# Resilient Synchronization Strategy for AC Microgrids Under Cyber Attacks

Sahoo, Subham; Yang, Yongheng; Blaabjerg, Frede

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

*DOI (link to publication from Publisher):*
10.1109/TPEL.2020.3005208

*Publication date:*
2021

*Document Version*
Accepted author manuscript, peer reviewed version

# Resilient Synchronization Strategy for AC Microgrids Under Cyber Attacks

Subham Sahoo, *Member, IEEE*, Yongheng Yang, *Senior Member, IEEE* and Frede Blaabjerg, *Fellow, IEEE*

***Abstract*—Although distributed control in microgrids is well-known for reliability and scalability, the absence of a global monitoring entity makes it highly vulnerable to cyber attacks. Considering that the detection of cyber attacks becomes fairly easy for distributed observers, a well-planned set of *balanced* attacks, commonly termed as *stealth* attack, can always bypass these observers with the control objectives being successfully met. In this letter, a mitigation technique is thus introduced to remove *stealth* attack on the frequency control input in AC microgrids. The mitigation is carried out using a novel event-driven attack-resilient controller for $N$ cooperative grid-forming converters (GfCs), which guarantees resilient synchronization for up to $N-1$ attacked units. Finally, the resilience capabilities and robustness of the proposed controller are discussed and verified under various scenarios.**

***Index Terms*—Grid-forming inverters, cyber attacks, distributed control, cyber-physical systems, AC microgrids.**

## I. Introduction

GRID-forming converters (GfCs) are an integral asset in the power electronic energy paradigm, as they serve as one of the most common energy conversion interfaces between renewable energy sources and the grid [1]. To enhance system reliability in the islanded mode of operation, multiple GfCs are usually employed to share the active and reactive power demand. To achieve more flexibility in control under transmission delays and information failures, cooperative/distributed controllers with robust performance towards cyber layer imperfections are preferred in recent times. However, distributed control brings large concern in the form of cyber attacks due to the omnipresence of communication links leaving behind vulnerable spots [2]. Such man-made hazards could easily lead to loss of synchronization, which unnecessarily activates the protection relays, leading to converter(s) outage.

To address this issue, a trust and confidence-based resilient control protocol was introduced in [3] for GfCs in AC microgrids. However, the online calculation of these factors, which involves additional layers of integration and division operations, assigns high computational burden. Moreover, to provide attack-resilient operation, it requires a minimum of half of the neighboring converters to be *trustworthy*, thereby limiting its resilience capability for worst-case attacks. Additionally in [4], the information received from the attacked unit(s) has been discarded by disabling the corresponding cyber link as an elementary approach to prevent the propagation of attack into the non-compromised units. As a result, the cyber network connectivity is affected, which leads to disruption in the consensus theory. Another cybersecure framework is proposed in [5], which mandates a specific connectivity criterion for the communication graph to ensure resilient operation of AC microgrid. Further in [6], a partial primal-dual algorithm is determined to detect the presence of *stealth* node and link attacks. However, it is limited to detection only, without providing any comprehensive steps of countermeasures to mitigate the attack element(s). In [7], a resilient framework for unbounded cyber attacks in AC microgrid is presented. However, the resilient control update is introduced using an hidden control layer, which can still be infiltrated by an attacker conducting a *stealth* attack with sufficient system information. To the best of authors' knowledge, the ability to mitigate *stealth* attacks [8] in AC microgrids has never been discussed.

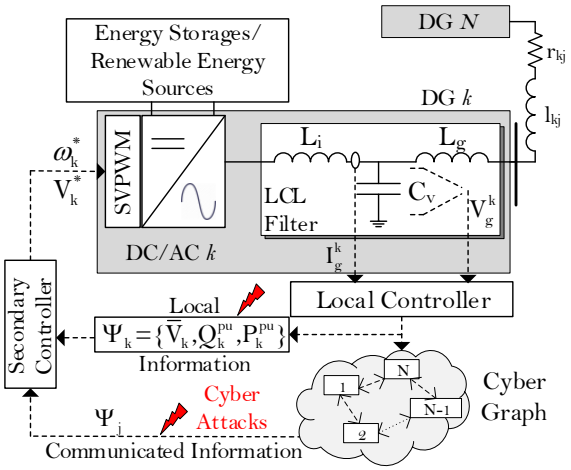


Fig. 1. Single-line diagram of a cyber-physical system consisting of $N$ grid-forming converters (GfCs) managed by a cooperative cyber topology–cyber attack (in red bolts) launched into local control input.

Hence, this letter introduces the mitigation of *stealth* attacks in cooperative AC microgrids. An asynchrony index based detection metric is proposed to detect the presence of attack signals in the frequency control input and immediately return an authentication signal to trigger the event-driven mitigation strategy. The mitigation strategy then reconstructs a *trustworthy* frequency signal and replaces it with the attacked signal. As opposed to the prior-art method, the proposed strategy can maintain resilient synchrony in the system only using a single *trustworthy* GfC.

This work was supported by THE VELUX FOUNDATIONS under the VILLUM Investigator Grant – REPEPS (Award Ref. No.: 00016591).

S Sahoo, Y Yang and F Blaabjerg are with the Department of Energy Technology, Aalborg University, Aalborg East, 9220, Denmark (e-mail: {sssa, yoy, fbl}@et.aau.dk)

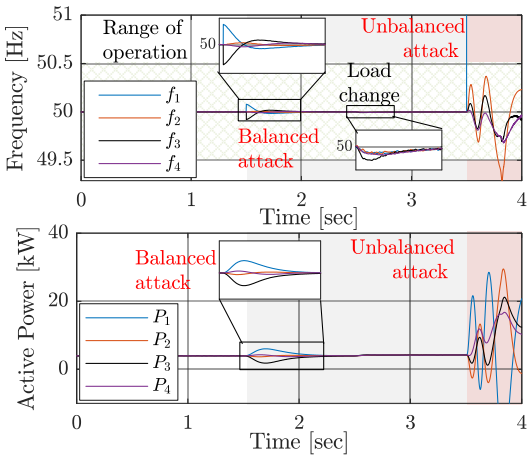


Fig. 2. Case study for $N$ = 4 GfCs – Attacker conducts a balanced attack first to deceive the system operator and then conducts an unbalanced attack resulting in operation outside the allowable range.

## II. Event-Driven Resilient Synchronization

As shown in Fig. 1, the $k^{th}$ GfC consists of a DC source (e.g., renewable energy or energy storage systems), an inverter bridge, a LCL filter and a controller using local measurements. In the system shown in Fig. 1 comprising of $N$ agents, each communication digraph is represented via edges to constitute an adjacency matrix $\mathbf{A} = [a_{kj}] \in R^{N\times N}$, where the communication weights are given by: $a_{kj} > 0$, if $(\psi_k, \psi_j) \in \mathbf{E}$, where $\mathbf{E}$ is an edge connecting two nodes with $\psi_k$ and $\psi_j$ being the local and neighboring node, respectively. Otherwise, $a_{kj} = 0$. $N_k = \{j|(\psi_k, \psi_j) \in \mathbf{E}\}$ denotes the set of all neighbors of $k^{th}$ agent. Further, the in-degree matrix $\mathbf{Z}_{in}$ = diag$\{z_{in}\}$ is a diagonal matrix with its elements given by $z_{in} = \sum_{j\in N_k} a_{kj}$. Further, the Laplacian matrix $\mathbf{L}$ is defined as $\mathbf{L} = \mathbf{Z}_{in} - \mathbf{A}$.

To improve their performance, neighboring GfCs' measurements, which are transmitted to the local GfC and vice-versa, are used in a cooperative secondary controller to regulate their respective bus' average voltage $\bar{V}_k$ and frequency $\omega_k$. The control objectives of the cooperative controller can be mathematically represented as:

$$\lim_{t\to\infty} \omega_k(t) = \omega^*, \ \lim_{t\to\infty} \bar{V}_k(t) = V^*, \ \forall\ k \in N \tag{1}$$

where $\omega^*$ and $V^*$ denote the global reference for frequency and voltage, respectively. Detailed control equations of cooperative secondary controller in AC microgrids can be referred from [9]. To achieve proportionate active power sharing alongwith frequency restoration, the primary layer droop control is modified into:

$$\omega_k(t) = \omega^* - m_k(P_k(t) - P_k^{ref}(t)) \tag{2}$$

where $m_k$, $P_k$ and $P_k^{ref}$ denote the active power droop coefficient, measured active power and secondary control active power reference in the $k^{th}$ agent, respectively. Basically, $P_k^{ref}$ compensates for the error introduced by the droop coefficient in (2). This is done using:

$$\dot{P}_k^{ref}(t) = k_1(\omega^* - \omega_k(t)) + k_2 \sum_{j\in N_k} a_{kj}(y_j(t) - y_k(t)) \tag{3}$$

with $k_1$ and $k_2$ being positive variables and $y = mP$. Substituting (3) in (2) for all the agents and multiplying $\mathbf{L}$ in both sides, we obtain $\mathbf{L}\boldsymbol{\omega}(t) = 0$ for (1) to hold true.

However, the objectives in (1) can be misconstrued in the presence of cyber attacks on the frequency signal in the $k^{th}$ agent using:

$$\omega_k^f(t) = \omega_k(t) + \kappa\omega_k^a \tag{4}$$

where $\kappa = 1$ denotes the presence of an attack element $\omega_k^a$ in the $k^{th}$ agent, or 0 otherwise. Further, these attacks can be conducted in a *coordinated* manner to deceive the system operator using:

$$\dot{\boldsymbol{\omega}}(t) = -(\mathbf{L}\boldsymbol{\omega}(t) + \boldsymbol{\omega}^a) \tag{5}$$

where $\boldsymbol{\omega}$ and $\boldsymbol{\omega}^a$ denote column matrices of the measured frequency and attack signal for $N$ GfCs, respectively.

***Remark I:*** *Considering the attack model in (5), the attack can be termed as:*

1) ***balanced*** *attack, if $\dot{\omega}(t) = 0$. Such attacks always lead to a stable and feasible solution, thereby satisfying the objectives in (1). More details on the design of stealth attacks in AC microgrids can be referred from [6].*
2) ***unbalanced*** *attack, if $\dot{\omega}(t) \neq 0$. They disregard the objectives in (1).*

***Remark II:*** *Based on the definition of balanced attacks, it can be concluded that $\sum_{k=1}^{N} \omega_k^a = 0$ for cooperative synchronization holds true. Conversely, $\sum_{k=1}^{N} \omega_k^a \neq 0$ for unbalanced attacks.*

A case study is carried out in Fig. 2 on an AC microgrid with $N$ = 4 GfCs to show the impact of balanced and unbalanced attacks on frequency control input. When an attack of $\boldsymbol{\omega}^a$ = $2\pi\{0.05,\ 0,\ -0.05,\ 0\}$ rad/s is introduced at t = 1.5 s, the frequency and active power of each agent converge back to the corresponding references, as defined in the control objectives. As per Remark I, all the necessary conditions are met, which certifies it as a balanced attack. However, at t = 3.5 s, the attacker maintains this discretion and increases one attack element in $\boldsymbol{\omega}^a$ = $2\pi\{10,\ 0,\ -0.05,\ 0\}$ rad/s. As a result, it can be seen that $\omega_1$ immediately goes outside the boundary of operation [49.5, 50.5] Hz (as highlighted in Fig. 2) defined for the microgrid. As the frequencies reach close to the aforementioned threshold, it could unnecessarily lead to the activation of protective relays, which could cause shutdown of the microgrid.

To detect the presence of such attack elements in AC microgrids, we consider the vector representation of a balanced attack (defined in Remark I) upon substituting (2) in (5) to get:

$$\mathbf{L}\boldsymbol{\omega}^* - \mathbf{LmP} + \mathbf{LmP}^{ref} + \boldsymbol{\omega}^a = 0 \tag{6}$$

where $\boldsymbol{\omega}^*_{N\text{x}1}$, $\mathbf{m}_{N\text{x}N}$, $\mathbf{P}_{N\text{x}1}$ and $\boldsymbol{\omega}^a_{N\text{x}1}$ denote the vector representation of $\omega^*$, $m_k$, $P_k$ and $\omega_k^a$, respectively. Since $\omega^*$ is constant for the whole microgrid, the first term in (6) can be eliminated with $\mathbf{L}$ being a symmetric matrix.

Further based on the timescale separation between the primary and secondary control layer, $\mathbf{LmP}$ = 0, by virtue of

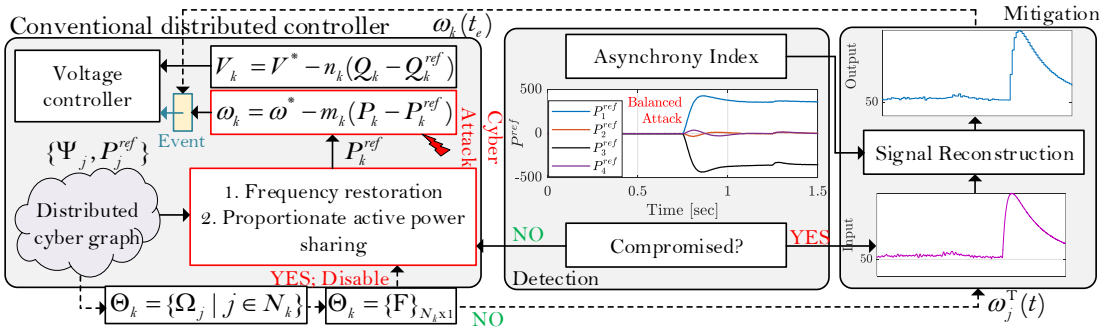


Fig. 3. Proposed resilient synchronization strategy in $k^{th}$ agent to mitigate balanced/unbalanced attacks in AC microgrid.

the dynamics of primary layer with $\mathbf{L}\omega$ already converging to zero. Hence, we get:

$$\mathbf{LmP}^{ref} + \boldsymbol{\omega}^a = 0. \tag{7}$$

***Remark III:*** *Using Remark II, every non-zero element(s) in $\boldsymbol{\omega}^a$ representing the attack signals will reflect an asymmetric relationship with $\mathbf{LmP}^{ref}$ for (7) to hold true. Hence, this asymmetry becomes the basis of detection for balanced and unbalanced attacks in cooperative AC microgrids.*

Accounting the asynchrony in $\mathbf{P}^{ref}$ under the presence of attacks, this letter proposes a novel detection metric, termed as asynchrony index $AI_k$, to detect possible cyber attacks in the $k^{th}$ agent using:

$$AI_k = l_k[\sum_{j \epsilon N_k} a_{kj}(P_j^{ref} - P_k^{ref})][\sum_{j \epsilon N_k} a_{kj}(P_j^{ref} + P_k^{ref})]. \tag{8}$$

***Remark IV:*** *Using Remark III, any value beyond an adaptive detection threshold $\gamma$ in (8) confirms the presence of an attack element in $k^{th}$ agent.*

To improve the transient performance under attacked scenarios, an adaptive detection threshold $\gamma_k$ has been designed such that the detection mechanism can be given by:

$$||AI_k|| > \underbrace{\beta \sum_{j \in N_k} ||a_{kj}(P_j - P_k)|| + \beta_0}_{\gamma_k} \tag{9}$$

where $\beta$ and $\beta_0$ are positive values. It is worth notifying that the first term in $\gamma_k$ and $\beta_0$ improves the detection performance during transients and steady-state condition, respectively. Since $\gamma_k$ is designed using the active power measurement $P_k$, which is obtained from a low-pass filter with a cut-off frequency $\omega_{ci}$ [9], the effect of measurement noise is reduced drastically. Following any disturbance in microgrids, the transients could affect the detection mechanism with a static threshold value. To address this issue, this letter employs a state-dependent adaptive threshold to provide accurate detection performance during both static and dynamic conditions. Further, the variance of noise in the measurements for a given system can be used as a good indicator to decide the minimum value of $\beta_0$ in advance.

Finally, to counteract against these attacks, this letter uses an event-driven signal reconstruction based mitigation strategy based on a follow-up signal from $AI_k$. Upon detection of the presence of attack element in $k^{th}$ agent, an authentication label $\Omega_k$ is generated for frequency in $k^{th}$ agent to alarm the presence of attack element (denoted as an *event* in this letter). It should be noted that the nature of this authentication label is binary, such that:

$$\Omega_k = \begin{cases} 0(\mathtt{F}), & \textbf{if } ||AI_k|| > \gamma_k \\ 1(\mathtt{T}), & \textbf{else} \end{cases} \tag{10}$$

To simplify the representation of authentication of the signals in $x = \{\omega, P\}$, $x^{\mathrm{T}}$ and $x^{\mathrm{F}}$ will be used to symbolize `True` (uncompromised) and `False` (compromised) for the corresponding signals using (10), respectively.

As long as (10) holds `True`, the compromised frequency signal is forced to follow the trajectories of non-compromised neighboring signals (with $\Omega_j$ labeled as `True`). As highlighted in Fig. 3, if the set of authentication signals $\Theta_k$ for $k^{th}$ agent is not a zero matrix (matrix comprising of signals $x$, only labeled with `F` as per (10)) in the presence of attack elements, event-driven resilient signals can be reconstructed using:

$$\omega_k(t_e) = \Xi[\omega_j^{\mathrm{T}}(t)] \tag{11}$$

where $\omega_k(t_e)$ (with $e$ as the triggering instant) denote the event-triggered samples of frequency in $k^{th}$ agent. It is worth notifying that $\Xi[x_j(t)]$ in (11) is a triggering function, which holds the input signal until the next instant of triggering. In (11), the input signals are the frequency of neighboring measurements $\omega_j^{\mathrm{T}}$ with authentication labeled as `T`. The event-driven signals are generated only when the detection mechanism in (9) holds true in the attacked agent. In particular, a trigger is generated when $||AI_k||$ hits the upper bounds of $\gamma$. A clear illustration of the event-driven resilient synchronization strategy is provided in Fig. 3.

The resilient action is completed by susbstituting the event-driven resilient signals with the attacked signal based on the local authentication signal according to:

$$\omega_k(t) = \Omega_k \omega_k^f(t) + (1 - \Omega_k)\omega_k(t_e) \tag{12}$$

Finally, the signal obtained in (12) is replaced with (2) to realize the mitigation of *stealth* cyber attacks in AC microgrids. As soon as the reconstructed signal in (12) obeys (1), the authentication label transmitted to the neighbors is switched back to `T`.

## III. Results

The proposed detection strategy has been tested in a distributed AC microgrid (as shown in Fig. 1) operating at a

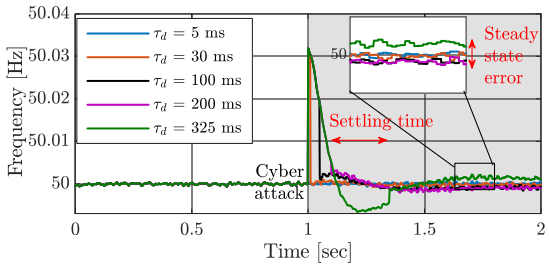


Fig. 4. Performance of the proposed event-driven attack resilient controller to follow (1) for different values of communication delay $\tau_d$ – Settling time keeps increasing and even settle at another set-point with increase in $\tau_d$.

global voltage and frequency reference of 311 V and 50 Hz, respectively with $N$ = 4 GfCs. Since each GfC is of equal capacity of 10 kVA, the droop coefficients $m_k$ are equal and hence, active power will be shared equally. Using the local and neighboring measurements, the proposed resilient strategy shown in Fig. 3 is modeled for every GfC to achieve resilient synchronization. All the parameters are provided in Appendix.

In Fig. 4, the performance of the microgrid is tested for different values of communication delay $\tau_d$. As soon as the attack is launched at t = 1 s, a *trustworthy* frequency signal from the neighboring measurements is communicated to the attacked unit. It can be seen in Fig. 4 that with increase in the value of $\tau_d$, the transient peak and the settling time to the reference set-point keeps increasing. However, for $\tau_d$ = 325 ms, it settles at another set-point. This behavior can be explained owing to the microgrid's operation within the maximum communication delay $\tau_d^{max}$ allowable for the cooperative cyber graph [9]. As the delay in the network goes beyond $\tau_d^{max}$, $\mathbf{L\omega}$ = 0 will not hold true anymore, thereby limiting the resilience capabilities of the proposed strategy.

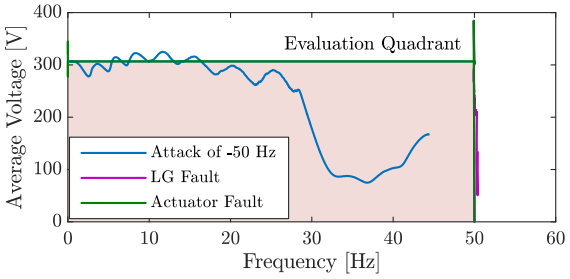


Fig. 5. Response of GfCs to malfunctioning events – Any trajectory inside the evaluation quadrant within 100 ms confirms the presence of cyber attack.

To differentiate between other malfunctioning events such as line-to-ground (LG) fault, actuator fault and cyber attacks, an evaluation theory for a GfC's response is presented in Fig. 5 for a window of 100 ms. This has been analyzed using a frequency-average voltage characteristics at the GfC bus responding to the aforementioned events with the evaluation quadrant ranging from within XY limits: [$\{X_{min}$ = 0, $X_{max}$ = $\frac{\omega^*}{2\pi}\}$, $\{Y_{min}$ = 0, $Y_{max}$ = $V^*\}$]. As it is evident from Fig. 5, the inception of LG and actuator faults causes immediate drop in voltages and frequency to zero, respectively. As they form the boundaries of the defined quadrant, an unbalanced attack of -50 Hz causes the trajectory to fall gradually towards zero with movement inside the quadrant owing to the control layer dynamics of the GfC. Hence, a trajectory movement inside the evaluation boundary (within a certain time frame $\approx$ 100 ms) can be used locally as a substantial indicator to assist the proposed scheme in differentiating between faults and cyber attacks.

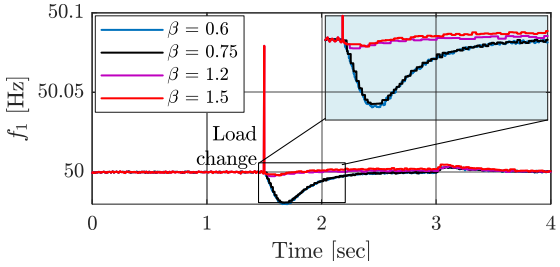


Fig. 6. Accuracy of signal reconstruction for different values of $\beta$ in the adaptive detection threshold $\gamma$.

Further, the accuracy of signal reconstruction is tested for different values of $\beta$ in adaptive threshold $\gamma$. As already explained earlier that the first term in $\gamma$ is to provide accuracy in detection during transient conditions, it can be seen in Fig. 6 that the accuracy can vary significantly when $\beta$ is less or more than 1. When $\beta$ < 1, the triggering instants become higher with increase in settling time. However when $\beta$ > 1, it can lead to peaky transients (up to 50.08 Hz) before the signal reconstruction is started, as the detection boundaries have increased leading to a decreased settling time.

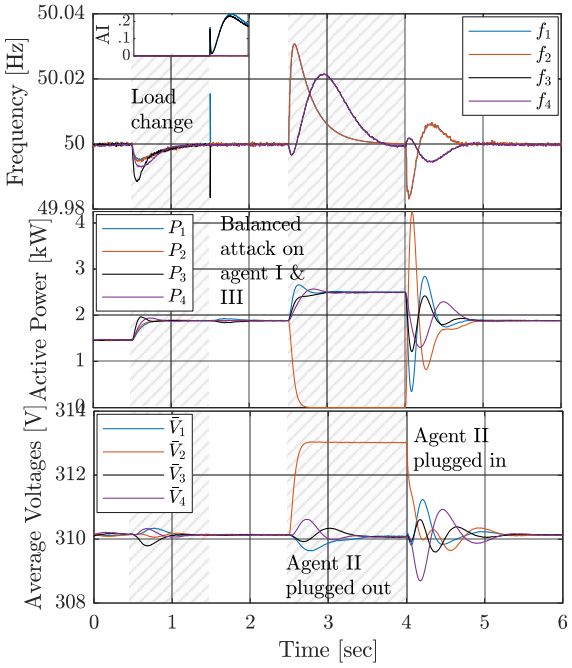


Fig. 7. Performance of $N$ = 4 GfCs with agent II plugged out and in at t = 2.5 & 4 s, respectively with agent I and III under a balanced attack at t = 1.5 s – Resilient operation achieved only using $\omega_4^T$.

Finally, the resilience capability of the proposed strategy is studied using only one *trustworthy* frequency input. In Fig. 7, it can be seen that the proposed detection mechanism does

TABLE I
COMPARATIVE EVALUATION OF THE PROPOSED RESILIENT STRATEGY IN AC MICROGRIDS.

| *Features* | [3] | [4] | [5] | [6] | [7] | **This letter** |
|---|---|---|---|---|---|---|
| Computational burden | High | Medium | Medium | Low | High | Low |
| Resilience capability | $\frac{N}{2}$[1] | Case-dependent[2] | Case-dependent | × | $\frac{N}{2}$ | $N-1$ |
| Cyber graph connectivity | Existing | Affected | Limited | Existing | Existing | Existing |
| Additional resources | × | × | × | × | Virtual control layer | × |
| Detection of *stealth* attack | × | × | × | ✓ | × | ✓ |
| Mitigation of *stealth* attack | × | × | × | × | × | ✓ |

[1] $N$ denotes the total number of GfCs in AC microgrid.
[2] It depends largely on the number of attacked cyber links/nodes, which ultimately affects the algebraic connectivity of cyber-graph.

not indicate any value above zero during a load change at t = 0.5 s. However, when a balanced attack of $\boldsymbol{\omega}^a = 2\pi\{0.75, 0, -0.75, 0\}$ rad/s is injected at t = 1.5 s, $AI_k$ rises into the positive region suggesting the presence of cyber attacks, which validates the selectivity in detection of cyber attacks. As a result, $\omega_2^{\mathrm{T}}$ and $\omega_4^{\mathrm{T}}$ are used to reconstruct signals immediately for agent I and III, respectively. When agent II is plugged out at t = 3.5 s, the incoming and outgoing communication link from agent II is lost. As a result, agent I immediately traverses to $\omega_4^T$ to ensure resilient synchronization. Further at t = 5 s, when agent II is plugged in back to the microgrid, it can be seen that the frequency of all agents are restored back to the reference value with active power shared equally among each other. As agent II is uncompromised, $\omega_2^{\mathrm{T}}$ is again made available for signal reconstruction. It can also be seen in Fig. 7 that the average voltages of the active GfCs also restore back to the voltage reference upon plug-in of agent II. This justifies that the proposed scheme can provide resilient synchronization for up to $N-1$ attacked units.

## IV. DISCUSSION

In this section, a comparative evaluation of the features provided by the proposed resilient controller as opposed to the existing solutions [3]-[7] has been provided in Table I. As evident from Table I, the proposed scheme assigning low computational burden provides resilience using the existing cyber infrastructure against both balanced and unbalanced attacks. Moreover, it provides a simple mitigation technique to substitute a reconstructed *trustworthy* frequency signal. The proposed method also offers the highest scale of resilience by restoring the system even when $N-1$ GfCs are attacked. In [4]-[5], the resilience capability is highly dependent on limited cyber graph connectivity, which may affect microgrid's performance even under the absence of attacks. On evaluating these terms, the contributions of this letter enhance the resilience of AC microgrids to a large extent in every aspect as compared to the prior art.

## V. CONCLUSIONS

A novel event-driven resilient control strategy is proposed to mitigate stealth cyber attacks in AC microgrids. The proposed strategy strategy is simple and offers the flexibility to build on the existing control framework without using any additional resources/information. Further, it offers the maximum scale of resilience, since it is capable of establishing synchronization even with $N-1$ compromised GfCs. The robustness of this theory has been tested under multiple scenarios and malfunctioning events to restrict the triggering of *events* only under the presence of cyber attacks without interfering in the normal operation of microgrids. Further investigation on providing resilience against *stealth* attacks on voltages can be considered as a future scope of work in AC microgrids.

## APPENDIX

Each GfC is equally rated with a capacity of 10 kVA. It should be noted that the controller gains are consistent for each GfC.

**Plant:** $N$ = 4, $L_i$= 1 mH, $C_v$= 10 $\mu$F, $L_g$= 3 mH, $r_1$ = 0.8 $\Omega$, $r_{12}$ = 0.25 $\Omega$, $r_{23}$ = 0.75 $\Omega$, $r_{34}$ = 1.2 $\Omega$, $l_{12}$ = 2.4 mH, $l_{23}$ = 1.8 mH, $l_{34}$ = 1.5 mH

**Controller:** $\omega^*$ = 314.15 rad/s, $V^*$ = 311 V, $m$ = 0.0014, $k_1$ = 320 , $k_2$ = 500, $\beta$ = 0.5, $\beta_0$ = 0.01, $l$ = 8.4

## REFERENCES


[1] J. Rocabert, A. Luna, F. Blaabjerg, and P. Rodriguez, "Control of Power Converters in AC Microgrids," *IEEE Trans. Power Electron.*, vol. 27, no. 11, pp. 4734-4749, Nov. 2012.

[2] S. Sahoo, T. Dragicevic, and F. Blaabjerg, "Cyber Security in Control of Grid-Tied Power Electronic Converters–Challenges and Vulnerabilities," *IEEE J. Emerg. Sel. Top. Power Electron.*, 2019, DOI: 10.1109/JESTPE.2019.2953480

[3] S. Abhinav, H. Modares, F.L. Lewis, F. Ferrese and A. Davoudi, "Synchrony in Networked Microgrids under Attacks," *IEEE Trans. Smart Grid*, vol. 6, no. 9, pp. 6731–6741, 2017.

[4] Q. Zhao, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A Cyber-Attack Resilient Distributed Control Strategy in Islanded Microgrids," *IEEE Trans. Smart Grid*, 2020, DOI: 10.1109/TSG.2020.2979160.

[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. Ind. Informat.*, vol. 16, no. 6, pp. 3881-3894, 2020.

[6] L. Y. Lu, H. J. Liu, H. Zhu, and C. C. Chu, "Intrusion Detection in Distributed Frequency Control of Isolated Microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6502-6515, 2019.

[7] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient Networked AC Microgrids Under Unbounded Cyber Attacks," *IEEE Trans. Smart Grid*, 2020, DOI: 10.1109/TSG.2020.2984266.

[8] S. Sahoo, S. Mishra, J.C.H. Peng, and T. Dragicevic, "A Stealth Attack Detection Strategy for DC Microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162-8174, 2019.

[9] R. Rana, S. Sahoo, J.C.H. Peng, and S. Mishra, "Performance Validation of Cooperative Controllers in Autonomous AC Microgrids Under Communication Delay," *2019 IEEE PES General Meeting*, pp. 1-5, Atlanta, USA, 2019.