tag{7}$$

where $\sigma=[\sigma_1,\ldots,\sigma_N]^T$ and $\rho=[\rho_1,\ldots,\rho_N]^T$, $\omega_n=[\omega_{n_1},\ldots,\omega_{n_N}]^T$, and $\mathbb{A}=\operatorname{diag}(g_1,\ldots,g_N)$. Without loss of generality, the pinning gain matrix $\mathbb{A}$ can be rewritten as $\mathbb{A}=\beta\operatorname{diag}(\tilde{g}_1,\ldots,\tilde{g}_N)$, where $\tilde{g}_i=1$ if and only if DG $i$ is a chosen pinned unit; otherwise, $\tilde{g}_i=0$. Note that the term $\beta\tilde{g}_i(\omega_{n_i}-\omega_{n_0})$ is not subject to FDI cyber-attacks as this term does not rely on any communications amongst neighbouring DG units and their local controllers.

In the presence of FDI cyber-attacks, the closed-loop system in (7) can be represented in the state-space form as follows:

$$\dot{\mathbf{e}}=\mathbf{A}\mathbf{e}+\mathbf{B}\mathbf{d}, \tag{8}$$

where $\mathbf{d}=\left[\mathbf{d}_{\omega_n}^T,\mathbf{d}_\sigma^T\right]^T$, $\mathbf{e}=\mathbf{x}-\bar{\mathbf{x}}$, where $\mathbf{x}=\left[\omega_n^T,\sigma^T,\rho^T\right]^T$ and $\bar{\mathbf{x}}=\left[\mathbf{1}_N^T\bar{\omega}_n,\mathbf{0}_{N\times1}^T,\mathbf{1}_N^T\bar{\omega}_n\right]^T$ is the equilibrium of (4) in the absence of the cyber-attacks $\mathbf{d}$. Note that $\bar{\omega}_n$ is the steady-state value of $\omega_{n_i}(t)$, $i\in\{1,\ldots,N\}$. The state space matrices $(\mathbf{A},\mathbf{B})$ are defined as follows:

$$\begin{aligned}
\mathbf{A}&=\begin{bmatrix}-K_\omega\left(\mathbb{L}+\mathbb{A}\right)-K\mathbf{I}_N & \beta\mathbb{L} & K\mathbf{I}_N\\ -\tau_\sigma^{-1}\beta\mathbb{L} & -\gamma\tau_\sigma^{-1}\mathbf{I}_N & \mathbf{0}_N\\ \tau_\rho^{-1}\mathbf{I}_N & \mathbf{0}_N & -\tau_\rho^{-1}\mathbf{I}_N\end{bmatrix},\\
\mathbf{B}&=\begin{bmatrix}\mathbf{I}_N & \mathbf{0}_N\\ \mathbf{0}_N & \tau_\sigma^{-1}\mathbf{I}_N\\ \mathbf{0}_N & \mathbf{0}_N\end{bmatrix}
\end{aligned} \tag{9}$$

The following lemma analyzes the stability of (8) using Lyapunov stability theory.

*Lemma 1:* $\mathbf{A}$ in (9) is a Hurwitz (stable) matrix.

*Proof 1:* Let us assume that $\mathbf{d}=0$. To show $\mathbf{A}$ is Hurwitz, it is sufficient to show the globally asymptotic stability of the origin in (8). To this end, the following Lyapunov candidate is chosen:

$$\mathcal{V}(\mathbf{e})=\frac{1}{2}\mathbf{e}^T\begin{bmatrix}\mathbf{I}_N & \mathbf{0}_N & \mathbf{0}_N\\ \mathbf{0}_N & \tau_\sigma\mathbf{I}_N & \mathbf{0}_N\\ \mathbf{0}_N & \mathbf{0}_N & K\tau_\rho\mathbf{I}_N\end{bmatrix}\mathbf{e}. \tag{10}$$

The time derivative of $\mathcal{V}(\mathbf{e})$ along the trajectories (8) is obtained as follows:

$$\begin{aligned}
\dot{\mathcal{V}}(\mathbf{e}) =& -K_\omega(\omega_n-\bar{\omega}_n)^T\left(\mathbb{L}+\mathbb{A}\right)(\omega_n-\bar{\omega}_n)-\gamma\sigma^T\sigma\\
&-K(\omega_n-\rho)^T(\omega_n-\rho).
\end{aligned} \tag{11}$$

Therefore, $\dot{\mathcal{V}}(\mathbf{e})<0$, $\forall\ \mathbf{e}\neq0$. Hence, the origin in (8) is globally asymptotically stable. As a result, $\mathbf{A}$ in (9) is a Hurwitz matrix.

### D. Attack-Resilience Analysis

The following theorem shows that the proposed resilient cooperative control in (4) guarantees the maximum scale of resilience in presence of cyber-attacks in (5). As a result, even if $N$ DG units are attacked, attack-resilience is achieved. More specifically, we will show that in an islanded AC microgrid augmented with the proposed resilient cooperative frequency control (4), the frequency synchronization and proportional active power sharing in (1) are achieved provided that the resilience index $\beta$ in (1) is sufficiently large. The details are given in Theorem 1.

*Theorem 1:* Consider the proposed cooperative frequency control in (4). It is assumed that all DG units are subject to FDI cyber-attacks $\mathbf{d}(t)$. For a sufficiently large value of the resilience index $\beta$, the objectives stated in (1) are guaranteed.

*Proof 2:* Since all DG units are attacked by false data injection in (5), all entries of $\mathbf{d}(t)$ are non-zero. From the linear dynamics in (8), the closed-loop error vector $\mathbf{e}$ can be obtained as follows:

$$\mathbf{e}(t)=e^{\mathbf{A}t}\mathbf{e}(0)+\int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{B}\mathbf{d}(\tau)d\tau. \tag{12}$$

Hence, it can be shown that

$$\begin{aligned}
\lim_{t\to\infty}\|\mathbf{e}(t)\| &\leq \lim_{t\to\infty}\left\|e^{\mathbf{A}t}\mathbf{e}(0)\right\|+\left\|\int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{B}\mathbf{d}(\tau)d\tau\right\|,\\
&\leq \lim_{t\to\infty}\left\|\int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{B}\mathbf{d}(\tau)d\tau\right\|,\\
&\leq \lim_{t\to\infty}\left\|\int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{\Delta}d\tau\right\|=\left\|-\mathbf{A}^{-1}\mathbf{\Delta}\right\|,
\end{aligned} \tag{13}$$

where $\Delta=\begin{bmatrix}\Delta_d^T & \mathbf{0}_{1\times N}\end{bmatrix}^T$ and $\Delta_d$ is a constant vector. Note that, since $\mathbf{A}$ is a stable matrix, $\lim_{t\to\infty}\left\|e^{\mathbf{A}t}\mathbf{e}(0)\right\|=0$. According to [12], $\mathbf{A}^{-1}$ is obtained as follows:

TABLE I
COMPARATIVE EVALUATION OF THE PROPOSED RESILIENT COOPERATIVE CONTROL STRATEGY (4) IN ISLANDED AC MICROGRIDS.

| *Features* | [1] | [9] | [5] | [3] | [2] | [4] | **This letter** |
|---|---|---|---|---|---|---|---|
| Computational burden | High | Medium | Medium | Medium | High | Low | Low |
| Resilience capability | $\frac{N}{2}$[1] | Case-dependent[2] | Case-dependent | $N$ [3] | $\frac{N}{2}$ | $N-1$ | $N$ |
| Additional resources | × | × | × | Virtual control layer | Virtual control layer | × | × |

[1] $N$ denotes the total number of DG units in AC microgrid.
[2] It depends largely on the number of attacked cyber links/nodes, which ultimately affects the algebraic connectivity of cyber-graph.
[3] It assumes that the virtual control layer is not subject to cyber-attacks.

TABLE II
PARAMETERS OF THE AC MICROGRID UNDER STUDY IN SECTION IV.

| | |
|---|---|
| Converters | $L_i = 3.4\ \mu H$ and $C_i = 50\ \mu F$. |
| Lines | $R_{12} = 0.23\ \Omega$, $L_{12} = 318.31\ \mu H$, $R_{23} = 0.35\ \Omega$, $L_{23} = 1.8462\ mH$, $R_{34} = 0.35\ \Omega$, and $L_{34} = 1.8462\ mH$. |
| Controller | $\tilde{g}_1 = 1$, $\tilde{g}_2 = \tilde{g}_3 = \tilde{g}_4 = 0$, $\tau_\sigma = \tau_\phi = 0.01$, $K_\omega = 5$, $K = 0.1$, $\gamma = 20$, and $\beta = 500$. |

$$\mathbf{A}^{-1} = \begin{bmatrix} \mathbf{a} & \frac{\beta\tau_\sigma}{\gamma}\mathbf{a}\mathbb{L} & K\tau_\rho\mathbf{a} \\ -\frac{\beta}{\gamma}\mathbb{L}\mathbf{a} & \mathbf{b} & -\frac{\beta K\tau_\rho}{\gamma}\mathbb{L}\mathbf{a} \\ \mathbf{a} & \frac{\beta\tau_\sigma}{\gamma}\mathbf{a}\mathbb{L} & -\tau_\rho\mathbf{I}_n + K\tau_\rho\mathbf{a} \end{bmatrix}, \quad (14)$$

where $\mathbf{a} = -(K_\omega(\mathbb{L}+\mathbb{A}) + \frac{\beta^2}{\gamma}\mathbb{L}^2)^{-1}$ and $\mathbf{b} = -\frac{\tau_\sigma}{\gamma}(\mathbf{I}_N + \frac{\beta^2}{\gamma}\mathbb{L}\mathbf{a}\mathbb{L})$. For a sufficiently large value of $\beta$, $\mathbf{a}$ converges to $-\epsilon\mathbf{1}_N\mathbf{1}_N^T$, where $\epsilon \in \mathbb{R}_+$ is a sufficiently small scalar ($\lim_{\beta\to\infty}\mathbf{a} = \mathbf{0}_N$). Moreover, considering that the time-constant $\gamma/\tau_\sigma$ is large, $\mathbf{b}$ also converges to a zero matrix. Hence, it can be shown that

$$\lim_{\beta\to\infty}\mathbf{A}^{-1}\mathbf{\Delta} = \mathbf{0}_{N\times 1} \quad (15)$$

Note that the above equality is satisfied for every possible attack vector $\mathbf{d}$ even if all DG units are attacked. As a result of (13) and (15), $\lim_{t\to\infty}\|\mathbf{e}(t)\| = 0$. Therefore, for a sufficiently large value of $\beta$, $\mathbf{e}(t)$ converges to zero in the steady-state. This implies that $\lim_{t\to\infty}\omega_i(t) = \omega_0$ for all $i \in \{1,\ldots,N\}$ and $\lim_{t\to\infty} m_{P_1}P_1(t) = \cdots = \lim_{t\to\infty} m_{P_N}P_N(t)$ in the presence of the cyber-attack vector $\mathbf{d}$.

**Remark 2:** The value of $\beta$ in (4) affects cyber-attack mitigation and transient behaviour in frequency regulation and power sharing responses. An optimal value of $\beta$ can be found by the optimal solution of an optimization problem with multiple objectives such as minimization of the $\mathcal{L}_2$ gain of the dynamical system in (8) considering $\mathbf{d}$ as a bounded disturbance, convergence rate, and robustness to time delays.

**Remark 3:** The main features of the proposed resilient cooperative frequency control (4) is that it provides full resilience to false data injection attacks on communication channels in the secondary frequency control of islanded AC microgrids. Moreover, although the proposed control structure is distributed, the design of control parameters for each DG unit is decentralized and does not require the knowledge of the entire microgrid and/or communication graph. Table I summarizes the main features of the proposed resilient control strategy in comparison to the existing methods in [1]–[5] and [9].

## IV. RESULTS

The proposed resilient distributed secondary control is tested on an islanded AC microgrids shown in Fig. 1 comprising of $N = 4$ converter-interfaced DG units. The microgrid operates at a global voltage and frequency reference $V^* = 310$ V and $f_0 = 50$ Hz. Since each converter has an equal capacity of 10 kVA, the droop coefficients $m_{P_i} = 0.00014\ radW^{-1}/s$ are equal. Therefore, active power will be shared equally. The system and control parameters are given in Table II. The switching frequency and sampling time are $f_s = 10$ kHz and $T_s = 20\ \mu$s, respectively. The performance of the microgrid is evaluated in terms of synchronization under several types of cyber-attacks.

The first case study evaluates the performance of the proposed resilient cooperative controller and the conventional cooperative frequency approach in (3) to load changes and resilient against cyber-attacks. To this end, it is worth notifying that: (i) a load of 1.55 kW is suddenly connected to point of common coupling 3 (PCC 3) at $t = 5$ s; (ii) time-varying false data $d_{\omega_{n_1}} = 6.3\cos(t)$, $d_{\omega_{n_2}} = -3.14$, $d_{\omega_{n_3}} = 6.3\sin(2t)$, and $d_{\omega_{n_4}} = 3.14$ are injected into all four converters at $t = 7$ s; (iii) a load of 1.55 kW is suddenly disconnected from PCC 3 at $t = 9$ s. The frequency responses and active power capability of DG units are depicted in Fig. 2.

In the second case study, we consider the impact of white noise on exchange data $P_j$ amongst the controllers of neighboring DG units. Moreover, in order to show the performance of the cooperative controller in (4) under non-identical $P-\omega$ droop coefficients, it is assumed that $m_{P_1} = m_{P_4} = 0.00014\ radW^{-1}/s$ and $m_{P_2} = m_{P_3} = 0.00007\ radW^{-1}/s$. The results of this case study are shown in Fig. 3.

As one can observe from Fig. 2 (c)-(d) and Fig. 3 (c)-(d), the conventional cooperative control can synchronize the frequencies of DG units to the nominal frequency of 50 Hz during the load change at $t = 5$ s; moreover, the total load power is shared amongst all DG units based on their active power rating. However, the synchronization and power sharing is lost once the attacks are launched. Furthermore, Fig. 2 (a)-(b) and Fig. 3 (a)-(b) indicate that the proposed resilient cooperative control approach in (4) mitigates the adverse effects of the cyber-attack; as a result, the synchronization is achieved in the presence of the attacks.

In the third case study, it is assumed that the cooperative frequency control system in (4) is subject to FDI attacks $\mathbf{d}_\sigma(t)$ ($d_{\sigma_1} = 6.3\cos(t)$, $d_{\sigma_2} = -3.14$, $d_{\sigma_3} = 6.3\sin(2t)$, and $d_{\sigma_4} = 3.14$) launched at $t = 3$ s. Fig. 4 shows the

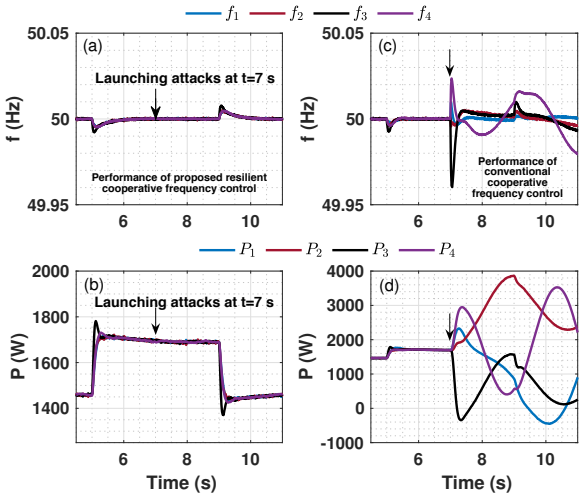


Fig. 2. Performance of the proposed resilient cooperative controller in (4) and the conventional cooperative frequency controller in (3) to load changes at $t = 5$ s and $t = 9$ s and FDI attacks $\mathbf{d}_\omega$ launched at $t = 7$ s: (a)-(b) frequency and active power of DGs via (4) and (c)-(d) frequency and active power of DG units via (3).

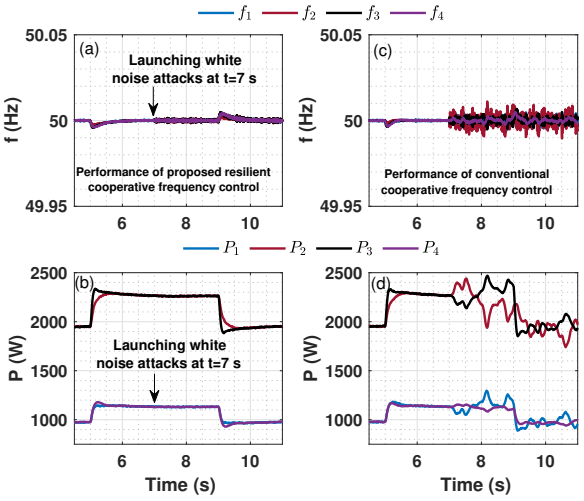


Fig. 3. Performance of the proposed and the conventional cooperative frequency controller in (4) and (3) with non-identical $P-\omega$ droop coefficients to load changes at $t = 5$ s and $t = 9$ s and white noise cyber-attacks launched at $t = 7$ s: (a)-(b) frequency and active power of DG units via (4) and (c)-(d) frequency and active power of DG units via (3).

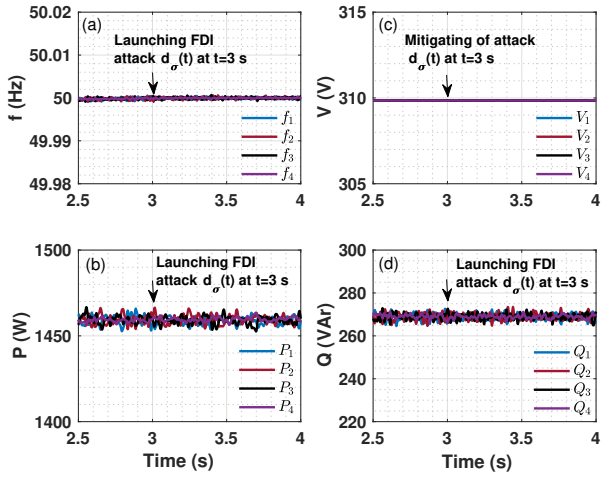


Fig. 4. Performance of the proposed resilient cooperative controller in (4) to FDI cyber-attacks $\mathbf{d}_\sigma(t)$ launched at $t = 3$ s: (a) frequency of DG units, (b) DG units' active power, (c) direct components of PCC voltages, and (d) DG units' reactive power.

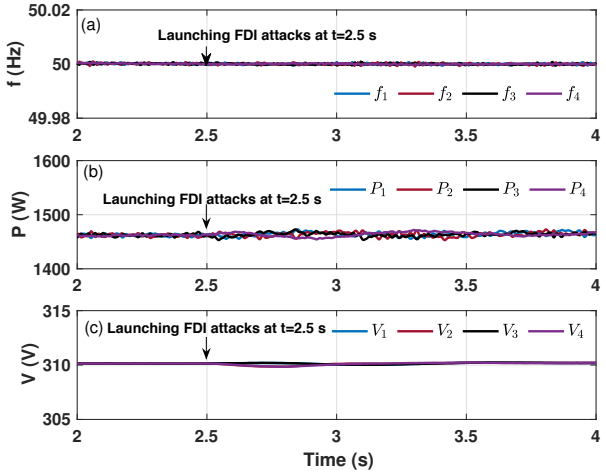


Fig. 5. Performance of the proposed resilient cooperative control strategy in (4) when all exchanged data are attacked at $t = 2.5$ s: (a) frequency of DG units, (b) DG units' active power, and (c) direct components of PCC voltages.

frequencies, active power, and reactive power of DGs as well as the direct component of PCC voltage signals. The results guarantee the resilience of the proposed cooperative frequency control against FDI attacks $\mathbf{d}_\sigma$.

The next case study carried out in Fig. 5 demonstrates the maximum level of resilience offered by the proposed distributed secondary control in (4). To this end, it is assumed that all the transmitted data in the microgrid frequency control system are subject to FDI attacks. This means that all exchanged data $(\omega_i, P_i, \sigma_i)$ from converter $i$ to converter $j \neq i$, $\forall i, j = 1, \ldots, 4$, are disrupted according to (5) at $t = 2.5$ s. The frequency, active power, and PCC voltage of converters are shown in Fig. 5. Upon launching the FDI attacks at $t = 2.5$ s, the proposed distributed control mechanism attenuates the adverse effects of attacks such that sychronization and proportionate active power sharing is not disrupted.

The last case study in Fig. 6 reveals the effects of the resilience index $\beta$ in cyber-attack resilience and microgrid dynamics in the presence of a load change at DG 1. From this figure, it is clear to see that increasing $\beta$ decreases the adverse effects of cyber-attacks on the frequency disruption. However, since $\beta$ plays the role of an integral gain for the proposed resilient cooperative controller in (4), increasing the value of $\beta$ might increase the overshoot and/or oscillation in the dynamics responses of islanded microgrids and might result in system instability. This has been highlighted in Fig. 7 where the impacts of $\beta$ in (4) can be directly attributed to the increased oscillatory behavior or system instability.

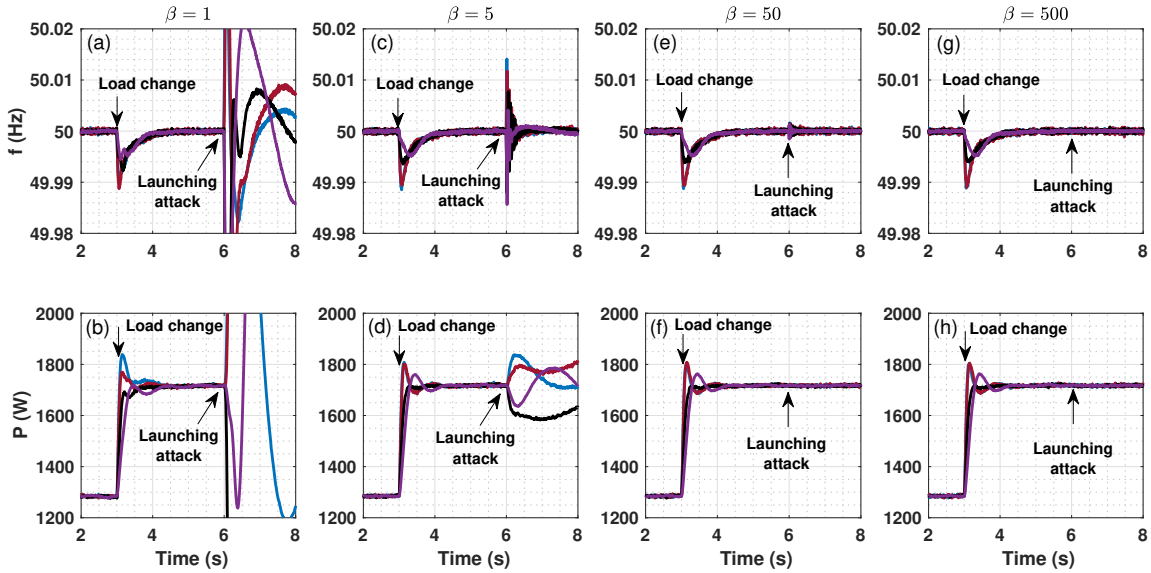


Fig. 6. Effects of the resilience index $\beta$ in synchronization in the presence of a load change at $t = 3$ s and launching FDI cyber-attacks at $t = 6$ s: (a)-(b) frequency and active power of DG units for $\beta = 1$, (c)-(d) frequency and active power of DG units for $\beta = 5$, (e)-(f) frequency and active power of DG units for $\beta = 50$, and (g)-(h) frequency and active power of DG units for $\beta = 500$.

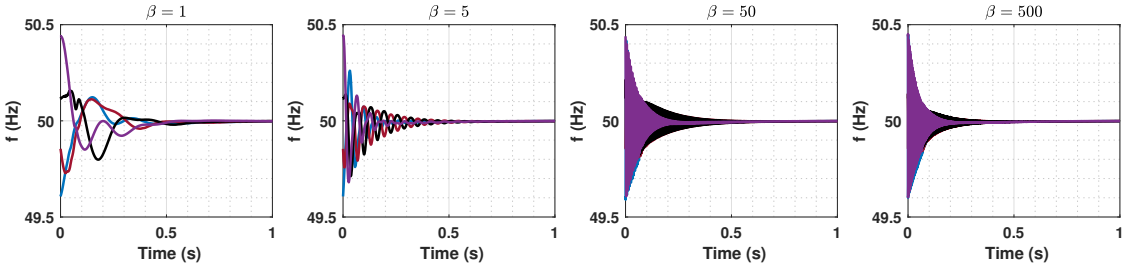


Fig. 7. Effects of $\beta$ in starting up the cooperative resilient controller in (4). Increasing $\beta$ results in more oscillation or instability in frequency responses.

## V. Conclusion

This letter presents a novel resilient secondary frequency control of AC microgrids. The proposed control framework offers maximum scale of false data injection cyber-attack resilience, as it guarantees the synchronization even if all converters are attacked. The performance of the proposed resilient secondary frequency control is evaluated under several case studies. The design of a resilient distributed control approach for voltage regulation and reactive power sharing in islanded AC microgrids and the optimal selection of the resilient parameter $\beta$ will be considered as a future scope of work.

## References


[1] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731–6741, Nov. 2018.

[2] 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, Sept. 2020.

[3] 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*, pp. 1–10, Dec. 2020.

[4] 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, Jan. 2021.

[5] A. Bidram, B. Poudel, L. Damodaran, R. Fierro, and J. M. Guerrero, "Resilient and cybersecure distributed control of inverter-based islanded microgrids," *IEEE Trans. Industr. Inform.*, vol. 16, no. 6, pp. 3881–3894, June 2020.

[6] S. Sahoo and J. C.-H. Peng, "A localized event-driven resilient mechanism for cooperative microgrid against data integrity attacks," *IEEE Transactions on Cybernetics*, pp. 1–12, 2020.

[7] S. Sahoo, R. Rana, M. Molinas, F. Blaabjerg, T. Dragicevic, and S. Mishra, "A linear regression based resilient optimal operation of ac microgrids," in *2020 IEEE 11th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2020, pp. 260–265.

[8] A. Bidram, A. Davoudi, and F. L. Lewis, "A multiobjective distributed control framework for islanded AC microgrids," *IEEE Trans. Industr. Inform.*, vol. 10, no. 3, pp. 1785–1798, Aug. 2014.

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

[10] A. Bidram, A. Davoudi, F. L. Lewis, and Z. Qu, "Secondary control of microgrids based on distributed cooperative control of multi-agent systems," *IET Gener. Transm. Distrib.,*, vol. 7, pp. 822–831, 2013.

[11] 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, Sept. 2020.

[12] R. A. Horn and C. R. Johnson, *Matrix Analysis*. United States of America: Cambridge University Press, Second Edition, 2013.