Cyber-Resilient Sliding Mode Consensus Secondary Control Scheme for Islanded AC Microgrids

Abianeh, Ali Jafarian ; Mardani, Mohammad Mehdi; Ferdowsi, Farzad; Gottumukkala, Raju ; Dragicevic, Tomislav

Published in:
IEEE Transactions on Power Electronics

Link to article, DOI:
10.1109/TPEL.2021.3125985

Publication date:
2022

Document Version
Peer reviewed version

Citation (APA):
Abianeh, A. J., Mardani, M. M., Ferdowsi, F., Gottumukkala, R., & Dragicevic, T. (2022). Cyber-Resilient Sliding Mode Consensus Secondary Control Scheme for Islanded AC Microgrids. *IEEE Transactions on Power Electronics*, *37*(5), 6074 - 6089. https://doi.org/10.1109/TPEL.2021.3125985

Cyber-Resilient Sliding Mode Consensus Secondary Control Scheme for Islanded AC Microgrids

Ali Jafarian Abianeh, *Student Member, IEEE,* Mohammad Mehdi Mardani, *Student Member, IEEE,* Farzad Ferdowsi, *Senior Member, IEEE,* Raju Gottumukkala, and Tomislav Dragičević, *Senior Member, IEEE*

Abstract—**In this paper, a cyber-resilient consensus based distributed control scheme is proposed for islanded AC microgrids. Considering the impacts of False Data Injection (FDI) attacks on the conventional consensus algorithms, a hybrid solution is presented based on the combination of multi-objective sliding mode control and communication link quality observer to provide a reliable performance against different types of FDIs. Unlike the commonly developed distributed observer based cyber-resilient algorithms, this approach aims to form a complete localized solution without the requirements for transmission of extra distributed signals in the secondary layer. Using the proposed method, the system reliability will not be impacted by the cyber intrusions on the distributed observer terms, and the system's dynamic performance is not deteriorated by the counteracting operation resulted from adaptive distributed observers under other system transient conditions such as load dynamics, which can be even worsened under communication delays. Using cyber-resilient offset compensation terms, performance of the proposed sliding mode control scheme is enhanced for multi-objective regulation. Integrating the sliding mode control with communication link observer also ensures effective isolation of the unbounded and extreme cyberattacks. Unlike the former indirect local observers, the proposed scheme operates directly based on monitoring the affected distributed signals rather than only power terms, which enhances its reliability on detection. The effectiveness of the proposed scheme is validated through a real-time model developed in Typhoon HIL-402 real-time simulator as well as the experimental tests.**

Index Terms—**Consensus, Cyber Security, Microgrid, Sliding mode control.**

I. Introduction

AC microgrids are referred as the reliable solution to the intermittency challenges associated with the renewable power sources, which are being increasingly integrated into evolving distributed power generation systems. While Distributed Energy Resources (DERs) in AC microgrids can still rely on the well-developed grid following algorithms when operated in grid-connected mode, their islanded mode of operation is still highly vulnerable to the previously undermined system disturbances such as nonlinear electronic load switching and cyberattacks. The resilient operation of the grid forming converters in this mode is of critical importance to the system performance and reliability levels, which in the case of failure can have detrimental impacts and even lead to the protective circuitry tripping and loss of power generation. The grid forming algorithms are commonly implemented through the multilayer hierarchical control structures. In this regard, local control layer is devoted to the voltage and frequency regulation, and secondary control layer is in charge of the voltage/frequency sharing and the active/reactive power sharing among DERs [1]. Using the decentralized control schemes along with the enhanced droop regulation methods, primary layered control algorithms featuring power sharing are also reported [2], but their dynamic performance under system disturbances and in presence of tightly regulated loads are not optimal. In terms of the secondary controllers, the centralised algorithms are being increasingly replaced with the distributed schemes in the recent years, as distributed ones are not susceptible to the single point of failure.

Among different types of distributed control algorithms, consensus based techniques have gained higher popularity due to their more efficient communication topologies [3]. Several different consensus based algorithms are presented in the literature with the aim to enhance the voltage/frequency sharing [4], power sharing [5] or multi-objective regulations using adjustable trade-off gains [6] and double-layered cascaded regulation [7]. However, the performance of these conventional consensus algorithms can be deteriorated under presence of the system uncertainties [8] as well as cyber-layer irregularities such as communication delays and cyberattacks [9].

In efforts to enhance the dynamic performance of distributed secondary controllers under existing system uncertainties, advanced control concepts such as Model Predictive Control (MPC) and Sliding Mode Control (SMC) are employed by researchers. Using the system discrete model for development of MPC based algorithms, the impacts of system nonlinearities are minimized and the secondary output terms are optimized based on the predicted future behavior [10], [11]. However, modeling inaccuracies make the MPC algorithms highly prone to the performance deterioration under different operating conditions and disturbances. In addition, utilization of higher order models and complicated cost functions can hinder their feasibility in terms of the complexity levels. To address these challenges of the model-based secondary controllers, the model-independent SMC consensus have been investigated by some researchers [8], [12]. In [8], a chattering-free voltage and frequency sharing scheme using the sliding mode concept is presented, but this scheme does not address the power

Ali Jafarian Abianeh and Farzad Ferdowsi are with the Electrical and Computer Engineering Department of the University of Louisiana at Lafayette, Louisiana, USA (e-mails: ali.jafarian-abianeh1@louisiana.edu, farzad.ferdowsi@louisiana.edu).

Raju Gottumukkala is with the Mechanical Engineering Department of the University of Louisiana at Lafayette, Louisiana, USA (e-mail: raju@louisiana.edu).

Mohammad Mehdi Mardani and Tomislav Dragičević are with the Electrical Engineering Department of Technical University of Denmark, Copenhagen, Denmark, (e-mails: mmema@elektro.dtu.dk, tomdr@elektro.dtu.dk).

sharing requirements. The active power regulation is added to the sliding mode consensus voltage and frequency sharing in [12], but the chattering effect is still not properly mitigated. In addition, the proposed sliding surface suffers from deviations due to the inevitably compromised regulation nature between the frequency and active power sharing schemes. To improve the resilience of the secondary voltage sharing schemes against parameter uncertainties and measurement noises, a fast terminal SMC algorithm in combination with a model-dependent Extended State Kalman-Bucy Filter (ESKBF) is presented by [13]. However, this scheme suffers from complexity associated with model-based algorithms, and it lacks consideration of power terms as well as frequency regulation into the proposed sliding surface. Despite the improved robustness against system uncertainties using the SMC algorithms, none of these schemes are studied under cyber-layer irregularities and only physical model considerations are considered.

In order to enhance the performance of the secondary controllers under presence of the inevitable communication delays, a multistage event-triggered compensation algorithm [14] and predictive Deep Neural Network (DNN) based scheme [15] are proposed, which are both activated based on the observed deviation levels on the distributed signals. Also, a delay-tolerant algorithm using Lyapunov-Krasovskii method with a descriptor is proposed in [16]. However, all these schemes are only focused on the compensation of temporary error terms introduced into the secondary regulation due to the latency on receiving the feedback signals, which can be effectively mitigated specially if delays are bounded to the reasonable thresholds and somewhat evenly distributed across the communication links. However, different forms of cyberattacks can significantly deteriorate the performance of all the aforementioned distributed control schemes, and drive the system's states toward unstable conditions even with minor intrusions. In this regard, the False Data Injection (FDI) is known as one of the most challenging types of cyberattacks as with minor offsetting terms both stealthy and destabilizing impacts can be generated [17]. Despite the broadly discussed destructive effects of such cyberattacks, the scarcity of effective detection and mitigation methods, especially in the microgrids-scale [18], is still undeniable. In terms of the reported FDI detection and mitigation methods for the AC microgrids, three main approaches are employed by the researchers.

First group has focused on mitigating the adverse impacts of such intrusions through introducing the adaptive compensatory terms into the secondary regulation scheme using the distributed adaptive observers. In [19], a cyber-resilient distributed frequency and active power regulation method is presented, where the distributed adaptive terms based on the frequency error observations from the neighbouring agents are integrated into the regulation scheme. Using distributed observers on the active and reactive power signals, compensatory terms are added to the output of conventional schemes to ensure a resilient frequency and voltage sharing performance in [20]. Also, an adaptive distributed observer based on monitoring the neighbouring errors on the frequency and active power terms is proposed in [21]. However, all these schemes heavily rely on the secure transmission of additional data signals, which can by itself be the target of malicious cyber intrusions. In addition, the dynamic performance of these schemes under load disturbances is not optimal as no systematic approaches for distinguishing between the errors introduced by loads and cyberattacks are considered. The lack of such a discernment approach usually results in excessive overshoots/undershoots. Furthermore, none of these algorithms are studied under the presence of the communication delays, which can be highly critical to the proper calculation of the distributed adaptive terms.

The second group incorporates the distributed observers to trigger isolation of the non-cooperative nodes, which is usually formed based on monitoring the power angles and distributed secondary output terms [22], [23]. Unlike the adaptive distributed observer based schemes, such algorithms do not interfere with the system dynamic performance, but still demand extra data packets transmission and installation of external Phasor Measurement Units (PMUs), which can be also manipulated through the cyberattacks. The third approach is focused on using the commonly transmitted data signals in the secondary layer without demanding for extra data signals. In [24] and [25], the observed errors on the active power terms are utilized to trigger the isolation of non-cooperative nodes affected by frequency FDIs. However, it is not a quite feasible approach as active power terms can be highly impacted by other parameters such as load switchings to deviate from an optimal sharing performance, which can deceive the detection unit into false isolation of nodes. Even selection of larger thresholds to alleviate this challenge can lead to larger transients observed before taking effective actions once cyberattacks are applied.

In this paper, a cyber-resilient secondary control algorithm based on the combination of sliding mode consensus control and localized Communication Link Quality (CLQ) Observer is proposed. The main aim of this approach is to utilize the robust performance of SMC controllers for providing a complete localized solution, with respect to the other cyber-resilient algorithms that were dominantly formed on the basis of distributed observers and adaptive compensators. By combining the proposed scheme with a localized observer on the available distributed signals, not only an effective and reliable isolation of the significantly non-cooperative nodes will be attainable, but also it protects the SMC scheme against unbounded cyberattacks. In addition, the performance of the proposed scheme is verified against communication delays. Such a consideration as well as experimental validations were not included in many of the previously presented cyber-resilient algorithms [19]- [24]. The performance of the proposed algorithm is verified with both Hardware In the Loop (HIL) simulation results using Typhoon HIL-402, and the experimental tests. Thus, the main contributions of this paper can be summarized as follows:

- A distributed cyber-resilient control algorithm for frequency/voltage and active/reactive power sharing in the secondary layer of AC microgrids is proposed, which is formed with a combination of multi-objective sliding mode control and a localized communication link quality observer. This hybrid FDI detection and mitigation algorithm provides a reliable solution against FDIs on both node and link signals.

- The proposed localized CLQ observer performs only based on the existing distributed signals on each node, and does not impose the requirements for transmission of additional signals from its neighbouring agents. In addition, it provides a much more reliable FDI detection performance against other system disturbances such as load switchings, as it does not rely on distributed power error terms for detection of FDIs on distributed frequency and voltage signals.
- The proposed multi-objective sliding surface is integrated with a cyber-resilient offset alleviating term, which also facilitate the secondary control parameter adjustments for both uniform and non-uniform AC microgrids (combination of high/low inertia DERs).
- The higher vulnerabilities of the conventional consensus algorithms to the FDIs on the frequency distributed signals (compared with voltage FDIs) is discussed based on the secondary control terms interactions, and mainly focused on destabilizing frequency FDIs. The algorithm's performance is verified by both HIL and experimental results.

This paper is organized as follows: in Section II, the cooperative control of islanded AC-microgrids as well as the associated impacts of FDI cyberattacks on the conventional consensus schemes are presented. The proposed cyber-resilient sliding mode consensus scheme is presented in Section III. The real-time HIL simulation results are presented in Section IV, followed by experimental validation results in section V and Section VI concludes this research study.

II. Cooperative control of islanded AC microgrids and FDI cyberattack impacts

The islanded AC microgrid term is generally referred to a set of DERs connected to a common electrical bus using different interconnection topologies while the connection to the infinite bus of the utility grid is eliminated. The DERs can be represented by any power generation unit including both renewable and non-renewable sources. In order to maintain the microgrid local variables of voltage and frequency within the permissible range, it is a common practice to implement a hierarchical multi-layered regulation scheme. Such a hierarchical scheme is usually divided into primary level, secondary level and the tertiary level. Since the main focus of this paper is on the secondary level, only the lower two layers are discussed and the tertiary level is excluded from the scope of this research study.

A. Primary Control

The primary control layer in AC microgrids usually consists of the cascaded local controllers for each DER, which based on their structure can operate in either grid following or the grid forming modes [26]. In the islanded AC microgrids, it is unavoidable to have the grid forming converters as a part of the electrical network since their presence is highly critical for the system stability due to absence of utility grid connections. In fact, the grid forming converters operate in the master mode as opposed to grid following converters, which always run in the slave mode. A failure in any of the master grid forming converters can lead to malfunctions on the connected slave DERs. Therefore, in the distributed control schemes it is more favorable to have all DERs configured in the master mode of operation. Using this approach, the system reliability is enhanced and vulnerability of multiple DERs to a single point of failure is alleviated.

In the grid forming converters, the power sharing between DERs is controlled by the droop control method. In an AC microgrid with inductive electrical connections, the active power can be regulated by adjusting the frequency value, whereas the reactive power control is attainable through voltage amplitude regulation [27]. Therefore, the voltage and frequency in the primary level are determined using the setpoints and droop terms represented in (1), where ω and V represent the frequency and voltage, and ω^* and V^* are reference values for the frequency and voltage signals. Also, P and Q denote the active and reactive power terms, and m_p and m_q are droop terms for active and reactive power, respectively.

$$\begin{cases}\omega = \omega^* - m_p P \\ V = V^* - m_q Q\end{cases} \tag{1}$$

B. Secondary Control

The main control objective in the secondary layer is to compensate the deviations observed on the locally measured voltage value, and frequency value as the global variable. Also, a more accurate power sharing performance between the DERs in this control layer can be achieved. The power setpoints are usually assigned with respect to the DER rated power values. These normalized power terms are represented by $P_{Ni} = \frac{P_i}{P_{rated,i}}$ and $Q_{Ni} = \frac{Q_i}{Q_{rated,i}}$, where P_i, Q_i represent the instantaneous active and reactive power values, respectively. P_{ratedi}, Q_{ratedi} also denote the rated active and reactive power values for node i, respectively. The voltage/frequency sharing as well as power sharing are accomplished by introducing extra regulatory terms into the local controllers as formulated in (2), which gives an additional degree of freedom for the more desirable regulation of the local variables. Thus, the local control setpoints are modified as follows, where $\Delta\omega_{sec}$ and ΔV_{sec} represent the secondary control terms for frequency and voltage signals, respectively.

$$\begin{cases}\omega = \omega^* - m_p P + \Delta\omega_{sec} \\ V = V^* - m_q Q + \Delta V_{sec}\end{cases} \tag{2}$$

The detailed block diagram of the local controller for a grid forming converter in presence of the secondary layer regulation terms is depicted in Fig. 1. The conventional approach was based on the centralized scheme where a central computation unit was in charge of calculating the secondary control terms through the communication with all DERs. In the distributed approach, the computations of secondary terms are performed at the place of each DER with respect to the data received from other DERs. Averaging and consensus based control techniques are the most common types of distributed

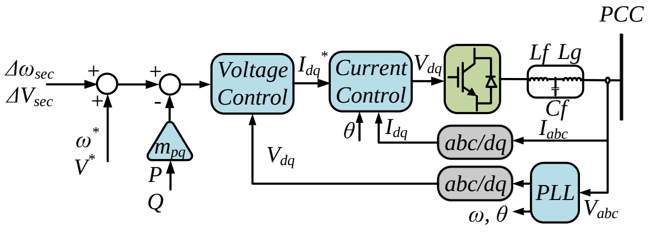


Fig. 1. Block diagram of the local controller on a grid forming converter in presence of the secondary layer regulation terms.

secondary controllers [3]. In the averaging scheme, a strong interconnection topology is established between all existing nodes, while in consensus the communication only between the adjacent nodes are established in a way that a robust communication network in the secondary layer is ensured.

For a microgrid with n nodes, the adjacency matrix is of size $n \times n$. The matrix elements (a_{ij}) are zero when there is no direct communication between nodes i and j, and $a_{ij} > 0$ when there is data transfer between them. The adjacency matrix and the consensus-based update rule on variable x for node i can be represented by (3) and (4), respectively [6].

$$A_{n,n} = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{bmatrix} \tag{3}$$

$$\dot{x_i} = -\sum_{j=1}^{n} a_{ij}(x_i - x_j) \tag{4}$$

By dividing both sides of equation (4) with $\frac{1}{\sum_{k=1}^{n} a_{ik}}$ and then rearranging it, (5) can be derived where $w_{ij} = \frac{a_{ij}}{\sum_{k=1}^{n} a_{ik}}$:

$$\frac{1}{\sum_{j=1}^{n} a_{ij}} \dot{x_i} = -x_i + \sum_{j=1}^{n} w_{ij} x_j \tag{5}$$

According to the above adaptation law, the variable x_i on node i converges to the weighted average of its neighbor values x_j with the time constant of $\sum_{j=1}^{n} a_{ij}$.

Using the general consensus law, the secondary control layer regulation set-point can be derived by (6) and (7) for voltage/frequency sharing and power sharing, respectively:

$$\begin{cases} \dot{\omega_i} = -(\sum_{j=1}^{n} a_{ij}(\omega_i - \omega_j) + k_{\omega i}(\omega_i - \omega_{ref})) \\ \dot{V_i} = -(\sum_{j=1}^{n} a_{ij}(V_i - V_j) + k_{Vi}(V_i - V_{ref})) \end{cases} \tag{6}$$

$$\begin{cases} \dot{P_{Ni}} = -\sum_{j=1}^{n} a_{ij}(P_{Ni} - P_{Nj}) \\ \dot{Q_{Ni}} = -\sum_{j=1}^{n} a_{ij}(Q_{Ni} - Q_{Nj}) \end{cases} \tag{7}$$

Where $k_{\omega i}$ and k_{Vi} are the proportional control gains for regulation of the ω and V with respect to the reference values in the secondary layer, and P_N and Q_N represent the normalized active and reactive power terms with respect to the rated power values for each node.

C. Consensus distributed control under FDI attacks

In this section, the impact of the cyberattacks on the conventional consensus-based voltage-frequency regulation scheme is analytically discussed. The main focus of this analysis is on the FDI attacks [17], but it can be generalized to other types of attacks such as Denial of Service (DOS). Considering the presence of a non-cooperative node k, which transmits a corrupted data frame to node m, while the data integrity over the rest of communication links and associated data packets are maintained, the consensus equation for node m can be represented by (8).

$$\begin{cases} \dot{\omega_m} = -(\sum_{j=1}^{n} a_{mj}(\omega_m - \omega_j) + k_{\omega m}(\omega_m - \omega_{ref}) \\ -a_{mk}\Delta\omega_{mk}) \\ \dot{V_m} = -(\sum_{j=1}^{n} a_{mj}(V_m - V_j) + k_{Vm}(V_m - V_{ref}) \\ -a_{mk}\Delta V_{mk}) \end{cases} \tag{8}$$

Where ω_m and V_m are the frequency and voltage terms at the place of the node m, a_{mj} and a_{mk} represent the neighboring coefficients for the communication link between nodes $m-j$ and $m-k$ on the adjacency matrix, $k_{\omega m}$ and k_{Vm} are proportional control gains for regulation of the ω and V at the place of the node m with respect to the reference values, and $\Delta\omega_{mk}$ and ΔV_{mk} denote the cyber intrusion terms for frequency and voltage distributed signals sent from node k to node m and generated only as a result of external manipulation.

Thus, the secondary control terms in (2) for node m will initially change in proportion with the cyber intrusion terms:

$$\begin{cases} \Delta\omega_{msec} \approx K_{m\omega 1}\Delta\omega_{mk} \\ \Delta V_{msec} \approx K_{mV1}\Delta V_{mk} \end{cases} \tag{9}$$

Where $k_{m\omega 1}$ and k_{mV1} are the proportional gains to deviations on secondary regulation terms for frequency and voltage at the place of node m as generated directly by external manipulations, respectively.

Since the frequency is the global variable, such an intrusion will proportionally impact the global frequency ω_{global}. Therefore, this impact will be reflected for all the nodes within the term $(\omega_i - \omega_{ref})$ in (6) and $(\omega_m - \omega_{ref})$ in (8) where the ω_i and ω_m are impacted with the variations on the ω_{global} introduced by $\Delta\omega_{mk}$, and resulting in minor attenuating contribution to secondary regulation terms for nodes indexed by m and i, as represented in (10) and (11).

$$\Delta\omega_{msec} \approx -K_{m\omega 2}\Delta\omega_{mk} \tag{10}$$

$$\Delta\omega_{isec} \approx -K_{i\omega 2}\Delta\omega_{mk} \tag{11}$$

Where $k_{m\omega 2}$ and $k_{i\omega 2}$ are the proportional gains to deviations on secondary regulation terms for frequency on nodes m and i as the indirect impact of cyber intrusion, respectively.

Since the direct impact of cyberattacks on the global frequency is always further attenuated by means of other cooperative nodes (indirect impact), the significance of neighboring error term (ω_m-ω_j) always outweighs the local error term (ω_m-ω_{ref}) in (8) and therefore the following for the node m will be justified:

$$k_{m\omega 1} \gg k_{m\omega 2} \tag{12}$$

Thus, the overall resultant impact of such an intrusion on the frequency terms in the secondary control layer for the nodes indexed by m and i can be formulated as follows:

$$\begin{aligned}\Delta\omega_{msec} &\approx (K_{m\omega 1} - K_{m\omega 2})\Delta\omega_{mk} \\ &, \, where\, K_{m\omega 1} \gg K_{m\omega 2} > 0\end{aligned} \tag{13}$$

$$\Delta\omega_{isec} \approx -K_{i\omega 2}\Delta\omega_{mk}, where K_{i\omega 2} > 0 \tag{14}$$

As a result, the aggregated direct and indirect impacts of such a cyber-intrusion on nodes m and i can be summarized as follows:

$$\begin{cases}\Delta\omega_{msec} > 0 \, and \, \Delta\omega_{isec} < 0 \, for \, \Delta\omega_{mk} > 0 \\ \Delta\omega_{msec} < 0 \, and \, \Delta\omega_{isec} > 0 \, for \, \Delta\omega_{mk} < 0\end{cases} \tag{15}$$

The impact on the global frequency is dominated by the term $\Delta\omega_{msec}$ while some attenuation through $\Delta\omega_{isec}$ is introduced. However, it should be noted that the deviations introduced into the secondary control terms will also lead to proportional deviations in the active powers. In the case of the islanded AC microgrids, the overall drawn active power is dictated by the microgrid loading condition. However, the incompatibility of frequency deviations generated by cyber-attacks and power regulatory terms as imposed by loading condition hinders the microgrid reaching the equilibrium point and drives the converters toward overloading or shut down conditions leading to the system instability.

The impact of such intrusion on the voltage sharing scheme is less detrimental as the voltage is a local variable measured at the PCC of each DER. Beside the direct impact of corrupted voltage terms on the secondary control regulation for the node m as represented by (9), the indirect impact on both m and i indexed nodes can be given by (16) and (17). In contrast with the indirect impacts on the frequency secondary term for node i as represented by (11), an additional error-following term ($k_{iV3}\Delta V_{mk}$) is introduced which is resulted from errors observed on adjacent voltage terms of (V_j-V_i):

$$\Delta V_{msec} \approx -K_{mV2}\Delta V_{mk} \tag{16}$$

$$\Delta V_{isec} \approx -K_{iV2}\Delta V_{mk} + K_{iV3}\Delta V_{mk} \tag{17}$$

Where k_{mV2}, k_{iV2} and k_{iV3} are the proportional gains to deviations on secondary regulation terms for voltage on nodes m and i as the indirect impact of cyber intrusion, respectively.

Thus, the overall resultant impact of such an intrusion on the voltage terms in the secondary control layer for the nodes indexed by m and i can be described as follows:

$$\begin{aligned}\Delta V_{msec} &\approx (K_{mV1} - K_{mV2})\Delta V_{mk}, \\ &, \, where\, K_{mV1} \gg K_{mV2} > 0\end{aligned} \tag{18}$$

$$\Delta V_{isec} \approx (-K_{iV2} + K_{iV3})\Delta V_{mk}, where\, K_{iV2} > 0 \tag{19}$$

In comparison with the (14), in (19) an additional contributing term as an indirect impact of cyber intrusion is introduced into voltage secondary control terms for the nodes indexed by i which gives an additional degree of freedom to reach the equilibrium point without driving the system into the unstable condition. It should be also added that the reactive power sharing will also be deviated based on the ΔV_{msec} and ΔV_{isec} at the equilibrium point.

III. Proposed cyber-resilient sliding mode consensus based control scheme

The sliding mode control strategy is formed on the basis of driving the system states toward the desired manifolds using the chosen discontinuous control signals. The proper selection of the sliding surfaces is a crucial step as it has to ensure the proper regulation performance while the states converge toward the specified manifolds [28]. Referring to the equations (6) and (7) and the known relationship between the $P-\omega$ and $Q-V$ over the inductive power lines from (1), the secondary layer frequency and voltage dependent control objectives are summarized by (20)-(22) and (23)-(25), respectively:

$$\Delta\omega_{\omega i} = \omega_{ref} - \omega_i \tag{20}$$

$$\Delta\omega_{\omega ij} = \sum_{j=1}^{n} a_{\omega ij}(\omega_j - \omega_i) \tag{21}$$

$$\Delta\omega_{Pij} = \sum_{j=1}^{n} a_{Pij}K_{\omega P}(P_{Nj} - P_{Ni}) \tag{22}$$

$$\Delta V_{vi} = V_{ref} - V_i \tag{23}$$

$$\Delta V_{vij} = \sum_{j=1}^{n} a_{vij}(V_j - V_i) \tag{24}$$

$$\Delta V_{Qij} = \sum_{j=1}^{n} a_{Qij}K_{VQ}(Q_{Nj} - Q_{Ni}) \tag{25}$$

Where $\Delta\omega_{\omega i}$, $\Delta\omega_{\omega ij}$, $\Delta\omega_{Pij}$ denote the frequency error terms for the agent i with respect to reference frequency value, adjacent neighboring frequency terms, and adjacent neighboring active power terms, respectively. Moreover, ΔV_{vi}, ΔV_{vij}, ΔV_{Qij} represent the voltage error terms for the agent i with respect to reference voltage value, adjacent neighboring voltage terms, and adjacent neighboring reactive power terms. Parameters $a_{\omega ij}$, a_{vij}, a_{Pij}, a_{Qij} are the adjacency coefficients for the frequency, voltage, active power and reactive power of node i with respect to the neighbor nodes as indexed by j. Also, $K_{\omega P}$ and K_{VQ} denote the scaling power error parameters to enable prioritizing the regulation with trade-off between local variable errors and power term errors.

In order to ensure the proper secondary layer regulation over the desired variables of the agent i with respect to the reference value and the adjacent neighboring terms, the sliding surfaces are proposed to be chosen by (26)-(31). As stated by (26) and (29), the selected surfaces consist of two complementary terms. The first term, as formulated by (27) and (30), utilizes the first order dynamics to ensure convergence to the reference values and minimizing the error terms. However, due to the known trade-off behavior between the $P-F$ and $Q-V$ terms, it is impossible to have the first terms in (26) and (29) equal to zero at any instant. This is mainly attributed to the fact that prioritizing the error minimization on $\Delta\omega_{\omega ij}$ and ΔV_{vij} will result in larger offsets on $\Delta\omega_{Pij}$ and ΔV_{Qij}, respectively and vice versa. This issue has not yet been considered in any of the previously reported sliding mode based secondary layer control schemes in the literature.

In order to mitigate the aforementioned shortcoming, a compensation term for each surface is introduced in this paper which counteracts the introduced offsets based on the applied flexible adjustments. The main advantage of this term is the more effective and straight forward selection of the boundary layer threshold (discussed in following sections and represented by (35)) and avoiding the excessive chattering effects attributed to the sliding switching function under some specific operating conditions. In order to alleviate the impact of cyber invasions on the proposed SMC scheme and avoiding excessive deviations from the manifolds once the cyberattacks occur, an attenuating exponential factor is applied to the second term in the surface formulations which is a function of neighboring frequency and voltage error terms. Without this exponential term, the sliding surface will be highly vulnerable to the cyber-attacks and only remains effective during the normal operating condition while there is no non-cooperative node. In fact, the second term in sliding surfaces cancels the offsets during the normal operating condition while being automatically filtered out upon detecting the excessive levels of cyber errors.

$$S_\omega = S_{\omega1} + S_{\omega2} \tag{26}$$

$$\begin{aligned} S_{\omega1} &= \Delta\omega_{\omega i} + \Delta\omega_{\omega ij} + \Delta\omega_{Pij} \\ &+ c_{\omega1}(\frac{d}{dt}\Delta\omega_{\omega i} + \frac{d}{dt}\Delta\omega_{\omega ij} + \frac{d}{dt}\Delta\omega_{Pij}) \end{aligned} \tag{27}$$

$$S_{\omega2} = K_{Pij}.e^{-K_{\omega exp}|\Delta\omega_{\omega ij}|}.\Delta\omega_{\omega ij} \tag{28}$$

$$S_v = S_{v1} + S_{v2} \tag{29}$$

$$\begin{aligned} S_{v1} &= \Delta V_{vi} + \Delta V_{vij} + \Delta V_{Qij} \\ &+ c_{v1}(\frac{d}{dt}\Delta V_{vi} + \frac{d}{dt}\Delta V_{vij} + \frac{d}{dt}\Delta V_{Qij}) \end{aligned} \tag{30}$$

$$S_{v2} = K_{Qij}.e^{-K_{vexp}|\Delta V_{vij}|}.\Delta V_{vij} \tag{31}$$

Where S_ω, S_v denote the overall selected sliding surface, $S_{\omega1}$, S_{v1} represent the first sliding surface term, and $S_{\omega2}$, S_{v2} are the second sliding surface term for the secondary layer sliding mode consensus control of frequency and voltage terms, respectively. The $c_{\omega1}$ and c_{v1} constants also denote the corresponding design constant gains for the chosen sliding surfaces and the K_{Pij} and K_{Qij} constants represent the offset compensation gains for addressing the surface deviations introduced by active and reactive power terms. In addition, $K_{\omega exp}$, K_{vexp} are the decaying rate constants for counteracting the adverse impact of cyber intrusions on the selected frequency and voltage terms for the sliding surface in the secondary control layer.

As the next step, it is necessary to ensure the convergence of the state variables towards the sliding surfaces and retaining it over the surfaces during the steady state condition. The regulation goals can be achieved when $S_\omega = S_v = 0$. By applying this to the equations (26)-(31), the following equations are obtained:

$$\begin{aligned} &\frac{d}{dt}(\Delta\omega_{\omega i} + \Delta\omega_{\omega ij} + \Delta\omega_{Pij}) = -\frac{1}{c_{\omega1}}(\Delta\omega_{\omega i} + \Delta\omega_{\omega ij} \\ &+ \Delta\omega_{Pij} + K_{Pij}.e^{-K_{\omega exp}|\Delta\omega_{\omega ij}|}.\Delta\omega_{\omega ij}) \end{aligned} \tag{32}$$

$$\begin{aligned} &\frac{d}{dt}(\Delta V_{vi} + \Delta V_{vij} + \Delta V_{Qij}) = -\frac{1}{c_{v1}}(\Delta V_{vi} + \Delta V_{vij} \\ &+ \Delta V_{Qij} + K_{Qij}.e^{-K_{vexp}|\Delta V_{vij}|}.\Delta V_{vij}) \end{aligned} \tag{33}$$

As previously discussed, the inherent offset values for $\Delta\omega_{Pij}$ and ΔV_{Qij} will be cancelled out by $S_{\omega2}$ and S_{v2} terms under the normal operating condition while these compensation terms are automatically equaled to zero under the excessive levels of cyber-attacks. Therefore, it is realized from (32) and (33) that the state variables converge to the specified surfaces for any positive values selected for the constant control gains of $c_{\omega1}$, c_{v1}. In this scheme, the constant control gains act as the low pass filters and thus the gains are selected with respect to the desired transient performance.

As the next step, it is required to enforce the sliding mode operation over the specified manifolds using the discontinuous control signals. For this purpose, the $sgn(.)$ function is used where higher sliding mode gain values of K_{smc} in (34) are in charge of enhancing the controller robustness.

$$\Delta x_{isec} = K_{smc} sgn(S_k) \tag{34}$$

Where Δx_{isec} denotes either the voltage or frequency secondary control term for the node i as presented by (2).

However, the improper high SMC gain values can lead to the excessive chattering due to the discontinuous nature of the applied control signals and this can potentially excite some unmodeled dynamics. In order to mitigate this problem, the pure $sgn(.)$ function is replaced with a continuous control function within the specified boundary layer of the sliding surface as represented by:

$$sgn_{cont}(S_k) = \begin{cases} 1, & \text{if } S_k > \varepsilon_k \\ \dfrac{S_k}{\varepsilon_k}, & \text{if } |S_k| < \varepsilon_k \\ -1, & \text{if } S_k < -\varepsilon_k \end{cases} \tag{35}$$

Where k denotes the index for the sliding surfaces and $\varepsilon_k > 0$ represents the boundary layer threshold as well as functioning as a smoothing factor for transition between the two schemes. $sgn_{cont}(.)$ is also the continuous form of $sgn(.)$ function.

The block diagram for the proposed sliding mode consensus based secondary control scheme is depicted in Fig. 2. Proof of stability for the proposed SMC scheme is also presented in the Appendix A. In order to enable a more realistic tuning approach for the SMC controllers and protect the algorithm against extreme or unbounded cyberattacks, it is essential to combine the SMC algorithm with CLQ unit to monitor the deviation levels in the distributed sharing terms and ensure they are always retained bounded to the specific levels. This is mainly considered due to the fact that extreme erroneous terms would demand much higher controller gain values and this would adversely impact the steady state performance of the secondary SMC controller. To address this concern, a Hysteresis-based Communication Link Quality (HCLQ) observer is introduced, as shown in Fig. 3. This scheme operates based on the direct observation of the distributed error terms to signal out the isolation command for the associated non-cooperative incoming communication links, and without relying on the other vulnerable distributed

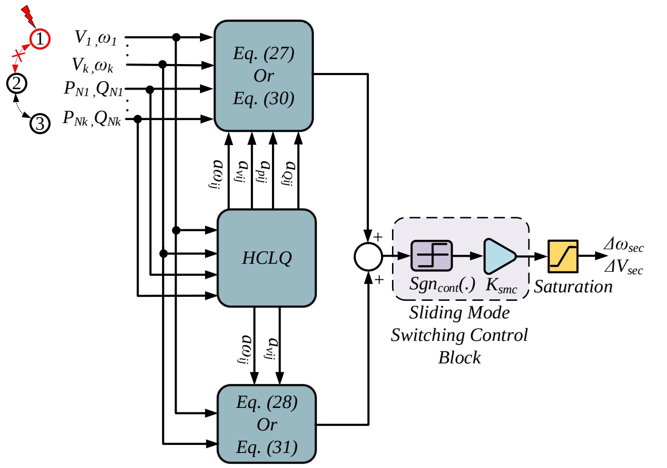


Fig. 2. Block diagram of the proposed cyber-resilient sliding mode consensus based secondary control scheme.

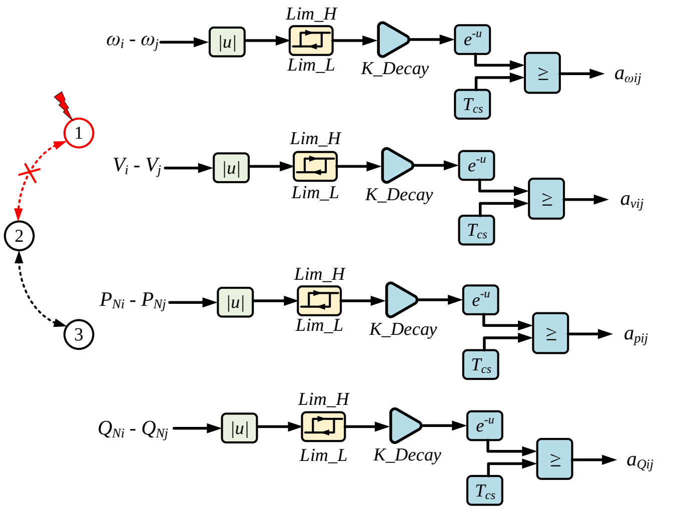
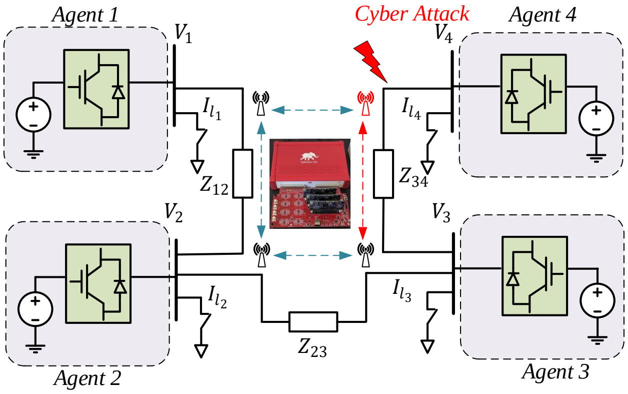


Fig. 3. Block diagram of the proposed hysteresis based communication link quality observer.

observer terms and indirect observation from power terms for frequency/voltage intrusion detection, it enables a complete localized cyber-resilient solution in combination with SMC. Basically, this scheme monitors the deviation levels in the distributed terms and uses the hysteresis upper bound level to trigger a one-shot decaying logarithmic function for isolating the non-cooperative node. In order to avoid frequent node partial isolations on common disturbances, a specified threshold on the decaying logarithmic output is utilized for immediate disconnection after certain timing interval from the exceeded error level in the adjacent distributed terms. The logarithmic delay unit is reset once the distributed term errors retrieves to a level lower than hysteresis lower bound value.

IV. Real-time simulation results

In order to verify the performance and effectiveness of the proposed cyber-resilient control scheme in combination with the HCLQ unit under common types of FDI intrusions, two different system configurations, are considered as shown in Fig. 4. In the first configuration, a combination of both high and low inertia DERs including diesel, solar and battery units are integrated into a 4-bus configuration system and a tightly regulated power electronic load is placed at the remaining bus. In the second configuration, four battery energy storage units are integrated into a 4-bus low voltage Islanded AC microgrid, similar to the case study in [25], where US standard voltage levels are applied. The system electrical and control parameters for both configurations are also presented in Appendix B. The main purpose of studying the proposed algorithm with presence of both high/low inertia DERs is to avoid the unrealistic assumption of always having uniform DERs and ensure a more insightful study into the system dynamic performance under cyberattacks. In this case, the detailed models of local controllers for both types of DERs are used including excitation and governor units for diesel. Using the second configuration, the common radial 4-bus AC microgrid with uniformly connected Battery Energy Storage Systems (BESSs) is investigated to enable a comparative study with the previously reported cyber-resilient algorithms, such as the one presented in [25]. In this section, the performance of the proposed algorithm is studied under several different test scenarios using the real-time simulation model developed in the Typhoon HIL 402. The test cases 1 to 4 are carried out on the first system configuration and the rest of real time simulation results are collected from the second system configuration.



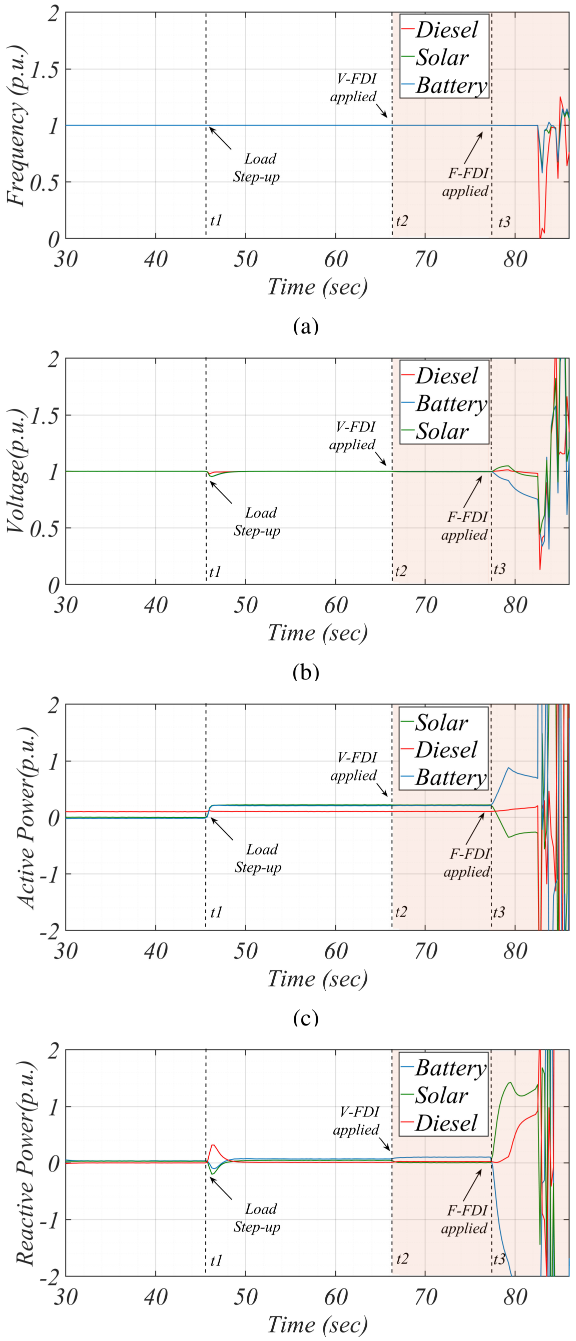
Agents	1	2	3	4
config 1	Electronic Load*	Battery	Solar	Diesel
config 2	Battery	Battery	Battery	Battery

*: Signals from the electornic load is not shared between agents in the secondary controller

Fig. 4. Electrical diagram for the distributed control of an islanded AC microgrid considering two different configurations.

A. Case 1: Conventional consensus under minor FDI attack

In this case, the impacts of minor false data injection attacks on the conventional consensus secondary control scheme is studied. The voltage, frequency, active power and reactive power sharing performance of the conventional consensus



(a)

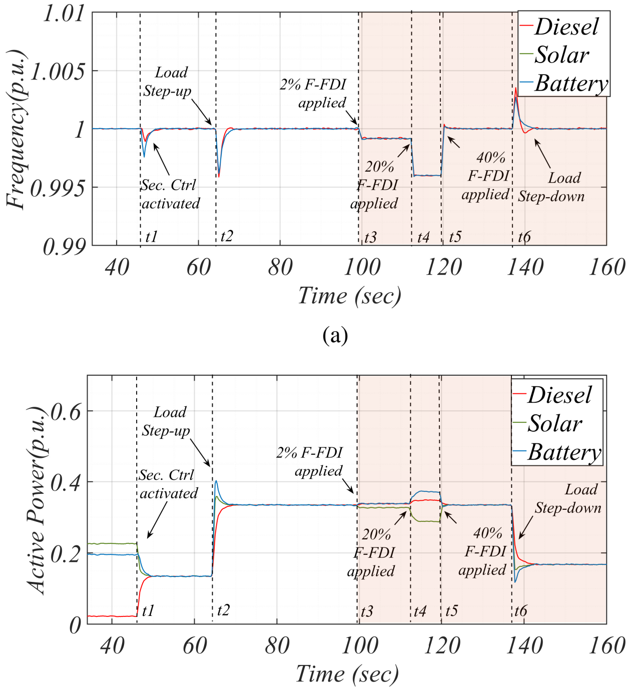
(b)

(c)

(d)

Fig. 5. The conventional consensus secondary control under minor (2% offset) voltage and frequency FDI attacks.

scheme under this scenario are depicted in Fig. 5, where secondary communication delay is set to 40 ms. In this case, the secondary controller is initially enabled, and then a load step from 200 kW to 1000 kW is applied at $t = t_1$. It is observed that the secondary algorithm ensures proper retrieving of frequency term, where for diesel node it takes about 0.5 seconds while for low inertia nodes it is resumed within 1.8 seconds. This performance is mainly attributed to the gain tuning applied to low inertia nodes to avoid excessive undershoots on the frequency signal. At $t = t_2$, a 2% voltage FDI (V-FDI) is applied, where the impact on reactive power sharing is reflected by about 0.04 $p.u$ power shift between the battery and solar nodes. Recalling the expected impacts of voltage FDI attack on the conventional consensus as stated in (18) and (19), the equilibrium point is reached and the voltage state variable does not diverge upon maintaining this bounded level of voltage cyber intrusion. However, when the same 2% drift is applied on the frequency term, the introduced offset drives the system state variables toward the unstable condition, which confirms the presented discussion on frequency FDIs (F-FDI) and the expected impacts as represented by (13) and (14). It is observed that the proper power control over all three nodes are lost as the power state variables are driven toward the overload condition and result in bus voltage deviations and loss of frequency synchronization. This can basically result in tripping the protective circuit breakers.



(a)

(b)

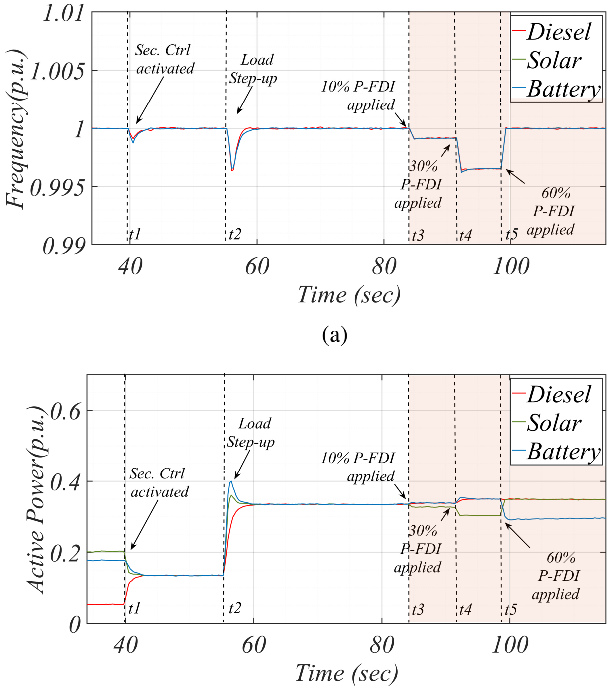
Fig. 6. The proposed secondary control scheme under load steps and different levels of frequency FDI attacks (2%, 20%, 40% offset).

B. Case 2: Proposed scheme under different levels of frequency-FDI attacks

In this scenario, the impacts of frequency FDI attacks on the proposed sliding mode consensus-based scheme is investigated. The frequency and active power terms for all three DERs with inclusion of 40 ms delay on secondary communication links are depicted in Fig. 6. While the microgrid DERs are initially regulated using only the local controllers, the secondary control scheme is activated at $t = t_1$. It is observed that the normalized active power terms converge smoothly to the consensus value of 0.135 $p.u$ within 4 seconds, which resulted in quick frequency retrieving after undershooting by less than 0.35%. The power sharing performance under load step-up at $t = t_2$ shows that the sluggish response on the diesel unit is leading to an overshoot on the other two DERs power terms, as they have to compensate for the introduced power shortage during the transient condition. . At $t = t_3$, the FDI attack level of 2% (same as case 1) is applied on the frequency term, which has only resulted in 0.1% frequency drift without causing the microgrid instability. Recalling the case 1, introducing 2 percent frequency FDI attack resulted in the total microgrid instability within less than 5 seconds, but the proposed scheme shows a robust performance even after much longer duration. This is mainly attributed to the enhanced SMC robustness to external disturbances, uncertainties and improved power sharing dynamics. At $t = t_4$, the FDI attack is increased to 20% drift in the frequency signal, and again it is observed that the system remains resilient to the applied disturbance and only 0.4% frequency drift is produced. By increasing the FDI intrusion level to the 40% at $t = t_5$, the HCLQ detects the non-cooperative communication node and isolates it from the secondary control configuration. In this case, the frequency drift is recovered within less than 0.1 seconds due to the quick isolation of the adjacency term by the HCLQ. This also ensures that the applied disturbances to the shared secondary signals never violates the bounded levels and the SMC stable operation is guaranteed. A load step down is applied at $t = t_6$, which shows that the proper power sharing performance is still maintained.

C. Case 3: Proposed scheme under different levels of active power-FDI attacks

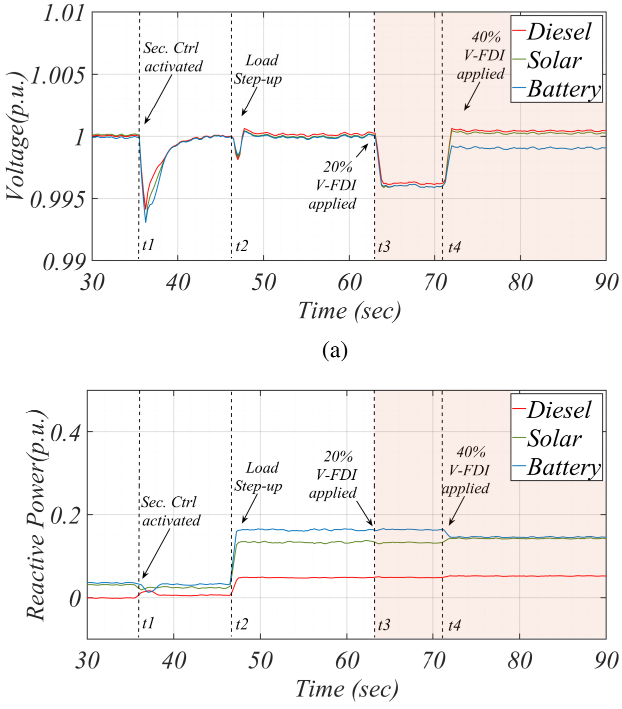
The frequency and active power terms for all three DERs are depicted in Fig. 7, where a communication delay of $40\ ms$ is applied. In this case, the same sequence of actions as presented in case 2 is applied at t_1 and t_2, where the sliding mode consensus scheme is activated at t_1 and then the same load step change is applied on t_2. A 10% FDI drift on the active power term is applied at t_3, which resulted in 0.1% frequency deviation. This is due to the phenomenon that introduced deviations on the distributed power terms produce a negative offset value on the secondary frequency actuation terms, which leads to the global frequency deviation. Having differently distorted secondary frequency terms along with new global frequency value results in different offset values on the DERs' power terms in the grid forming operation mode. At t_4, the active power FDI (P-FDI) level is increased by 30%, and about 0.35% frequency deviation is observed. By increasing the FDI level to 60% at t_5, the corrupted signal term from the non-cooperative node is detected by HCLQ module and then the corresponding node is automatically isolated. Having the non-cooperative node isolated, the frequency is retrieved within less than $150\ ms$. The active power graph shows that the deviation is mainly imposed on the solar power term as it encounters receiving corrupted shared signals from its neighbor node (Battery node). After detection of the FDI attack and isolating the battery distributed power term, the battery starts operating in the decentralized mode based on its local droop term, while the remaining level of power is properly shared between the two nodes of solar and diesel.



(a)

(b)

Fig. 7. The proposed secondary control scheme under load steps and different levels of active power FDI attacks (10%, 30%, 60% offset).



(a)

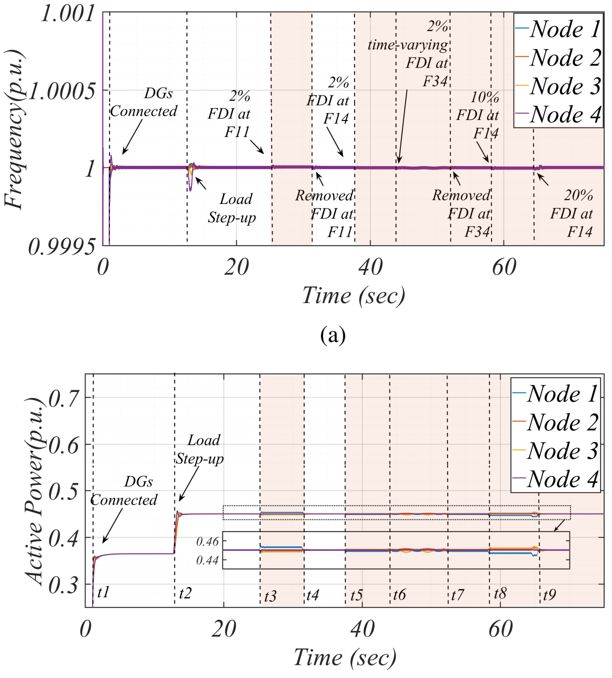
(b)

Fig. 8. The proposed secondary control scheme under load steps and different levels of voltage FDI attacks (20%, 40% offset).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3125985, IEEE Transactions on Power Electronics

D. Case 4: Proposed scheme under different levels of voltage-FDI attacks

The effectiveness of the proposed scheme is also studied under the presence of voltage FDI attacks and a communication delay of $40ms$. The voltage sharing performance for each DER along with the reactive power sharing performance are depicted in Fig. 8. For regulation of the $V-Q$ sharing performance, a trade-off adjustment with a priority given to the voltage regulation is applied. At t_1, the proposed secondary controller is enabled and it is observed that the bus voltages are converged within less than 5 seconds, while the observed voltage undershoot is less than 0.9%. A quicker convergence is also attainable at the expense of larger voltage transient undershoot peaks by increasing the sliding mode control gains. At t_2, the reactive load steps up to $600\ kVar$. It is observed that the voltage deviation is retrieved within about 2 seconds, where only a 0.3% voltage deviation is observed on the transient period. Having adjustable adaptive regulatory parameters for distributed voltage and reactive power terms within the sliding surface mathematical representation provides flexibility for the convergence rate tuning. A 20% voltage FDI attack is applied at t_3, which only resulted in 0.4% voltage deviation at PCCs. By increasing the FDI intrusion level on voltage to 40%, the HCLQ detected and isolated the non-cooperative node. As a result, the voltage deviations for solar and diesel node are restored while the battery is operating in decentralized mode.



(a)

(b)

Fig. 9. The proposed secondary control scheme under load steps and 2% of node/link frequency FDI, concurrent FDIs and time varying FDIs.

E. Case 5: Proposed scheme under node/link frequency FDIs, concurrent FDIs and time-varying FDIs

After investigating the impacts of FDI attacks on the neighbouring communication link in the first configuration throughout the first four test cases, the performance of the proposed cyber-resilient scheme is further examined under node FDIs, concurrent link FDIs, and time-varying FDIs on the second configuration, as shown in Fig.9. Due to the higher vulnerability of the consensus scheme to the frequency FDIs, as previously discussed, only F-FDIs are investigated for the following three test scenarios applied on the second configuration. In this case, the secondary communication delay is set at 60 ms. At $t1$, all four Distributed Generators (DGs) are connected with initially enabled secondary regulation scheme, where proper convergence to the consensus power value is attained within less than 1 s, as shown in Fig.9b. It is also observed that with uniform DGs, the dynamic power sharing under load step-up, which is applied at $t2$ on node 4 by increasing it with 4 kW, provides an optimal performance with an overshoot level of only 2% in power terms and an undershoot of 0.01% on frequency terms. During $t3-t4$, a node F-FDI attack from primary to secondary shared frequency term on node 1 ($F11$) of 2% is applied and removed, where the proposed scheme shows a highly resilient performance with only 0.1% deviation on the power terms. During $t5-t9$, first a 2% F-FDI is introduced on the received neighbouring signal at node 1 from node 4 (F14), then maintaining this intrusion, a time-varying F-FDI of $2.sin(t)\%$ is applied at the received signal at node 3 from node 4 (F34), and removed at $t7$, and then, the intrusion term F14 is increased to 10% at $t8$. It can be seen that deviations at frequency terms and power terms are maintained to the values lower than 0.01% for frequency and 0.05% for power terms, throughout this period. By increasing the F-FDI on signal F14 to 20%, the HCLQ unit triggers the isolation of the no-cooperative node, which results in proper removal of deviations introduced on the shared signals as well.

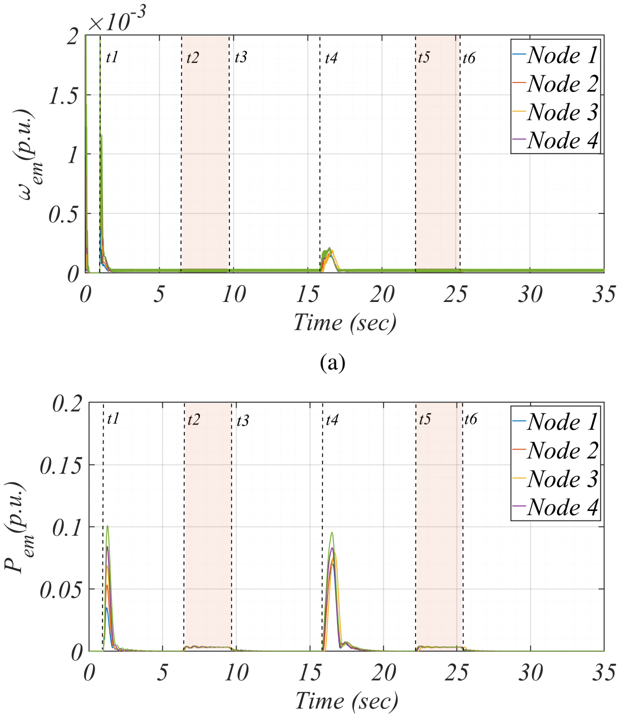
F. Case 6: Impacts of the communication delays on the proposed scheme

To study the possible impacts of communication delays on the performance of the proposed scheme, its operation under the common range of communication delays in the secondary cyber layer is investigated in this test scenario. In this case, the DGs with the initially enabled secondary regulation are connected at $t1$, then, a 2% frequency FDI is applied to the signal received at node 2 from node 1 (F21). After that, a load step-up by 4 kW is introduced at node 2 at $t4$, which is followed by insertion and removal of a 2% F-FDI on the received signal at node 1 coming from node 4 (F14), at $t5$ and $t6$, respectively. To quantify the overall effects of the communication delays, the following two metrics are proposed for evaluating the frequency and power sharing:

$$\begin{cases} \omega_{em} = \sum_{i=1}^{n} \sum_{j=1}^{k} a_{ij} \mid \omega_i - \omega_j \mid \\ P_{em} = \sum_{i=1}^{n} \sum_{j=1}^{k} a_{ij} \mid P_{Ni} - P_{Nj} \mid \end{cases} \tag{36}$$

where ω_{em} and P_{em} are the error metric terms for distributed frequency and normalized active power signals, and n and k represent the total number of nodes and incoming communication links to the node i, respectively.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3125985, IEEE Transactions on Power Electronics



(a)

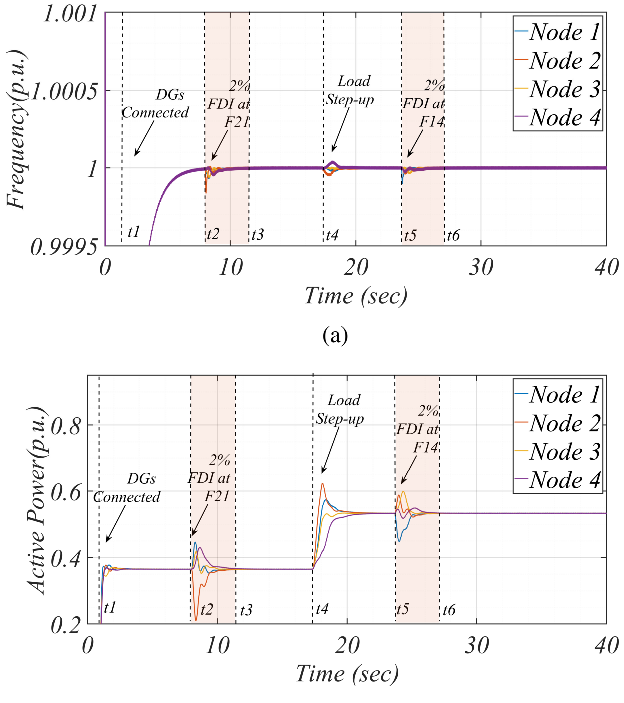
(b)

Fig. 10. The impacts of communication delays on the performance of the proposed scheme under load steps and link frequency FDIs of 2%.

Using the above metrics, the system secondary layer sharing performance for frequency and active power terms under the occurrence of disturbances such as power-up, load steps, and cyberattacks can be quantitatively examined. As shown in Fig. 10, the most significant impact of communication delays is reflected on the power sharing under connection of DGs, where by increasing the communication delay by four times from 30 ms to 120 ms, the P_{em} also shows about 0.06 difference on the peak values. However, the power sharing is much less impacted on the load step, where only about 0.02 difference is observed in P_{em} and the response to the application of F-FDIs remained almost identical even with higher delays. These observations are attributed to the robustness of the proposed SMC scheme against system disturbances in presence of signal latencies, where in the case of powerup, the existing latency on compensation of large size errors has resulted in a minor deviation in P_{em}. It is also noteworthy that the ω_{em} has remained almost unchanged for different levels of communication delays.

G. Case 7: Comparative study with the proposed cyber-resilient method in [25]

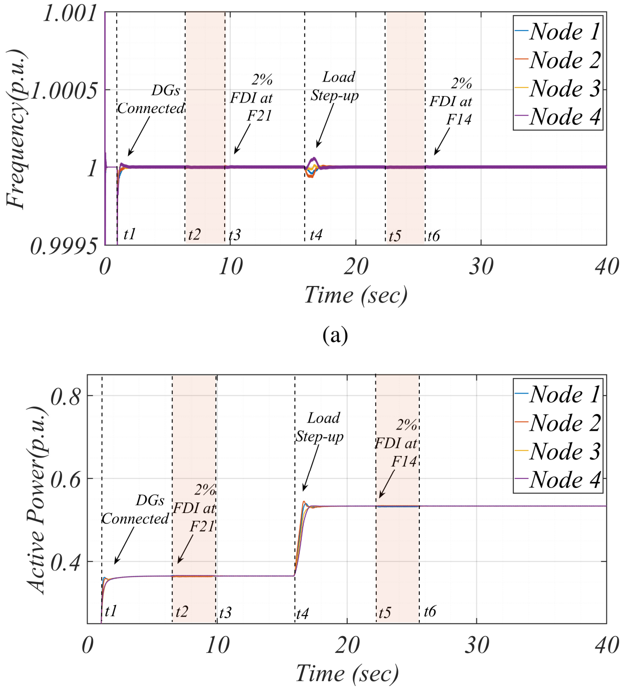
In order to evaluate the performance of the proposed algorithm against one of the recently reported cyber-resilient schemes, the same test scenario as discussed for Case 6 is applied to both proposed scheme and the algorithm presented in [25]. In this case, the communication delay for both systems are set at 50 ms. From Fig. 11 and Fig. 12, it can



(a)

(b)

Fig. 11. The performance of the cyber-resilient scheme reported in [25] under minor link frequency FDIs and load steps.



(a)

(b)

Fig. 12. The performance of the proposed scheme under minor link frequency FDIs and load steps.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3125985, IEEE Transactions on Power Electronics

be seen that the secondary frequency regulation of the other scheme results in a sluggish convergence upon connection of all DGs at $t1$. While the proposed scheme provides a highly resilient performance for both frequency and power sharing under minor link F-FDIs, as applied at the moments of $t2$ and $t5$, the frequency regulation of other scheme experiences undershoots by up to 0.02% and their corresponding power sharing encounters a severe transient condition before proper detection and triggering the isolation of the non-cooperative node. Since their method is based on observing the power error terms for reconstructing the affected signals, the selection of the proper thresholds without false detection under load step events is quite challenging. Using our proposed method, the robustness of SMC algorithm against FDI attacks highly facilitates integration of more effective CLQ unit which is detects the F-FDIs from the observed error signals at the distributed frequency terms.

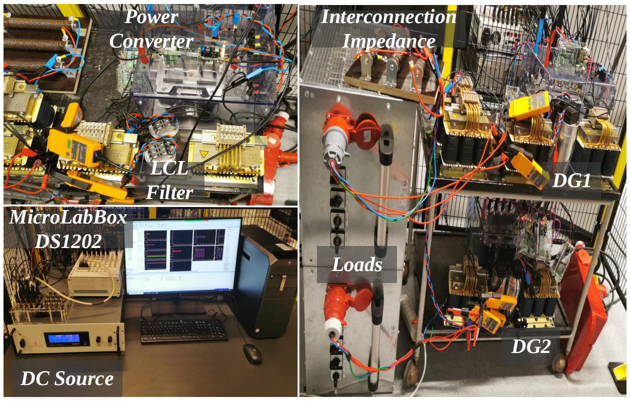
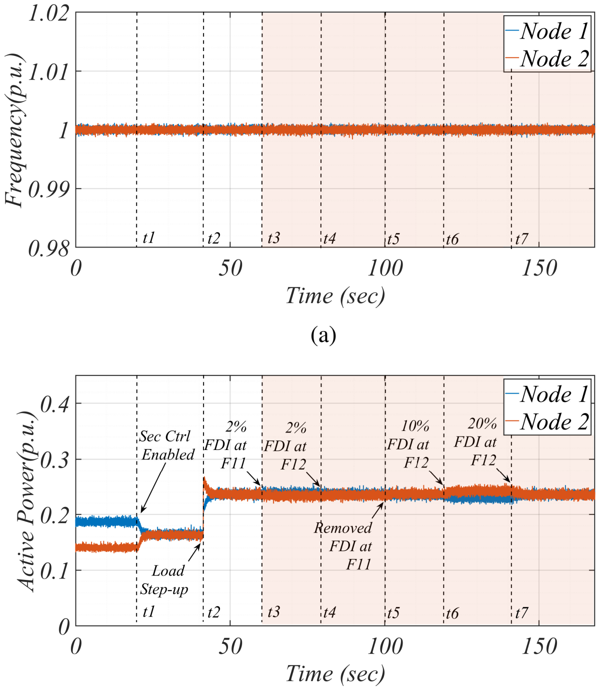


Fig. 13. Experimental setup



(a)

(b)

Fig. 14. The performance of the proposed cyber-resilient scheme under load step and node/link frequency FDIs.

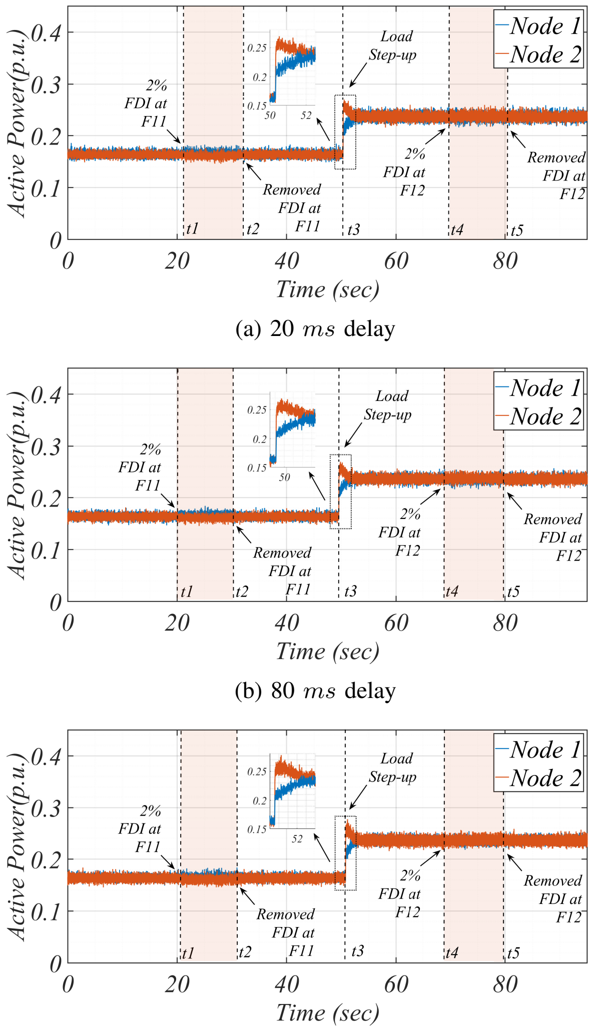
V. Experimental results

The performance of the proposed cyber-resilient control algorithm is also evaluated using the experimental testbed shown in Fig. 13 with the system settings listed in Appendix B. The setup is configured with interconnecting two Semikron power converters with LCL output filters, where their input DC bus voltages are supplied by means of Delta adjustable DC source. The selectable resistive loads are also connected to the output of each DG unit. For implementation of both primary and secondary layer controllers, dSPACE MicroLabBox DS1202 is utilized, which its sampling rate is adjusted at 100 μs.

The proposed algorithm is firstly examined in terms of the frequency regulation and active power sharing performance in presence of both node and link frequency FDIs under 30 ms communication delay, as depicted in Fig. 14. It can be seen that desirable convergences within 1.5 s on the activation of the secondary control algorithm and the subsequent load step-up, as applied at the place of node 2 from 3 kW to 7 kW, are attained at the instances of $t1$ and $t2$, respectively. By applying a sequence of node FDI, concurrent node/link FDI, and link FDI on the incoming frequency terms at the place of node 1, it is observed that the algorithm provides a highly resilient operation with only slight deviations on the distributed power terms. By increasing the incoming link frequency FDI from 2% to 10% at t_6, the power term deviation is further increased by about 0.015 p.u. A level-up on the FDI intrusion term to the 40% has resulted in automatic isolation of the compromised link by HCLQ unit after less than 1 s at t_7.

To experiment the impacts of the communication delays on the proposed scheme, the power sharing performance under a similar test scenario that was applied to the simulation test cases 6 and 7 is considered for communication delays of 20 ms, 80 ms and 160 ms, as shown in Fig. 15. It is observed that for different communication delay values, the resilient performance of the proposed algorithm under both node and link frequency FDIs, which are capable of destabilizing the system regulated with the conventional secondary scheme, are well maintained and only minor power term deviations specially for the node attacks are observed. In terms of power regulation on the load step-up at the place of node 2 from 3 kW to 7 kW, it can be seen that the convergence is slightly delayed by about 0.3 s for 80 ms and 160 ms cases, and this is accompanied with slightly higher peak values in the case of 160 ms. This test scenario also verifies the robustness of the proposed algorithm against the communication delays as it was also previously proven through the HIL simulation results.

The resilient performance of the proposed scheme under both node and link voltage FDIs are also evaluated as shown in Fig. 16. While the secondary control, with prioritized voltage regulation, is initially enabled, subsequent 5% voltage FDIs are applied on node 1 at t_1 and the incoming link to node 1

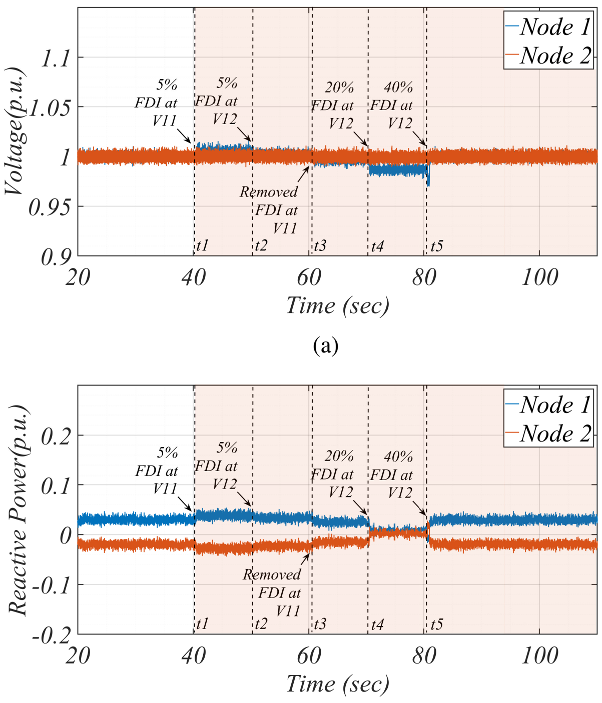


(a) 20 ms delay

(b) 80 ms delay

(c) 160 ms delay

Fig. 15. The power sharing performance of the proposed cyber-resilient scheme under distributed communication delays of 20 ms, 80 ms, and 160 ms and minor frequency FDIs.



(a)

(b)

Fig. 16. The performance of the proposed cyber-resilient scheme under node/link voltage FDIs.

at t_2. Whereas the node attack has resulted in slight voltage deviations by about 0.5 %, this offset is highly alleviated when the similar attack is concurrently applied on the link signal. Such an observation further highlights the vulnerability of the cyber-resilient algorithms solely operated based on the differential signal observations, which can fail on proper detection of minor cyberattacks, but our proposed algorithm performs quite resilient against such intrusions. After removing the node FDI at t_3, and increasing the link FDI by 15% at t_4, the voltage deviations are further intensified to about 1.2 %. From the reactive power signal, it is also observed that such a intrusion has resulted in overlapping Q values, which can challenge the algorithms formed on the sole observation of the reactive power error terms. By increasing the FDI level to the 40% at t_5, the non-cooperative link is detected by the CLQ unit and automatically isolated, which results in resuming both voltage and reactive power sharing.

A comparison between the proposed algorithm and other cyber-resilient methods for islanded AC microgrids is summarized in Table I. From the obtained results on HIL simulation and experimental tests, it is shown that this scheme is capable of providing resilient performance under different types of FDIs, without requirement for extra distributed terms, which can be themselves the target of FDIs, as well as lower time delay vulnerability. Also, the proposed approach provides a more reliable detection and isolation compared with other schemes as it directly operates on the compromised signal term errors rather than their indirect effects.

VI. Conclusions

This paper proposes a hybrid cyber-resilient consensus-based distributed control scheme that combines consensus sliding mode control with a localized communication link quality observer. Cyber-resilient offset compensation terms are also employed on the sliding surfaces to ensure superior steady state performance under normal operating conditions and facilitate the control parameters adjustment for different operating conditions. Using a hysteresis based communication link quality observer, it is ensured that external perturbations on the distributed signals remain bounded to the certain levels. Also, the proposed CLQ unit operates only based on the direct observation of existing distributed error terms. Using this combinative localized approach, the reliability of the proposed distributed control scheme will not be dependent on security of other auxiliary distributed terms, as typically used by other distributed observer based cyber-resilient schemes.

TABLE I. Comparative evaluation of the cyber-resilient methods for islanded AC microgrids

	[20]	**[21]**	**[23]**	**[25]**	**This paper**
Method	Adaptive distributed observer	Adaptive distributed observer	Distributed Observer	Localized Observer	SMC + Localized Observer
FDI protection type	F-FDI, V-FDI	F-FDI, V-FDI	F-FDI, V-FDI	F-FDI	F-FDI, V-FDI, PQ-FDI
Extra distributed term requirement	Yes	Yes	Yes	No	No
Cyberattack susceptibility	High	High	High	Low	Low
False detection vulnerability	Low	Low	Medium	High	Low
Time delay vulnerability	High	High	medium	medium	Low
Verification tool	PSCAD/EMTDC	Matlab, Opal- RT HIL OP5600	Matlab	Matlab	Typhoon HIL 402, Experimental testbed

It is shown for the conventional consensus schemes that even a minor 2% F-FDI attack is capable of forcing the converters toward the overloading condition and cause tripping the protective circuits and leading to the unstable operating condition. The performance of the proposed scheme against different types of FDIs are verified using HIL simulation results and experimental testbeds. From the presented test scenarios, it is evident that the scheme performs highly resilient against node/link FDIs, concurrent FDIs and time-varying FDIs without compromising on the dynamic load sharing performance. In addition, it is also shown that the algorithm performance under the common range of communication delays is well maintained.

Acknowledgment

This work was partially supported by Louisiana Board of Regents under grant number: LEQSF(2021-24)-RD-B-06.

Appendix A

To prove the stability of the proposed sliding mode control algorithm, the following Lyapunov Candidate Function (LCF) is considered:

$$V = \sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}a_{ij}(x_i - x_j)^2 \tag{37}$$

where x represents any of the frequency and voltage signals, as denoted in this paper with ω and V. The time derivative of the LCF function in (37) can be derived as follows:

$$\dot{V} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}(x_i - x_j)(\dot{x_i} - \dot{x_j}) \tag{38}$$

By inserting the chosen control function for the sliding surfaces, $\dot{x_i} = K_{smc,i}sgn(S_i)$, into (38):

$$\dot{V} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}(x_i - x_j)(K_{smc,i}sgn(S_i) - K_{smc,j}sgn(S_j)) \tag{39}$$

By selection of the equal K_{smc} gains between the neighbouring agents i, j, and considering $a_{ij} \geq 0$, the stability of the proposed algorithm can be guaranteed if the product of error terms in (39) for each of the n nodes ensure a non-positive value and satisfies $\dot{V} \leq 0$. This can be ensured if the following conditions for the error terms on $\dot{V}$ are always met:

$$\begin{cases} sgn(S_i) \leq sgn(S_j), & \text{if } x_i \geq x_j \\ sgn(S_i) \geq sgn(S_j), & \text{if } x_i \leq x_j \end{cases} \tag{40}$$

These conditions can be surely satisfied if only $sgn(S_i)$ meet the below conditions:

$$\begin{cases} sgn(S_i) = -1, & \text{if } x_i \geq x_j \\ sgn(S_i) = 1, & \text{if } x_i \leq x_j \end{cases} \tag{41}$$

Recalling the sliding surface function terms stated in (26)-(31), and using the proportional relationship between the power error term Δy_{ij} and the associated local variable error term Δx_{ij}, as generally represented by $\Delta y_{ij} = m_i \Delta x_{ij}$, with $m_i \gg 1$, the general representation of the sliding surface equation can be rearranged as below:

$$S_i = B + D(x_j - x_i) \tag{42}$$

where B and D terms are defined as:

$$\begin{cases} B = (x_{ref} - x_i) + c_1(\frac{d}{dt}\Delta x_i + \frac{d}{dt}\Delta x_{ij} + \frac{d}{dt}\Delta y_{ij}) \\ D = (1 + K_{xy}m_i + K_{ij}e^{-K_{exp}|\Delta x_{ij}|}) \end{cases} \tag{43}$$

To ensure that the selected surface S_i satisfies the condition in (41) and thus the algorithm stability, the parameters c_1, K_{xy}, K_{ij} and K_{exp} need to be selected in a way that:

$$B \leq D|x_j - x_i| \tag{44}$$

Noting the low pass filter role of parameter c_i, as explained in (32) and (33), and its desired range of values ($c_i < 0.0001$), as well as the significant m_x values with respect to the droop term relationship, the task of parameter regulation for ensuring stability can be simply handled by only regulating parameters K_{xy}, K_{ij} and K_{exp} to meet condition (44).

Appendix B

Configuration 1:

Electrical Parameters: Rated power: 2.5 MVA (Diesel), 2 MVA (Solar), 1.6 MVA (Battery), 2.2MVA (Load), V_n = 480 v, F_n = 60 Hz, f_{sw} = 10 kHz, Z_{12}, Z_{23}, Z_{34}: R_{12} = 1.2 Ω , R_{23} = 0.8 Ω, R_{34} = 1.6 Ω , L_{12} = 36 mH, L_{23} = 24 mH, L_{34} = 48 mH.

Local Control Parameters: Diesel: K_p = 0.025, K_i= 0.03 for Excitation control,K_p = 15 for Governor control, Solar: K_p = 0.3, K_i = 2 for voltage control, K_p = 0.1, K_i = 10 for current control, Battery: K_p = 0.8, K_i = 2 for voltage control, K_p = 0.5, K_i = 50 for current control.

Secondary Control Parameters: Diesel: C_w, C_v = 0.01, K_{pij}, K_{Qij} = 0.5, K_{wexp} = 100, K_{vexpt} = 80, K_{vsmc},K_{wsmc} = 0.01, ϵ_k = 0.08, $HystLim_{w,v}$ = [0.3,0.2], $HystLim_{P,Q}$ = [0.15,0.1], K_{decay} = 5, T_sc = 0.5. Solar, Battery: C_w, C_v = 0.0001, K_{pij}, K_{Qij} = 1, K_{wexp} = 100, K_{vexpt} = 80, K_{vsmc}, K_{wsmc} = 0.01, ϵ_k = 0.08, $HystLim_{w,v}$ = [0.3,0.2], $HystLim_{P,Q}$ = [0.15,0.1], K_{decay} = 5, T_{sc} = 0.5.

Configuration 2:

Electrical Parameters: Rated power: 6 kVA, V_n = 480 v, F_n = 60 Hz, f_{sw} = 10 kHz, Z_{12}, Z_{23}, Z_{34}: R_{12} = 0.387 Ω , R_{23} = 0.696 Ω, R_{34} = 1.16 Ω , L_{12} = 3.1 mH, L_{23} = 2.3 mH, L_{34} = 1.9 mH.

Local Control Parameters: K_p = 2, K_i = 50 for voltage control, K_p = 0.5, K_i = 20 for current control.

Secondary Control Parameters: C_w, C_v = 0.0001, K_{pij}, K_{Qij} = 0.5, K_{wexp} = 100, K_{vexpt} = 80, K_{vsmc},K_{wsmc} = 0.01, ϵ_k = 0.08, $HystLim_{w,v}$ = [0.3,0.2], $HystLim_{P,Q}$ = [0.15,0.1], K_{decay} = 4, T_{sc} = 1.

Experimental setup:

Electrical Parameters: $V_{in-dc} = 500V$, V_n = 240 V, Rated current: 30 A, , F_n = 60 Hz, f_{sw} = 10 kHz, Z_{12}: R_{12} = 0.5 Ω, L_{12} = 4.4 mH, LCL filter: L_f, L_g = 2.2 mH, $C_f = 5\ \mu F$.

Local Control Parameters: K_p = 5, K_i = 15 for voltage control, K_p = 0.01, K_i = 30 for current control.

Secondary Control Parameters: C_w, C_v = 0.00001, $K_{\omega P}$, K_{VQ} = 1, K_{pij}, K_{Qij} = 0.5, K_{wexp} = 100, K_{vexpt} = 80, K_{vsmc},K_{wsmc} = 0.01, ϵ_k = 0.1, $HystLim_{w,v}$ = [0.35,0.15], $HystLim_{P,Q}$ = [0.15,0.1], K_{decay} = 4, T_{sc} = 1.

REFERENCES

[1] A. C. Z. de Souza and M. Castilla, *Microgrids design and implementation*. Springer, 2019.

[2] C. Dou, Z. Zhang, D. Yue, and M. Song, "Improved droop control based on virtual impedance and virtual power source in low-voltage microgrid," *IET Generation, Transmission & Distribution*, vol. 11, no. 4, pp. 1046–1054, 2017.

[3] A. J. Abianeh and F. Ferdowsi, "Real time analysis of a multi-agent based distributed control strategy for islanded ac microgrids," in *2020 Clemson University Power Systems Conference (PSC)*. IEEE, 2020, pp. 1–6.

[4] J. Hu and P. Bhowmick, "A consensus-based robust secondary voltage and frequency control scheme for islanded microgrids," *International Journal of Electrical Power & Energy Systems*, vol. 116, p. 105575, 2020.

[5] D. Wu, F. Tang, J. M. Guerrero, J. C. Vasquez, G. Chen, and L. Sun, "Autonomous active and reactive power distribution strategy in islanded microgrids," in *2014 IEEE Applied Power Electronics Conference and Exposition-APEC 2014*. IEEE, 2014, pp. 2126–2131.

[6] J. W. Simpson-Porco, Q. Shafiee, F. Dörfler, J. C. Vasquez, J. M. Guerrero, and F. Bullo, "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 11, pp. 7025–7038, 2015.

[7] A. Bidram, A. Davoudi, and F. L. Lewis, "A multiobjective distributed control framework for islanded ac microgrids," *IEEE Transactions on industrial informatics*, vol. 10, no. 3, pp. 1785–1798, 2014.

[8] A. Pilloni, A. Pisano, and E. Usai, "Robust finite-time frequency and voltage restoration of inverter-based microgrids via sliding-mode cooperative control," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 1, pp. 907–917, 2017.

[9] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab, and A. Abusorrah, "Distributed control and communication strategies in networked microgrids," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2586–2633, 2020.

[10] P. Ojaghi and M. Rahmani, "Lmi-based robust predictive load frequency control for power systems with communication delays," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 4091–4100, 2017.

[11] G. Lou, W. Gu, W. Sheng, X. Song, and F. Gao, "Distributed model predictive secondary voltage control of islanded microgrids with feedback linearization," *IEEE Access*, vol. 6, pp. 50 169–50 178, 2018.

[12] M. A. Shahab, B. Mozafari, S. Soleymani, N. M. Dehkordi, H. M. Shourkaei, and J. M. Guerrero, "Distributed consensus-based fault tolerant control of islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 37–47, 2019.

[13] P. Ge, Y. Zhu, T. C. Green, and F. Teng, "Resilient secondary voltage control of islanded microgrids: An eskbf-based distributed fast terminal sliding mode control approach," *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 1059–1070, 2021.

[14] Z. Zhang, C. Dou, D. Yue, B. Zhang, S. Xu, T. Hayat, and A. Alsaedi, "An event-triggered secondary control strategy with network delay in islanded microgrids," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1851–1860, 2018.

[15] Z. Zhang, Y. Mishra, D. Yue, C. Dou, B. Zhang, and Y.-C. Tian, "Delay-tolerant predictive power compensation control for photovoltaic voltage regulation," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 4545–4554, 2020.

[16] S. Alghamdi, J. Schiffer, and E. Fridman, "Synthesizing sparse and delay-robust distributed secondary frequency controllers for microgrids," *IEEE Transactions on Control Systems Technology*, vol. 29, no. 2, pp. 691–703, 2020.

[17] S. S. Ullah, A. J. Abianeh, F. Ferdowsi, K. Basulaiman, and M. Barati, "Measurable challenges in smart grid cybersecurity enhancement: A brief review," in *2011 The Thirteenth Annual IEEE Green Technologies (GreenTech) Conference*. IEEE, 2021.

[18] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2019.

[19] M. S. Sadabadi, S. Sahoo, and F. Blaabjerg, "A fully resilient cyber-secure synchronization strategy for ac microgrids," *IEEE Transactions on Power Electronics*, 2021.

[20] M. Shi, X. Chen, M. Shahidehpour, Q. Zhou, and J. Wen, "Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded ac microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1953–1963, 2021.

[21] X. Li, Q. Xu, and F. Blaabjerg, "Adaptive resilient secondary control for islanded ac microgrids with sensor faults," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2020.

[22] A. Bidram, L. Damodaran, and R. Fierro, "Cybersecure distributed voltage control of ac microgrids," in *2019 IEEE/IAS 55th Industrial and Commercial Power Systems Technical Conference (I&CPS)*. IEEE, 2019, pp. 1–6.

[23] A. Bidram, B. Poudel, L. Damodaran, R. Fierro, and J. M. Guerrero, "Resilient and cybersecure distributed control of inverter-based islanded microgrids," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 3881–3894, 2019.

[24] S. Sahoo, T. Dragičević, Y. Yang, and F. Blaabjerg, "Adaptive resilient operation of cooperative grid-forming converters under cyber attacks," in *2020 IEEE CyberPELS (CyberPELS)*. IEEE, 2020, pp. 1–5.

[25] S. Sahoo, Y. Yang, and F. Blaabjerg, "Resilient synchronization strategy for ac microgrids under cyber attacks," *IEEE Transactions on Power Electronics*, vol. 36, no. 1, pp. 73–77, 2021.

[26] T. Dragicevic, S. Vazquez, and P. Wheeler, "Advanced control methods for power converters in dg systems and microgrids," *IEEE Transactions on Industrial Electronics*, 2020.

[27] A. Bidram, V. Nasirian, A. Davoudi, and F. L. Lewis, *Cooperative synchronization in distributed microgrid control*. Springer, 2017.

[28] A. J. Abianeh, "Chattering-free classical variable structure direct torque controlled ipm synchronous motor drive by using pi controller within boundary layer," in *2011 6th IEEE Conference on Industrial Electronics and Applications*. IEEE, 2011, pp. 651–656.

Ali Jafarian Abianeh (S'19) received his M. Eng. degree in Electrical Engineering from University of Malaya, Kuala Lumpur, Malaysia, in 2010. He is currently working toward his Ph.D. degree at Department of Electrical and Computer Engineering at University of Louisiana at Lafayette, USA. He developed some solid professional expertise through several years of working in the industry as a power electronics engineer with the main focus on electric motor drives, and grid-tied power converters. His current research interests include application of advanced control algorithms and machine learning techniques to AC/DC microgrids, power converters, motor drive control, distributed control, fault tolerant control algorithms and cybersecurity.

Mohammad Mehdi Mardani (S'20) received his M.Sc. and Ph.D. degrees from the Shiraz University of Technology, Shiraz, Fars, Iran in 2015 and 2019, respectively, both in Control Engineering. He spent his sabbatical at the Energy Technology Department of the Aalborg University, Aalborg, Denmark from Nov. 2017 to Nov. 2018. Since 2020, he has been a double degree research Ph.D. student in Electrical Power Engineering at the electrical engineering department of the Technical University of Denmark (DTU). His partner university is the Sino-Danish College (SDC), University of Chinese Academy of Science (UCAS). He is the author or co-author of 13 conference papers and 14 journal papers. His current research interests include advanced control, machine learning, microgrids, renewable energy, power electronics, and its application in power systems.

Farzad Ferdowsi (S'13–M'17-SM'20) is an Assistant Professor at University of Louisiana at Lafayette. He is with the Electrical and Computer Engineering Dept. Prior to joining UL Lafayette, Farzad worked as a research associate at the Center for Energy Studies at Louisiana State University. He received his Ph.D. from Florida State University in 2016. His research interests include power system stability and control and application of power electronic-based components in power systems.

Raju Gottumukkala is an Assistant Professor with the College of Engineering at UL Lafayette. He is with the Mechanical Engineering department. He also serves as the Director of Research for the Informatics Research Institute. Before joining UL Lafayette, he received his Ph.D. from Louisiana Tech University and worked as a research intern for both Xerox Research and Oak Ridge National Laboratory. His research interests are in the areas of cyber-physical systems, distributed computing, and machine learning. He has published over 40 peer-reviewed research papers, has 2 US patents, and has garnered over $7M in external research funding. He currently serves as the associate editor for the Springers Data-Enabled Discovery and Applications and serves on numerous program committees for various international conferences.

Tomislav Dragičević (S'09-M'13-SM'17) received the M.Sc. and the industrial Ph.D. degrees in Electrical Engineering from the Faculty of Electrical Engineering, University of Zagreb, Croatia, in 2009 and 2013, respectively. From 2013 until 2016 he has been a Postdoctoral researcher at Aalborg University, Denmark. From 2016 until 2020 he was an Associate Professor at Aalborg University, Denmark. From 2020 he is a Professor at the Technical University of Denmark. He made a guest professor stay at Nottingham University, UK during spring/summer of 2018. His research interest is application of advanced control, optimization and artificial intelligence inspired techniques to provide innovative and effective solutions to emerging challenges in design, control and cyber-security of power electronics intensive electrical distributions systems and microgrids. He has authored and co-authored more than 250 technical publications (more than 120 of them are published in international journals, mostly in IEEE), 8 book chapters and a book in the field. He serves as an Associate Editor in the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, in IEEE TRANSACTIONS ON POWER ELECTRONICS, in IEEE Emerging and Selected Topics in Power Electronics and in IEEE Industrial Electronics Magazine. Dr. Dragičević is a recipient of the Končar prize for the best industrial PhD thesis in Croatia, a Robert Mayer Energy Conservation award, and he is a winner of an Alexander von Humboldt fellowship for experienced researchers.