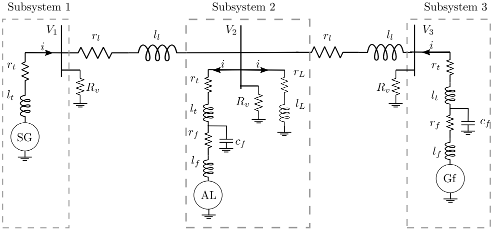
Understanding the Vulnerability of a Mixed-Source Microgrid to Malicious Control of an Active Load

SPADES Workshop
2^{nd} December 2020

Introduction

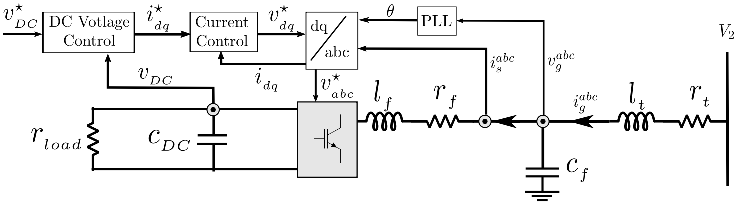
- Previous work examined malicious control for synchronous machine dominated bulk power system [1-3]
- We focus on mixed-source microgrid for two main reasons:
  - the relative size of individual loads may make it easier for an adversary to gain sufficient controllability
  - these systems are among the first to achieve very high penetration of converter-based generation
- We examine the use of eigenstructure assignment, eigenvalue and eigenvector design, to develop a feedback controller to destabilize a vulnerable mode of the system
  - Will consider two distinct attacks as well as two different levels of adversarial control within each attack

Microgrid Model



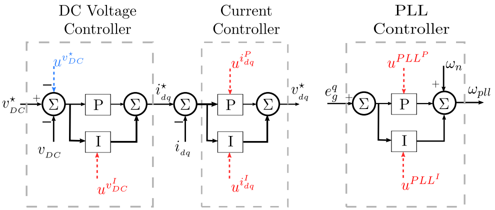
- Nominal loading of 1 p.u.
- Synchronous machine (SG), Active Load (AL), and Grid-following converter (Gf)
  - System has 80% penetration of Gf with AL 5% nominal active power
- State space $x \in \mathbb{R}^{46}$
  - $x^{SG} \in \mathbb{R}^{13}$, $x^{AL} \in \mathbb{R}^{12}$, $x^{Gf} \in \mathbb{R}^{15}$, $x^{PI} \in \mathbb{R}^{2}$, $x^{Net} \in \mathbb{R}^{4}$

Active Load



- AL consists three different PI control loops
  1. a phase-locked loop (PLL) for alignment of internal and network synchronously-rotating (*dq*) reference frame (SRF)
  2. an outer-loop voltage controller for maintaining a constant DC voltage across the DC-link capacitor
  3. and an inner-loop current controller for current tracking

Adversarial Level of Access



- For each attack we consider two different levels of adversarial control
    1. For setpoint control, the adversary only has the ability to change the DC voltage setpoint. In this case, we have that the input $u \in \mathbb{R}$.
    2. For full control, the adversary has full access to the inner control loops and, therefore, $u \in \mathbb{R}^5$.
- The dimension of the input will determine the flexibility in designing the eigenvector(s) for the unstable eigenvalue(s)

Adversarial Objective

We linearize our set of non-linear equations about an operating point to give us

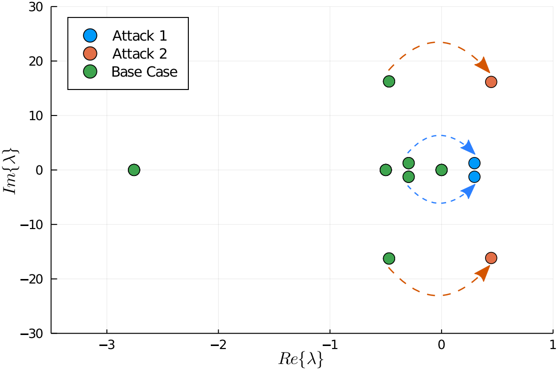
$$\Delta \dot{\boldsymbol{x}} = \boldsymbol{A}\Delta \boldsymbol{x} + \boldsymbol{B}\Delta \boldsymbol{u}, \tag{1}$$

We want to design a linear state feedback controller for the AL to force a stable mode of $\boldsymbol{A}$ to become unstable wile minimizing the participation of the AL in this new unstable mode. The participation of state i in mode j is defined as

$$p_{ij} = \frac{w_{ij} v_{ji}}{\boldsymbol{w}_j^T \boldsymbol{v}_j}, \tag{2}$$

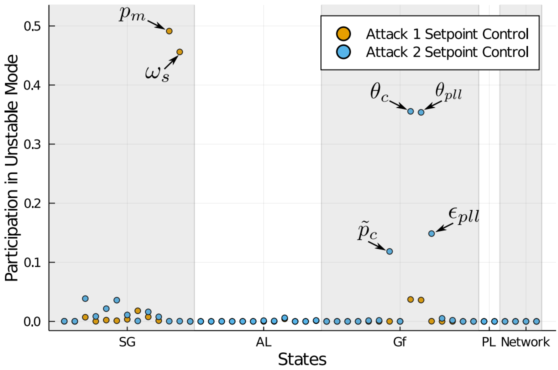
were w and v are the left and right eigenvectors respectively. We will optimize the elements of the eigenvector $\hat{v}$, corresponding to the desired unstable eigenvalue $\hat{\lambda}$, to minimize the participation of the AL in the unstable mode[2]. (See Appendix)

Destabilizing Modes



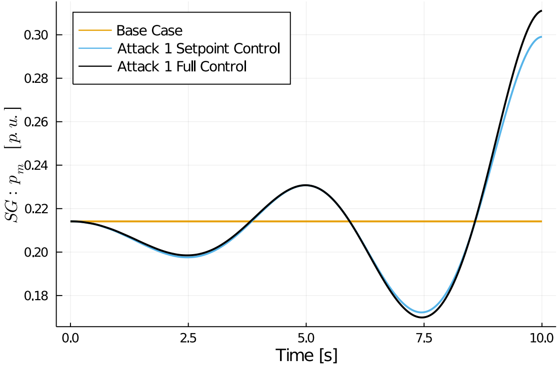
- Attack 1: $\lambda = -0.29 \pm 1.279j \rightarrow \hat{\lambda} = 0.29 \pm 1.279j$
- Attack 2: $\lambda = -0.45 \pm 16.16j \rightarrow \hat{\lambda} = 0.45 \pm 16.16j$

Participation Factors for Unstable Mode



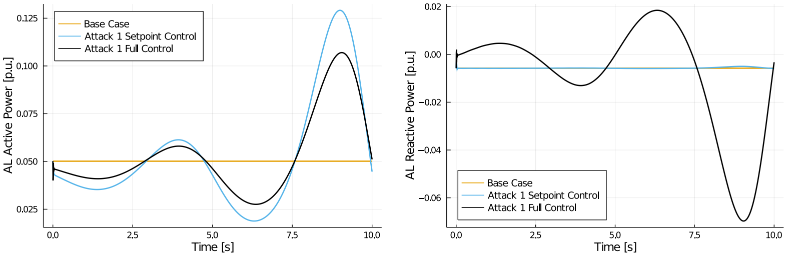
- Attack 1: SG mechanical power, p_m and angular frequency, ω_s are the dominant states
- Attack 2: The states for the Gf active power controller and PLL are dominant states

Attack 1: SG Behavior



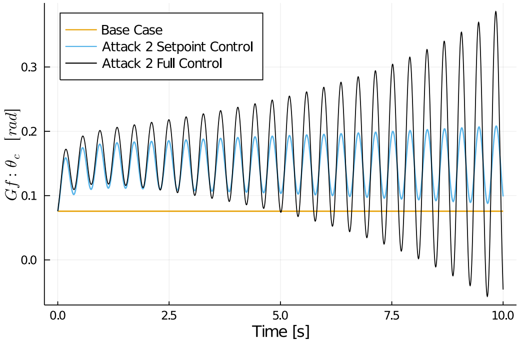
- Attack 1 is largely SG based and closely resembles attack reported in prior work
- Similar behavior for both levels of adversarial access considered

Attack 1: AL Behavior



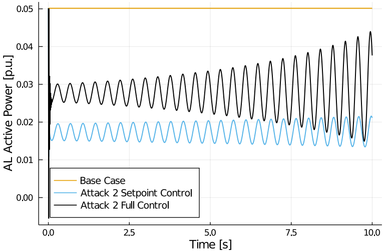
- Full control allows adversary to independently control active and reactive power
  - Setpoint control can only affect the active power demand
- For full control, AL appears capacitive when maximizing active power demand
  - Raising/lowering the voltage the voltage dependency of the constant impedance load

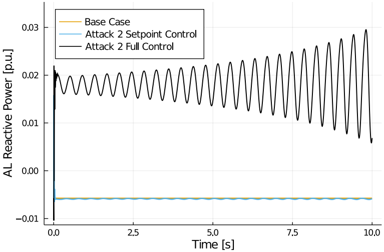
Attack 2: Gf Behavior



- Attack 2 is largely Gf based and is first identified in this work
- Response very different for each level of access
  - Oscillation grows at a much faster rate for case of full control

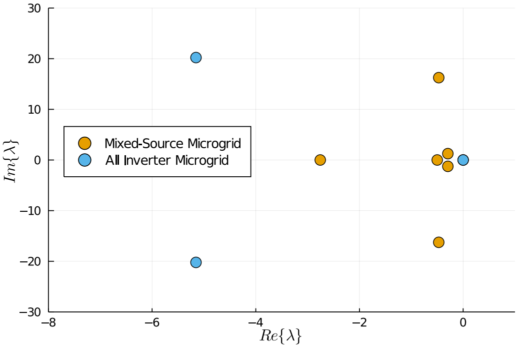
Attack 2: AL Behavior





- Similar to previous attack, setpoint control only controls active power
- In the case, full control exerts less control effort to induce instability
  - Both active power and reactive power oscillation magnitude ≈2-3%

Hardening the System



- What if we replace synchronous machine with a grid-forming inverter?
- Initial analysis suggests we increase the stability boundary and harden the system against the particular attack vector considered

Future Work

- Consideration of more sophisticated adversarial attacks, e.g. non-linear controllers characterized by neural networks
- Impact of microgrid composition, i.e. continual examination of grid following vs grid forming, different levels of synchronous generation
- Examination of adaptive paramertization of controllers to increase stability margin

Appendix

Once we have identified a candidate mode to be destabilized with a desired eigenvalue $\hat{\lambda}$, we begin by constructing the corresponding Hautus matrix $\boldsymbol{S}_{\hat{\lambda}}$ given by

$$\boldsymbol{S}_{\hat{\lambda}} = [(\hat{\lambda}\boldsymbol{I} - \boldsymbol{A}) \quad \boldsymbol{B}] \tag{3}$$

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

$$\boldsymbol{K}_{\hat{\lambda}} = \begin{bmatrix} \boldsymbol{N}_{\hat{\lambda}} \\ \boldsymbol{M}_{\hat{\lambda}} \end{bmatrix}, \tag{4}$$

whose columns form a basis for nullspace of $\boldsymbol{S}_{\hat{\lambda}}$. $\boldsymbol{N}_{\hat{\lambda}} \in \mathbb{R}^{n\times m}$ and $\boldsymbol{M}_{\hat{\lambda}} \in \mathbb{R}^{m\times m}$.

Appendix

The eigenvector $\hat{\boldsymbol{v}}$, is then expressed as

$$\hat{\boldsymbol{v}} = \boldsymbol{N}_{\hat{\lambda}} \boldsymbol{k} \tag{5}$$

for some $\boldsymbol{k} \in \mathbb{R}^{m \times 1}$. 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. 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.

$$\begin{aligned} \max_{\boldsymbol{k}} \quad & \frac{\boldsymbol{k}'[\boldsymbol{N}_{\hat{\lambda} T}]' \boldsymbol{N}_{\hat{\lambda} T} \boldsymbol{k}}{\boldsymbol{k}'[\boldsymbol{N}_{\hat{\lambda} C}]' \boldsymbol{N}_{\hat{\lambda} C} \boldsymbol{k}} \\ \text{s.t.} \quad & \boldsymbol{k}' \boldsymbol{k} = 1, \end{aligned} \tag{6}$$

Appendix

Defining the matrices $\boldsymbol{G}$ and $\boldsymbol{H}$ as

$$\boldsymbol{G} = [\boldsymbol{N}_{\hat{\lambda}T}]'\boldsymbol{N}_{\hat{\lambda}T} \quad \boldsymbol{H} = [\boldsymbol{N}_{\hat{\lambda}C}]'\boldsymbol{N}_{\hat{\lambda}C}, \tag{7}$$

we rewrite this optimization as

$$\max_{\boldsymbol{\nu}} \frac{\boldsymbol{\nu}'(\boldsymbol{H}^{-1/2})^T \boldsymbol{G}\boldsymbol{H}^{-1/2}\boldsymbol{\nu}}{\boldsymbol{\nu}'\boldsymbol{\nu}}. \tag{8}$$

The optimal design vector $\boldsymbol{k}^\star$ is constructed using the eigenvector $\boldsymbol{\nu}_{max}$ corresponding to the largest eigenvalue of (8), and is given by

$$\boldsymbol{k}^\star = \boldsymbol{H}^{-1/2}\boldsymbol{\nu}_{max}. \tag{9}$$

Appendix

We then construct the feedback matrix $\boldsymbol{F}$ follows. Let us define

$$\hat{\boldsymbol{w}} = \boldsymbol{M}_{\hat{\lambda}} \boldsymbol{k}^{\star}\,,\ \hat{\boldsymbol{v}} = \boldsymbol{N}_{\hat{\lambda}} \boldsymbol{k}^{\star}, \tag{10}$$

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

$$\boldsymbol{W} = [Re\{\hat{\boldsymbol{w}}\}\ Im\{\hat{\boldsymbol{w}}\}\ 0\ \ldots\ 0], \tag{11a}$$

$$\boldsymbol{V} = [Re\{\hat{\boldsymbol{v}}\}\ Im\{\hat{\boldsymbol{v}}\}\ Re\{\boldsymbol{v}_3\}\ Im\{\boldsymbol{v}_3\}\ \ldots\ \boldsymbol{v}_{n-1}\ \boldsymbol{v}_n], \tag{11b}$$

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 (1). The feedback matrix $\boldsymbol{F}$ is then given by

$$F = \boldsymbol{W}\boldsymbol{V}^{-1}. \tag{12}$$

References

1. DeMarco, Christopher L., J. V. Sariashkar, and Fernando Alvarado. "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, pp. 462-467. IEEE, 1996.
2. DeMarco, Christopher L. "Design of predatory generation control in electric power systems." In Proceedings of the Thirty-First Hawaii International Conference on System Sciences, vol. 3, pp. 32-38. IEEE, 1998.
3. Brown, Hilary E., and Christopher L. DeMarco. "Risk of cyber-physical attack via load with emulated inertia control." IEEE Transactions on Smart Grid 9, no. 6 (2017): 5854-5866.