Design of Secure, Spatially-Distributed, Data-Driven Control and Optimization Algorithms

Zhihua Qu, Pegasus Professor
University of Central Florida, Orlando, Florida, USA

American Control Conference
June 30, 2020

Acknowledgements

Partial support under grants from

- US National Science Foundation (award #s: CCF-0956501, ECCS-1308928, ECCS-1927994)
- US Department of Energy (award #s: DE-EE0006340, DE-EE0007327, and DE-EE0007998)
- US Department of Transportation (grant #: DTRT13-G-UTC51)

Table of Contents

Networked Operation of Heterogeneous Dynamic Systems

Why "distributed intelligence"?

- Information is distributed
- Actions are distributed
- more efficient
- more resilient
- Plug-and-play operation is essential for many operations

Consensus: all the "chosen" state variables (i.e., outputs) converge to the same value (or certain property). Applications:

- synchronization (velocity, frequency, etc)
- rendezvous, formation control, ...
- fair distribution of resources, ...
- distributed estimation of certain quantity
- distributed search for a global optimal solution of any kind

Consensus can be reached by collaborative entities (by employing cooperative control or distributed optimization or distributed estimation)

Applicable to multi-entity cooperative games

Cooperative Behaviors: Consensus

Bird flocking:

Formation flying of UAVs:

Table of Contents

Standard Stability Analysis

Linear systems: given $x(t_0) = x_0$,

$$\dot{x} = Ax, \quad x(t_0) = x_0;$$

or

$$x_{k+1} = Dx_k.$$

Eigen-analysis: solutions λ_i from

$$\text{det}[\lambda I - A] = 0, \quad \text{det}[\lambda I - D] = 0.$$

Stability: system is asymptotically stable if, for all i,

$$\text{Re}[\lambda_i(A)] < 0, \quad |\lambda_i(D)| < 1.$$

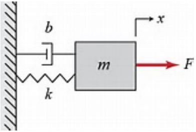
Example:

$$\dot{x} = Ax, \quad A = \begin{bmatrix} 0 & 1 \\ -k_p & -k_v \end{bmatrix}.$$

$$\Delta(\lambda I - A) = \lambda^2 + k_v \lambda + k_p = 0.$$

The system is asymptotically stable if and only if $k_v, k_p > 0$.

Example: Simple Systems



Spring-damper system:

$$m\ddot{x} \quad = \quad -b\dot{x} - kx + F,$$

where F is the control, b is the damping, and k is the spring constant.

Typical tracking control is:

$$F = \ddot{x}^d + b\dot{x}^d + kx^d.$$

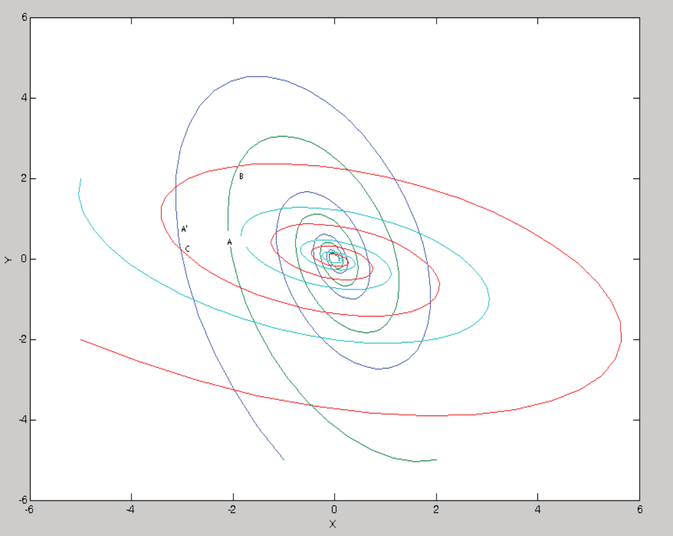
The closed loop system becomes: $e = x - x^d$,

$$\ddot{e} + k_v\dot{e} + k_p e = 0,$$

where $k_v = d/m$ and $k_p = k/m$.

Question: What happens if the systems are interconnected intermittently?

Stability and Robustness under Switching



Question: What systems can be networked in a plug-and-play manner?

Table of Contents

A Simple Cooperative System

First-order (agent) model: $x \in \Re^n$,

$$\dot{x}_i = u_i, \quad \Longrightarrow \quad \dot{x} = u.$$

Communication network model:

$$S(t) = [s_{ij}(t)] \in \Re_+^{n \times n}, \quad s_{ii} \equiv 1.$$

Leaderless linear cooperative control design (consensus law):

$$u_i = \sum_{j=1}^{n} s_{ij}(t)[x_j(t) - x_i(t)], \quad \text{or} \quad u = -L(t)x(t),$$

where $L \in \Re^{n \times n}$ is the Laplacian:

$$L_{ij}(t) = \begin{cases} -s_{ij}(t) & i \neq j \\ \sum_{l \neq i} s_{il}(t) & i = j \end{cases}$$

Conclusions:
(a) No matter what $S(t)$, the system is uniformly bounded.
(b) If the cumulative graph of $S(t)$ is strongly connected, consensus is reached.

Why Stability/Consensus Is Guaranteed?

Closed-loop dynamics of the ith agent:

$$\dot{x}_i = \sum_{j=1}^{n} s_{ij}(t)[x_j(t) - x_i(t)].$$

Let i^* be the index such that

$$x_{i^*}(t) = \max_i x_i(t),$$

then, for all j,

$$s_{i^*j}(t)[x_j(t) - x_{i^*}(t)] \leq 0$$

and the inequality is strict unless $s_{i^*j}(t) = 0$ or $x_j(t) = x_{i^*}(t)$. Therefore,

$$\dot{x}_{i^*} \leq 0,$$

and the maximum never increases and it always decreases if there is any connection with non-maximum agents.

Similarly, the minimum never decreases and it always increases if there is any connection with non-minimum agents.

A Leader-Followers Design

First-order (agent) model: $x \in \Re^n$,

$$\dot{x}_i = u_i, \quad \Longrightarrow \quad \dot{x} = u.$$

The leader state is designated as x_0, and communication matrices are

$$S(t) = [s_{ij}(t)] \in \Re_+^{n \times n}, \quad s_{ii} \equiv 1, \quad s_{i0}(t) \in \Re_+, \quad s_{0i} \equiv 0.$$

Leader-follower linear cooperative control design (consensus law):

$$u_i = s_{i0}[x_0 - x_i(t)] + \sum_{j=1}^{n} s_{ij}(t)[x_j(t) - x_i(t)].$$

Conclusions:
(a) No matter what $s_{ij}(t)$, the system is uniformly bounded.
(b) If the cumulative graph is strongly connected, consensus of x_0 is reached.

How about more general classes of systems?

Table of Contents

Dissipativity Theory

Heterogenous systems:

$$\dot{z}_i = \mathcal{F}_i(z_i, v_i), \quad y_i = H_i(z_i),$$

where

$$v_i = v_{s_i}(z_i) + u_i.$$

Dissipativity (Willems): for p.s.d. storage function V_i and a supply rate $\Phi_i(\cdot)$,

$$V_i(z_i) - V_i(z_i(0)) \leq -\int_0^t \Phi_i(z_i, u_i) ds,$$

where, if $\Phi_i(\cdot)$ is quadratic,

$$\Phi_i(z_i, u_i) = -\eta_i(z_i) + u_i^T y_i + \frac{\epsilon_i}{2}\|u_i\|^2 - \frac{\varrho_i}{2}\|y_i\|^2.$$

Common forms of dissipativity:

- Passivity: $\eta_i(\cdot)$ p.s.d., $\epsilon_i \leq 0$ and $\varrho_i \geq 0$.
- L_2 gain: $\eta_i(\cdot)$ p.s.d., $\varrho_i > 0$, and $\epsilon_i > 0$.
- Passivity shortage (PS):
  Input PS (input-feedforward passive): $\eta_i(\cdot)$ p.s.d., $\epsilon_i > 0$, and $\varrho_i \geq 0$.
  Output PS (output-feedback passive): $\eta_i(\cdot)$ p.s.d., $\epsilon_i \leq 0$, and $\varrho_i < 0$.
  PS: $\eta_i(\cdot)$ p.s.d., $-1 \leq \epsilon_i \varrho_i < 0$.

Passive Systems

Heterogenous systems:

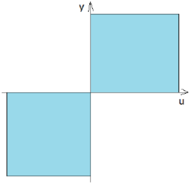
$$\dot{z}_i = \mathcal{F}_i(z_i, v_i), \quad y_i = H_i(z_i),$$

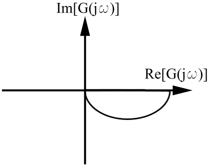
where $z_i \in \Re^{n_i}$, $v_i, y_i \in \Re^m$, $\partial H(z_i)/\partial z_i$ has rank m, and

$$v_i = v_{s_i}(z_i) + u_i.$$

Passivity: for p.s.d. storage function V_i and p.s.d. function η_i,

$$V_i(z_i) - V_i(z_i(0)) \leq -\int_0^t \eta_i(z_i)ds + \int_0^t u_i^T y_i ds.$$





Linear systems:
$\dot{z}_i = F_i^c z_i + G_i u_i, \; y_i = H_i z_i,$

- positive real
- relative-degree-one
- minimum-phase
- Lyapunov function P_i: $G_i^T P_i = H_i$

Input Passivity-Short Systems

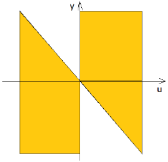
Heterogenous systems:

$$\dot{z}_i = \mathcal{F}_i(z_i, v_{s_i}(z_i) + u_i), \quad y_i = H_i(z_i).$$

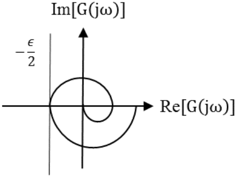
Input passivity-short system: for p.s.d. storage function V_i, p.s.d. function η_i and constant $\epsilon_i \geq 0$,

$$V_i(z_i) - V_i(z_i(0)) \leq -\int_0^t \eta_i(z_i)ds + \int_0^t u_i^T y_i ds + \frac{\epsilon_i}{2}\int_0^t \|u_i\|^2 ds,$$

where ϵ_i is the so-called *impact coefficient*.



$(-\epsilon_i/2)$ is the slope above;
as $\epsilon_i \to \infty$, the whole plane is covered.



(a) Most Lyapunov stable systems
(b) All Lyapunov-stable linear systems can be made PS under an output feedback control

PS Systems with Self Output Feedback — an L_2 Gain

Heterogenous systems:

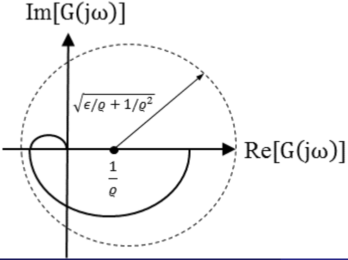
$$\dot{z}_i = \mathcal{F}_i(z_i, v_{s_i}(z_i) + u_i), \quad y_i = H_i(z_i).$$

The ith system is said to be PS and have an L_2-gain ϱ_i if, for some $\varrho_i, \epsilon_i > 0$,

$$V_i(z_i) - V_i(z_i(0)) \leq -\frac{\varrho_i}{2}\int_0^t \|y_i\|^2 ds + \int_0^t u_i^T y_i ds + \frac{\epsilon_i}{2}\int_0^t \|u_i\|^2 ds.$$

For linear system $G(s)$, it follows that

$$\varrho_i \left[\left(\text{Re}[G(jw)] - \frac{1}{\varrho_i} \right)^2 + \text{Im}^2[G(jw)] - \frac{1}{\varrho_i^2} \right] \leq \epsilon_i.$$



If $\varrho_i \to 0$, we recover the input PS result.

Admissible area: Inside the cycle centered at $1/\varrho_i$ and of radius $\sqrt{\epsilon_i/\varrho_i + 1/\varrho_i^2}$.

For a large enough value of ϵ, the circle will contain Nyquist plot of any Hurwitz system.

Physical Meanings of ϵ and ϱ

Consider the linear system

$$\dot{x} = Ax + Bu, \quad y = Cx, \quad A = \begin{bmatrix} 0 & 1 \\ -w_n^2 & -2\xi w_n \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 \\ 0 \end{bmatrix}^T.$$

It follows from Lyapunov function

$$V = x^T P x, \quad P = \begin{bmatrix} p_1 & p_2 \\ p_2 & p_3 \end{bmatrix}.$$

that

$$\dot{V} \leq -\frac{\varrho}{2} y^2 + uy + \frac{\epsilon}{2} u^2,$$

if and only if $p_1 > 0$, $p_1 p_3 > p_2^2$ and

$$W \triangleq \begin{bmatrix} -2w_n^2 p_2 + 0.5\varrho & p_1 - 2\xi w_n p_2 - w_n^2 p_3 & p_2 - 0.5 \\ p_1 - 2\xi w_n p_2 - w_n^2 p_3 & 2(p_2 - 2\xi w_n p_3) & p_3 \\ p_2 - 0.5 & p_3 & -0.5\epsilon \end{bmatrix} < 0.$$

Solutions of ϵ and ϱ using Lyapunov function from $A^T P + PA = \text{diag}\{-w_n, \ -1/w_n\} I$:

$$\varrho = w_n \quad \Longrightarrow \quad \epsilon = \frac{1}{w_n}\left(1 - \frac{1}{w_n}\right)^2 + 2\frac{1}{(2\xi w_n)^2 w_n}.$$

As ξ becomes smaller, ϵ increases.

Why PS Systems but not Passive Systems?

Some systems are passive:

First-order Hurwitz systems (e.g., $1/(s+a)$) are passive.

Parallel connection of two passive systems is passive.

Negative loop connection of two passive systems is passive.

Most high-order systems are not passive even though they consist of passive elements:

Serial connection of two passive systems is generally **not** passive, e.g., $1/(s+1)^2$.

Time delay is not passive

Discretization of passive systems is typically not passive, e.g., $1/s$.

Passive short (PS) systems form a much broader of systems:

All Lyapunov stable linear systems are either PS or can be made PS under an output feedback control

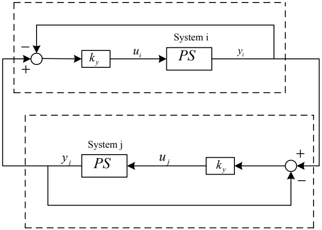
PS systems can be interconnected: parallel, series, negative feedback loop, positive feedback loop, etc.

The passive short framework applies directly to discretized systems.

Fundamental Property of Passivity-Short Systems

Consider a positive feedback connection of two PS systems. Cooperative stability (consensus) is ensured if

$$0 < k_y < 2/(\epsilon_i + \epsilon_j).$$



Impact on networked operation is revealed. Asymptotic stability could be further concluded if the systems are zero-state observable.

Proof: Consider
$\overline{V} \triangleq V_i + V_j$, $u_i = k_y(y_j - y_i)$, and $u_j = k_y(y_i - y_j)$. Then,

$$\begin{aligned}\overline{V} &\le \sum_{k=i,j}\left[V_k(z_k(0)) - \int_0^t [\eta_k(z_k) + u_k^T y_k + \frac{\epsilon_k}{2}\|u_k\|^2]ds\right] \\ &\le \overline{V}(0) - \frac{1}{2}[2-(\epsilon_i+\epsilon_j)k_y]k_y \int_0^t \|y_i - y_j\|^2 ds.\end{aligned}$$

Hence, we have

$$z_i, z_j \in L_\infty, \quad (y_i - y_j) \in L_2, \quad (y_i - y_j) \to 0.$$

Other interconnections (e.g., negative feedback connection) work as well.

Table of Contents

Control of Uncoupled Heterogeneous Systems Using an Information Graph

Communication graph: $S(t)$ with $S_{ii} \equiv 1$ and $S_{ij} \in \{0, 1\}$.

Network topology: Laplacian $L(t)$, where $D = \text{diag}\{S\mathbf{1}\}$ and $L = (D - S)$.

Heterogeneous systems:

$$\dot{z}_i = \mathcal{F}_i(z_i, v_i), \quad y_i = H_i(z_i),$$

each of which is passivity short with impact coefficient ϵ_i.

Cooperative control protocol:

$$u_i = k_{y_i} \sum_j (y_j - y_i) S_{ij}.$$

Impact Equivalence Principle: **As for fictitious systems $\dot{\mathbf{y}}_\mathbf{i} = \mathbf{u}_\mathbf{i}$**, consensus is ensured if the graph has at least one global reachable node and $k_{y_i} \le \overline{k}_y$ (which depends upon $\max \epsilon_i$).

If L is irreducible and fixed,

$$\overline{k}_y = \frac{\lambda_2(\Gamma L + L^T \Gamma)}{2(\max_i \epsilon_i)\lambda_{max}(L^T \Gamma L)}.$$

where $\gamma_1^T L = 0$, Γ is a diagonal matrix of entries in γ_1.

Advantages: networked systems, modularized design, plug-and-play operation.

Table of Contents

Example: Discrete-time 3-D Attitude Synchronization

Special Orthogonal group: $SO(3) \triangleq \{R \in \Re^{3\times3} | RR^T = I_3, \ \det(R) = 1\}$.

Given inertial frame $\sum_w$, attitude of body i (body frame $\sum_i$) is denoted by exponential coordinate $e^{\hat{\xi}\theta_{w_i}}$, where $\xi_{w_i} \in \Re^3$ and $\theta_{w_i} \in (-\pi + \epsilon, \pi - \epsilon)$ are the axis and angle of the rotation matrix, respectively.

$so(3) \triangleq \{S \in \Re^{3\times3} | S^T = -S\}$ is the Lie algebra of $SO(3)$.

Operator $\hat{\ } : \Re^3 \to so(3)$ (whose inverse is denoted by $\check{\ }$) is defined by

$$\hat{a} = (a)^{\wedge} \triangleq \begin{bmatrix} 0 & -a_3 & a_2 \\ a_3 & 0 & -a_1 \\ -a_2 & a_1 & 0 \end{bmatrix}.$$

Discrete-time 3-D Attitude Synchronization

Angular velocity of body i with respect to $\sum_w$ is

$$\omega^b_{w_i} \triangleq \left(e^{-\hat{\xi}\theta_{w_i}} \dot{e}^{\hat{\xi}\theta_{w_i}}\right)^{\check{}}.$$

A precise discrete-time model of rigid body motion to preserve the $SO(3)$ structure is

$$e^{\hat{\xi}\theta_{w_i}(k+1)} = e^{\hat{\xi}\theta_{w_i}(k)} e^{h\hat{\omega}^b_{w_i}(k)}.$$

Passivity-short property:

$$\phi(e^{\hat{\xi}\theta_{ij}(k+1)}) - \phi(e^{\hat{\xi}\theta_{ij}(k)}) \leq \left(\mathsf{sk}(e^{h\hat{\omega}^b_{w_i}(k)})^{\check{}}\right)^T \mathsf{sk}(e^{\hat{\xi}\theta_{w_i}(k)})^{\check{}} + \|\mathsf{sk}(e^{h\hat{\omega}^b_{w_i}(k)})^{\check{}}\|^2,$$

where

$$\mathsf{sk}(e^{\hat{\xi}\theta}) = \frac{1}{2}(e^{\hat{\xi}\theta} - e^{-\hat{\xi}\theta}), \quad \mathsf{sk}(e^{\hat{\xi}\theta})^{\check{}} = \hat{\xi}\sin\theta, \quad \mathsf{sk}(e^{h\hat{\omega}^b_{w_i}(k)})^{\check{}} = \omega^b_{w_i}\frac{\sin(h\|\omega^b_{w_i}\|)}{\|\omega^b_{w_i}\|}.$$

Discrete-time 3-D Attitude Synchronization Law

Control objective:

$$\lim_{k\to\infty} \phi(e^{\hat{\xi}\theta_{ij}(k)}) = 0,$$

where

$$e^{\hat{\xi}\theta_{ij}} \triangleq e^{-\hat{\xi}\theta_{w_i}} e^{\hat{\xi}\theta_{w_j}}, \quad \phi(e^{\hat{\xi}\theta_{ij}}) \triangleq \frac{1}{4}\|I_3 - e^{\hat{\xi}\theta_{ij}}\|_F^2 = \frac{1}{2}\mathsf{tr}(I_3 - e^{\hat{\xi}\theta_{ij}}).$$

Discrete-time synchronization law (based on passivity shortage):

$$\mathsf{sk}(e^{h\hat{\omega}^b_{w_i}(k)})^{\check{}} = hk_i \sum_{j\in\mathcal{N}_i} w_{ij}\mathsf{sk}(e^{h\hat{\xi}\theta_{ij}(k)})^{\check{}}.$$

Stability condition:

$$k_i < \frac{\sin\epsilon}{2h|\mathcal{N}_i| \max_{j\in\mathcal{N}_i} w_{ij}}.$$

Simulation of Discrete-time 3-D Attitude Synchronization

20 rigid bodies with $h = 0.02$ sec, randomly generated initial conditions, $\epsilon = \pi/10$:

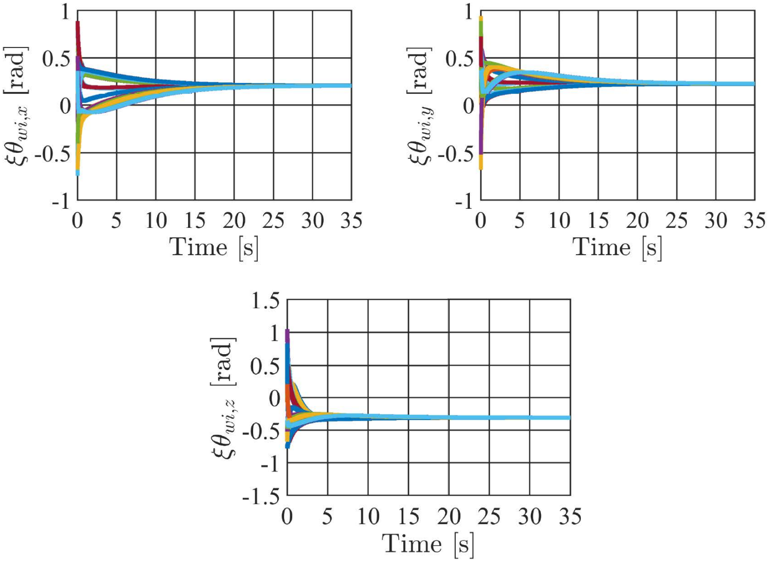


Table of Contents

Interconnected Heterogeneous Systems

Interconnected heterogeneous systems:

$$\dot{x}_i = A_i(x_i)x_i + B_i(x_i)v_i + \sum_{j\in\mathcal{N}_i} H_{ij}(y_i, y_j)(y_j - y_i), \quad y_i = C_i(x_i)x_i.$$

Local control: $v_i = -K_i(x_i)x_i + u_i$, which yields $\overline{A}_i(x_i) = A_i(x_i) - B_i(x_i)K_i(x_i)$.

If

$$\overline{M}_i(x_i, y_j) = \left[\begin{array}{c|cccc} \begin{array}{c}\overline{A}_i^T(x_i)P_i + P_i\overline{A}_i(x_i) + \rho_i C_i^T C_i \\ -\sum_{j\in\mathcal{N}_i}(P_i H_{ij} C_i + C_i^T H_{ij}^T P_i)\end{array} & \cdots & P_i H_{ij}(y_i, y_j) & \cdots & P_i B_i - C_i^T \\ \hline \vdots & \vdots & 0 & \vdots & 0 \\ H_{ij}^T(y_i, y_j)P_i & 0 & -\epsilon_{ij} I & 0 & 0 \\ \vdots & \vdots & 0 & \vdots & 0 \\ B_i^T P_i - C_i & 0 & 0 & 0 & -\epsilon_{ii} I \end{array}\right] \le 0,$$

then

$$\dot{V}_i \le u_i^T y_i + \frac{\epsilon_{ii}}{2}\|u_i\|^2 - \frac{\rho_i}{2}\|y_i\|^2 + \frac{1}{2}\sum_{j\in\mathcal{N}_i}\epsilon_{ij}\|y_j\|^2.$$

Modular and Data-Driven Control Design

Network-level model:

$$\dot{V}_i \le u_i^T y_i + \frac{\epsilon_{ii}}{2}\|u_i\|^2 - \frac{\rho_i}{2}\|y_i\|^2 + \frac{1}{2}\sum_{j\in\mathcal{N}_i}\epsilon_{ij}\|y_j\|^2.$$

Local design criterion:

$$\min \sum_{j\in\mathcal{N}_i}\alpha_{ij}\epsilon_{ij}$$

subject to $\alpha_{ij} > 0$ and $\overline{M}_i(x_i, y_j) \le 0$.

Networked control on an information graph:

$$u_i = -k_{c_i}\sum_j S_{ij}^c(t)(y_j - y_i) = -K_c L y.$$

Cooperative control design criterion: Find k_{c_i} such that

$$Q = \Gamma L^T + L\Gamma - L^T K_c W L + \Psi > 0,$$

where $\Psi = \text{diag}\{\psi_i\}$ with

$$\psi_i = \frac{\gamma_i\rho_i}{k_{c_i}} - \sum_{j=1:n;\; i\in\mathcal{N}_j}\frac{\gamma_j}{k_{c_j}}\epsilon_{ji},$$

Advantages: networked systems, modularized design, plug-and-play operation, and data-driven.

Table of Contents

Destabilizing Attacks

A system under attack:

$$\dot{y} = -L_s y + L_a d, \quad \dot{d} = F_a d + B_a y$$

Consider the case $L_a = L_s$ and the injection model is a low-pass filter with $F_a = -\lambda_a I$ and $B_a = I$. Then y grows **unbounded** for all $\lambda_a \in (0, 1)$

The overall system is

$$\begin{bmatrix} \dot{d} \\ \dot{y} \end{bmatrix} = \begin{bmatrix} -\lambda_a I & I \\ L_s & -L_s \end{bmatrix} \begin{bmatrix} d \\ y \end{bmatrix} \Rightarrow \text{det}[s^2 I + (L_s + \lambda_a I)s + (\lambda_a - 1)L_s] = 0$$

which is unstable for $\lambda_a < 1$.

There are numerous choices of F_a, B_a that leads to instability.

$\Rightarrow$ need to make the system robust to any possible attacks.

Table of Contents

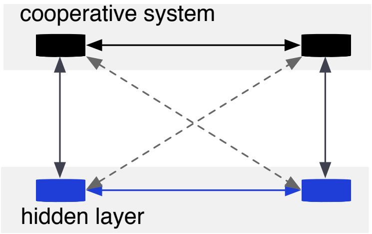
Example: A Two-Node Robust Cooperative System

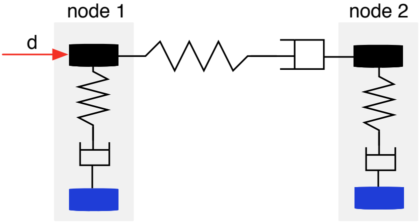
Consider a network with two nodes interconnected with a hidden layer:

$$\begin{bmatrix} \dot{y}_1 \\ \dot{y}_2 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} + \beta \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} + \begin{bmatrix} d_1 \\ d_2 \end{bmatrix}$$
$$\begin{bmatrix} \dot{z}_1 \\ \dot{z}_2 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} - \beta \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$$

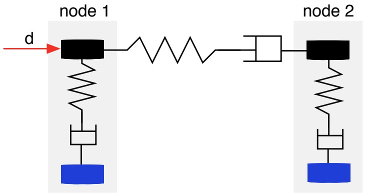
which can be rewritten as

$$\begin{bmatrix} \dot{y}_1 \\ \dot{z}_1 \end{bmatrix} = \begin{bmatrix} -1 & \beta \\ -\beta & -1 \end{bmatrix} \begin{bmatrix} y_1 \\ z_1 \end{bmatrix} + \begin{bmatrix} 1 & -\beta \\ \beta & 1 \end{bmatrix} \begin{bmatrix} y_2 \\ z_2 \end{bmatrix} + \begin{bmatrix} d_1 \\ 0 \end{bmatrix}$$
$$\begin{bmatrix} \dot{y}_2 \\ \dot{z}_2 \end{bmatrix} = \begin{bmatrix} -1 & \beta \\ -\beta & -1 \end{bmatrix} \begin{bmatrix} y_2 \\ z_2 \end{bmatrix} + \begin{bmatrix} 1 & -\beta \\ \beta & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ z_1 \end{bmatrix} + \begin{bmatrix} d_2 \\ 0 \end{bmatrix}$$





Intuitive Explanation of Competitive Interaction



Transfer function for node 1 from attack/disturbance d_1 to y_1 is given by

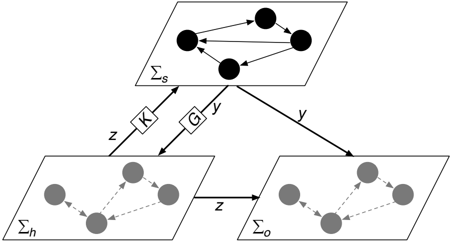
$$\frac{Y_1}{d} = \frac{s+1}{s^2 + 2s + 1 + \beta^2}$$

The resonance frequency is $1 + \beta^2$. Hence, $\beta \uparrow$ yields resonance frequency $\uparrow$.

Robustness design against attacks: 1) superiority of information access; 2) design *virtual nodes* so they do not impact normal operation of the system; 3) automatic activation when attacks appear anywhere in the system; 4) *synthetic anchors* to maintain system stability while state estimation is in progress; 5) Mitigation measures embedded

Table of Contents

Topology Condition on Hidden Layer Design



Networked system nodes y (Σ_s), virtual nodes z (Σ_h), observation nodes (Σ_o):

$$\dot{y} = -L_s y + \beta K z + L_s d,$$
$$\dot{z} = -L_h z - \beta G y,$$
$$\dot{d} = F_a d + B_a y,$$

where:
$\beta > 0$: design parameter

Lemma: If $d = 0$, $y \to \mathbf{1}\nu_{s1}^T x(0)/(\nu_{s1}^T \mathbf{1})$ as $t \to \infty$ provided that:

$$\Gamma_h G = K^T \Gamma_s, \text{ and } \nu_{s1}^T K = 0,$$

where $\Gamma_s = \text{diag}\{\nu_{s1}\}$ and $\Gamma_h = \text{diag}\{\nu_{h1}\}$.

Note: $G\mathbf{1} = 0 \implies$ consensus value of z is not impacted by y

Sketch of proof: Lyapunov candidate $V(y, z) = y^T \Gamma_s y + z^T \Gamma_h z$

Robust Design of Cooperative Systems

System:

$$\dot{y} = -L_s y + \beta L_s z + L_s d,$$
$$\dot{z} = -L_h z - \beta \Gamma_h^{-1} L_s^T \Gamma_s y,$$
$$\dot{d} = F_a d + B_a y,$$

Theorem: $y \in \mathcal{L}_\infty$ for all possible choices of F_a and B_a and, by increasing β, y converges to an arbitrarily small neighborhood

$$\lim_{t\to\infty} y(t) = \frac{\nu_{s1}^T y(t_0)}{\nu_{s1}^T \mathbf{1}} \mathbf{1} + (I + F_a^{-1} B_a + \beta^2 M_h)^{-1} \left[(c_1 + \beta c_2)\mathbf{1} - F_a^{-1} B_a \frac{\nu_{s1}^T y(t_0)}{\nu_{s1}^T \mathbf{1}} \mathbf{1} \right],$$

where $\Gamma_h^{-1} L_s^T \Gamma_s = L_h M_h$, and c_1 and c_2 are some constants.

Sketch of proof: $V = \beta \tilde{y}^T \Gamma_s \tilde{y} + \beta \tilde{z}^T \Gamma_h \tilde{z} + d^T P_a d + 2\tilde{z}^T \Gamma_h d,$

$$\dot{\tilde{y}} = -L_s(\tilde{y} - \beta \tilde{z} - d),$$
$$\dot{\tilde{z}} = -L_h(\tilde{z} + \beta M_h \tilde{y}),$$
$$\dot{d} = F_a d + B_a \tilde{y}.$$

Identification of Stealthy Attacks

When there is **no** attack

$$y \to \mathbf{1}\nu_{s1}^T y(t_0)/(\nu_{s1}^T \mathbf{1}), \quad z \to \mathbf{1}\nu_{h1}^T z(t_0)/(\nu_{h1}^T \mathbf{1}).$$

Under attacks, states y, z deviate from above values by $\tilde{y}^e, \tilde{z}^e$

Let $\mathcal{A}$ with $\dim(\mathcal{A}) = m < n$ be a set of nodes being attacked and

$$d^e = (\tilde{x}^e - \beta \tilde{z}^e) - c_1 \mathbf{1}$$

which is not unique.

If $m \leq \lfloor n/2 \rfloor$, the set $\mathcal{A}$ can be found uniquely by solving $\hat{c}_1$ in

$$\hat{c}_1 = \text{argmin}_{c_1} \|(\tilde{x}^e - \beta \tilde{z}^e) - c_1 \mathbf{1}\|_{l_0}$$

where $\|y\|_{l_0}$ is the number of non-zero elements in vector y.
Note: ν_{s1}, ν_{h1} can be estimated distributively.

References

Plug & play control of passivity-short systems:

- Z. Qu and M. A. Simaan, "Modularized Design for Cooperative Control and Plug-And-Play Operation of Networked Heterogeneous Systems," *Automatica*, vol.50, no.9, pp.2405-2414, September 2014.
- Ying Xu, Zhihua Qu, and Toru Namerikawa, "Data-Driven Wide-Area Control Design of Power System Using the Passivity Shortage Framework," *IEEE Transactions on Power Systems*, revision under review.

SO(3) control

- T. Ibuki, T. Hatanaka and Z. Qu, "Discrete-time 3-D Attitude Synchronization Based on Passivity Shortage," *IEEE Conference on Decision and Control*, Fontainebleau, Miami Beach, FL, USA, Dec. 17-19, 2018.

Robustification using competitive interaction

- A. Gusrialdi, Z. Qu, and M. A. Simaan, "Competitive Interaction Design of Cooperative Systems Against Attacks," *IEEE Transactions on Automatic Control*, vol.63, no.9, pp.3159-3166, September 2018.

Distributed estimation:

- A. Gusrialdi and Z. Qu, "Distributed Estimation of All the Eigenvalues and Eigenvectors of Matrices Associated with Strongly Connected Digraphs," *IEEE Control Systems Letters*, vol.1, no.2, pp. 328-333, October 2017.

Q&A

Thanks!