Cyber-physical attacks on coupled phase oscillators

Melvyn Tyloo

Director's Postdoc Fellow, T-4 and CNLS

Los Alamos NATIONAL LABORATORY

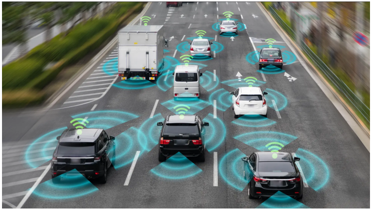
website: melvyntyloo.com

mtyloo@lanl.gov — 1/10/24

MT, J. Phys. Complex. **4** 045005 (2023).

Phase oscillators: some examples

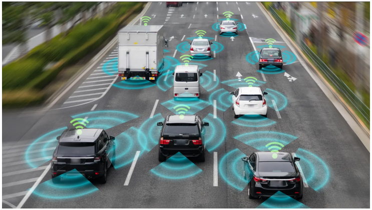
Autonomous vehicular platoon



source: topgear.com
URL

Phase oscillators: some examples

Autonomous vehicular platoon

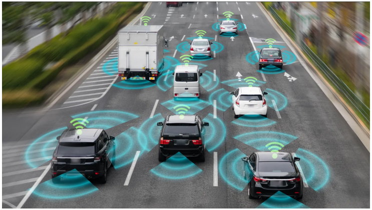


source: topgear.com
URL

Electric power grids

Phase oscillators: some examples

Autonomous vehicular platoon



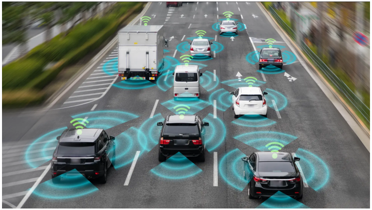
source: topgear.com
URL

Electric power grids

Collective states

Phase oscillators: some examples

Autonomous vehicular platoon



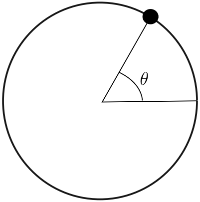
source: topgear.com
URL

Electric power grids

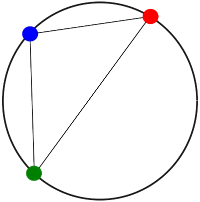
Collective states →Physical perturbation and cyber attacks

Phase oscillators

Single phase oscillator: $\dot{\theta} = \omega$



Coupled phase oscillators: $\dot{\theta}_i = \omega_i - \sum_j a_{ij} f(\theta_i - \theta_j)$



Synchronization: phase-locked $\dot{\theta}_i(t) = \dot{\theta}_j(t)\,,\ \forall i, j\,.$

Kuramoto model

$$\dot{\theta}_i = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i - \theta_j)\,, \text{for } i = 1, ..., N\,. \tag{1}$$

ω_i: natural frequencies.
a_{ij}: adjacency matrix.

J. A. Acebrón, L. L. Bonilla, Conrad J. Pérez Vicente, F. Ritort, and R. Spigler, Rev. Mod. Phys. **77**, 137 (2005)

Dörfler and Bullo, Automatica **50** (6), 1539-1564, (2014)

Kuramoto model

$$\dot{\theta}_i = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i - \theta_j)\,, \text{for } i = 1, ..., N\,. \tag{1}$$

ω_i: natural frequencies.
a_{ij}: adjacency matrix.
Stable fixed point(s)

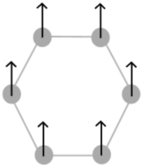
$$0 = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i^{(0)} - \theta_j^{(0)})\,, \text{for } i = 1, ..., N\,. \tag{2}$$

J. A. Acebrón, L. L. Bonilla, Conrad J. Pérez Vicente, F. Ritort, and R. Spigler, Rev. Mod. Phys. **77**, 137 (2005)

Dörfler and Bullo, Automatica **50** (6), 1539-1564, (2014)

Stable fixed point(s)

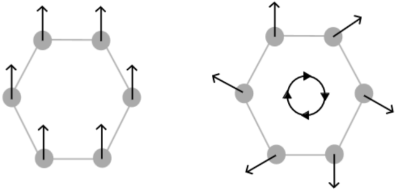
$$0 = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i^{(0)} - \theta_j^{(0)}) \,, \text{for } i = 1, ..., N \,. \tag{3}$$



Delabays, MT, Jacquod, Chaos **27**(10), 103109 (2017)

Stable fixed point(s)

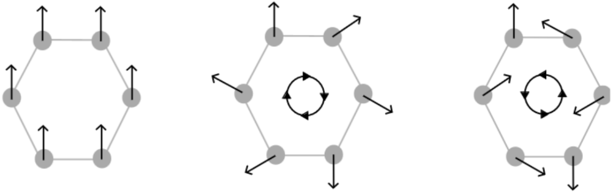
$$0 = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i^{(0)} - \theta_j^{(0)}) \,, \text{for } i = 1, ..., N \,. \quad (3)$$



Delabays, MT, Jacquod, Chaos **27**(10), 103109 (2017)

Stable fixed point(s)

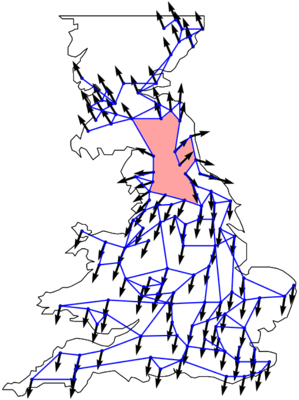
$$0 = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i^{(0)} - \theta_j^{(0)})\,, \text{for } i = 1, ..., N\,. \tag{3}$$



Delabays, MT, Jacquod, Chaos **27**(10), 103109 (2017)

Stable fixed point(s)

$$0 = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i^{(0)} - \theta_j^{(0)}) \, , \text{for } i = 1, ..., N \, . \quad (4)$$



Delabays, MT, Jacquod, Chaos **27**(10), 103109 (2017)

Synchronization on networks

Kuramoto model

$$\dot{\theta}_i = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i - \theta_j)\,, \text{for } i = 1, ..., N\,. \tag{5}$$

ω_i: natural frequencies.
a_{ij}: adjacency matrix.

J. A. Acebrón, L. L. Bonilla, Conrad J. Pérez Vicente, F. Ritort, and R. Spigler, Rev. Mod. Phys. **77**, 137 (2005)

Dörfler and Bullo, Automatica **50** (6), 1539-1564, (2014)

Kuramoto model

$$\dot{\theta}_i = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i - \theta_j)\,, \text{for } i = 1, ..., N\,. \tag{5}$$

ω_i: natural frequencies.
a_{ij}: adjacency matrix.
Physical perturbation $\omega_k \to \tilde{\omega_k}$ or $a_{kl} \to \tilde{a_{kl}}$.

J. A. Acebrón, L. L. Bonilla, Conrad J. Pérez Vicente, F. Ritort, and R. Spigler, Rev. Mod. Phys. **77**, 137 (2005)

Dörfler and Bullo, Automatica **50** (6), 1539-1564, (2014)

Synchronization on networks

Kuramoto model

$$\dot{\theta}_i = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i - \theta_j)\,, \text{for } i = 1, ..., N\,. \quad (5)$$

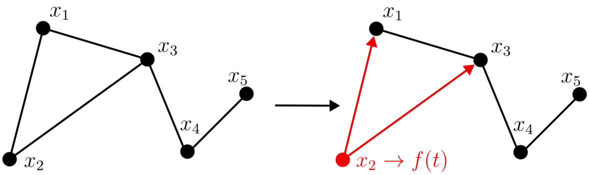
ω_i: natural frequencies.
a_{ij}: adjacency matrix.
Physical perturbation $\omega_k \to \tilde{\omega_k}$ or $a_{kl} \to \tilde{a_{kl}}$.

Cyber attack $\theta_k \to f(t)$.

J. A. Acebrón, L. L. Bonilla, Conrad J. Pérez Vicente, F. Ritort, and R. Spigler, Rev. Mod. Phys. **77**, 137 (2005)

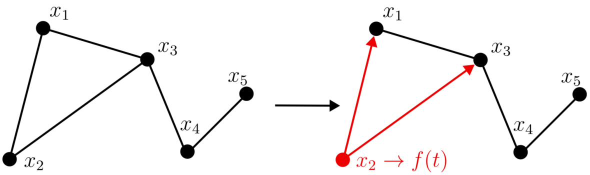
Dörfler and Bullo, Automatica **50** (6), 1539-1564, (2014)

Cyber attack



MT, J. Phys. Complex. **4** 045005 (2023).

Cyber attack

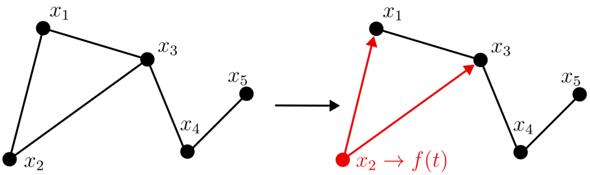


$$\dot{\theta}_i = \omega_i - \sum_j a_{ij} \sin(\theta_i - \theta_j)\,, i \neq k\,, i \notin \mathcal{N}(k)\,, \tag{6}$$

$$\dot{\theta}_i = \omega_i - \sum_{j \neq k} a_{ij} \sin(\theta_i - \theta_j) - a_{ik} \sin[\theta_i - f(t)]\,, i \in \mathcal{N}(k)\,, \tag{7}$$

MT, J. Phys. Complex. **4** 045005 (2023).

Cyber attack



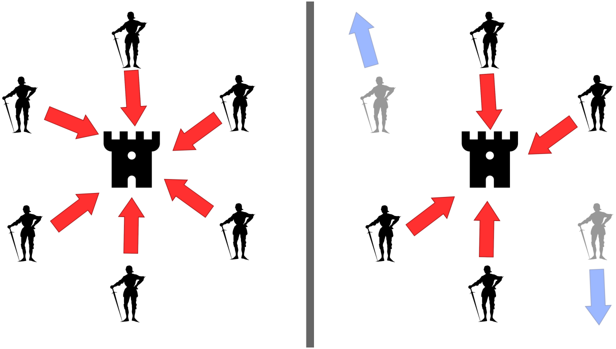
$$\dot{\theta}_i = \omega_i - \sum_j a_{ij} \sin(\theta_i - \theta_j)\,, i \neq k\,, i \notin \mathcal{N}(k)\,, \quad (6)$$

$$\dot{\theta}_i = \omega_i - \sum_{j \neq k} a_{ij} \sin(\theta_i - \theta_j) - a_{ik} \sin[\theta_i - f(t)]\,, i \in \mathcal{N}(k)\,, \quad (7)$$

Byzantine type of attack.

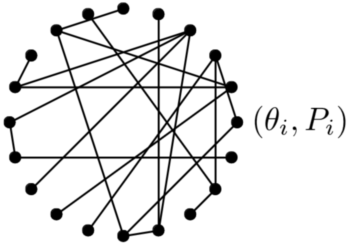
MT, J. Phys. Complex. **4** 045005 (2023).

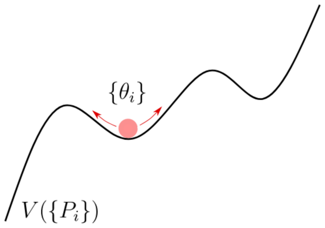
Byzantine generals problem



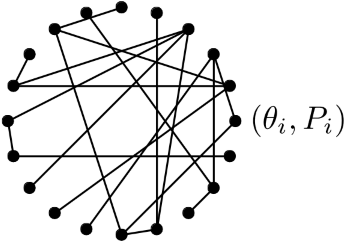
By Lord Belbury - Own work This file was derived from:Noun Project - Castle tower.svg:KnightSilhouette2.svg:, https://commons.wikimedia.org/w/index.php?curid=108234603

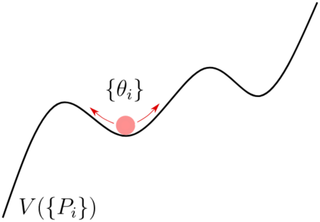
Robustness of synchronous networks





Robustness of synchronous networks





- Size of the basin of attraction
- Near equilibrium dynamics
- Transitions between fixed points

Synchronization error in the near equilibrium dynamics.

Near equilibrium dynamics

$$0 = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i^{(0)} - \theta_j^{(0)}) \,, \text{for } i = 1, ..., N \,. \tag{8}$$

Robustness of synchronous networks to input signals

Near equilibrium dynamics

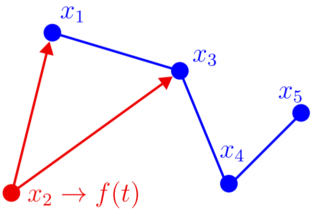
$$0 = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i^{(0)} - \theta_j^{(0)})\,, \text{for } i = 1, ..., N\,. \tag{8}$$

$$\delta\dot{\theta}_i = -\sum_{j=1}^{N} \mathbb{L}_{ij}\, \delta\theta_j + \eta_i(t)\,, \text{for } i = 1, ..., N\,. \tag{9}$$

$\eta_i(t)$: input signal.
More complicated for cyber attacks!

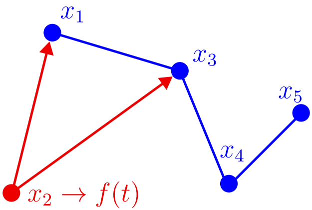
Cyber attacks

$$\delta\dot{\theta}_i = \begin{cases} -\sum_j \tilde{\mathbb{L}}_{ij}\,\delta\theta_j \quad \text{for } i \neq k\,, i \notin \mathcal{N}(k)\,, \\ -\sum_{j\neq k} \tilde{\mathbb{L}}_{ij}\,\delta\theta_j - a_{ik}\tilde{f}(t) \\ \quad \text{for } i \neq k\,, i \in \mathcal{N}(k) \\ \dot{f}(t) \quad \text{for } i = k\,, \end{cases} \tag{10}$$



Cyber attacks

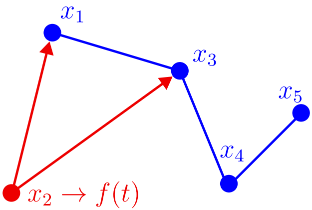
$$\delta\dot{\theta}_i = \begin{cases} -\sum_j \tilde{\mathbb{L}}_{ij}\,\delta\theta_j \quad \text{for } i \neq k\,, i \notin \mathcal{N}(k)\,, \\ -\sum_{j\neq k} \tilde{\mathbb{L}}_{ij}\,\delta\theta_j - a_{ik}\tilde{f}(t) \\ \quad \text{for } i \neq k\,, i \in \mathcal{N}(k) \\ \dot{f}(t) \quad \text{for } i = k\,, \end{cases} \tag{10}$$



$$\boldsymbol{\delta\dot{\theta}} = -(\tilde{\mathbb{L}} + \mathbf{K})\,\boldsymbol{\delta\theta} + \tilde{\mathbf{f}}(t)\,, \tag{11}$$

Cyber attacks

$$\delta\dot{\theta}_i = \begin{cases} -\sum_j \tilde{\mathbb{L}}_{ij}\,\delta\theta_j \quad \text{for } i \neq k\,, i \notin \mathcal{N}(k)\,, \\ -\sum_{j\neq k} \tilde{\mathbb{L}}_{ij}\,\delta\theta_j - a_{ik}\tilde{f}(t) \\ \quad \text{for } i \neq k\,, i \in \mathcal{N}(k) \\ \dot{f}(t) \quad \text{for } i = k\,, \end{cases} \tag{10}$$

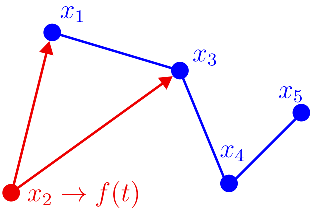


$$\boldsymbol{\delta\dot{\theta}} = -(\tilde{\mathbb{L}} + \mathbf{K})\,\boldsymbol{\delta\theta} + \tilde{\mathbf{f}}(t)\,, \tag{11}$$

$(\tilde{\mathbb{L}} + \mathbf{K})$, with eigenvalues $0 < \lambda_1 \leq \lambda_2 \leq ... \leq \lambda_{N-1}$.

Cyber attacks

$$\delta\dot{\theta}_i = \begin{cases} -\sum_j \tilde{\mathbb{L}}_{ij}\,\delta\theta_j \quad \text{for } i \neq k\,, i \notin \mathcal{N}(k)\,, \\ -\sum_{j\neq k} \tilde{\mathbb{L}}_{ij}\,\delta\theta_j - a_{ik}\tilde{f}(t) \\ \quad \text{for } i \neq k\,, i \in \mathcal{N}(k) \\ \dot{f}(t) \quad \text{for } i = k\,, \end{cases} \tag{10}$$



$$\boldsymbol{\delta\dot{\theta}} = -(\tilde{\mathbb{L}} + \mathbf{K})\,\boldsymbol{\delta\theta} + \tilde{\mathbf{f}}(t)\,, \tag{11}$$

$(\tilde{\mathbb{L}} + \mathbf{K})$, with eigenvalues $0 < \lambda_1 \leq \lambda_2 \leq ... \leq \lambda_{N-1}$.

Quantify the impact

Synchronization error

$$\mathcal{P}(t) = \sum_{i<j} \tilde{a}_{ij}[\delta\theta_i(t) - \delta\theta_j(t)]^2 \,. \tag{12}$$

Quantify the impact

Synchronization error

$$\mathcal{P}(t) = \sum_{i<j} \tilde{a}_{ij}[\delta\theta_i(t) - \delta\theta_j(t)]^2\,. \tag{12}$$

Cyber attack

$$\begin{aligned}\mathcal{P}(t) &= \sum_{i,j} \delta\theta_i(t)\,\tilde{\mathbb{L}}_{ij}\,\delta\theta_j(t) \\ &= \sum_{\alpha} \tilde{\lambda}_\alpha\,\tilde{c}_\alpha^2(t) + \sum_{j\in\mathcal{N}(k)} \delta\theta_j^2(t)\,,\end{aligned} \tag{13}$$

Quantify the impact

Synchronization error

$$\mathcal{P}(t) = \sum_{i<j} \tilde{a}_{ij}[\delta\theta_i(t) - \delta\theta_j(t)]^2 \,. \tag{12}$$

Cyber attack

$$\begin{aligned} \mathcal{P}(t) &= \sum_{i,j} \delta\theta_i(t)\, \tilde{\mathbb{L}}_{ij}\, \delta\theta_j(t) \\ &= \sum_{\alpha} \tilde{\lambda}_\alpha\, \tilde{c}_\alpha^2(t) + \sum_{j\in\mathcal{N}(k)} \delta\theta_j^2(t)\,, \end{aligned} \tag{13}$$

Solution

$$\tilde{c}_\alpha(t) = e^{-\tilde{\lambda}_\alpha\, t} \int_0^t e^{\tilde{\lambda}_\alpha\, t'} \sum_j f_j(t')\tilde{u}_{\alpha,k}\,\mathrm{d}t' \,. \tag{14}$$

Robustness of synchronous networks to noise inputs

Uncorrelated white noise

$$\langle \eta_i(t)\eta_j(t')\rangle = \sigma\, \delta_{ij}\, \delta(t - t') \tag{15}$$

Robustness of synchronous networks to noise inputs

Uncorrelated white noise

$$\langle \eta_i(t)\eta_j(t')\rangle = \sigma\,\delta_{ij}\,\delta(t-t') \tag{15}$$

$$\langle \mathcal{P}\rangle = \frac{\sigma^2}{2}\sum_{j\in\mathcal{N}(k)}\tilde{a}_{jk}^2 + \sigma^2\sum_{\alpha,\beta}\sum_{i,j,l\in\mathcal{N}(k)}\tilde{a}_{ik}\tilde{a}_{jk}\frac{u_{\alpha,i}u_{\beta,j}u_{\alpha,l}u_{\beta,l}}{\lambda_\alpha+\lambda_\beta}\,. \tag{16}$$

Robustness of synchronous networks to noise inputs

Uncorrelated white noise

$$\langle \eta_i(t)\eta_j(t')\rangle = \sigma\,\delta_{ij}\,\delta(t-t') \tag{15}$$

$$\langle \mathcal{P} \rangle = \frac{\sigma^2}{2}\sum_{j\in\mathcal{N}(k)} \tilde{a}_{jk}^2 + \sigma^2 \sum_{\alpha,\beta}\sum_{i,j,l\in\mathcal{N}(k)} \tilde{a}_{ik}\tilde{a}_{jk}\frac{u_{\alpha,i}u_{\beta,j}u_{\alpha,l}u_{\beta,l}}{\lambda_\alpha+\lambda_\beta}\,. \tag{16}$$

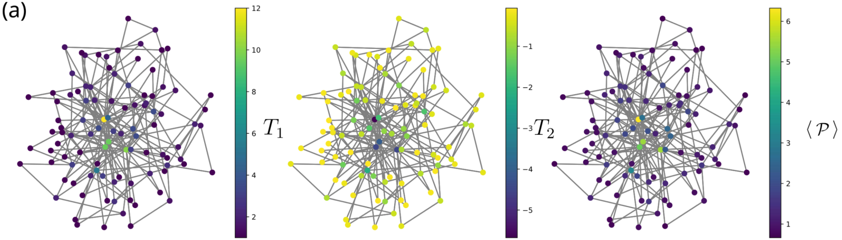
$$T_1 = \frac{\tau_0}{2}\sum_{j\in\mathcal{N}(k)} \tilde{a}_{jk}^2\,, \tag{17}$$

$$T_2 = -\tau_0\sum_{\alpha,\beta}\sum_{i,j,l\in\mathcal{N}(k)} \tilde{a}_{ik}\tilde{a}_{jk}\tilde{a}_{lk}\frac{u_{\alpha,i}u_{\beta,j}u_{\alpha,l}u_{\beta,l}}{\lambda_\alpha+\lambda_\beta}\,. \tag{18}$$

Robustness of synchronous networks to noise inputs

$$T_1 = \frac{\tau_0}{2} \sum_{j\in\mathcal{N}(k)} \tilde{a}_{jk}^2 \,, \tag{19}$$

$$T_2 = -\tau_0 \sum_{\alpha,\beta} \sum_{i,j,l\in\mathcal{N}(k)} \tilde{a}_{ik}\tilde{a}_{jk}\tilde{a}_{lk} \frac{u_{\alpha,i}u_{\beta,j}u_{\alpha,l}u_{\beta,l}}{\lambda_\alpha + \lambda_\beta} \,. \tag{20}$$

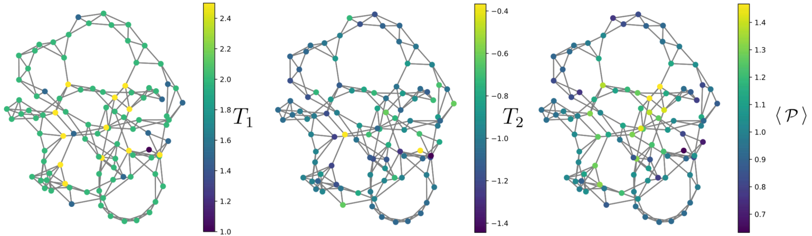


Robustness of synchronous networks to noise inputs

$$T_1 = \frac{\tau_0}{2} \sum_{j \in \mathcal{N}(k)} \tilde{a}_{jk}^2 \,, \tag{21}$$

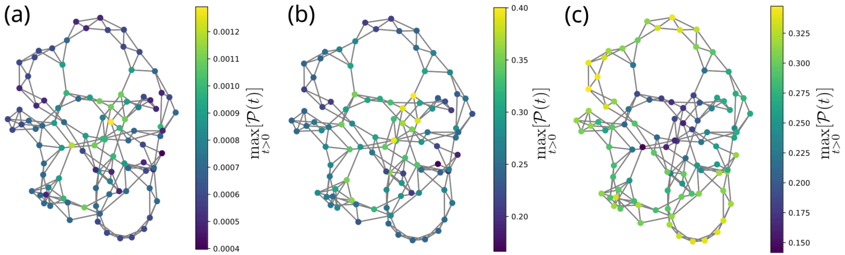
$$T_2 = -\tau_0 \sum_{\alpha,\beta} \sum_{i,j,l \in \mathcal{N}(k)} \tilde{a}_{ik} \tilde{a}_{jk} \tilde{a}_{lk} \frac{u_{\alpha,i} u_{\beta,j} u_{\alpha,l} u_{\beta,l}}{\lambda_\alpha + \lambda_\beta} \,. \tag{22}$$

(b)



Periodic signal

$$f(t) = \gamma \cos(\omega t)\,, \tag{23}$$



Conclusion and future work

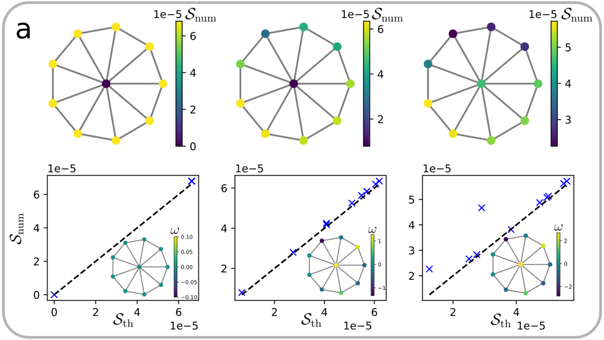
So far

- Cyber attacks $\rightarrow$ different from physical perturbations.

MT, J. Phys. Complex. **4** 045005 (2023).

So far

- Cyber attacks → different from physical perturbations.
- Effects of heterogeneity



MT, J. Phys. Complex. **4** 045005 (2023).