Exploiting the Inherent Cyber Resilience of Inverter-Dominated Microgrids against PLL Attack

Alkistis Kontou, *Student Member, IEEE,* Mazheruddin Syed, *Senior Member, IEEE,* Alexandros Paspatis, *Member, IEEE,* Zhiwang Feng, *Member, IEEE,* Charalambos Konstantinou, *Senior Member, IEEE,* Nikos Hatziargyriou, *Life Fellow, IEEE*

***Abstract*—This letter assesses the impact of phase locked-loop (PLL) cyberattacks on inverter-dominated microgrids considering the current limitation of the grid forming (GFM) and grid following (GFL) inverters. By reducing the PI gains of the PLL, an adversary can induce significant voltage sags by exploiting the dynamic coupling between the GFL's synchronization loop and the GFM's droop controller. The study demonstrates that preemptive tuning of lower droop gains in GFM inverters can mitigate the effects of such attacks. Leveraging this inherent cyber-resilience of inverter-dominated microgrids, an active decentralized droop adjustment mechanism is proposed. Power hardware-in-the-loop experiments validate the time-domain analysis and the effectiveness of the proposed mitigation strategy.**

***Index Terms*—Controller interaction, current limitation, cyberattack, inverter-dominated microgrid, phase-locked loop.**

I. Introduction

THE synchronization of grid-following (GFL) inverters is primarily governed by the dynamics of the phase-locked loop (PLL), recognized as a critical and potentially vulnerable component. Adversaries can exploit this vulnerability through cyberattacks targeting the PLL, potentially disrupting system behavior or inducing instability [1]. Most of the research works consider attacks that manipulate the input signal of PLL. For example, a false voltage pulse signal is injected and superimposed on the grid voltage to distort the zero crossing points, leading to incorrect detection of the phase angle and frequency by the inverter-based resource (IBR) [2]. In [3], an excitation component utilizing the natural frequency of the PLL is introduced into the measurement signals of a doubly-fed induction generator, creating undesired oscillations with a greater impact at lower PLL damping. Authors in [4] quantify the impact of corrupted measurements and control reference values on the small-signal stability of converter-based power systems using the structured ϵ-pseudospectrum theory. In [5], a sequential multi-timescale current limiting strategy is proposed to counter cyberattacks on the grid voltage signal that induce artificial voltage drops or non-zero phase differences between the PLL and the power grid.

A few recent works investigate the impact of maliciously altering the gains of the PLL's PI controller. In [1], an adversary exploits the PLL's PI tuning to alter the active and reactive power exchange during off-nominal frequency operation, and the attack is detected based on the created artificial voltage error. Similarly, a delayed dual second-order generalized integrator PLL is proposed in [6] that prevents steady-state active and reactive power offsets under off-nominal frequency operation caused by adversarial manipulation of PI gains. In [7], the authors suggest a detection strategy utilizing state-of-the-art model-based detectors and benchmark their performance against cyberattacks on sensor measurements and controller gains of a wind turbine converter system.

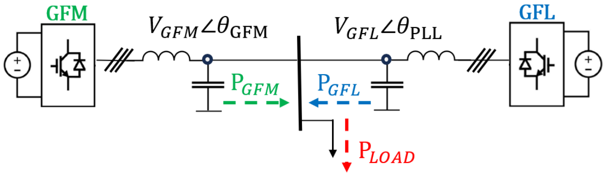

GFM
$V_{GFM}\angle\theta_{\mathrm{GFM}}$
$V_{GFL}\angle\theta_{\mathrm{PLL}}$
GFL
P_{GFM}
P_{GFL}
P_{LOAD}

Fig. 1: Islanded microgrid topology.

Recent research highlighted the interaction between the synchronization loop of a GFL inverter, implemented using a PLL, and the power controller of a grid forming (GFM) inverter [8]. The findings show that a lower PLL bandwidth can lead to small-signal instability when the GFM inverter operates with higher droop gains. This interaction warrants further investigation, particularly under the lens of a cyberattack.

National Institute of Standards and Technology defines cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources". This paper demonstrates that ensuring small-signal stability with low enough droop gain might not be sufficient to ensure a cyber resilient operation of the inverter-dominated microgrids. Specifically, this paper assesses the so far unexplored scenario in which an adversary may exploit the dynamic interaction between GFM and GFL using a stealthy PLL cyberattack to trigger inverter disconnections or even a microgrid blackout. The attack is designed to reduce the gains of PLL's PI controller while ensuring that the system remains within the small-signal stability region. Unlike previous works, this paper considers the non-linear power constraints of the inverters implemented through current limitation, and reveals that carefully designed stealthy attacks can result in substantial voltage sags when load changes occur, even as the microgrid retains its ability to return to a stable operating point. Thus, an adversary might utilize this attack to cause the disconnection of IBRs by violating their fault ride through (FRT) capabilities. A sensitivity analysis of the attack vector design contributing to the imminent voltage sag is conducted, and the impact of different current limitation strategies under the PLL attack is evaluated. It is then demonstrated that operating the GFM inverter with a lower droop gain can serve as an effective passive mitigation strategy. Furthermore, an adaptive mitigation approach is proposed, leveraging the inherent resilience of inverter-based microgrids to PLL cyberattacks.

II. Cyberattack Framework

This section presents a reduced-order model of an islanded microgrid, as shown in Fig. 1, to design and analyze a stealthy

Corresponding authors: Alkistis Kontou; Zhiwang Feng

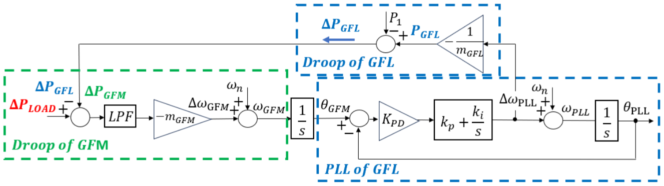


Fig. 2: Equivalent reduced block diagram of the microgrid.

PLL cyberattack and introduces a mathematical formulation to support the problem statement.

A. Droop Controller & Synchronization Loop Interaction

The GFM inverter employs frequency droop control as

$$\Delta\omega_{\text{GFM}} = -m_{\text{GFM}} \frac{\omega_c}{s+\omega_c} \Delta P_{\text{GFM}}, \quad \Delta\omega_{\text{GFM}} = s\Delta\theta_{\text{GFM}} \tag{1}$$

where $\Delta\omega_{\text{GFM}}$ is the difference between the measured frequency (ω_{GFM}) and the frequency setpoint (ω_n), m_{GFM} is the frequency droop gain and ΔP_{GFM} is the difference between the measured and the reference active power of the GFM inverter. The active power is filtered using a low-pass filter with cut-off frequency ω_c, which additionally introduces virtual inertia [9]. $\Delta\theta_{\text{GFM}}$ is the GFM inverter angle deviation related to $\Delta\omega_{\text{GFM}}$.

The GFL inverter implements a droop controller and synchronizes to the bus voltage through a commonly used synchronous reference frame (SRF)-PLL. Hence, the dynamics of the GFL inverter can be written as

$$\Delta P_{\text{GFL}} = -\frac{1}{m_{\text{GFL}}} \Delta\omega_{\text{PLL}}, \quad \Delta\omega_{\text{PLL}} = s\Delta\theta_{\text{PLL}} \tag{2}$$

$$\Delta\omega_{\text{PLL}} = (k_p + \frac{k_i}{s}) K_{\text{PD}} (\Delta\theta_{\text{GFM}} - \Delta\theta_{\text{PLL}}) \tag{3}$$

where ΔP_{GFL} is the difference between the measured active power (P_{GFL}) and the active power setpoint (P_1) of the GFL inverter, m_{GFL} is the frequency droop gain, and $\Delta\omega_{PLL}$ is the difference between the measured frequency (ω_{PLL}) and the nominal frequency (ω_n). $\Delta\theta_{\text{PLL}}$ is the GFL inverter angle deviation related to $\Delta\omega_{\text{PLL}}$. Eq. 3 presents the linearized model of the PLL with k_p, k_i, K_{PD} as the proportional, integral and phase detector gains. Finally, it can be proven that $\Delta\theta_{\text{GFM}} - \Delta\theta_{\text{PLL}} = \theta_{\text{GFM}} - \theta_{\text{PLL}}$. The power balance of the microgrid subject to a load change is given by

$$\Delta P_{\text{GFL}} + \Delta P_{\text{GFM}} = \Delta P_{\text{Load}} \tag{4}$$

where ΔP_{Load} is the active power change in load.

The system model is represented by the equivalent block diagram in Fig. 2, with the corresponding GFM inverter frequency response to load disturbances given in Eq. 5.

B. Stealthy PLL Cyberattack

During the design phase, vulnerabilities such as backdoors can be intentionally or unintentionally embedded in the inverter, creating potential entry points for cyberattacks post-deployment, as reported recently in the real-world paradigm of the air conditioning systems [10]. Furthermore, insiders with legitimate access could exploit their privileges to manipulate critical control parameters, such as reducing the PLL's PI gains. This deliberate adjustment can lower the PLL's bandwidth and damping ratio, leading to degraded inverter performance, disrupted synchronization, and compromised system stability. While the proportional gain (k_p) exclusively affects the damping ratio of the PLL, the integral gain (k_i) influences both the damping ratio and the bandwidth [11].

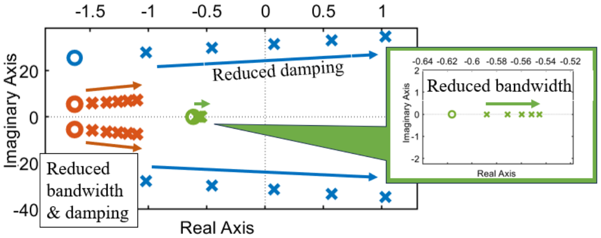


Fig. 3: Impact of droop gain (1% to 5%) on the small-signal stability for reduced PLL damping or/and bandwidth.

TABLE I: Microgrid and controller parameters.

Parameter	Value	Parameter	Value
$V_{RMS,nom}$	400 (230) V	K_{pc}, cur. control	11
S_{nom}, inv. power	12 kVA	K_{ic}, cur. control	12.5
r_f, filter resistance	0.1 Ω	K_{pv}, volt. control	0.08
L_{f1}, filter inductance	2.3 mH	K_{iv}, volt. control	60
L_{f2}, filter inductance	0.93 mH	K_{PD}	326.6
C_f, filter capacitance	8.8 uF	k_p, k_i	0.2, 2
n_{GFM}, voltage droop	5%	ω_c	62.83 rad/s

It has been proven that reducing the PLL's bandwidth and damping in a GFM-GFL system can lead to small-signal instability as the droop gain of the GFM inverter increases [8]. Considering the PLL's PI gains listed in Table I, the original tuning corresponds to a bandwidth (f_n) of 4 Hz and a damping ratio (ζ) of 1.27. Fig. 3 presents the pole-zero map of the microgrid to demonstrate the impact of changing droop gain under the following scenarios: a) the k_p is reduced by 20 times ($f_n = 4$ Hz, $\zeta = 0.064$), b) both k_p and k_i are reduced, leading to a 20-fold decrease in bandwidth while maintaining the damping ratio ($f_n = 0.20$ Hz, $\zeta = 1.27$), c) both k_p and k_i are reduced by a factor of 20 ($f_n = 0.91$ Hz, $\zeta = 0.29$).

As shown in Fig. 3, a skilled adversary can stealthily reduce the PLL gains to levels that preserve small-signal stability, keeping the microgrid operational. If launched at nominal frequency, the attack causes no immediate observable deviations, making it effectively undetectable. However, substantial voltage drops may occur in response to disturbances, such as routine load changes, potentially leading to the disconnection of generation units. Next section establishes the relationship between the voltage drop and the k_p, k_i and m_{GFM} values.

C. Problem Formulation

At any operating point the power balance in the microgrid is maintained, with the GFM and GFL inverters sharing the load power

$$P_{\text{GFM}} + P_{\text{GFL}} = P_{\text{Load}} \tag{6}$$

The output active power of the GFL is

$$\begin{aligned} P_{\text{GFL}} &= \frac{3}{2}\left(I^*_{d,\text{GFL}} V_{d,\text{GFL}} + I^*_{q,\text{GFL}} V_{q,\text{GFL}}\right) \\ &= \frac{3}{2}\left[I^*_{d,\text{GFL}} V \cos(\theta_0 - \theta_{\text{PLL}}) + I^*_{q,\text{GFL}} V \sin(\theta_0 - \theta_{\text{PLL}})\right] \end{aligned}$$

during current limitation $I^*_{d,\text{GFL}} = I_{\text{GFL}}, I^*_{q,\text{GFL}} = 0$, thus

$$P_{\text{GFL}} = \frac{3}{2}\left[I_{\text{GFL}} V \cos(\theta_0 - \theta_{\text{PLL}} - a_0)\right] \tag{7}$$

$$\frac{\omega_{GFM}}{P_{Load}} = -\frac{m_{GFL} m_{GFM} \omega_n s^2 + m_{GFL} m_{GFM} \omega_n K_{PD} k_p s + m_{GFL} m_{GFM} \omega_n K_{PD} k_i}{m_{GFL} s^3 + m_{GFL}(K_{PD} k_p + \omega_n) s^2 + K_{PD}(m_{GFM} \omega_n k_p + m_{GFL} k_i + m_{GFL} \omega_n k_p) s + K_{PD}(m_{GFM} \omega_n k_i + m_{GFL} \omega_n k_i)} \tag{5}$$

where $V_{dq,\mathrm{GFL}}$ and V denote the dq components and the amplitude of the bus voltage, respectively, I_{GFL} represents the amplitude of GFL maximum current, and $I^{*}_{dq,\mathrm{GFL}}$ the reference dq current components. The power factor angle of the GFL, denoted as $a_0 = \arctan(I^{*}_{q,\mathrm{GFL}}/I^{*}_{d,\mathrm{GFL}})$, is set to zero. Finally, θ_0 is the angle of the sinusoidal bus voltage and θ_{PLL} is the estimated angle by the PLL.

Only ohmic loads are assumed in the microgrid; therefore, the active power consumption of the load is given by

$$P_{\mathrm{Load}} = \frac{3V^2}{2R} \tag{8}$$

Substituting (7) and (8) into (6) and simplifying yields:

$$V^2 - RI^{*}_{\mathrm{GFL}} \cos\left(\theta_0 - \theta_{\mathrm{PLL}}\right) V - \frac{2}{3} RP_{\mathrm{GFM}} = 0 \tag{9}$$

In order for Eq. (9) to have at least one solution with respect to V, the discriminant of the quadratic equation must be greater than or equal to zero, leading to the condition

$$\left(RI^{*}_{\mathrm{GFL}} \cos\left(\theta_0 - \theta_{\mathrm{PLL}}\right)\right)^2 + \frac{8}{3} RP_{\mathrm{GFM}} \geq 0. \tag{10}$$

This condition is always satisfied for positive values of P_{GFM}. Thus, Eq. 9 has two solutions (Eqs. 11). The second solution is negative and therefore lacks physical significance.

$$\begin{aligned} V_{1,2} = &\frac{1}{2} RI^{*}_{\mathrm{GFL}} \cos\left(\theta_0 - \theta_{\mathrm{PLL}}\right) \\ &\pm \frac{1}{2}\sqrt{\left(RI^{*}_{\mathrm{GFL}} \cos\left(\theta_0 - \theta_{\mathrm{PLL}}\right)\right)^2 + \frac{8}{3} RP_{\mathrm{GFM}}} \end{aligned} \tag{11}$$

The frequency of the GFM changes according to the the droop gain m_{GFM}, and the phase is set by integrating the frequency: $\omega_{\mathrm{GFM}} = \omega_n - m_{\mathrm{GFM}} P_{\mathrm{GFM}}$, $\dot{\theta}_{\mathrm{GFM}} = \omega_{\mathrm{GFM}}$. During current limitation it is assumed that the voltage regulation does not take place, thus inspired by the angle dynamics of microgrid small signal analysis, the effect of current limitation into the droop control operation, seen from an arbitrary common reference frame, is modeled as an error angle dynamic as follows

$$\theta_{\mathrm{GFM}} = \theta_0 + \delta_{\mathrm{error}} \tag{12}$$

The GFM inverter's angle modeled on its own reference frame is determined by its power controller, thus

$$\dot{\delta}_{\mathrm{error}} = -m_{\mathrm{GFM}} P_{\mathrm{GFM}},\ \delta_{\mathrm{error}} = -m_{\mathrm{GFM}} \int P_{\mathrm{GFM}}\, dt \tag{13}$$

By rewriting Eq. 12 as $\theta_0 = \theta_{\mathrm{GFM}} - \theta_{\mathrm{error}}$, and substituting into Eq.11 we obtain

$$\begin{aligned} V_1 = &RI^{*}_{\mathrm{GFL}} \cos\left(\theta_{\mathrm{GFM}} - \delta_{\mathrm{error}} - \theta_{\mathrm{PLL}}\right) \\ &+ \sqrt{\left(RI^{*}_{\mathrm{GFL}} \cos\left(\theta_{\mathrm{GFM}} - \delta_{\mathrm{error}} - \theta_{\mathrm{PLL}}\right)\right)^2 + \frac{8}{3} RP_{\mathrm{GFM}}} \end{aligned} \tag{14}$$

Finally the PLL frequency is given by

$$\omega_{\mathrm{PLL}} = \omega_n + K_p v_{\mathrm{PCC},q} + K_i \int_0^t v_{\mathrm{PCC},q}\, d\tau \tag{15}$$

where the angle θ_{PLL} is set by integrating the frequency. It is known that the dynamics of PLL angle is heavily influenced by the PI gains of the PLL.

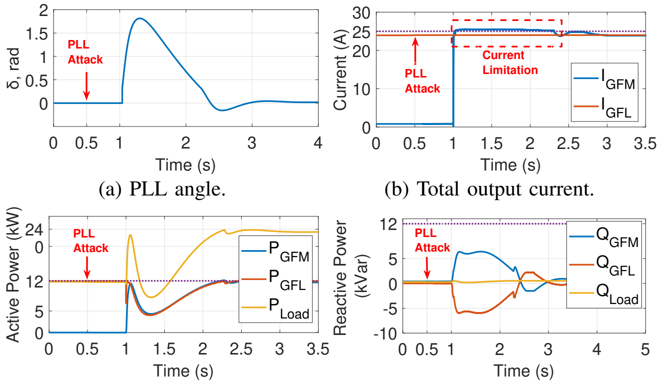
Analyzing Eqs. 13-15, it becomes evident that the bus voltage is strongly influenced by the term $\cos\left(\theta_{\mathrm{GFM}} - \delta_{\mathrm{error}} - \theta_{\mathrm{PLL}}\right)$. As the GFM droop gain (m_{GFM}) increases, the resulting angle deviation becomes larger, causing the cosine term to decrease. Similarly, when the PI gains are reduced, the estimated angle by the PLL deviates from the bus voltage value, leading also to a reduction in the cosine term.

III. Time Domain Analysis with Current Limitation

This section highlights how frequency tracking errors from a compromised PLL interact with current limitation. This non-linear behavior cannot be captured by a linear model, necessitating time-domain analysis. This is followed by a sensitivity study across attack vectors and impact of different current limitation methods.

A. Effect of PLL Attack

The initial 12 kW load of the microgrid is supplied by the GFL inverter. At t = 0.5 s an attacker reduces the PLL's PI gains by a factor of 20, through its control environment [1], without jeopardizing the stability of the system. When the microgrid operates at its nominal frequency, the attack is covert as no change is exhibited. At t = 1 s, the load increases to its maximum value of 24 kW. The GFL inverter's frequency tracking is deteriorated due to the attack, creating a transient frequency and phase difference between the two inverters, the magnitude of which is strongly dependent on the GFM inverter's droop gain, as showcased in Figs. 4 and 5. The error in frequency and angle tracking generates erroneous dq0 components that lead to the GFL inverter reducing its output active power and absorbing reactive power (GFL lags, Figs 4d). To maintain the power balance (therefore the voltage) within the microgrid, the GFM inverter provides the active and reactive power, however is unable to do so due to current limitation (Fig. 4b). This leads to a voltage sag (Fig. 6a), the duration of which depends on the k_p and k_i values and the droop gain of GFM inverter.



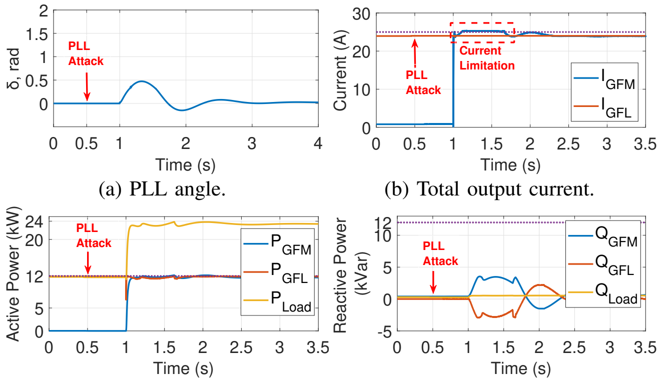
(a) PLL angle.

(b) Total output current.

(c) Active power response.

(d) Reactive power response.

Fig. 4: Dynamic response to load increase under compromised PLL (k_p, k_i/20), m_{GFM} 5%.



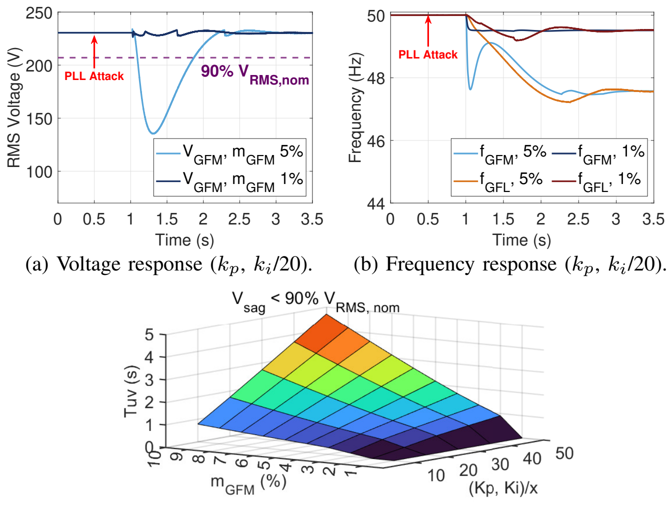
(a) PLL angle.

(b) Total output current.

(c) Active power response.

(d) Reactive power response.

Fig. 5: Dynamic response to load increase under compromised PLL (k_p, k_i/20), m_{GFM} 1%.



(a) Voltage response (k_p, $k_i/20$). (b) Frequency response (k_p, $k_i/20$).

(c) Voltage sag duration.

Fig. 6: Influence of PLL attack in voltage and frequency response for varied GFM droop gains.

The power supply remains insufficient (Fig. 4c) until the GFL inverter's frequency matches that of the GFM inverter. For GFM 1% droop, the frequency deviation is much smaller (Fig. 6b) resulting in a smaller angle error (Fig. 5a) and the described issue no longer exists as in Figs. 5 and 6a.

Fig. 7 shows the duration of voltage sag, below 90% of the nominal value, influenced by the k_p, k_i and m_{GFM} values. According to the German Grid Code FRT requirements [12], after a fault clearance, if the voltage at the point of connection is less than or equal to 90% of the nominal value for more than 1.5 s, the non-synchronous generator is allowed to disconnect. Emphasis is placed on the post-fault requirements, as the current scenario does not consider any fault cases, thereby maintaining generality. Based on Fig. 6c, when the gains of the PLL are reduced 40 times or more and the GFM droop is equal or higher than 5%, the voltage drops will last more than 1.5 s. This can cause a false trigger of the FRT scheme implemented either on the GFL, GFM or both inverters.

B. Attack Vector Sensitivity Analysis

A sensitivity analysis is conducted by varying the PLL PI gains, with red lines in Figs. 7 and 8 indicating constant k_p and blue lines constant k_i. Holding k_p constant while reducing k_i lowers the PLL bandwidth and increases the damping ratio, slowing angle error convergence. As evident from Fig. 7, lower k_i values has a significant influence on the duration of the voltage sag. Reducing only k_p lowers PLL's damping ratio, causing poorly damped oscillations and potentially compromising the system's stability. In the area where the damping ratio is equal or less than 1 (Fig. 8), the minimun value of the voltage sag is mainly influenced by the k_p, whereas for very small values, both gains have similar effect. As indicated by the green dots, the most severe response occurs when both gains are reduced equally. Furthermore, the symmetric manipulation can preserve small-signal stability while avoiding significant deviations in the observable system response, thereby offering a more stealthy and effective attack strategy.

C. Impact of Current Limitation Method

A comparative analysis of three current limitation methods: d-axis prioritization, q-axis prioritization, and circular limitation, is presented in Fig. 9. While d-axis prioritization is commonly adopted in commercial inverters for its alignment to meet active power export/import objectives during

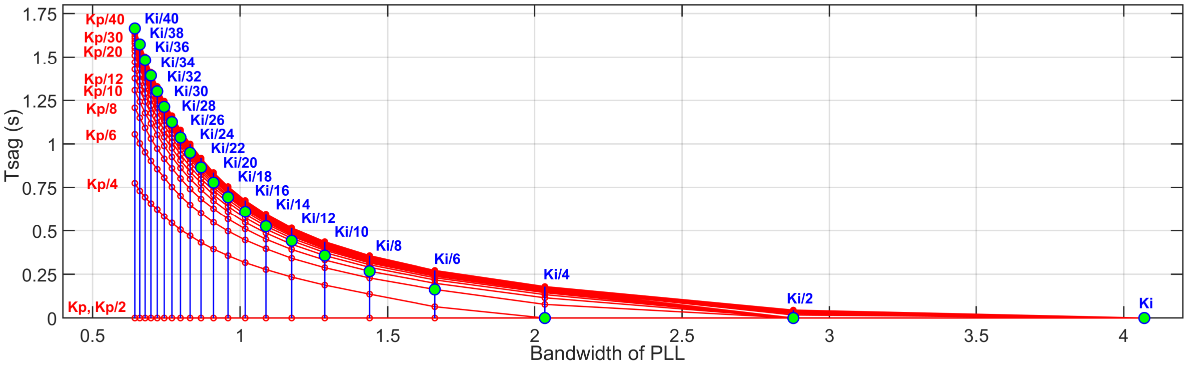


Fig. 7: Voltage sag duration (less than 90%Vnom) under varying PI gain attack vectors (m_{GFM} 5%).

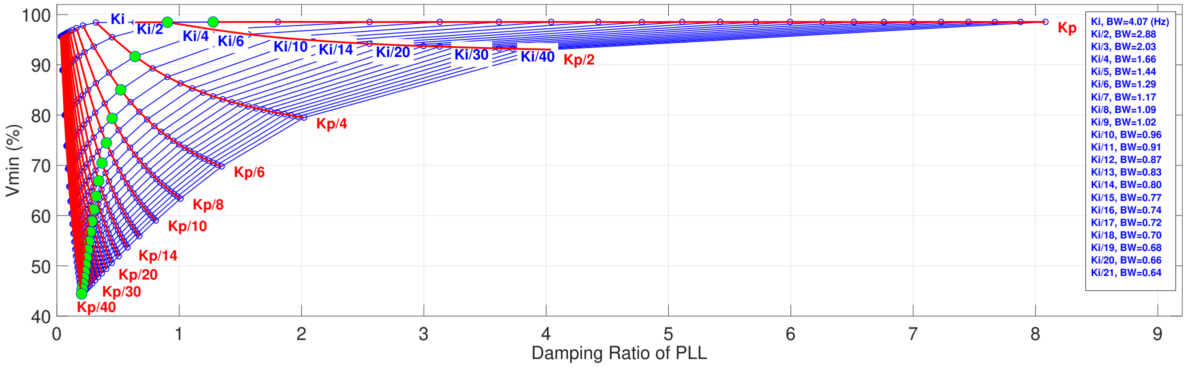
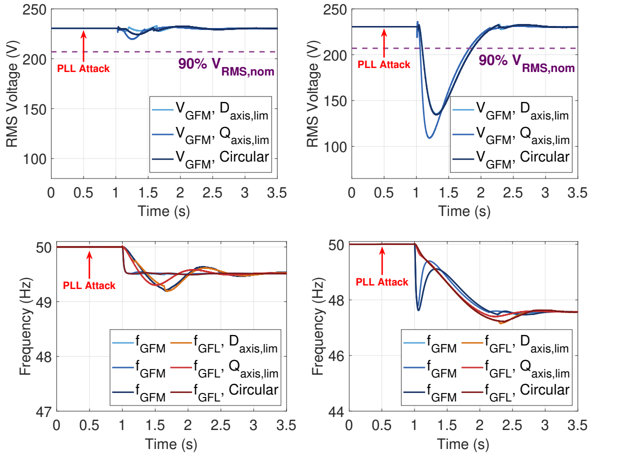


Fig. 8: Minimum voltage under varying PI gain attack vectors (m_{GFM} 5%).



(a) m_{GFM} 1% (b) m_{GFM} 5%

Fig. 9: Voltage and frequency responses under compromised PLL (k_p, k_i/20), for different current limitation methods.

normal operation, q-axis prioritization may enhance voltage support under faults. However, in the studied scenario, q-axis prioritization led to degraded dynamic performance as it worsens the power balance of the microgrid. The circular prioritization method enforces current limits while preserving the pre-limitation ratio of d–q axis contributions, and in the studied scenario, its performance closely resembles that of d-axis prioritization.

IV. Enhancing Cyber Resilience

Enhanced cyber resilience against PLL-targeted attacks in microgrids can be achieved through a passive design strategy, where preemptively lower droop gains are selected for GFM inverters. In this section, an adaptive droop adjustment mechanism that dynamically reduces the GFM inverter's droop gain when its output current exceeds a predefined threshold while the voltage remains within operation range $[V_{-}, V^{+}]$ is introduced as follows

$$m(t) = \begin{cases} \alpha \cdot m_{\text{nom}}, \; I(t) \geq I_{\text{lim}} \;\& \;... \\ \quad ... \; V(t) \subset [V_{-}, V^{+}], \; t \subset [t_0, t_0 + T_h] \\ \alpha \cdot m_{\text{nom}} + (1-\alpha) \cdot m_{\text{nom}} \cdot \dfrac{t - (t_0 + T_h)}{T_r}, \\ \text{ s.t. } \; t \subset [t_0 + T_h, t_0 + T_h + T_r] \\ m_{\text{nom}}, \quad \text{otherwise} \end{cases} \tag{16}$$

where t_0 is the time current limitation is triggered, T_{h} is the hold time at reduced droop, T_{r} is the ramp time back to nominal droop m_{nom}, and factor $\alpha \ll 1$ temporarily reduces droop. To support recovery after disturbances, the droop gain is held at a reduced value temporarily and then smoothly ramped back to its nominal setting using a piecewise function, as defined in Eq 16. This ensures short-term dynamic performance without long-term degradation of frequency regulation or power sharing accuracy. This mitigation strategy is fully decentralized: each GFM inverter autonomously adjusts its droop gain based on local conditions, enabling coordinated system-wide responses without explicit communication.

V. Experimental Validation

For experimental validation, a power hardware-in-the-loop (PHIL) setup is implemented as shown in Fig. 10. The microgrid model comprising two GFM inverters, one GFL inverter, their respective controls, a passive load, and distribution lines, is developed in Novacor (digital real-time simulator from RTDS Technologies) and run at a simulation time step of 50 μs. The hardware under test is a Triphase 15 kVA (TP15KVA) back-to-back voltage source converter configured as the second GFL inverter, interfaced with the Novacor by means of Triphase 90 kVA power amplifier. Ideal transformer model coupling structure is employed as detailed in [13].

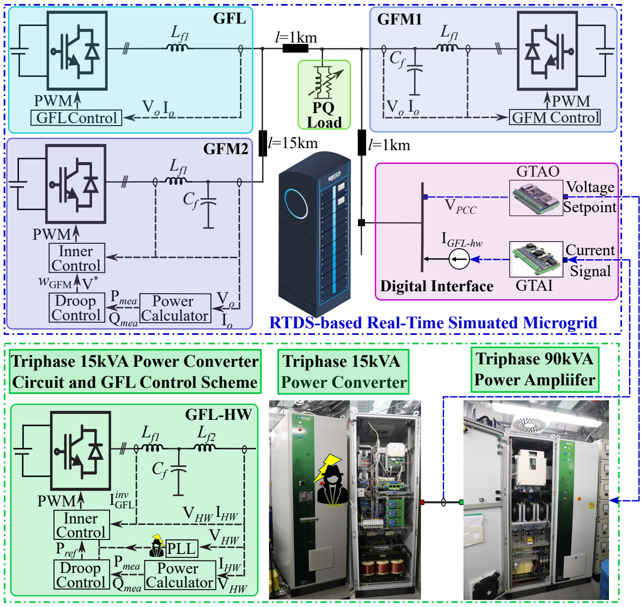


Fig. 10: Experimental PHIL setup.

Due to hardware protection considerations, the power rating of the inverters (hardware and simulated) is chosen as 6 kVA with remainder of the simulation parameters employed as in Tab. I. With the microgrid operating at its nominal frequency, at t = 0.5 s, the k_p and k_i gains of the PLL of the hardware inverter are reduced via the user interface of the TP15KVA. The emulation of the cyberattack leads to no observable transients in the system. At t = 1 s, the load increases from 12 kW to 20 kW. The corresponding responses of the microgrid inverters under higher and lower droop coefficients for the GFM inverters, are shown in Figs. 11 and 12. FRT curves are not implemented in the inverters to allow for a direct comparison and validation of the time domain analysis.

The higher droop gain leads to a greater deviation in frequency resulting in a significant tracking error in the output frequency and phase of the PLL. This leads to a voltage sag that lasts more than 2 s. This demonstrates that the impact of PLL attacks persist in this larger configuration, underscoring the vulnerability of multi-inverter systems to such disturbances. Operating the GFM inverters with 1% droop gain serves as a passive mitigation strategy against PLL cyberattacks, effectively attenuating any anomalies.

Fig. 13 demonstrates the effectiveness of the adaptive mitigation strategy proposed in Section IV, with α=0.2, T_h=3s and T_R=1.33s. Upon load change, only GFM1 that is closer to the compromised GFL-HW reaches current limitation and dynamically adjusts its droop gain. This is evident from the temporary unequal power sharing of the two GFM inverters.

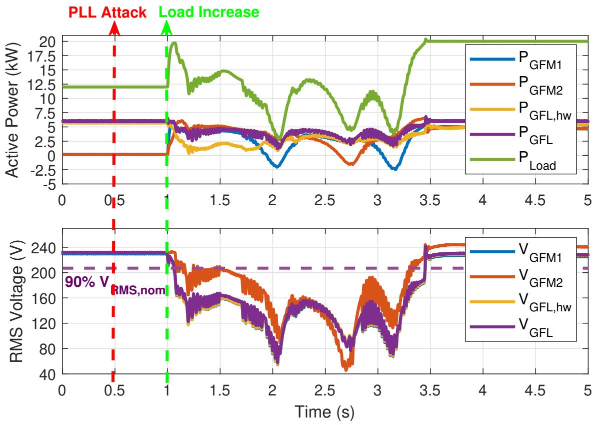


Fig. 11: Response under compromised PLL, m_{GFM} 5%.

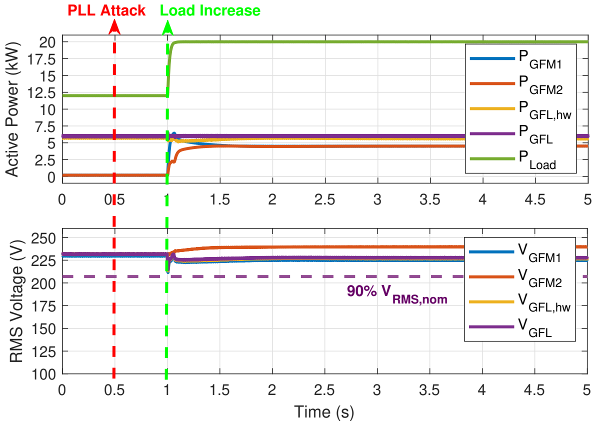


Fig. 12: Response under compromised PLL, m_{GFM} 1%.

After the defined period, GFM1 smoothly ramps its droop back to nominal value thus restoring the power sharing within the microgrid. This demonstrates the simplicity, scalability, and effectiveness of the proposed decentralized mitigation strategy.

VI. Conclusions

This letter identifies a critical cyber vulnerability in inverter-dominated microgrids, wherein phase-locked loop (PLL) attacks on grid-following (GFL) inverters can degrade dynamic performance through nonlinear interactions with the droop control of grid-forming (GFM) inverters under current limitations. In severe cases, this can lead to inverter disconnections or even system-wide blackout. An analytical formulation is developed to characterize this interaction and validated through time-domain simulations. To enhance cyber resilience, it is shown that low GFM droop gains help mitigate the impact of PLL attacks; building on this, an adaptive decentralized droop adjustment strategy is proposed. The strategy enables autonomous adjustment of droop gains based on local current measurements without requiring communication among inverters. The effectiveness and scalability of the proposed strategy are validated using power hardware-in-the-loop experiments with a multi-inverter microgrid setup. The results highlight that microgrid design and operation must extend beyond small-signal stability to explicitly incorporate cyber resilience, leveraging the inherent adaptability and cyber-resilient characteristics of inverter-based systems. Future work will explore system behavior and mitigation strategies under off-nominal frequency conditions, ultra-weak grid connections and broader disturbance scenarios.

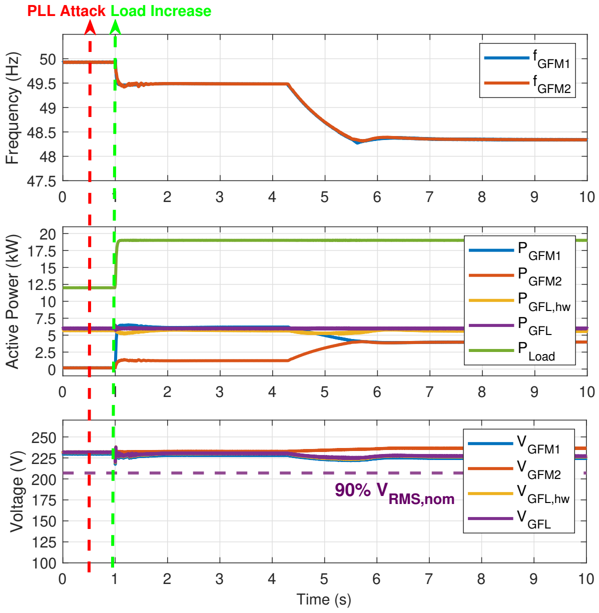


Fig. 13: Dynamic response of proposed mitigation strategy.

References

[1] A. Bamigbade, Y. Dvorkin, and R. Karri, "Cyberattack on phase-locked loops in inverter-based energy resources," *IEEE Trans. Smart Grid*, 2024.

[2] H. M. Albunashee *et al.*, "A test bed for detecting false data injection attacks in systems with distributed energy resources," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 1, pp. 1303–1315, 2022.

[3] M. Ansari, M. Ghafouri, and A. Ameli, "Cybersecurity vulnerabilities in phase-locked loop (PLL) of DFIG-based wind power plants," in *2023 IEEE 2nd Ind. Electron. Society Annual On-Line Conference (ONCON)*, 2023, pp. 1–6.

[4] T. Ding *et al.*, "Quantifying cyber attacks on industrial MMC-HVDC control system using structured pseudospectrum," *IEEE Trans. Power Electron.*, vol. 36, no. 5, pp. 4915–4920, 2021.

[5] X. Zha, Y. Liu, and M. Huang, "Resilient power converter: A grid-connected converter with disturbance/attack resiliency via multi-timescale current limiting scheme," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 1, pp. 59–68, 2021.

[6] A. Bamigbade and F. d. León, "Secure voltage-modulated vector current control of distributed energy resources using delayed DSOGI under distorted and unbalanced grid conditions," *IEEE Trans. Ind. Appl.*, 2024.

[7] M. Gómez, L. Navarro-Hilfiker, and R. Wiśniewski, "Model-based detection of data-injection cyber-attacks on wind turbine controllers," in *2024 10th International Conference on Control, Decision and Information Technologies (CoDIT)*, 2024, pp. 1780–1785.

[8] Y. Wu *et al.*, "Influence of PLL on stability of interconnected grid-forming and grid-following converters," *IEEE Trans. Power Electron.*, 2024.

[9] S. D'Arco and J. A. Suul, "Equivalence of virtual synchronous machines and frequency-droops for converter-based microgrids," *IEEE Trans. on Smart Grid*, vol. 5, no. 1, pp. 394–395, 2014.

[10] Cybersecurity and Infrastructure Security Agency (CISA), "ICS Advisory (ICSA-22-160-01): Vulnerability in Industrial Control Systems," 2022, accessed: January 5, 2025. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-22-160-01

[11] S.-K. Chung, "A phase tracking system for three phase utility interface inverters," *IEE Proceedings - Electric Power Applications*, vol. 147, no. 3, pp. 213–219, 2000.

[12] A. Al-Shetwi, M. Sujod, and N. L. Ramli, "A review of the fault ride through requirements in different grid codes concerning penetration of PV system to the electric power network," *ARPN J. Eng. Appl. Sci.*, 2015.

[13] Z. Feng *et al.*, "Adaptive Smith predictor for enhanced stability of power hardware-in-the-loop setups," *IEEE Trans. Ind. Electron.*, 2023.