The Observability Radius of Network Systems

Minimum-norm structured perturbations preventing observability

G. Bianchin **P. Frasca** A. Gasparri F. Pasqualetti

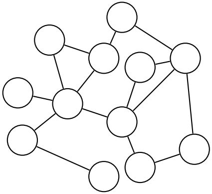
NeCS meeting
Grenoble, France
November 2, 2016

Perturbations against observability

- Dynamical network described by

$$\text{graph } \mathcal{G} = (\mathcal{V}, \mathcal{E})$$
$$x(t+1) = A\,x(t)$$

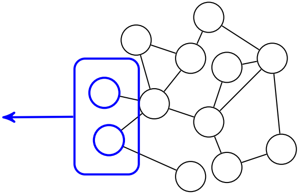
A is consistent with the graph



Perturbations against observability

- Dynamical network described by

$$\text{graph } \mathcal{G} = (\mathcal{V}, \mathcal{E})$$
$$x(t+1) = A\,x(t)$$
$$A \text{ is consistent with the graph}$$



- Monitored by sensor nodes $\mathcal{O} \subseteq \mathcal{V}$

$$y(t) = C_{\mathcal{O}} x(t)$$

Perturbations against observability

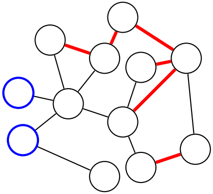
- Dynamical network described by

$$\begin{aligned} &\text{graph } \mathcal{G} = (\mathcal{V}, \mathcal{E}) \\ &x(t+1) = A\,x(t) \\ &\quad A \text{ is consistent with the graph} \end{aligned}$$

- Monitored by sensor nodes $\mathcal{O} \subseteq \mathcal{V}$

$$y(t) = C_{\mathcal{O}} x(t)$$

- Attacks/failures occur at some edges $\mathcal{M} \subseteq \mathcal{E}$



Perturbations against observability

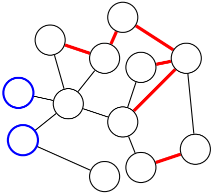
- Dynamical network described by

$$\text{graph } \mathcal{G} = (\mathcal{V}, \mathcal{E})$$
$$x(t+1) = A\,x(t)$$
$$A \text{ is consistent with the graph}$$

- Monitored by sensor nodes $\mathcal{O} \subseteq \mathcal{V}$

$$y(t) = C_{\mathcal{O}} x(t)$$

- Attacks/failures occur at some edges $\mathcal{M} \subseteq \mathcal{E}$



Perturbations against observability

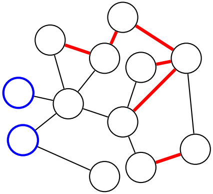
- Dynamical network described by

$$\text{graph } \mathcal{G} = (\mathcal{V}, \mathcal{E})$$
$$x(t+1) = A\,x(t)$$
$$A \text{ is consistent with the graph}$$

- Monitored by sensor nodes $\mathcal{O} \subseteq \mathcal{V}$

$$y(t) = C_{\mathcal{O}} x(t)$$

- Attacks/failures occur at some edges $\mathcal{M} \subseteq \mathcal{E}$



- Can the adversary make the dynamics unobservable?
- How large the perturbation must be?

Topics in this talk

1. Observability radius: from classical systems to networks
   - The observability radius of linear systems
   - The observability radius of network systems
2. An algorithm for the observability radius
3. The role of topology: networks with random weights
4. Attacks on power systems

Classical observability radius

Before perturbation, (A, C) is observable

$$\begin{aligned} x(t+1) =& A\,x(t) \\ y(t) =& C\,x(t) \end{aligned}$$

The observability radius is

$$\mu(A, C) = \min_{\Delta_A, \Delta_C} \left\| \begin{bmatrix} \Delta_A \\ \Delta_C \end{bmatrix} \right\|_2,$$

$$\text{s.t. } (A + \Delta_A, C + \Delta_C) \text{ is unobservable}$$

Classical observability radius

Before perturbation, (A, C) is observable

$$\begin{aligned} x(t+1) =& A\,x(t) \\ y(t) =& C\,x(t) \end{aligned}$$

The observability radius is

$$\mu(A, C) = \min_{\Delta_A, \Delta_C} \left\| \begin{bmatrix} \Delta_A \\ \Delta_C \end{bmatrix} \right\|_2 ,$$

$$\text{s.t. } (A + \Delta_A, C + \Delta_C) \text{ is unobservable}$$

Typical result: $\mu(A, C) = \min_{s \in \mathbb{C}} \sigma_n \left(\begin{bmatrix} sI - A \\ C \end{bmatrix} \right)$

R. Eising. Between controllable and uncontrollable. *Systems & Control Letters*, 4(5):263–264, 1984

Shortcomings:

- unstructured: Δ_A and Δ_C are full matrices
- both A and C are perturbed
- 2-norm does not quantify the effort of an attacker

Our problem: perturbations of dynamical networks

Localized observation matrix:

$\mathcal{O} = \{o_1, \ldots, o_p\}$ and $C_{\mathcal{O}} = \begin{bmatrix} e_{o_1} & \cdots & e_{o_p} \end{bmatrix}^\top$

The network observability radius is

$$\min_{\Delta} \|\Delta\|_F^2 ,$$

$$\text{s.t. } (A + \Delta, C_{\mathcal{O}}) \text{ is unobservable}$$

$$\Delta \cdot M = 0$$

where

- *structure* is imposed: $M_{ij} = 0$ if $(i,j) \in \mathcal{M}$, $M_{ij} = 1$ if $(i,j) \notin \mathcal{M}$
  $\cdot$ is entrywise product
- Frobenius norm $||\Delta||_F^2 = \sum_{i,j} \delta_{ij}^2$ is chosen
- only A is perturbed

Computing the observability radius

Computing the observability radius

More explicitly:

$\min_{\Delta,\lambda,x}$	$\|\|\Delta\|\|_F^2$	Frobenius norm
s.t.	$C_{\mathcal{O}} x = 0$	unobservability
	$(A+\Delta)x = \lambda x$	eigenvalue constraint
	$\|x\|_2 = 1$	normalization
	$\Delta \cdot M = 0$	structural constraint

Comments:

- The optimization is performed over Δ, λ, and x
- Not convex
- Not always feasible (feasible if $\mathcal{M} = \mathcal{E}$)
- Since (A, C) is observable, Δ must be nonzero

Idea for an algorithm

Step 1: Fix λ and solve

$$\min_{x,\Delta} ||\Delta||_F^2$$

$$\text{s.t.} \quad C_{\mathcal{O}} x = 0$$
$$(A + \Delta)x = \lambda x$$
$$\|x\|_2 = 1$$
$$\Delta \cdot M = 0$$

Step 2: Search for the best $\lambda \in \mathbb{C}$

Exhaustive search seems unavoidable:

G. Hu and E. J. Davison. Real controllability/stabilizability radius of LTI systems. *IEEE Transactions on Automatic Control*, 49(2):254–257, 2004

Algorithm (Step 1)

Derivation (sketch):

1. Incorporate structural constraints in $||\Delta||_F^2$ (approximately)

$$\text{cost: } \sum_{i=1}^{n}\sum_{j=1}^{n}\delta_{ij}^2 \longrightarrow \sum_{i=1}^{n}\sum_{j=1}^{n}\delta_{ij}^2(1-m_{ij})^{-1}$$

Algorithm (Step 1)

Derivation (sketch):

1. Incorporate structural constraints in $||\Delta||_F^2$ (approximately)

$$\text{cost: } \sum_{i=1}^{n}\sum_{j=1}^{n}\delta_{ij}^2 \longrightarrow \sum_{i=1}^{n}\sum_{j=1}^{n}\delta_{ij}^2(1-m_{ij})^{-1}$$

2. Decompose $\lambda = \lambda_{\Re} + \mathrm{i}\lambda_{\Im}$, $x = x_{\Re} + \mathrm{i}x_{\Im}$ and divide real and imaginary parts

Algorithm (Step 1)

Derivation (sketch):

1. Incorporate structural constraints in $||\Delta||_F^2$ (approximately)

$$\text{cost: } \sum_{i=1}^{n}\sum_{j=1}^{n}\delta_{ij}^2 \longrightarrow \sum_{i=1}^{n}\sum_{j=1}^{n}\delta_{ij}^2(1-m_{ij})^{-1}$$

2. Decompose $\lambda = \lambda_{\Re} + \mathrm{i}\lambda_{\Im}$, $x = x_{\Re} + \mathrm{i}x_{\Im}$ and divide real and imaginary parts
3. Define Lagrange multipliers for the other constraints and write $\nabla\mathcal{L} = 0$

Algorithm (Step 1)

Derivation (sketch):

1. Incorporate structural constraints in $||\Delta||_F^2$ (approximately)

   $$\text{cost: } \sum_{i=1}^{n}\sum_{j=1}^{n}\delta_{ij}^2 \longrightarrow \sum_{i=1}^{n}\sum_{j=1}^{n}\delta_{ij}^2(1-m_{ij})^{-1}$$

2. Decompose $\lambda = \lambda_{\Re} + \mathrm{i}\lambda_{\Im}$, $x = x_{\Re} + \mathrm{i}x_{\Im}$ and divide real and imaginary parts
3. Define Lagrange multipliers for the other constraints and write $\nabla\mathcal{L} = 0$
4. Rewrite as generalized nonlinear eigenvalue problem:

   finding scalar σ and vector z such that $Hz = \sigma K_z z$

Algorithm (Step 1)

Derivation (sketch):

1. Incorporate structural constraints in $||\Delta||_F^2$ (approximately)

$$\text{cost: } \sum_{i=1}^{n}\sum_{j=1}^{n}\delta_{ij}^2 \longrightarrow \sum_{i=1}^{n}\sum_{j=1}^{n}\delta_{ij}^2(1-m_{ij})^{-1}$$

2. Decompose $\lambda = \lambda_{\Re} + \mathrm{i}\lambda_{\Im}$, $x = x_{\Re} + \mathrm{i}x_{\Im}$ and divide real and imaginary parts
3. Define Lagrange multipliers for the other constraints and write $\nabla\mathcal{L} = 0$
4. Rewrite as generalized nonlinear eigenvalue problem:

   finding scalar σ and vector z such that $Hz = \sigma K_z z$

Algorithm (Step 1)

Derivation (sketch):

1. Incorporate structural constraints in $||\Delta||_F^2$ (approximately)

$$\text{cost: } \sum_{i=1}^{n}\sum_{j=1}^{n}\delta_{ij}^2 \longrightarrow \sum_{i=1}^{n}\sum_{j=1}^{n}\delta_{ij}^2(1-m_{ij})^{-1}$$

2. Decompose $\lambda = \lambda_{\Re} + \mathrm{i}\lambda_{\Im}$, $x = x_{\Re} + \mathrm{i}x_{\Im}$ and divide real and imaginary parts
3. Define Lagrange multipliers for the other constraints and write $\nabla\mathcal{L} = 0$
4. Rewrite as generalized nonlinear eigenvalue problem:

   finding scalar σ and vector z such that $Hz = \sigma K_z z$

Solve it iteratively by "freezing" the nonlinearity K_z (inverse iteration method)

If convergent, the algorithm gives a suboptimal solution

Based on ideas from

B. De Moor. Total least squares for affinely structured matrices and the noisy realization problem. *IEEE Transactions on Signal Processing*, 42(11):3104–3113, 1994

Networks with random weights

The effect of disconnecting cuts

Define the minimal observability-preventing perturbation as

$$\delta := \min_{\lambda, x, \Delta} \|\Delta\|_F$$

$$\text{s.t.} \quad C_{\mathcal{O}} x = 0$$

$$(A + \Delta)x = \lambda x$$

$$\|x\|_2 = 1$$

$$\Delta \cdot M = 0 \quad (\mathcal{M} = \mathcal{E})$$

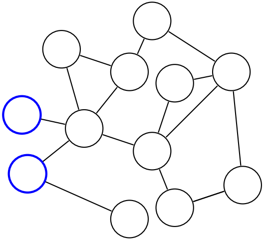
If a_{ij} are independent random variables uniformly distributed in $[0, 1]$, then

$$\mathbb{E}[\delta] \leq \frac{\Gamma(1/k)}{\sqrt{k}} \frac{\Gamma(\omega + 1)}{\Gamma(\omega + 1 + 1/k)}$$

where

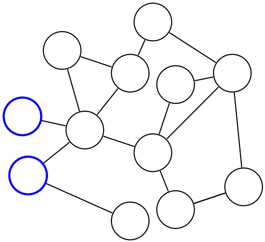
- $\Gamma(z) = \int_0^\infty x^{z-1} e^{-x} \, dx$ is the Gamma function
- $\Omega_k(\mathcal{O})$ is a collection of disjoint cuts of size k, where each cut disconnects a non-empty subset of nodes from $\mathcal{O}$
- $\omega = |\Omega_k(\mathcal{O})|$ is the number of such cuts

Example of application



Looking for disconnecting cuts. . .

Example of application



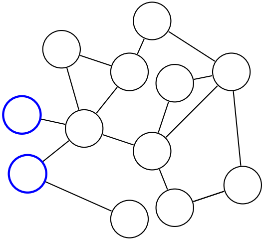
Looking for disconnecting cuts...

Note:

- The *number* of disconnecting cuts is essential:

$$\frac{\Gamma(1/k)}{\sqrt{k}} \frac{\Gamma(\omega+1)}{\Gamma(\omega+1+1/k)} \geq 0.8 \frac{1}{\omega+1}, \quad \text{increasing in } k$$

Example of application



Looking for disconnecting cuts. . .

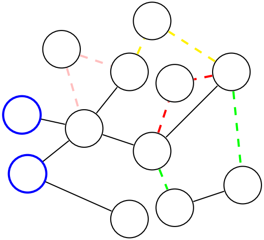
Note:

- The *number* of disconnecting cuts is essential:

$$\frac{\Gamma(1/k)}{\sqrt{k}} \frac{\Gamma(\omega+1)}{\Gamma(\omega+1+1/k)} \geq 0.8 \frac{1}{\omega+1}, \quad \text{increasing in } k$$

- To have a small bound, we need many small cuts

Example of application



Looking for disconnecting cuts. . .

$k = 2, \omega = 4 \Longrightarrow$

$$\mathbb{E}[\delta] \leq \frac{\Gamma(1/2)}{\sqrt{2}} \frac{\Gamma(5)}{\Gamma(5 + 1/2)} = 0.5747$$

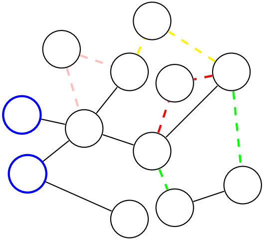
Note:

- The *number* of disconnecting cuts is essential:

$$\frac{\Gamma(1/k)}{\sqrt{k}} \frac{\Gamma(\omega + 1)}{\Gamma(\omega + 1 + 1/k)} \geq 0.8 \frac{1}{\omega + 1}, \quad \text{increasing in } k$$

- To have a small bound, we need many small cuts

Example of application



Looking for disconnecting cuts...

$k = 2, \omega = 4 \implies$

$$\mathbb{E}[\delta] \leq \frac{\Gamma(1/2)}{\sqrt{2}} \frac{\Gamma(5)}{\Gamma(5 + 1/2)} = 0.5747$$

Note:

- The *number* of disconnecting cuts is essential:

$$\frac{\Gamma(1/k)}{\sqrt{k}} \frac{\Gamma(\omega + 1)}{\Gamma(\omega + 1 + 1/k)} \geq 0.8 \frac{1}{\omega + 1}, \quad \text{increasing in } k$$

- To have a small bound, we need many small cuts
- Often, the best choice is just isolating single nodes

Large networks

Consider a sequence of networks with increasing size $n \to \infty$:
If $\omega \to \infty$ and k constant, then

$$\frac{\Gamma(1/k)\,\Gamma(\omega+1)}{\sqrt{k}\,\Gamma(\omega+1+1/k)} \sim \frac{\Gamma(1/k)}{\sqrt{k}}\frac{1}{(\omega+1)^{1/k}}$$

The network becomes less robust to perturbations as the size of the network increases, with a rate determined by k

Large networks

Consider a sequence of networks with increasing size $n \to \infty$:
If $\omega \to \infty$ and k constant, then

$$\frac{\Gamma(1/k)\,\Gamma(\omega+1)}{\sqrt{k}\,\Gamma(\omega+1+1/k)} \sim \frac{\Gamma(1/k)}{\sqrt{k}}\frac{1}{(\omega+1)^{1/k}}$$

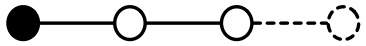
The network becomes less robust to perturbations as the size of the network increases, with a rate determined by k

Questions:

- Is the bound tight?
- How do optimal perturbations look like?

The role of graph topology: Examples

Line network



Line is strongly structurally observable

$\Downarrow$

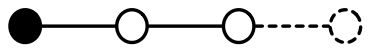
Best perturbation is disconnecting

$$\delta = \max_i \{a_{i,i+1}\}$$

$$\mathbb{E}[\delta(n)] = \frac{1}{n}$$

The role of graph topology: Examples

Line network



Line is strongly structurally observable

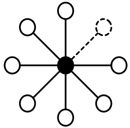
$\Downarrow$

Best perturbation is disconnecting

$$\delta = \max_i \{a_{i,i+1}\}$$

$$\mathbb{E}[\delta(n)] = \frac{1}{n}$$

Star network



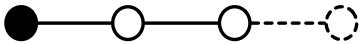
Best perturbation introduces an artificial symmetry

$$\delta = \min_{i,j\geq 2, i\neq j} \frac{|a_{ii} - a_{jj}|}{\sqrt{2}}$$

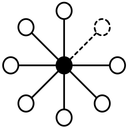
$$\mathbb{E}[\delta(n)] \sim \frac{1}{\sqrt{2}\, n^2} \quad \text{as } n \to \infty$$

The role of graph topology: Examples

Line network



Star network



Line is strongly structurally observable

$\Downarrow$

Best perturbation is disconnecting

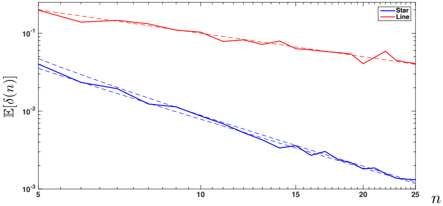
$$\delta = \max_i \{a_{i,i+1}\}$$

$$\mathbb{E}[\delta(n)] = \frac{1}{n}$$

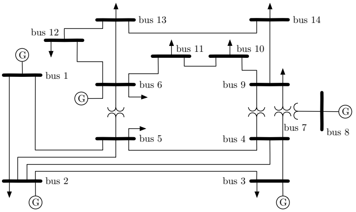
Best perturbation introduces an artificial symmetry

$$\delta = \min_{i,j \geq 2, i \neq j} \frac{|a_{ii} - a_{jj}|}{\sqrt{2}}$$

$$\mathbb{E}[\delta(n)] \sim \frac{1}{\sqrt{2}\, n^2} \quad \text{as } n \to \infty$$



Real example



IEEE 14 grid observed from bus 1

Small-signal model is linear descriptor system

$$\underbrace{\begin{bmatrix} I & 0 & 0 \\ 0 & M_g & 0 \\ 0 & 0 & 0 \end{bmatrix}}_{E} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \\ \dot{\theta} \end{bmatrix} = -\underbrace{\begin{bmatrix} 0 & -I & 0 \\ \mathcal{S}_{gg} & D_g & \mathcal{S}_{gl} \\ \mathcal{S}_{lg} & 0 & \mathcal{S}_{ll} \end{bmatrix}}_{A} \begin{bmatrix} \delta \\ \omega \\ \theta \end{bmatrix} + \begin{bmatrix} 0 \\ P_\omega \\ P_\theta \end{bmatrix}$$

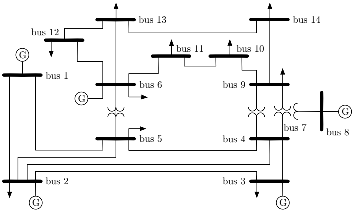
δ: generator rotor angles

ω: generator rotor frequencies

θ: voltage angles at the buses

Goal: inducing an unobservable unstable mode

Attacks on power systems



IEEE 14 grid observed from bus 1

Small-signal model is linear descriptor system

$$\underbrace{\begin{bmatrix} I & 0 & 0 \\ 0 & M_\mathrm{g} & 0 \\ 0 & 0 & 0 \end{bmatrix}}_{E} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \\ \dot{\theta} \end{bmatrix} = - \underbrace{\begin{bmatrix} 0 & -I & 0 \\ \mathcal{S}_\mathrm{gg} & D_\mathrm{g} & \mathcal{S}_\mathrm{gl} \\ \mathcal{S}_\mathrm{lg} & 0 & \mathcal{S}_\mathrm{ll} \end{bmatrix}}_{A} \begin{bmatrix} \delta \\ \omega \\ \theta \end{bmatrix} + \begin{bmatrix} 0 \\ P_\omega \\ P_\theta \end{bmatrix}$$

δ: generator rotor angles
ω: generator rotor frequencies
θ: voltage angles at the buses

Goal: inducing an unobservable unstable mode

Perturbation	$\|\Delta\|_F$	Unobservable mode
Disconnect load 1 ($[\mathcal{S}_\mathrm{ll}]_{1,2} = 0$)	4.60	10.92
Stop generator 1 ($\dot{\delta}_1 = 0$)	2.59	$10.92 \pm 20.95j$
Modify impedance (53 lines modified)	2.34	$10.92 \pm 10^4 j$

Creating artificial dynamical symmetries seems to require smaller perturbations than disconnecting the network

Conclusion

Summary

1. New resilience measure for network systems
   - extending classical observability radius
2. Formulation as optimization problem
   - heuristic algorithm for its solution
3. Study of networks with random weights
   - focus on network topology
   - different types of graphs $\longrightarrow$ different observability radii

Note: everything can be translated to controllability

Conclusion

Summary

1. New resilience measure for network systems
   - extending classical observability radius
2. Formulation as optimization problem
   - heuristic algorithm for its solution
3. Study of networks with random weights
   - focus on network topology
   - different types of graphs $\longrightarrow$ different observability radii

Note: everything can be translated to controllability

Open problems

- Effective computation of radius δ
- Refine the upper bound on $\mathbb{E}[\delta]$
- Find a lower bound on $\mathbb{E}[\delta]$
- Find more tractable examples (complete graph, grids?)
- Study other random network models
- Apply to more realistic networks