The Observability Radius of Network Systems

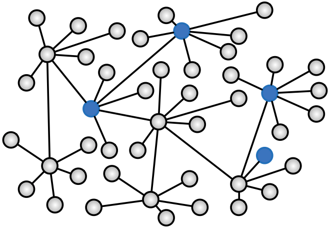
Minimum norm perturbations that prevent observability

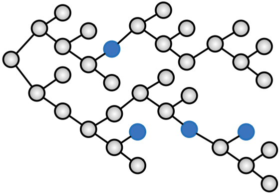
G. Bianchin[1], P. Frasca[2], A. Gasparri[3], and F. Pasqualetti[1]

[1]University of California, Riverside
[2]University of Twente
[3]Roma Tre University

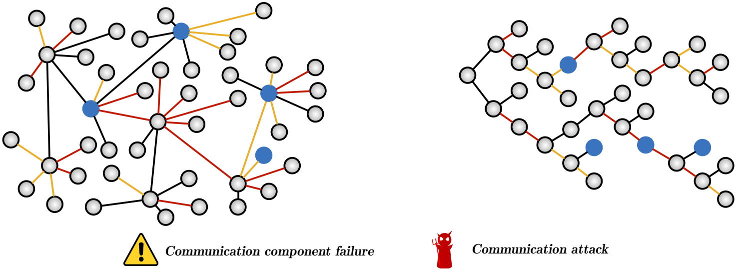
July 6, 2016

In this talk...





In this talk...



Which network is more resilient to communication components failures or attacks, in terms of state reconstruction capabilities ?

- Networks Observability

In this talk... (2)

Network systems robustness to different contingencies :

- Communication components failures
- Variations in network weights : unmodeled uncertainties, attacks

We aim at measuring robustness in terms of :

- Size of smallest perturbation needed to prevent observability

We incorporate the topology in the study

- Require the perturbation to match with structural constraints :

Outline

Preliminary : Perturbations that prevent observability

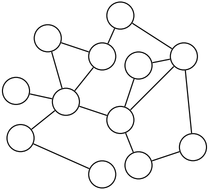
- Network $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ described by

$$x(t+1) = Ax(t)$$

- 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 is the perturbation required to be ?

Preliminary : Perturbations that prevent observability

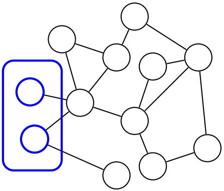
- Network $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ described by

$$x(t+1) = Ax(t)$$

- 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 is the perturbation required to be ?

Preliminary : Perturbations that prevent observability

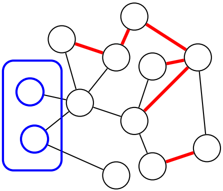
- Network $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ described by

$$x(t+1) = Ax(t)$$

- 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 is the perturbation required to be ?

Preliminary : Perturbations that prevent observability

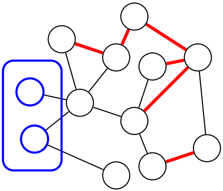
- Network $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ described by

$$x(t+1) = Ax(t)$$

- 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 is the perturbation required to be ?

Preliminary : The observability radius

Before perturbation, $(A, C_{\mathcal{O}})$ is observable

$$\begin{aligned} x(t+1) &= Ax(t) \\ y(t) &= C_{\mathcal{O}} x(t) \end{aligned}$$

The network observability radius is

$$\begin{aligned} \min_{\Delta} \; & \|\Delta\|_F^2 \\ \text{s.t.} \; & (A+\Delta, C_{\mathcal{O}}) \text{ is unobservable} \\ & \Delta \in \mathcal{A}_H \end{aligned}$$

- *A* only is perturbed
- Structure is imposed : Δ must be compatible with a *constraint graph*
- Frobenius norm $\|\Delta\|_F^2 = \sum_{i,j} \delta_{ij}^2$ is chosen

Preliminary : The observability radius

Before perturbation, $(A, C_{\mathcal{O}})$ is observable

$$\begin{aligned} x(t+1) =& Ax(t) \\ y(t) =& C_{\mathcal{O}}x(t) \end{aligned}$$

The network observability radius is

$$\begin{aligned} &\min_{\Delta} \|\Delta\|_F^2 \\ &\text{s.t.} \quad (A+\Delta, C_{\mathcal{O}}) \text{ is unobservable} \\ &\qquad \Delta \in \mathcal{A}_H \end{aligned}$$

- A only is perturbed
- Structure is imposed : Δ must be compatible with a *constraint graph*
- Frobenius norm $\|\Delta\|_F^2 = \sum_{i,j} \delta_{ij}^2$ is chosen

Computing the observability radius

More explicitly :

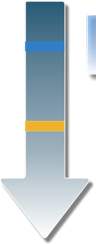
$$
\begin{array}{lll}
\min_{\Delta,\lambda,x} & ||\Delta||_F^2 & \text{Frobenius norm} \\
\text{s.t.} & C_{\mathcal{O}} x = 0 & \text{unobservability} \\
 & (A+\Delta)x = \lambda x & \text{eigenvalue constraint} \\
 & \|x\|_2 = 1 & \text{normalization} \\
 & \Delta \in \mathcal{A}_H & \text{structural constraint}
\end{array}
$$

- The optimization is performed over Δ and λ, x
- Not convex
- Not necessarily feasible
- Because $(A, C_{\mathcal{O}})$ is observable, Δ must be nonzero

Solving the optimization

Proposed approach

Two steps approach :



Solve the optimization for a fixed λ

Proposed approach

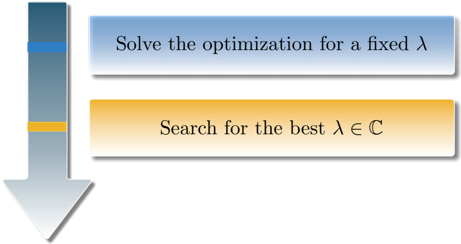
Two steps approach :

Solve the optimization for a fixed λ

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

Proposed approach

Two steps approach :



1. Exhaustive search seems unavoidable :

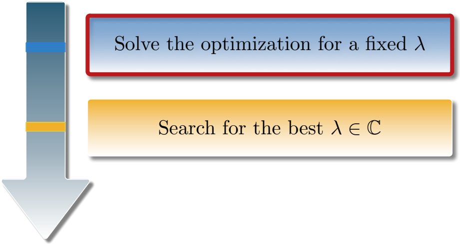
   Guangdi Hu and Edward J Davison. Real controllability/stabilizability radius of lti systems. *IEEE transactions on automatic control*, 49(2):254–257, 2004

2. For some topologies optimal λ can be found analytically

3. The choice of λ may be guided by the application

Proposed approach

Two steps approach :



1. Exhaustive search seems unavoidable :

   Guangdi Hu and Edward J Davison. Real controllability/stabilizability radius of lti systems. *IEEE transactions on automatic control*, 49(2):254–257, 2004

2. For some topologies optimal λ can be found analytically

3. The choice of λ may be guided by the application

Optimization solution (1)

Step 1

Incorporate structural constraints in $||\Delta||_F^2$:

$$||\Delta||_F^2 = \sum_{i=1}^{n}\sum_{j=1}^{n}(b_{ij} - a_{ij})^2 v_{ij}^{-1}, \qquad v_{ij} \in \{0, 1\}$$

and the observability constraint

$$(A + \Delta) := B \quad \Rightarrow \quad Bx = \lambda x$$

Optimization solution (1)

Step 1

Incorporate structural constraints in $||\Delta||_F^2$:

$$||\Delta||_F^2 = \sum_{i=1}^{n}\sum_{j=1}^{n}(b_{ij}-a_{ij})^2 v_{ij}^{-1}, \qquad v_{ij}\in\{0,1\}$$

and the observability constraint

$$(A+\Delta) := B \quad \Rightarrow \quad Bx = \lambda x$$

Step 2

We decompose $\lambda = \lambda_{\Re} + \mathrm{i}\lambda_{\Im}$ and $x = x_{\Re} + \mathrm{i}x_{\Im}$ and rewrite an equivalent optimization problem:

$$\|\bar{\Delta}^*\|_{\mathrm{F}}^2 = \min_{\bar{B},x_{\Re}^2,x_{\Im}^2} \quad \textstyle\sum_{i=1}^{n}\sum_{p+1}^{n}(\bar{b}_{ij}-\bar{a}_{ij})^2 v_{ij}^{-1},$$

$$\text{s.t.} \qquad \begin{bmatrix}\bar{B}-\bar{N} & \bar{M}\\ -\bar{M} & \bar{B}-\bar{N}\end{bmatrix}\begin{bmatrix}x_{\Re}^2\\ x_{\Im}^2\end{bmatrix} = 0$$

Optimization solution (1)

Step 1

Incorporate structural constraints in $||\Delta||_F^2$:

$$||\Delta||_F^2 = \sum_{i=1}^{n}\sum_{j=1}^{n}(b_{ij}-a_{ij})^2 v_{ij}^{-1}, \qquad v_{ij}\in\{0,1\}$$

and the observability constraint

$$(A+\Delta) := B \quad \Rightarrow \quad Bx = \lambda x$$

Step 2

We decompose $\lambda = \lambda_{\Re} + \mathrm{i}\lambda_{\Im}$ and $x = x_{\Re} + \mathrm{i}x_{\Im}$ and rewrite an equivalent optimization problem:

$$\|\bar{\Delta}^*\|_{\mathrm{F}}^2 = \min_{\bar{B},x_{\Re}^2,x_{\Im}^2} \quad \textstyle\sum_{i=1}^{n}\sum_{p+1}^{n}(\bar{b}_{ij}-\bar{a}_{ij})^2 v_{ij}^{-1},$$

$$\text{s.t.} \qquad \begin{bmatrix}\bar{B}-\bar{N} & \bar{M}\\ -\bar{M} & \bar{B}-\bar{N}\end{bmatrix}\begin{bmatrix}x_{\Re}^2\\ x_{\Im}^2\end{bmatrix} = 0$$

TOTAL LEAST SQUARES MINIMIZATION PROBLEM!!

Optimization solution (2)

Step 3

Define Lagrange multipliers and write $\nabla\mathcal{L} = 0$

Optimization solution (2)

Step 3

Define Lagrange multipliers and write $\nabla\mathcal{L} = 0$

Step 4

Optimality conditions yield to the problem of computing z and $\bar{\sigma}$ s.t.

$$\underbrace{\begin{bmatrix} 0 & \tilde{A}^{\mathsf{T}} \\ \tilde{A} & 0 \end{bmatrix}}_{H} \underbrace{\begin{bmatrix} x \\ y \end{bmatrix}}_{z} = \bar{\sigma} \underbrace{\begin{bmatrix} D_y & 0 \\ 0 & D_x \end{bmatrix}}_{D} \underbrace{\begin{bmatrix} x \\ y \end{bmatrix}}_{z}$$

Optimization solution (2)

Step 3

Define Lagrange multipliers and write $\nabla \mathcal{L} = 0$

Step 4

Optimality conditions yield to the problem of computing z and $\bar{\sigma}$ s.t.

$$\underbrace{\begin{bmatrix} 0 & \tilde{A}^{\mathsf{T}} \\ \tilde{A} & 0 \end{bmatrix}}_{H} \underbrace{\begin{bmatrix} x \\ y \end{bmatrix}}_{z} = \bar{\sigma} \underbrace{\begin{bmatrix} D_y & 0 \\ 0 & D_x \end{bmatrix}}_{D} \underbrace{\begin{bmatrix} x \\ y \end{bmatrix}}_{z}$$

GENERALIZED NONLINEAR EIGENVALUE PROBLEM: Finding smallest nonzero $\bar{\sigma}$ and z s.t.

$$Hz = \bar{\sigma} D_z z$$

Optimization solution (2)

Step 3

Define Lagrange multipliers and write $\nabla \mathcal{L} = 0$

Step 4

Optimality conditions yield to the problem of computing z and $\bar{\sigma}$ s.t.

$$\underbrace{\begin{bmatrix} 0 & \tilde{A}^\mathsf{T} \\ \tilde{A} & 0 \end{bmatrix}}_{H} \underbrace{\begin{bmatrix} x \\ y \end{bmatrix}}_{z} = \bar{\sigma} \underbrace{\begin{bmatrix} D_y & 0 \\ 0 & D_x \end{bmatrix}}_{D} \underbrace{\begin{bmatrix} x \\ y \end{bmatrix}}_{z}$$

GENERALIZED NONLINEAR EIGENVALUE PROBLEM:
Finding smallest nonzero $\bar{\sigma}$ and z s.t.

$$Hz = \bar{\sigma} D_z z$$

Step 5

Solve iteratively by “freezing” the nonlinearity D_z (inverse power iteration method)

Power iteration method : when convergent gives (sub)-optimal solutions

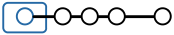
Bart De Moor. Total least squares for affinely structured matrices and the noisy realization problem. *IEEE Transactions on Signal Processing*, 42(11):3104–3113, 1994

The role of topology

The role of graph topology

When weights are chosen randomly $\mathcal{U}[0,1]$...

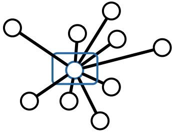
Line topology



Line is structurally observable
$\Rightarrow$ disconnection

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

Star topology



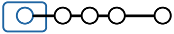
Best perturbation introduces an artificial symmetry

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

The role of graph topology

When weights are chosen randomly $\mathcal{U}[0,1]$...

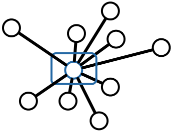
Line topology



Line is structurally observable
$\Rightarrow$ disconnection

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

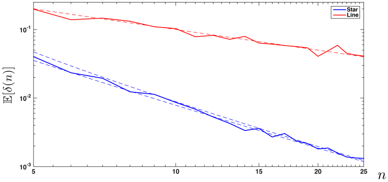
Star topology



Best perturbation introduces an artificial symmetry

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

The bound is tight :



Conclusions

In this talk...

1. Extend classical observability radius to networks
2. Resilience measure for network systems
3. Optimal problem formulation
4. Heuristic algorithm for its solution
5. Results can be extended to controllability

Research questions...

1. How do we chose λ
2. More on the role of topology

G. Bianchin, P. Frasca, A. Gasparri, and F. Pasqualetti. The observability radius of network systems.
In *American Control Conference*, Boston, MA, USA, Jul. 2016

G. Bianchin, P. Frasca, A. Gasparri, and F. Pasqualetti. The observability radius of network systems: Algorithms and estimates for random networks.
In *IEEE Transactions on Automatic Control [Submitted]*, 2016

The Observability Radius of Network Systems

Thank you !

Questions ?

EXTRAS : More about total least squares

From...

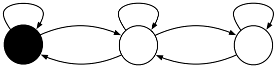
Bart De Moor. Total least squares for affinely structured matrices and the noisy realization problem. *IEEE Transactions on Signal Processing*, 42(11):3104–3113, 1994

"The *Total least squares* problem reduces to finding a matrix approximation B in Frobenius norm to a given matrix A. This can be formulated as :"

$$\min_{B\in\mathbb{R}^{n\times n}, y\in\mathbb{R}^n} \|A-B\|_F^2 \qquad \text{subject to} \qquad By=0 \quad y^\top y = 1$$

EXTRAS : Algorithm performance

$$A = \begin{bmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{bmatrix}$$



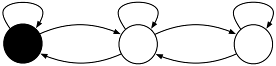
Optimal perturbations can be computed analytically :

$$\begin{bmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{bmatrix} + \Delta = \begin{bmatrix} a_{11} & 0 & 0 \\ a_{21} & b_{22} & b_{23} \\ 0 & b_{32} & b_{33} \end{bmatrix}$$

$$\begin{aligned} (b_{22} - a_{22}) - (b_{33} - a_{33}) + \frac{b_{33} - b_{22}}{b_{32}}(b_{23} - a_{23}) &= 0, \\ (b_{32} - a_{32}) - \frac{b_{23}}{b_{32}}(b_{23} - a_{23}) &= 0, \\ 2\lambda_{\Re} + b_{22} + b_{33} &= 0, \\ b_{22}b_{33} - b_{23}b_{32} - \lambda_{\Re}^2 + \lambda_{\Im}^2 &= 0. \end{aligned}$$

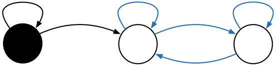
EXTRAS : Algorithm performance

$$A = \begin{bmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{bmatrix}$$



Optimal perturbations can be computed analytically :

$$\begin{bmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{bmatrix} + \Delta = \begin{bmatrix} a_{11} & 0 & 0 \\ a_{21} & b_{22} & b_{23} \\ 0 & b_{32} & b_{33} \end{bmatrix}$$



$$\begin{aligned} (b_{22} - a_{22}) - (b_{33} - a_{33}) + \frac{b_{33} - b_{22}}{b_{32}}(b_{23} - a_{23}) &= 0, \\ (b_{32} - a_{32}) - \frac{b_{23}}{b_{32}}(b_{23} - a_{23}) &= 0, \\ 2\lambda_{\Re} + b_{22} + b_{33} &= 0, \\ b_{22}b_{33} - b_{23}b_{32} - \lambda_{\Re}^2 + \lambda_{\Im}^2 &= 0. \end{aligned}$$

EXTRAS : Algorithm performance

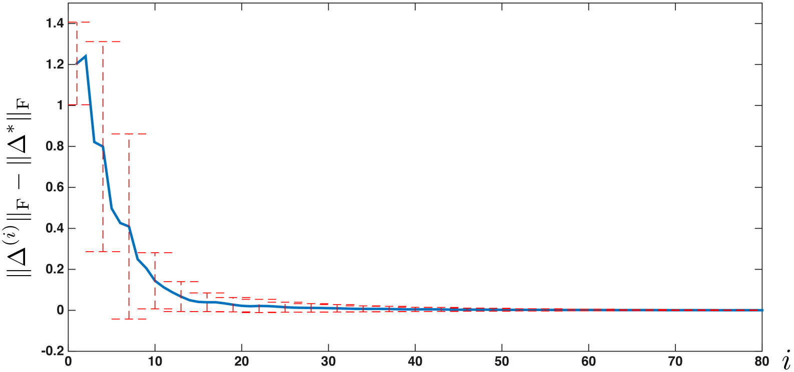


FIGURE: Mean and standard deviation of the approximation error over 100 simulation executions.

Our algorithm converges to a solution which has the same norm as the optimal perturbation.

EXTRAS : Algorithm implementation (1)

Optimality conditions can be written in matrix form as

$$\underbrace{\begin{bmatrix} 0 & \tilde{A}^{\mathsf{T}} \\ \tilde{A} & 0 \end{bmatrix}}_{H} \underbrace{\begin{bmatrix} x \\ y \end{bmatrix}}_{z} = \bar{\sigma} \underbrace{\begin{bmatrix} D_y & 0 \\ 0 & D_x \end{bmatrix}}_{D} \underbrace{\begin{bmatrix} x \\ y \end{bmatrix}}_{z}.$$

Lemma

(Generalized eigenvalues of (H, D)) *Given a vector $z \in \mathbb{R}^{2n+2p}$. Then,*

1. $0 \in spec(H, D)$;
2. *if $\lambda \in spec(H, D)$, then $-\lambda \in spec(H, D)$; and*
3. *if (H, D) is regular, then $spec(H, D) \subset \mathbb{R}$.*

EXTRAS : Algorithm implementation (2)

Observations :

- the zero eigenvalue of (H, D) leads the inverse iteration to instability
- the presence of eigenvalues of (H, D) with equal magnitude may induce non-decaying oscillations in the solution vector

We employ the following shifting mechanism :

1. z is iteratively updated by solving the equation $(H - \mu D)z_{k+1} = Dz_k$
2. If $\sigma \in \text{spec}(H, D)$, then $\sigma + \mu \in \text{spec}(H - \mu D, D)$
3. The pairs $(H - \mu D, D)$ and (H, D) share the same eigenvectors
4. By selecting $\mu = \psi \cdot \min\{\sigma \in \text{spec}(H, D) \;:\; \sigma > 0\}$, the pair $(H - \mu D, D)$ has nonzero eigenvalues with distinct magnitude

EXTRAS : Algorithm implementation (2)

Observations :

- the zero eigenvalue of (H, D) leads the inverse iteration to instability
- the presence of eigenvalues of (H, D) with equal magnitude may induce non-decaying oscillations in the solution vector

We employ the following shifting mechanism :

1. z is iteratively updated by solving the equation $(H - \mu D)z_{k+1} = Dz_k$
2. If $\sigma \in \text{spec}(H, D)$, then $\sigma + \mu \in \text{spec}(H - \mu D, D)$
3. The pairs $(H - \mu D, D)$ and (H, D) share the same eigenvectors
4. By selecting $\mu = \psi \cdot \min\{\sigma \in \text{spec}(H, D) \ : \ \sigma > 0\}$, the pair $(H - \mu D, D)$ has nonzero eigenvalues with distinct magnitude

EXTRAS : Algorithm implementation (3)

Algorithm 1 Inverse power iteration with shifting

Input: Matrix H ; max iterations $\max_{\text{iter}}$; $\psi \in (0.5, 1)$.
Output: σ and z
repeat

$z \leftarrow (H - \mu D)^{-1} Dz$
$\sigma \leftarrow \|z\|$
$z \leftarrow z/\sigma$
$\mu = \psi \cdot \min\{\sigma \in \text{spec}(H, D) \ : \ \sigma > 0\}$
update D $i \leftarrow i + 1$

until convergence or $i > \max_{\text{iter}}$;
return $(\sigma + \mu, z)$ **or fail if** $i = \max_{\text{iter}}$

- Bart De Moor.
  Total least squares for affinely structured matrices and the noisy realization problem.
  IEEE Transactions on Signal Processing, 42(11) :3104–3113, 1994.
- **G. Bianchin**, P. Frasca, A. Gasparri, and F. Pasqualetti.
  The observability radius of network systems.
  In *American Control Conference*, Boston, MA, USA, Jul. 2016.
- **G. Bianchin**, P. Frasca, A. Gasparri, and F. Pasqualetti.
  The observability radius of network systems : Algorithms and estimates for random networks.
  In *IEEE Transactions on Automatic Control [Submitted]*, 2016.
- Guangdi Hu and Edward J Davison.
  Real controllability/stabilizability radius of lti systems.
  IEEE transactions on automatic control, 49(2) :254–257, 2004.