Byzantine attacks on networked phase oscillators

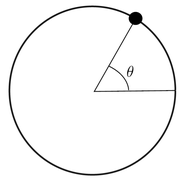
Melvyn Tyloo | Theoretical Division and Center for Nonlinear Studies (CNLS), Los Alamos National Laboratory, NM, USA

Autonomous vehicular platoon

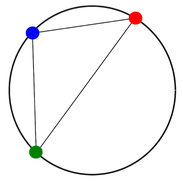
source: topgear.com
URL

Electric power grids

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

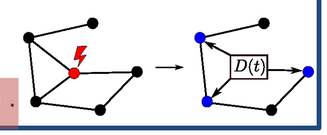
$$\dot{\theta}_i = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i - \theta_j), \text{for } i = 1, ..., N.$$

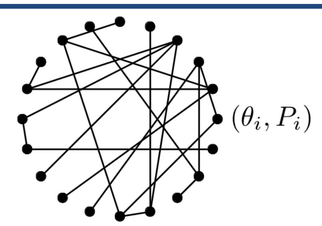
ω_i: natural frequencies.
a_{ij}: adjacency matrix.
Stable fixed point(s)

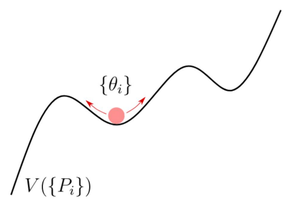
$$0 = \omega_i - \sum_{j=1}^{N} a_{ij} \sin(\theta_i^{(0)} - \theta_j^{(0)}), \text{for } i = 1, ..., N.$$

Physical perturbation $\omega_k \to \tilde{\omega_k}$ or $a_{kl} \to \tilde{a_{kl}}$.

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







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

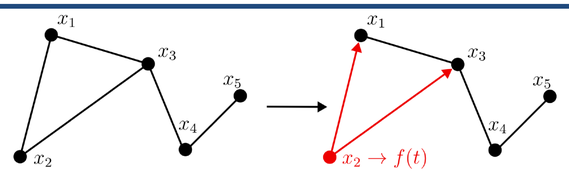
Synchronization error in the near equilibrium dynamics.

Near equilibrium dynamics

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

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

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

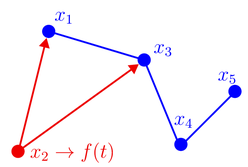


$$\dot{\theta}_i = \omega_i - \sum_j a_{ij} \sin(\theta_i - \theta_j), i \neq k, i \notin \mathcal{N}(k),$$

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

Byzantine type of attack.

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



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

Synchronization error

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

Cyber attack

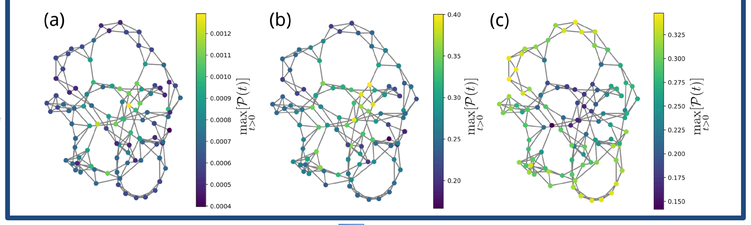
$$\mathcal{P}(t) = \sum_{i,j} \delta\theta_i(t)\, \tilde{\mathbb{L}}_{ij}\, \delta\theta_j(t) = \sum_{\alpha} \tilde{\lambda}_\alpha\, \tilde{c}_\alpha^2(t) + \sum_{j \in \mathcal{N}(k)} \delta\theta_j^2(t),$$

Solution

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

Periodic signal

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



Cyber attacks: different from physical perturbations
Future works: implementing a budget for the attacker, consider larger deviations, etc.

Managed by Triad National Security, LLC, for the U.S. Department of Energy's NNSA. LA-UR-24-23687

M. Tyloo, Journal of Physics: Complexity **4** (4), 045005 (2023)