Outer-loop Adaptive Control of Converter-Interfaced Generation for Cyber-Physical Security

Ciaran Roberts
Lawrence Berkeley
National Laboratory
cmroberts@lbl.gov

Duncan S. Callaway
University of California, Berkeley
dcal@berkeley.edu

Daniel Arnold
Lawrence Berkeley
National Laboratory
dbarnold@lbl.gov

Abstract

The integration of converter-interfaced generation into our power systems is changing how we control and operate these networks. While these fast-acting resources are more controllable than conventional synchronous machines, this additional controllability presents some challenges. One of these challenges is the increased cyber-physical attack surface arising from interactions among the numerous digital control loops of these devices. In this work, we present a supervisory adaptive controller that temporarily increases the outer-loop controller bandwidth of these devices in the event of sustained oscillatory behavior. We design this controller to inherently remain inactive during normal operation and only become active during sustained abnormal operating conditions. We show how this proposed controller can mitigate a cyber-physical attack, even when the attacker has full knowledge of the network model and access to real-time state information for state-feedback control.

Keywords: Cyber-physical security, adaptive control, stability, defensive controller, microgrid

1. Introduction

As our power systems shift from centralized synchronous machine-based systems to more geographically dispersed converter-interfaced generation (CIG) networks, the stability properties and dynamical response of these systems are also changing. These fast-acting power electronic connected resources, and their multiple layered digital control loops, have a significantly larger control bandwidth relative to conventional synchronous machines [Hatziargyriou et al., 2021]. This increase in controllability allows us greater flexibility in shaping the dynamical response of these resources. However, it also brings new challenges and vulnerabilities, for example, in cyber-physical security [Sahoo et al., 2021].

Traditionally, cyber-physical security for power systems has been primarily focused on protecting individual devices against attacks by securing communication channels, ensuring data integrity, and restricting access, both physical and remote, to these devices. While these approaches are critical, they are not exhaustive. These devices are connected through a dynamical network which can result in unexpected controller coupling, particularly with CIG [Cheng et al., 2022]. This unexpected dynamic controller coupling can be coincidental or can result from malicious control of a device by an adversary.

Malicious control of dynamical devices in power systems is a research area which has received some attention over the years. Some of the early work in this space studied the potential for a malicious actor to control a subset of synchronous generators to destabilize other generators on the system [DeMarco et al., 1996, DeMarco, 1998]. This work was motivated by considering the potential competitive advantage of such an approach in a market environment. More recent work examined how an aggregation of loads providing emulated inertia as a system service might be maliciously controlled to cause unstable oscillatory modes in the system [Brown and Demarco, 2018].

This research was supported in part by the Director, Cybersecurity, Energy Security, and Emergency Response, Risk Management and Tools program, of the U.S. Department of Energy, under contract DE-AC02-05CH11231. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect those of the sponsors of this work.

URI: https://hdl.handle.net/10125/102959
978-0-9981331-6-4

Similarly, the introduction of electric vehicles, and manipulation of their charging behavior, has also been considered as a destabilizing resource in [Acharya et al., 2020]. Other works have considered discrete switching loads and how they may be maliciously controlled [Hammad et al., 2018, Wu et al., 2018, Hammad et al., 2015]. In each of these cases, the resource under the control of the adversary was being controlled to cause an electromechanical instability, i.e., the adversary was causing synchronous machines to oscillate against each other.

The continual integration of CIG into our networks requires a revisiting of these types of malicious attacks. These resources are introducing new dynamical modes into the system that are currently significantly less well understood [Cheng et al., 2022] and invalidating classical timescale separation assumptions we have used to understand these systems [Markovic et al., 2021]. These new modes have been observed as abnormal sustained oscillations in weak grid conditions [Cheng et al., 2022] and have been shown to be vulnerable to attack at high CIG penetration, assuming sufficient knowledge of the system [Roberts et al., 2021].

In this work, we consider an isolated microgrid where an adversary controls an active load, i.e., a load connected to the grid through power electronics. These loads introduce additional dynamics into the system that can destabilize an otherwise stable network [Bottrell et al., 2013]. We adapt the attack vector from [Roberts et al., 2021] and target the CIG by destabilizing an electromagnetic mode in which the CIG participates. We propose a local supervisory controller that observes the states of the CIG and adaptively changes the control logic of the converter to desensitize it against the malicious attack while continuing to deliver its normal grid services. Specifically, we adaptively increase the filter frequency of the low-pass filter in the CIG outer-loop control block. This rate of increase is sampled from a pre-defined normal distribution and, consequently, helps mitigate the adversarial attack by invalidating any deterministic state-space model used to design the destabilizing controller. The proposed controller is designed to inherently remain inactive during normal operation and only alter the converters control logic in the event of sustained abnormal oscillatory behavior. Similar approaches have already been shown to mitigate oscillatory behavior due to poorly designed DER volt-var droop curves [Arnold et al., 2022]. In this work we focus on a much more severe attack where we assume the adversary has access to both a system model and real-time state information to carry out their attack. We show how our proposed controller can introduce a minimal amount of stochastic behavior to invalidate the state-space model used by the attacker, and ultimately, mitigate the impact of the attack.

2. Power System Models

We consider a CIG plant, in Fig. 1, with its active power controller operating in grid-following mode and its reactive power controller in droop mode. Grid-following mode is commonly associated with real-world recorded oscillatory behavior when operating under weak grid conditions, primarily due to the phase-lock loop (PLL) [Cheng et al., 2022].

All control loops in Fig. 1 operate in the dq frame, which is achieved by a linear transformation, T_{dq} in (1), from the 3-phase instantaneous voltage and current values, where θ_c is an internal state of the converter, discussed in Section 2.3.

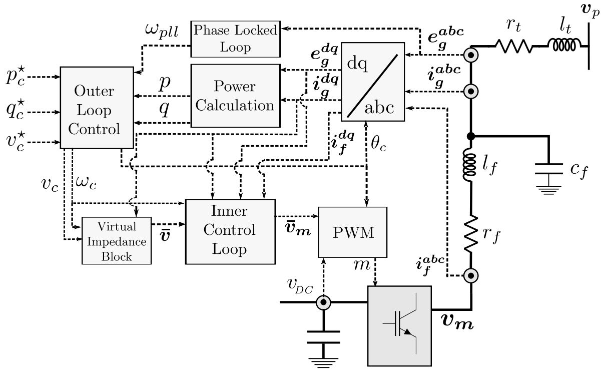
ω_{pll}
Phase Locked Loop
$p_c^\star$
$q_c^\star$
$v_c^\star$
Outer Loop Control
p
q
Power Calculation
$\boldsymbol{e}_{\boldsymbol{g}}^{\boldsymbol{dq}}$
$\boldsymbol{i}_{\boldsymbol{g}}^{\boldsymbol{dq}}$
dq
abc
$\boldsymbol{e}_{\boldsymbol{g}}^{\boldsymbol{abc}}$
$\boldsymbol{i}_{\boldsymbol{g}}^{\boldsymbol{abc}}$
r_t
l_t
$\boldsymbol{v}_p$
$\boldsymbol{i}_{\boldsymbol{f}}^{\boldsymbol{dq}}$
θ_c
l_f
c_f
v_c
ω_c
Virtual Impedance Block
$\bar{\boldsymbol{v}}$
Inner Control Loop
$\bar{\boldsymbol{v}}_{\boldsymbol{m}}$
PWM
r_f
m
$\boldsymbol{i}_{\boldsymbol{f}}^{\boldsymbol{abc}}$
v_{DC}
$\boldsymbol{v}_{\boldsymbol{m}}$

Figure 1. Grid-following control structure

$$T_{dq} = \sqrt{\frac{2}{3}} \begin{bmatrix} \cos(\theta_c) & \cos(\theta_c - 2\pi/3) & \cos(\theta_c + 2\pi/3) \\ \sin(\theta_c) & \sin(\theta_c - 2\pi/3) & \sin(\theta_c + 2\pi/3) \end{bmatrix} \tag{1}$$

In this work, our analysis will be carried out in the dq reference frame. We denote complex vectors using bold lowercase symbols as in (2).

$$\boldsymbol{x} = \boldsymbol{x}^{dq} = x^d + jx^q \tag{2}$$

2.1. Electrical Interface and Power Calculation

The CIG is interfaced to the grid in Fig. 1 through an RLC filter (r_f, l_f, c_f) for harmonic filtering, and a transformer, with resistance and inductance r_t and l_t respectively. The differential equations describing its electrical variables are given by (3):

$$\dot{\boldsymbol{i}}_f = \frac{\omega_b}{l_f}(\boldsymbol{v}_m - \boldsymbol{e}_g) - \left(\frac{r_f}{l_f}\omega_b + j\omega_b\omega_c\right)\boldsymbol{i}_f \tag{3a}$$

$$\dot{\boldsymbol{i}}_g = \frac{\omega_b}{l_t}(\boldsymbol{e}_g - \boldsymbol{v}_p) - \left(\frac{r_t}{l_t}\omega_b + j\omega_b\omega_c\right)\boldsymbol{i}_g \tag{3b}$$

$$\dot{\boldsymbol{e}}_g = \frac{\omega_b}{c_f}(\boldsymbol{i}_f - \boldsymbol{i}_g) - j\omega_c\omega_b\boldsymbol{e}_g \tag{3c}$$

where $\boldsymbol{i}_f$ is the current through the filter inductance, $\boldsymbol{i}_g$ is the current injected into the grid, $\boldsymbol{e}_g$ is the voltage across the filter capacitance, $\boldsymbol{v}_m$ is the modulated voltage at the terminals of the CIG, $\boldsymbol{v}_p$ is the voltage at the point-of-connection to the grid, ω_c is the frequency of the internal synchronously-rotating reference frame (SRF) in per-unit (p.u.) and ω_b is the base system frequency. The converter active and reactive power is then calculated from (4):

$$p_c = \Re(\boldsymbol{e}_g\boldsymbol{i}_g^\star) \qquad q_c = \Im(\boldsymbol{e}_g\boldsymbol{i}_g^\star) \tag{4}$$

where $i_g^\star$ denotes the complex conjugate of the current vector, and $\Re(.)$ and $\Im(.)$ are the real and imaginary part respectively. These active and reactive power measurements, along with the estimated system frequency from the PLL, are then passed into the outer-loop control block.

2.2. Phase-lock loop

The purpose of the PLL is to track the frequency and phase of the externally measured grid voltage. It does so by aligning the $d-$axis of the internal SRF with the externally measured voltage vector, resulting in its $q-$ vector component of the internal SRF being equal to zero. Its dynamics are given by (5):

$$\hat{\boldsymbol{e}}_g = \boldsymbol{e}_g e^{-j\theta_{pll}} \tag{5a}$$

$$\dot{\theta}_{pll} = \omega_{pll}\omega_b \tag{5b}$$

$$\dot{\varepsilon} = \hat{e}_g^q \tag{5c}$$

$$\omega_{pll} = \omega_0 + K_p^{pll}\hat{e}_g^q + K_i^{pll}\varepsilon \tag{5d}$$

where ε is the integrator state of the PLL, ω_{pll} is the estimated frequency, and K_p^{pll} and K_i^{pll} are the proportional and integral gains respectively of the PI control loop in (5d). One difficulty with parameterizing the control gains of a PLL is the requirement that it produces an accurate and stable estimation of the grid-frequency across all grid operating conditions, i.e., a weak and strong grid, while also not being overly sensitive to natural grid-disturbances, e.g., faults. This is one of the reasons why the PLL is often identified as one of the contributors to undesirable oscillatory behavior [Cheng et al., 2022].

2.3. Outer-loop control

Once the PLL estimates the grid frequency, ω_{pll} in (5d), this estimation is passed to the outer-control loop. This control loop is responsible for determining control set-points to achieve a desired active and reactive power injection. It is typically one of the slower control loops of the CIG and can also contribute to undesirable oscillatory behavior [Cheng et al., 2022]. Within the outer-control loop, the CIG first low-pass filters the measured active and reactive power in (6a) and (7a) respectively. The filter frequency, ω_z, determines the bandwidth of the outer-loops. In this work, we will consider ω_z as a state within our supervisory controller and adjust it to change the outer-loop control bandwidth of the CIG during sustained abnormal behavior. The specific control structure to achieve this will be introduced in Section 3.2.

$$\dot{\tilde{p}}_c = \omega_z(p_c - \tilde{p}_c) \tag{6a}$$

$$\omega_c = \omega_{pll} + R_p(p_c^\star - \tilde{p}_c) \tag{6b}$$

$$\dot{\theta}_c = \omega_c\omega_b \tag{6c}$$

The output of these low-pass filters, $\tilde{p}$ and $\tilde{q}$, are then used to determine the control set-points ω_c and v_c in (6b) and (7b) respectively, where R_p and R_q are the active and reactive power droop gains respectively.

$$\dot{\tilde{q}}_c = \omega_z(q_c - \tilde{q}_c) \tag{7a}$$

$$v_c = v_c^\star + R_q(q_c^\star - \tilde{q}_c) \tag{7b}$$

The angular frequency, ω_c, also determines the angle θ_c, in (6c), for the linear transformation, T_{dq} in (1).

2.4. Virtual Impedance

These outer-loop control set-points are then passed to the virtual impedance control block in Fig. 1, with a virtual resistance and inductance, r_v and l_v respectively. This additional degree of freedom is used for active stabilization and disturbance rejection [Wang et al., 2015].

$$\bar{v}_c^d = v_c - r_v i_g^d + \omega_c l_v i_g^q \tag{8a}$$

$$\bar{v}_c^q = -r_v i_g^q - \omega_c l_v i_g^d \tag{8b}$$

Additionally, the use of a virtual impedance can increase the apparent X/R ratio of the network and improve the small-signal stability of the system by strengthening the p/f and q/v coupling of the system.

2.5. Inner control loop

Finally, a dual-loop PI controller is used in the inner-loop for reference tracking. The output of the virtual impedance control block, $\bar{\boldsymbol{v}}_c$ is first passed to a PI voltage controller in (9)

$$\bar{\boldsymbol{i}}_f = K_p^v(\bar{\boldsymbol{v}}_c - \boldsymbol{e}_g) + K_i^v\boldsymbol{\xi} + j\omega_c c_f\boldsymbol{e}_g + K_f^v\boldsymbol{i}_g \quad (9a)$$

$$\dot{\boldsymbol{\xi}} = \bar{\boldsymbol{v}}_c - \boldsymbol{e}_g \quad (9b)$$

whose output, $\bar{\boldsymbol{i}}_s$, is then passed into another PI control loop, in (10), to determine the output voltage reference used for the averaged modulated signal.

$$\bar{\boldsymbol{v}}_m = K_p^i(\bar{\boldsymbol{i}}_f - \boldsymbol{i}_f) + K_i^i\boldsymbol{\gamma} + j\omega_c c_f\boldsymbol{i}_f + K_f^i\boldsymbol{e}_g \quad (10a)$$

$$\dot{\boldsymbol{\gamma}} = \bar{\boldsymbol{i}}_f - \boldsymbol{i}_f \quad (10b)$$

In both (9) and (10), the controller gains K_p^v/K_p^i and K_i^v/K_i^i are the proportional and integral gains of the PI loop respectively and K_f^v/K_f^i is a binary feed-forward term.

3. Methodology

Prior to introducing the proposed defensive controller in Section 3.2, we first begin with a brief overview of the attack model. Understanding the attack methodology of the adversary, and how they develop a destabilizing controller, is necessary to motivate the formulation of the proposed defensive controller.

3.1. Attack model

Our model of the adversary follows the approach of [Roberts et al., 2021] and is summarized here. We assume that the adversary has access to both 1) a detailed model of the system and 2) real-time state information to build a state-feedback controller. During the attack, this real-time state information can come directly from measurements or can be estimated using a state-observer, assuming sufficient observability of the system, i.e., the adversary has access to high-rate current and voltage data.

Under these assumptions, the goal of the adversary is to design a destabilizing state-feedback controller such that an eigenvalue of the linearized state-space model is in the right-half plane, i.e., the system is unstable. That is, given a linearized model of the system in (11)

$$\Delta\dot{\boldsymbol{x}} = \boldsymbol{A}\Delta\boldsymbol{x} + \boldsymbol{B}\Delta\boldsymbol{u}, \quad (11)$$

the adversary seeks to design a controller of the form $\boldsymbol{u} = -\boldsymbol{F}\Delta\boldsymbol{x}$ such that the closed loop system in (12) has at least one eigenvalue whose real part is positive.

$$\Delta\dot{\boldsymbol{x}} = (\boldsymbol{A} - \boldsymbol{B}\boldsymbol{F})\Delta\boldsymbol{x} \quad (12)$$

Additionally, we assume the adversary minimizes its own participation in this unstable mode. Simply put, the adversary seeks to excite the system to cause other devices on the grid to oscillate against each other. The measure of participation of a state i in a system mode j is given by (13)

$$p_{ij} = \frac{w_{ij}v_{ij}}{\boldsymbol{w}_j^T\boldsymbol{v}_j}, \quad (13)$$

where w_{ij} and v_{ij} are the i^{th} elements in the left and right eigenvector respectively associated with the j^{th} eigenvalue. This adversarial destabilizing controller design is mathematically expressed in (14) and admits a closed form solution [Roberts et al., 2021]:

$$\min_{F} \quad \sum p_{ij} \quad \forall i \in \boldsymbol{\Gamma} \quad (14a)$$

$$\text{s.t.} \quad \exists \quad \Re(\lambda_j) > 0 \quad (14b)$$

$$(\boldsymbol{A} - \boldsymbol{B}\boldsymbol{F})\boldsymbol{v}_j = \lambda_j\boldsymbol{v}_j \quad (14c)$$

where $\boldsymbol{v}_j$ is the eigenvector associated with λ_j and $\boldsymbol{\Gamma}$ denotes the set of states indices for the active load under control of the adversary. This closed form solution is summarized in Appendix A for the reader. In [Roberts et al., 2021], the authors identified both an electromechanical and electromagnetic mode that the adversary could seek to destabilize. In this work, we focus on the attack that destabilizes the electromagnetic mode, as this is the most damaging attack for CIG.

The proposed attack model assumes a significant level of system knowledge to carry-out. An alternative attack model is a data-driven approach that estimates vulnerable system modes based on measurement data during disturbances [Hammad et al., 2018, Hammad et al., 2015], e.g., measurement data during faults. The adversary then designs a local controller to try to destabilize these estimated modes. In both cases, model-based or measurement-based, the adversary seeks to design a destabilizing controller based on their understanding of the system. Our proposed approach is motivated by invalidating their understanding of the system during sustained abnormal oscillatory behavior. Therefore, the proposed controller is not tailored to mitigate the specific attack vector considered here, but rather any attack vector that relies on a fixed understanding of the system. Due to the stochastic nature of our controller, designed to remain inactive during inherent system transients, the proposed approach will remain effective in mitigating the severity of the attack for both model and measurement-based attacks.

3.2. Defensive controller

One commonality across all prior work that has considered destabilizing adversarial attacks is the requirement of a deterministic state-space model to build a state-feedback controller [Roberts et al., 2021, DeMarco, 1998, Brown and Demarco, 2018, Acharya et al., 2020]. This state-space model allows the adversary to identify vulnerable system modes to destabilize with state-feedback control. As a last line of defense against these types of attacks, we propose a non-linear supervisory controller that introduces a small amount of stochastic behavior into the system to invalidate the state-space model the adversary used in its controller design. This controller, in (15), is designed to inherently remain inactive during normal operation and only become activated during sustained abnormal oscillatory behavior. Therefore, the CIG will respond as expected to normal grid disturbances, e.g., faults, line trips and frequency events.

The proposed controller uses an observer, shown in Fig. 2, to estimate the energy of the observed oscillation, similar to [Arnold et al., 2022]. It monitors the integrator state of the PLL, ε, and uses a high-pass filter in (15a) to remove any DC offset, or low-frequency behavior, in the signal. We choose the integrator state of the PLL based on analysis in [Roberts et al., 2021] and due to the PLL being identified as being a major cause of instability in real-world observed oscillations [Cheng et al., 2022]. Once the low frequency behavior has been removed, we multiply the resultant signal, ε_h, by a normalization constant, c, then square it and pass it through a low-pass filter in (15b) to obtain a stable control signal. This low-pass filter also desensitizes the proposed controller to naturally occurring system transients, e.g., faults and line trips. By first removing the low-frequency content and then squaring the signal, we are estimating the energy of the oscillation in the PLL integrator state, ε. We then use this measure of energy to increase the outer-control loop filter frequency, ω_z, in (15c) where $\alpha \sim \mathcal{N}(\mu, \sigma^2)$.

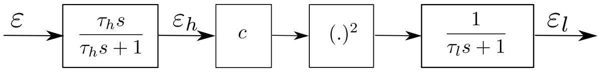

Figure 2. Estimating energy of oscillation.

$$\dot{\varepsilon}_h = \frac{\tau_h \dot{\varepsilon} - \varepsilon_h}{\tau_h} \tag{15a}$$

$$\dot{\varepsilon}_l = \frac{(c\varepsilon_h)^2 - \varepsilon_l}{\tau_l} \tag{15b}$$

$$\dot{\omega}_z = \omega_z^\star - \omega_z + \alpha\varepsilon_l \tag{15c}$$

This proposed controller runs continuously on the CIG. It is not threshold activated but instead uses the high- and low-pass filters to reject normally occurring disturbances on the external grid.

As previously discussed, this filter frequency, ω_z, determines the bandwidth of the outer-control loops of the CIG. By temporarily increasing the controller bandwidth of the outer-loop, we are breaking any controller coupling that the adversary is seeking to exploit. The structure of (15c) also ensures that when the oscillation is mitigated, the filter frequency returns to its normal operating point, $\omega_z^\star$. The stochastic nature of α, not remotely accessible via communication and updated at a low frequency, e.g., seconds or minutes, ensures that the adversary never has access to a deterministic state-space model to build a state-feedback controller.

Fig. 3 shows how increasing the outer-loop bandwidth can temporarily move a pair of system eigenvalues, and consequently, mitigate any attack that specifically targets these eigenvalues based on a model or measurement data. The specific eigenvalues highlighted in Fig. 3 have high state-participation from both the PLL and outer-loop controls and can move towards the right-half plane during weak grid conditions and/or because of inter-IBR controller coupling.

The proposed adaptive control loop, shown in Fig. 4, should be parameterized to ensure sufficient timescale separation between the proposed controller and existing control loops of the CIG. This will help ensure that the controller does not increase the oscillations during the attacks considered here.

4. Results

To demonstrate the effectiveness of the proposed controller we consider the 3-bus microgrid in Fig. 5. This system has a synchronous generator (SG), a grid-following (Gf) converter, an active load (AL) and a constant impedance load. The adversary has control over the active load and designs a state-feedback

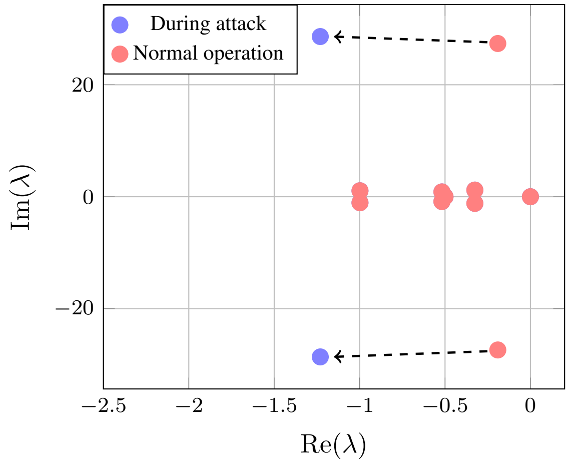

Figure 3. Changing eigenspectrum during attack

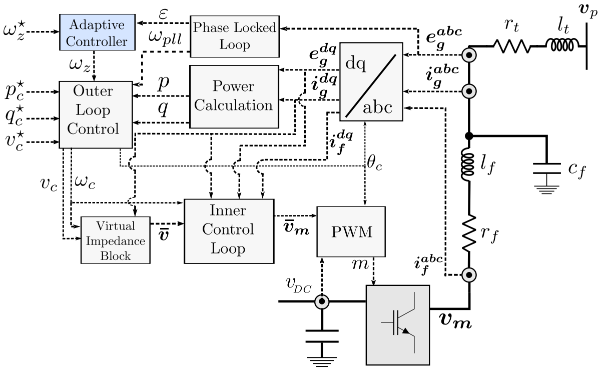

Figure 4. Grid-following control structure with proposed control loop

controller for modulating active and reactive power demand to cause the system to become unstable. The parameters of the synchronous-machine and grid-following converter are from [Markovic, 2020] and the details of the AL and the destabilizing adversarial controller can be found in [Roberts et al., 2021]. The steady-state active and reactive power operating conditions are summarized in Table 1.

Table 1. Steady-state operating conditions.

	P [p.u.]	Q [p.u.]
SG	0.32	0.14
Gf	0.70	0.12
AL	0.05	0.0
rl load	0.97	0.11

The proposed defensive controller from Section 3.2, with experimental parameters in Table 2, is deployed on the grid-following converter and monitors the integrator state of the PLL.

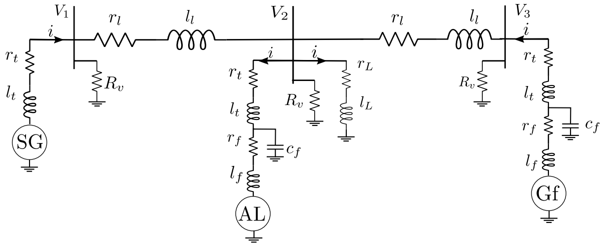

Figure 5. Three-bus mixed source microgrid

Table 2. Supervisory Controller Parameters.

τ_h	τ_l	c	μ	σ
0.795	0.159	1×10^4	15	2

Fig. 6 shows the active power injection from the grid-following converter in the case of no attack and during an attack with and without the proposed supervisory controller. Without the proposed controller, we see that the CIG is exhibiting unstable oscillatory behavior. With the proposed supervisory controller, however, we see that the unstable behavior is mitigated within seconds following its onset.

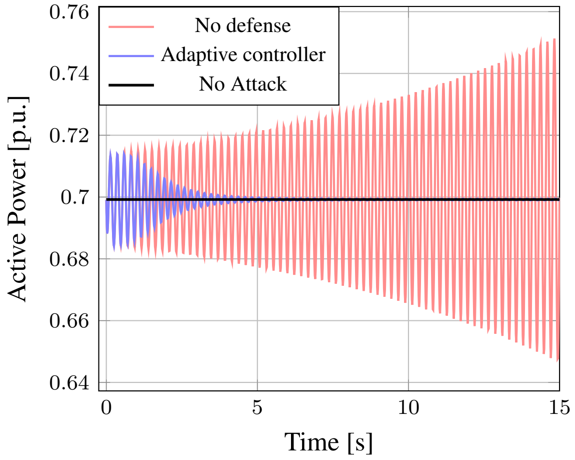

Figure 6. Grid-following converter active power

Contrasting the active and reactive power demand from the adversary controlled active load in Fig. 7 to the oscillatory active power injection from the grid-following converter in Fig. 6, we see that the adversary has exerted minimal observable control effort to destabilize the system. The amplitude of its load modulation is under 2% of the total microgrid load. This level of load modulation is consistent with prior work on adversarial load control for destabilizing electromechanical modes on the transmission grid [Brown and Demarco, 2018]. Additionally, this load oscillatory amplitude is significantly smaller than the amplitude of the oscillatory behavior in the active power behavior of the CIG in Fig. 6. This additional oscillatory active power from the CIG is being absorbed primarily by the constant impedance, due to oscillations in the nodal voltages, and the synchronous machine.

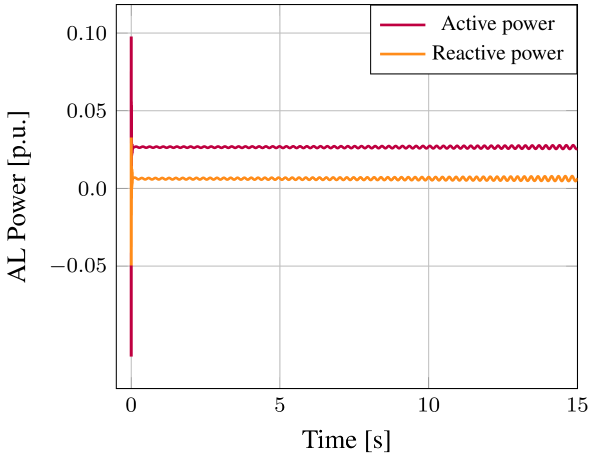

Figure 7. Adversary load power

To understand the behavior of the supervisory defensive controller we examine the behavior of both the observer, for estimating the energy of the oscillation, and the filter frequency ω_z. Fig. 8 plots the time-series of ε_l, the output of a low-pass filter from (15b). Initially, we see relatively large values for ε_l as the amplitude of the oscillations grow in Fig. 6. With the inclusion of the proposed controller, we see these oscillations decay until they settle around constant oscillatory amplitude.

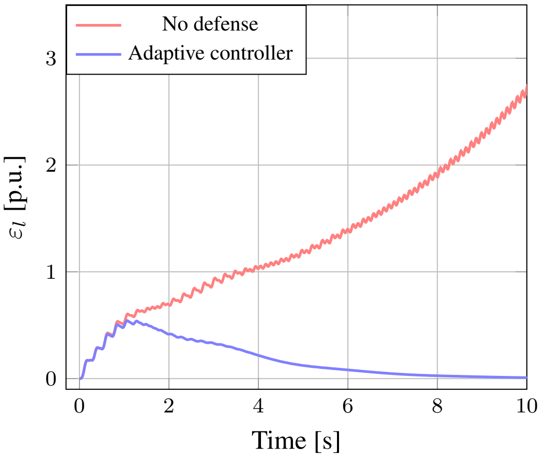

Figure 8. ε_l time series during attack

This filtered signal, ε_l, in Fig. 8 is a stable control signal that is then used to adaptively increase the outer-loop filter frequency, as shown in Fig. 9.

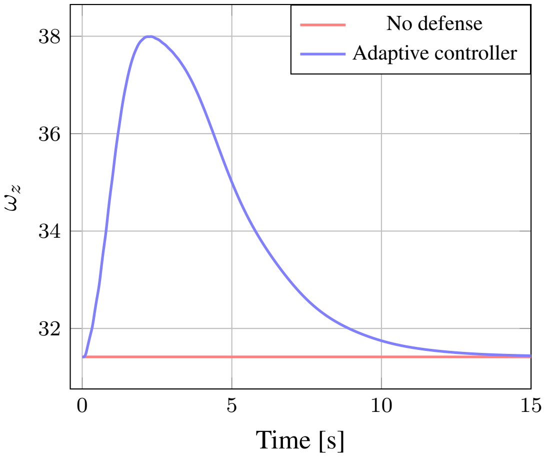

Figure 9. Time series of ω_z during attack

The filter-frequency, ω_z, is only marginally increased in this case to mitigate the attack. This helps limit the randomness introduced by the defensive controller and ensures that, even during a sustained adversarial load attack, the CIG exhibits largely deterministic behavior. Additionally, we see that once the oscillatory amplitude in Fig. 6 decays, ω_z tends back towards its set-point, $\omega_z^\star$, in Fig. 9. Once the adversarial controller is deactivated, either by the adversary themselves or a higher-level intrusion detection scheme, the proposed controller ensures that ω_z returns to its normal operating value, $\omega_z^\star$.

In this work, we demonstrated our proposed controller on a simple 3-bus microgrid. Recent analysis has shown how electrically close CIG can adversely interact with each other in larger systems [Fan, 2022]. This presents an alternative attack vector for adversaries to destabilize local CIG. Future work will examine how the proposed controller performs under such an attack.

5. Conclusions

In this work we presented a local supervisory controller designed to be the last line of defense against a destabilizing cyber-physical attack against CIG within a micro-grid. This defensive controller was designed to stochastically increase the outer-loop bandwidth of the CIG to invalidate any deterministic state-space model that an adversary may have used to design their attack. A key design feature of the proposed controller is that is does not impede normal operation of the CIG and is only activated in the event of sustained oscillatory behavior.

With the continual proliferation of microgrids, coupled with the control complexity of the CIG, the attack surface of these systems is increasing [Sahoo et al., 2021]. Hardening these systems against adversarial attacks, both direct and indirect, will require a cross-disciplinary approach with multiple fail-safe systems. This work was a first step at designing a last line of defense that would allow the CIG to remain online and delivering its required grid services while protecting itself against a targeted attack. The hope is that this last line of defense would mitigate any adverse physical impacts of the attack, e.g., damaging equipment, as well as allow operators and/or other defensive layers additional time to respond.

Further work is required to further analyze, and test, the proposed controller and its stability properties to guarantee its satisfactory performance. Additionally, we will consider the effectiveness of the proposed controller under different attack models, including attacks that attempt to be robust with respect to uncertainties in the system model. These more sophisticated attacks may require adjusts to the proposed controller, e.g., saturating the value of the filter frequency, ω_z, to ensure that the proposed controller does not increase the bandwidth of the outer-loop such that it adversely interacts with the inner-control loop.

Appendix A

We assume the adversary has a linear state-space model of the form

$$\Delta\dot{\boldsymbol{x}} = \boldsymbol{A}\Delta\boldsymbol{x} + \boldsymbol{B}\Delta\boldsymbol{u}, \tag{16}$$

with $\boldsymbol{x} \in \mathbb{R}^n$, $\boldsymbol{A} \in \mathbb{R}^{n\times n}$, $\boldsymbol{B} \in \mathbb{R}^{n\times m}$ and $\boldsymbol{u} \in \mathbb{R}^m$. To design a destabilizing feedback controller, we first identify a suitable mode of the linearized matrix $\boldsymbol{A}$ to destabilize. Following this, we seek to design a feedback controller that achieves a desired closed-loop unstable eigenvalue $\hat{\lambda}$. In addition to meeting the eigenvalue specification criteria, we seek to design the corresponding eigenvector $\hat{\boldsymbol{v}}$ to minimize the participation of the states of the control group in the unstable mode. To achieve this, we seek to design an eigenvector $\hat{\boldsymbol{v}}$ that maximizes the participation of the target group (relative to the control group) in the unstable mode. We then begin by constructing the corresponding Hautus matrix $\boldsymbol{S}_{\hat{\lambda}}$ given by (17)

$$\boldsymbol{S}_{\hat{\lambda}} = [(\hat{\lambda}\boldsymbol{I} - \boldsymbol{A}) \quad \boldsymbol{B}] \tag{17}$$

where $\boldsymbol{I}$ is the identity matrix. We then determine the matrix $\boldsymbol{K}_{\hat{\lambda}}$ of the form

$$\boldsymbol{K}_{\hat{\lambda}} = \begin{bmatrix} \boldsymbol{N}_{\hat{\lambda}} \\ \boldsymbol{M}_{\hat{\lambda}} \end{bmatrix}, \tag{18}$$

whose columns form a basis for nullspace of $\boldsymbol{S}_{\hat{\lambda}}$. Note that the rows of $\boldsymbol{K}_{\hat{\lambda}} \in \mathbb{R}^{(n+m)\times m}$ are partitioned in a similar manner to the columns of $\boldsymbol{S}_{\hat{\lambda}}$, i.e. $\boldsymbol{N}_{\hat{\lambda}} \in \mathbb{R}^{n\times m}$ and $\boldsymbol{M}_{\hat{\lambda}} \in \mathbb{R}^{m\times m}$. The dimension, m, of the input vector, u, will determine the dimension of the nullspace and consequently the degree of flexibility in designing the eigenvector $\hat{\boldsymbol{v}}$, expressed as

$$\hat{\boldsymbol{v}} = \boldsymbol{N}_{\hat{\lambda}}\boldsymbol{k} \tag{19}$$

for some $\boldsymbol{k} \in \mathbb{R}^{m\times 1}$. The i^{th} entry of $\hat{\boldsymbol{v}}$, therefore, is given by

$$\hat{v}_i = \sum_{j=1}^{m} [N_{\hat{\lambda}}]_{i,j} k_j. \tag{20}$$

Here, we let $\boldsymbol{N}_{\hat{\lambda}T}$ and $\boldsymbol{N}_{\hat{\lambda}C}$ denote the rows of $\boldsymbol{N}_{\hat{\lambda}}$ whose indices correspond to the states of the target and control group, respectively. The target group represents the states of the devices we wish to destabilize while the control group is the set of states under the control of the adversary. We then seek to determine the optimal design vector $\boldsymbol{k}^\star$ for maximizing the ratio of ℓ_2-norm of the eigenvector entries corresponding to the target states and the ℓ_2-norm of the eigenvector entries corresponding to the control group. Similar to [DeMarco, 1998], we mathematically express this optimization problem as

$$\begin{aligned} \max_{\boldsymbol{k}} \quad & \frac{\boldsymbol{k}'[\boldsymbol{N}_{\hat{\lambda}T}]'\boldsymbol{N}_{\hat{\lambda}T}\boldsymbol{k}}{\boldsymbol{k}'[\boldsymbol{N}_{\hat{\lambda}C}]'\boldsymbol{N}_{\hat{\lambda}C}\boldsymbol{k}} \\ \text{s.t.} \quad & \boldsymbol{k}'\boldsymbol{k} = 1, \end{aligned} \tag{21}$$

where $[.]'$ denotes the transpose operator. Defining the matrices $\boldsymbol{G}$ and $\boldsymbol{H}$ as

$$\boldsymbol{G} = [\boldsymbol{N}_{\hat{\lambda}T}]'\boldsymbol{N}_{\hat{\lambda}T} \quad \boldsymbol{H} = [\boldsymbol{N}_{\hat{\lambda}C}]'\boldsymbol{N}_{\hat{\lambda}C}, \tag{22}$$

we rewrite this optimization as

$$\begin{aligned} \max_{\boldsymbol{k}} \quad & \frac{\boldsymbol{k}'\boldsymbol{G}\boldsymbol{k}}{\boldsymbol{k}'\boldsymbol{H}\boldsymbol{k}} \\ \text{s.t.} \quad & \boldsymbol{k}'\boldsymbol{k} = 1. \end{aligned} \tag{23}$$

Note that we assume that the matrix $\boldsymbol{H}$ is positive definite. Otherwise, we could choose the optimal design vector $\boldsymbol{k}^\star$ such that the control group would have zero participation in the unstable mode, i.e. $\boldsymbol{N}_{\hat{\lambda}C}\boldsymbol{k}^\star = \boldsymbol{0}$, which would be the best case for the adversary.

Having $\boldsymbol{H}$ as positive definite, we can safely assume that it has a well-defined square root. We now introduce a linear transformation given by

$$\boldsymbol{k} = \boldsymbol{H}^{-1/2}\boldsymbol{\nu}, \tag{24}$$

and substitute this into (23), which yields

$$\max_{\boldsymbol{\nu}} \frac{\boldsymbol{\nu}'(\boldsymbol{H}^{-1/2})^T\boldsymbol{G}\boldsymbol{H}^{-1/2}\boldsymbol{\nu}}{\boldsymbol{\nu}'\boldsymbol{\nu}}. \tag{25}$$

Note that (25) takes the form of the Rayleigh quotient and is therefore easily solvable. The optimal design vector $\boldsymbol{k}^\star$ is constructed using the eigenvector $\boldsymbol{\nu}_{max}$ corresponding to the largest eigenvalue of (25), and is given by

$$\boldsymbol{k}^\star = \boldsymbol{H}^{-1/2}\boldsymbol{\nu}_{max}. \tag{26}$$

We then construct the destabilizing feedback matrix $\boldsymbol{F}$ as follows. Let us define the vectors $\hat{\boldsymbol{w}}$ and $\hat{\boldsymbol{w}}$ in (27).

$$\hat{\boldsymbol{w}} = \boldsymbol{M}_{\hat{\lambda}}\boldsymbol{k}^\star \, , \, \hat{\boldsymbol{v}} = \boldsymbol{N}_{\hat{\lambda}}\boldsymbol{k}^\star, \tag{27}$$

and construct the real matrices $\boldsymbol{W}$ and $\boldsymbol{V}$ of the form

$$\boldsymbol{W} = [Re\{\hat{\boldsymbol{w}}\}\, Im\{\hat{\boldsymbol{w}}\}\, \boldsymbol{0} \, \ldots \, \boldsymbol{0}], \tag{28a}$$

$$\boldsymbol{V} = [Re\{\hat{\boldsymbol{v}}\}\, Im\{\hat{\boldsymbol{v}}\}\, Re\{\boldsymbol{v}_3\}\, Im\{\boldsymbol{v}_3\} \, \ldots \, \boldsymbol{v}_{n-1}\, \boldsymbol{v}_n], \tag{28b}$$

where $[\boldsymbol{v}_3, \ldots.\boldsymbol{v}_{n-1}, \boldsymbol{v}_n]$ are the remaining original eigenvectors from the state-space matrix $\boldsymbol{A}$ given in (16). The feedback matrix $\boldsymbol{F}$ is then given by

$$F = \boldsymbol{W}\boldsymbol{V}^{-1}. \tag{29}$$

Provided that the columns in (28b) are linearly independent, the matrix $\boldsymbol{F}$ given by (29) exists and is unique [Moore, 1976].

Appendix B

Nomenclature

γ	Inner-loop current controller integrator
$\boldsymbol{e}_g$	Gf capacitor voltage
$\boldsymbol{i}_f$	Gf filter current
$\boldsymbol{i}_g$	Gf grid current
$\boldsymbol{v}_j$	Right eigenvector for j^{th} mode
$\boldsymbol{v}_m$	CIG terminal voltage
$\boldsymbol{v}_m$	Gf terminal voltage
$\boldsymbol{w}_j$	Left eigenvector for j^{th} mode
α	Adaptive filter frequency control gain
$\bar{\boldsymbol{i}}_f$	Gf current set-point
$\bar{\boldsymbol{v}}_m$	Gf voltage set-point
Γ	Set of indices denoting the states of the active load
$\hat{e}_g$	q-axis voltage in Gf PLL SRF
ω_b	System base frequency
ω_c	Frequency of Gf internal SRF
ω_{pll}	PLL frequency estimate
ω_z	Gf outer-loop filter frequency
$\omega_z^\star$	Reference Gf outer-loop filter frequency
τ_h	Time constant of high-pass filter
τ_l	Time constant of low-pass filter
θ_{pll}	Angle of Gf PLL
$\tilde{p}_c$	Gf low-pass filtered active power
$\tilde{q}_c$	Gf low-pass filtered reactive power
ε	Integrator state of the PLL
ε_h	Output of controller high-pass filter
ε_l	Output of controller low-pass filter
c	Normalization constant
p_c	Gf active power
p_{ij}	Participation of state i in mode j
q_c	Gf reactive power
v_c	Gf outer-loop voltage setpoint
v_{ij}	i^{th} element in right eigenvector for j^{th} mode
w_{ij}	i^{th} element in left eigenvector for j^{th} mode
$\boldsymbol{\xi}$	Inner-loop voltage controller integrator
θ_c	Angle of the CIG active power controller

References

[Acharya et al., 2020] Acharya, S., Dvorkin, Y., and Karri, R. (2020). Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable? *IEEE Transactions on Smart Grid*, 11(6):5099–5113.

[Arnold et al., 2022] Arnold, D., Saha, S. S., Ngo, S.-T., Roberts, C., Scaglione, A., Johnson, N. G., Peisert, S., and Pinney, D. (2022). Adaptive control of distributed energy resources for distribution grid voltage stability. *IEEE Transactions on Power Systems*, pages 1–1.

[Bottrell et al., 2013] Bottrell, N., Prodanovic, M., and Green, T. C. (2013). Dynamic stability of a microgrid with an active load. *IEEE Transactions on Power Electronics*, 28(11):5107–5119.

[Brown and Demarco, 2018] Brown, H. E. and Demarco, C. L. (2018). Risk of cyber-physical attack via load with emulated inertia control. *IEEE Transactions on Smart Grid*, 9(6):5854–5866.

[Cheng et al., 2022] Cheng, Y., Fan, L., Rose, J., Huang, F., Schmall, J., Wang, X., Xie, X., Shair, J., Ramamurthy, J., Modi, N., Li, C., Wang, C., Shah, S., Pal, B. C., Miao, Z., Isaacs, A., Mahseredjian, J., and Zhou, Z. J. (2022). Real-world subsynchronous oscillation events in power grids with high penetrations of inverter-based resources. *IEEE Transactions on Power Systems*, pages 1–1.

[DeMarco, 1998] DeMarco, C. (1998). Design of predatory generation control in electric power systems. In *Proceedings of the Thirty-First Hawaii International Conference on System Sciences*, volume 3, pages 32–38 vol.3.

[DeMarco et al., 1996] DeMarco, C., Sariashkar, J., and Alvarado, F. (1996). The potential for malicious control in a competitive power systems environment. In *Proceeding of the 1996 IEEE International Conference on Control Applications IEEE International Conference on Control Applications held together with IEEE International Symposium on Intelligent Contro*, pages 462–467.

[Fan, 2022] Fan, L. (2022). Inter-ibr oscillation modes. *IEEE Transactions on Power Systems*, 37(1):824–827.

[Hammad et al., 2015] Hammad, E., Khalil, A. M., Farraj, A., Kundur, D., and Iravani, R. (2015). Tuning out of phase: Resonance attacks. In *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 491–496.

[Hammad et al., 2018] Hammad, E., Khalil, A. M., Farraj, A., Kundur, D., and Iravani, R. (2018). A class of switching exploits based on inter-area oscillations. *IEEE Transactions on Smart Grid*, 9(5):4659–4668.

[Hatziargyriou et al., 2021] Hatziargyriou, N., Milanovic, J., Rahmann, C., Ajjarapu, V., Canizares, C., Erlich, I., Hill, D., Hiskens, I., Kamwa, I., Pal, B., Pourbeik, P., Sanchez-Gasca, J., Stankovic, A., Van Cutsem, T., Vittal, V., and Vournas, C. (2021). Definition and classification of power system stability – revisited & extended. *IEEE Transactions on Power Systems*, 36(4):3271–3281.

[Markovic, 2020] Markovic, U. (2020). *Towards reliable operation of converter-dominated power systems: Dynamics, optimization and control*. PhD thesis, ETH Zurich, Zurich.

[Markovic et al., 2021] Markovic, U., Stanojev, O., Aristidou, P., Vrettos, E., Callaway, D., and Hug, G. (2021). Understanding small-signal stability of low-inertia systems. *IEEE Transactions on Power Systems*, 36(5):3997–4017.

[Moore, 1976] Moore, B. (1976). On the flexibility offered by state feedback in multivariable systems beyond closed loop eigenvalue assignment. *IEEE Transactions on Automatic Control*, 21(5):689–692.

[Roberts et al., 2021] Roberts, C., Markovic, U., Arnold, D., and Callaway, D. S. (2021). Malicious control of an active load in an islanded mixed-source microgrid. In *2021 IEEE Madrid PowerTech*, pages 1–6.

[Sahoo et al., 2021] Sahoo, S., Dragičević, T., and Blaabjerg, F. (2021). Cyber security in control of grid-tied power electronic converters—challenges and vulnerabilities. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 9(5):5326–5340.

[Wang et al., 2015] Wang, X., Li, Y. W., Blaabjerg, F., and Loh, P. C. (2015). Virtual-impedance-based control for voltage-source and current-source converters. *IEEE Transactions on Power Electronics*, 30(12):7019–7037.

[Wu et al., 2018] Wu, Y., Wei, Z., Weng, J., Li, X., and Deng, R. H. (2018). Resonance attacks on load frequency control of smart grids. *IEEE Transactions on Smart Grid*, 9(5):4490–4502.