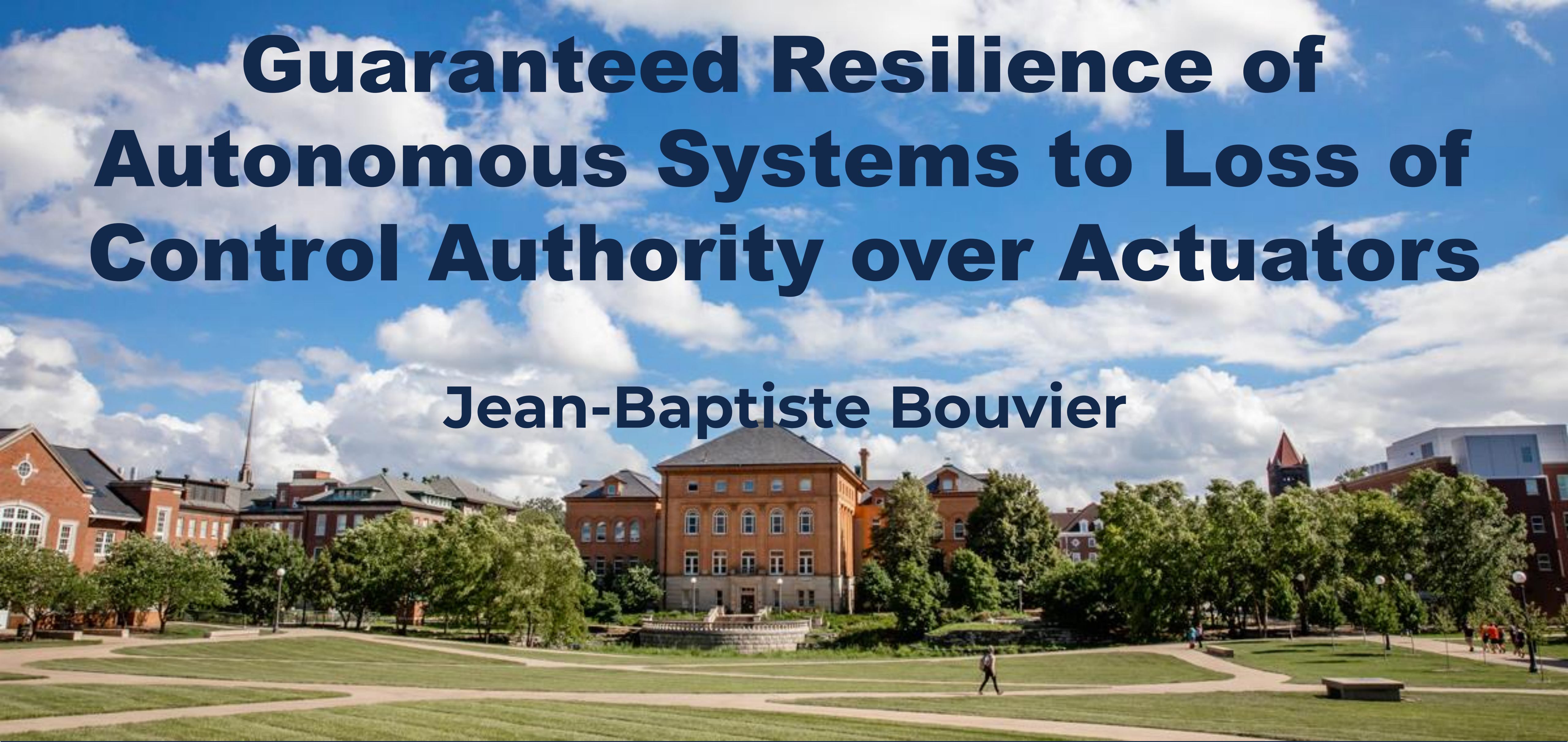
Guaranteed Resilience of Autonomous Systems to Loss of Control Authority over Actuators

Jean-Baptiste Bouvier



Grainger College of Engineering
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Aerospace Engineering
Elevating Ideas Since 1944

Motivating examples

More than 1m litres of untreated sewage released into waterways and local parks

Maroochy SCADA attack, 2013

The Nauka module of the ISS lost control authority over its thrusters.

M. Bartels, “Russia says ’software failure’ caused thruster misfire at space station,” space.com, 2021.
J. Slay and M. Miller, “Lessons learned from the Maroochy water breach,” in Critical Infrastructure Protection, Springer, 2008.

Framework

Loss of control authority over an actuator, that now produces uncontrolled and possibly **undesirable inputs** with its full actuation capacity.

Fault Detection and Isolation module measuring in real-time all actuators outputs.

J. Davidson, F. Lallman, and T. Bundick, “Real-time adaptive control allocation applied to a high-performance aircraft,” in 5th SIAM Conference on Control, 2001.

Framework

Nominal system

$$\dot{x}(t) = f(x(t), \bar{u}(t)), \qquad x(0) = x_0, \qquad \bar{u}(t) \in \bar{\mathcal{U}}.$$

After a partial loss of control authority over actuators, we split $\bar{u}$ into u (controls) and w (undesirable inputs).

Malfunctioning system

$$\dot{x}(t) = f(x(t), [u(t)\, w(t)]), \qquad x(0) = x_0, \qquad u(t) \in \mathcal{U}, \qquad w(t) \in \mathcal{W}.$$

Problems of interest (1)

Can the malfunctioning system still complete the nominal mission?

Target $\mathcal{T}$ is **resiliently reachable** from x_0 by the malfunctioning system if for all $w \in \mathcal{W}$ there exists $u_w \in \mathcal{U}$ and $T \geq 0$ such that $x(T) \in \mathcal{T}$.

Problem 1: Under what condition is a target $\mathcal{T}$ resiliently reachable by the malfunctioning system?

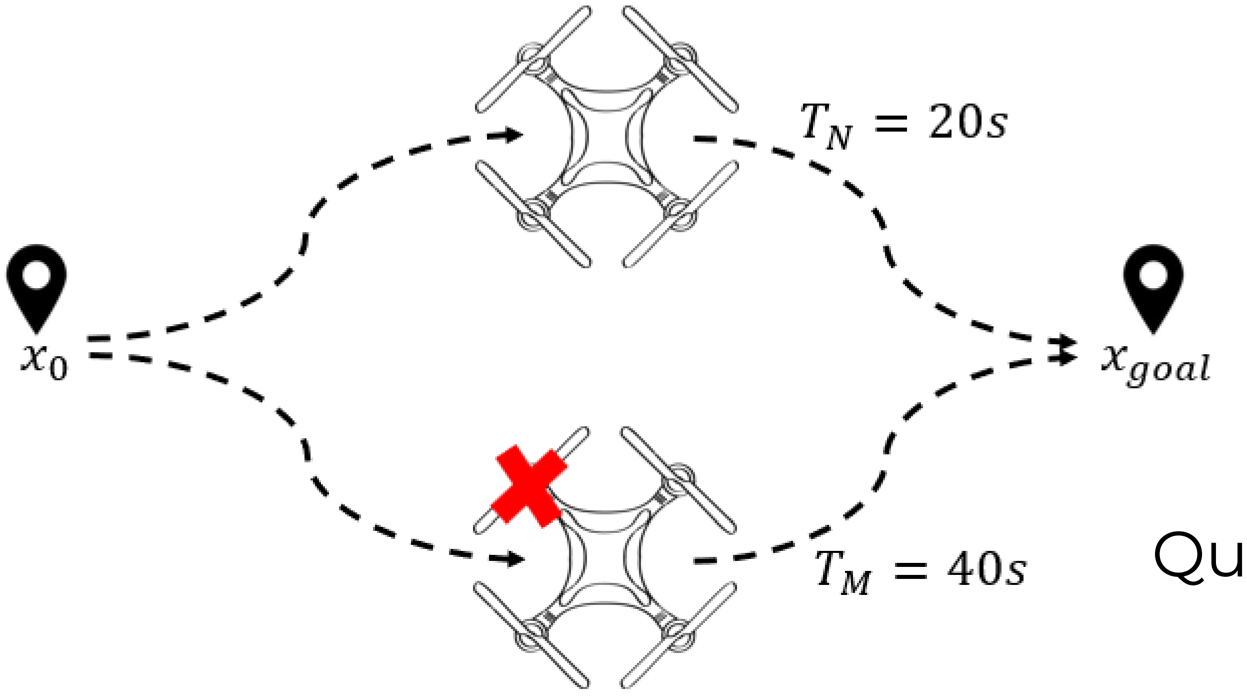
Problems of interest (2)

Safety critical systems should be capable of resiliently completing their mission despite a loss of control authority over any one of their actuators.

Nominal system is **resilient** to a loss of control authority if any target $\mathcal{T}$ is resiliently reachable by malfunctioning system.

Problem 2: How to design a system resilient to the loss of control authority over any one of its actuators?

Problems of interest (3)



Nominal reach time $T_N^*(x_0,\ x_{goal})$

Malfunctioning reach time $T_M^*(x_0,\ x_{goal})$

Quantitative resilience $r_q = \inf\limits_{x_0, x_{goal}} \frac{T_N^*(x_0, x_{goal})}{T_M^*(x_0, x_{goal})}$

Problem 3: How to calculate efficiently the quantitative resilience of an autonomous system?

Problems of interest (4)

Limiting assumptions:

- the controller $u(t)$ has immediate knowledge of the undesirable input $w(t)$
- the nominal mission is to reach a target $\mathcal{T}$
- the nominal dynamics are linear: $\dot{x}(t) = Ax(t) + \bar{B}\bar{u}(t)$.

Problem 4: How to extend the scope of resilience theory?

Outline

I. Linear systems with bounded energy
   A. Resilient reachability
   B. Resilience of driftless systems
   C. Control synthesis

II. Linear systems with bounded amplitude
   A. Resilient reachability
   B. Quantitative resilience of driftless systems
   C. Quantitative resilience of linear systems

III. Latest contributions to resilience theory
   A. Extensions of resilience theory
   B. Resilience of an orbital inspection mission
   C. Resilience of linear networks

Linear systems with bounded energy

Nominal system: $\dot{x}(t) = Ax(t) + \bar{B}\bar{u}(t)$ $x(0) = x_0.$

Partial loss of control authority: split $\bar{B}$ in B controlled actuators and C uncontrolled actuators. Similarly, $\bar{u}$ is split in controls u and undesirable inputs w .

Malfunctioning system: $\dot{x}(t) = Ax(t) + Bu(t) + Cw(t)$ $x(0) = x_0.$

Energy bounded inputs: $\|u\|_{L_2}^2 = \int_0^\infty \|u(t)\|^2 dt \leq 1$ and $\|w\|_{L_2}^2 \leq 1.$

Outline

I. Linear systems with bounded energy
   A. Resilient reachability
   B. Resilience of driftless systems
   C. Control synthesis

II. Linear systems with bounded amplitude
   A. Resilient reachability
   B. Quantitative resilience of driftless systems
   C. Quantitative resilience of linear systems

III. Latest contributions to resilience theory
   A. Extensions of resilience theory
   B. Resilience of an orbital inspection mission
   C. Resilience of linear networks

Resilient reachability

From [Delfour], target $\mathcal{T} = \{x \in \mathbb{R}^n : \|x - x_{goal}\| \leq \varepsilon\}$ is resiliently reachable from x_0 in a time T if and only if

$$\sup_{\|x^*\|=1} \left\{ x^*(e^{AT}x_0) + \inf_{u \in U}\{S^*x^*(u)\} + \sup_{w \in W}\{R^*x^*(w)\} - \sup_{y \in \mathcal{T}}\{x^*(y)\} \right\} \leq 0.$$

With the Riesz representation theorem, it simplifies to

$$\max_{\|h\|=1} \left\{ h^\top\left(e^{AT}x_0 - x_{goal}\right) - \sup_{\|u\|=1} \left\{ h^\top \int_0^T e^{A(T-t)}Bu(t)\,dt \right\} + \sup_{\|w\|=1} \left\{ h^\top \int_0^T e^{A(T-t)}Cw(t)\,dt \right\} \right\} \leq \varepsilon.$$

M. Delfour and S. Mitter, “Reachability of perturbed systems and min sup problems”, SIAM Journal on Control and Optimization, 1969.

J.-B. Bouvier and M. Ornik, “Resilient reachability for linear systems”, IFAC 2020.

Resilient reachability

Driftless linear systems: $\dot{x}(t) = Bu(t) + Cw(t) \quad x(0) = x_0, \quad \|u\|_{L_2}^2 \leq 1, \quad \|w\|_{L_2}^2 \leq 1.$

The integral condition becomes $\max\limits_{\|h\|=1} \left\{ h^\top \left(x_0 - x_{goal} \right) + \sqrt{T} \left(\|C^\top h\| - \|B^\top h\| \right) \right\} \leq \varepsilon.$

Resilient reachability **before some time** is dictated by the sign of

$$g(h) \coloneqq \|C^\top h\| - \|B^\top h\|.$$

A driftless systems is resilient if and only if $\max\limits_{\|h\|=1} g(h) < 0$ or if $BB^\top - CC^\top \succ 0.$

J.-B. Bouvier and M. Ornik, "Resilient reachability for linear systems", IFAC 2020.

Outline

I. Linear systems with bounded energy
   A. Resilient reachability
   B. Resilience of driftless systems
   C. Control synthesis

II. Linear systems with bounded amplitude
   A. Resilient reachability
   B. Quantitative resilience of driftless systems
   C. Quantitative resilience of linear systems

III. Latest contributions to resilience theory
   A. Extensions of resilience theory
   B. Resilience of an orbital inspection mission
   C. Resilience of linear networks

Resilience of driftless systems

System $\dot{x} = \bar{B}\bar{u}$ is **p-resilient**, if it is resilient to the loss of any p columns of $\bar{B}$.

How much overactuation is needed for 1-resilience?

$\bar{B} = \begin{bmatrix} 1 & 1 \end{bmatrix}$ 🚫 $\bar{B} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$ ✓

$\bar{B} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ 🚫 $\bar{B} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$ ✓ $\bar{B} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0.5 \\ 0 & 1 & 0 & 1 & 0.5 \end{bmatrix}$ ✓

In n dimensions, $2n + 1$ actuators are the minimum for 1-resilience.
2-resilience is much harder.

J.-B. Bouvier and M. Ornik, “Designing resilient linear systems”, IEEE Transactions on Automatic Control, 2022.

Outline

I. Linear systems with bounded energy
   A. Resilient reachability
   B. Resilience of driftless systems
   C. Control synthesis

II. Linear systems with bounded amplitude
   A. Resilient reachability
   B. Quantitative resilience of driftless systems
   C. Quantitative resilience of linear systems

III. Latest contributions to resilience theory
   A. Extensions of resilience theory
   B. Resilience of an orbital inspection mission
   C. Resilience of linear networks

Control synthesis

A resilient control law u_w, $\|u_w\|_{L_2} \leq 1$ should drive the state of $\dot{x}(t) = Bu(t) + Cw(t)$ from x_0 to x_{goal} despite any undesirable input w satisfying $\|w\|_{L_2} \leq 1$.

If $\mathrm{BB}^\top - \mathrm{CC}^\top \succ 0$, there exists $\alpha > 0$ such that

$$u_w(\mathrm{t}) = B^\top (BB^\top)^{-1}\Big(-Cw(t) + \alpha\big(x(t) - x_{goal}\big)\Big).$$

α depends on $x_{goal} - x_0$: the further the target, the smaller the control.

u_w yields asymptotical convergence.

J.-B. Bouvier and M. Ornik, “Designing resilient linear systems”, IEEE Transactions on Automatic Control, 2022.

Outline

I. Linear systems with bounded energy
   A. Resilient reachability
   B. Resilience of driftless systems
   C. Control synthesis

II. Linear systems with bounded amplitude
   A. Resilient reachability
   B. Quantitative resilience of driftless systems
   C. Quantitative resilience of linear systems

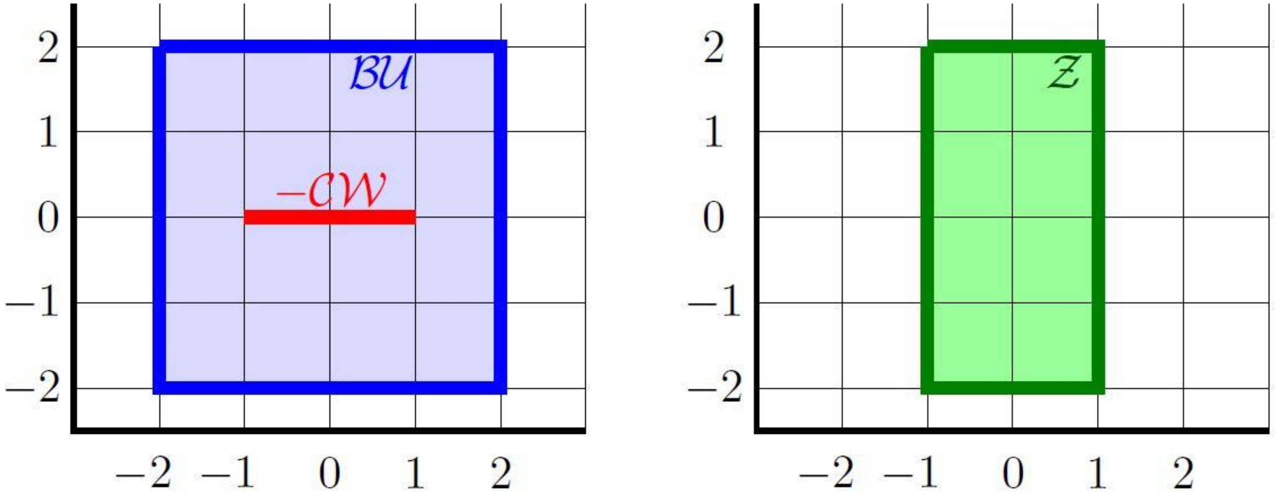
III. Latest contributions to resilience theory
   A. Extensions of resilience theory
   B. Resilience of an orbital inspection mission
   C. Resilience of linear networks

Linear systems with bounded amplitude

Malfunctioning system: $\dot{x}(t) = Ax(t) + Bu(t) + Cw(t) \qquad x(0) = x_0.$

Amplitude bounded inputs: $u(t) \in \mathcal{U}$ and $w(t) \in \mathcal{W}$, hyperrectangles.

For $B = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ and $C = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, with $\mathcal{U} = [-1,1]^4$ and $\mathcal{W} = [-1,1]$:



$\mathcal{Z} = B\mathcal{U} \ominus (-C\mathcal{W}) = \{z \in B\mathcal{U} \colon \forall\, w \in \mathcal{W},\ z - Cw \in B\mathcal{U}\}$ Minkowski difference of $B\mathcal{U} = \{Bu : u \in \mathcal{U}\}$ and $-C\mathcal{W} = \{-Cw : w \in \mathcal{W}\}$.

J.-B. Bouvier and M. Ornik, “Quantitative resilience of linear systems”, European Control Conference 2022.

Outline

I. Linear systems with bounded energy
  A. Resilient reachability
  B. Resilience of driftless systems
  C. Control synthesis

II. Linear systems with bounded amplitude
  A. Resilient reachability
  B. Quantitative resilience of driftless systems
  C. Quantitative resilience of linear systems

III. Latest contributions to resilience theory
  A. Extensions of resilience theory
  B. Resilience of an orbital inspection mission
  C. Resilience of linear networks

Resilient reachability

Extension of Hájek's duality theorem: $\dot{x}(t) = Ax(t) + Bu(t) + Cw(t)$ is resilient if and only if $\dot{x}(t) = Ax(t) + z(t)$ is controllable, with $z(t) \in \mathcal{Z} = \mathcal{BU} \ominus (-\mathcal{CW})$.

The system is resilient if and only if $Re\big(\lambda(A)\big) = 0,\ rank[Z\ AZ\ \ \dots A^{n-1}Z] = n,$ and there is no real eigenvector v of $A^\top$ satisfying $v^\top z \leq 0$ for all $z \in \mathcal{Z}$.

Matrix Z is built such that $Image(Z) = span(\mathcal{Z})$.

O. Hájek, "Duality for differential games and optimal control", Mathematical Systems Theory, 1974.
R. Brammer, "Controllability in linear autonomous systems with positive controllers", SIAM Journal on Control, 1972.
J.-B. Bouvier and M. Ornik, "Resilience of linear systems to loss of control authority", Automatica, 2023.

Outline

I. Linear systems with bounded energy

   A. Resilient reachability

   B. Resilience of driftless systems

   C. Control synthesis

II. Linear systems with bounded amplitude

   A. Resilient reachability

   B. Quantitative resilience of driftless systems

   C. Quantitative resilience of linear systems

III. Latest contributions to resilience theory

   A. Extensions of resilience theory

   B. Resilience of an orbital inspection mission

   C. Resilience of linear networks

Quantitative resilience

Nominal reach time $T_N^*(x_0, x_{goal}) = \inf_{\bar{u} \in \bar{U}_\infty} \{T : x(T) = x_{goal}\}$

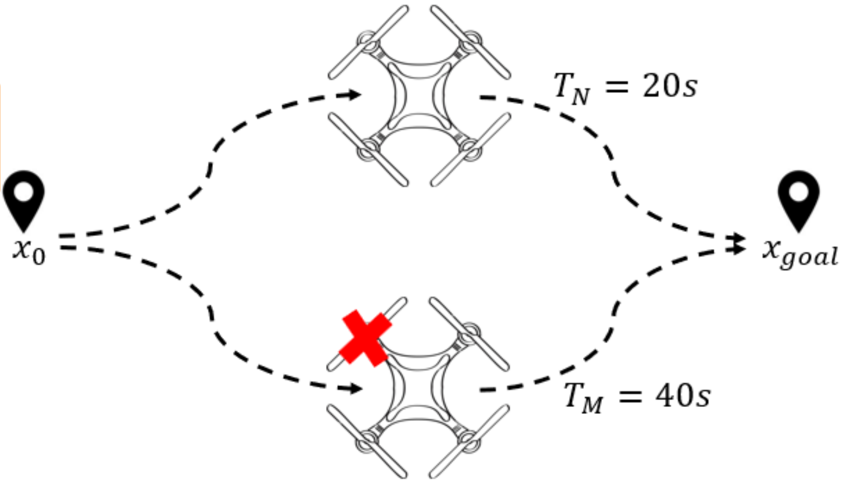
for $\dot{x}(t) = Ax(t) + \bar{B}\bar{u}(t)$.

Malfunctioning reach time $\mathrm{T}_\mathrm{M}^*(x_0, x_{goal}) = \sup_{w \in W_\infty} \left\{ \inf_{u \in U_\infty} \{T : x(T) = x_{goal}\} \right\}$

for $\dot{x}(t) = Ax(t) + Bu(t) + Cw(t)$.

Quantitative resilience $r_q = \inf_{x_0, x_{goal}} \frac{T_N^*(x_0, x_{goal})}{T_M^*(x_0, x_{goal})} \leq 1.$

How to calculate r_q?



Quantitative resilience of driftless systems

Nominal reach time $T_N^*(d) = \min_{\bar{u} \in \bar{\mathcal{U}}} \{ T : \bar{B}\bar{u}T = d\}$

for $\dot{x}(t) = \bar{B}\bar{u}(t)$ and with $d = x_{goal} - x_0$.

Malfunctioning reach time $\mathrm{T}_{\mathrm{M}}^*(d) = \max_{w \in \mathcal{V}} \left\{ \min_{u \in \mathcal{U}} \{T \geq 0 : (Bu + Cw)T = d\} \right\}$

for $\dot{x}(t) = Bu(t) + Cw(t)$ and with $\mathcal{V}$ vertices of $\mathcal{W}$.

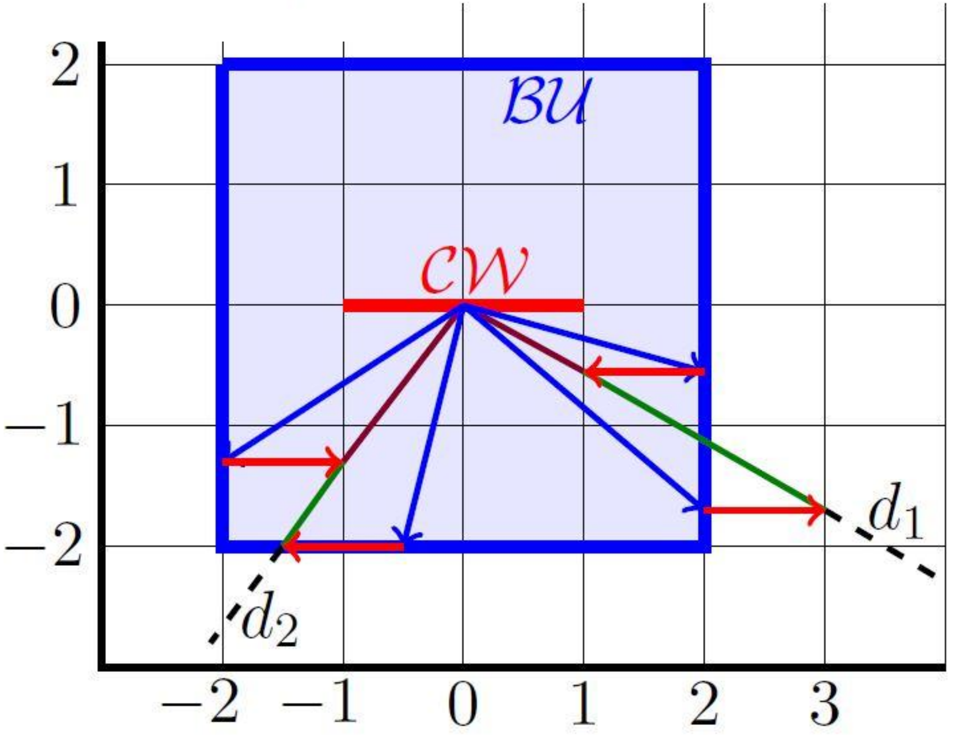
Quantitative resilience $r_q = \inf_{d \in \mathbb{R}^n} \frac{T_N^*(d)}{T_M^*(d)} \leq 1.$

J.-B. Bouvier, K. Xu and M. Ornik, "Quantitative resilience of linear driftless systems", SIAM Conference on Control and its Applications, 2021.

Quantitative resilience of driftless systems

$$r_q = \inf_{d\,\in\,\mathbb{R}^n} \frac{T_N^*(d)}{T_M^*(d)} = \inf_{d\,\in\,\mathbb{S}} \frac{T_N^*(d)}{T_M^*(d)} = \inf_{d\,\in\,\mathbb{S}} \frac{\min\limits_{x\,\in\,\mathcal{CW}}\left\{\max\limits_{y\,\in\,\mathcal{BU}}\big\{\|x+y\| : x+y \in \mathbb{R}^+ d\big\}\right\}}{\max\limits_{x\,\in\,\mathcal{CW},\, y\,\in\,\mathcal{BU}}\big\{\|x+y\| : x+y \in \mathbb{R}^+ d\big\}}.$$

$$r_q = \min_{d\,\in\,\mathbb{S}} \frac{\mathit{purple}}{\mathit{purple} + \mathit{green}}$$



The Maximax Minimax Quotient Theorem states that the maximum occurs for d aligned with $\mathcal{CW}$.

J.-B. Bouvier and M. Ornik, “The Maximax Minimax Quotient Theorem”, Journal of Optimization Theory and Applications, 2022.

Outline

I. Linear systems with bounded energy
   A. Resilient reachability
   B. Resilience of driftless systems
   C. Control synthesis
II. Linear systems with bounded amplitude
   A. Resilient reachability
   B. Quantitative resilience of driftless systems
   C. Quantitative resilience of linear systems
III. Latest contributions to resilience theory
   A. Extensions of resilience theory
   B. Resilience of an orbital inspection mission
   C. Resilience of linear networks

Quantitative resilience of linear systems

$T_N^*(x_0)$ nominal reach time to 0 for $\dot{x}(t) = Ax(t) + \bar{B}\bar{u}(t)$.
$T_M^*(x_0)$ malfunctioning reach time to 0 for $\dot{x}(t) = Ax(t) + Bu(t) + Cw(t)$.

- Optimal inputs are bang-bang.
- Geometrical approach cannot be adapted.
- No closed form solution like in the driftless case.
- Numerous algorithms to compute T_N^*.
- Algorithms from pursuit-evasion game framework to compute T_{M}^*.

J. Eaton, "An iterative solution to time-optimal control," Journal of Mathematical Analysis and Applications, 1962.
M. Athans, "The status of optimal control theory and applications for deterministic systems," IEEE Transactions on Automatic Control, 1966.
Y. Sakawa, "Solution of linear pursuit-evasion games", SIAM Journal on Control, 1970.

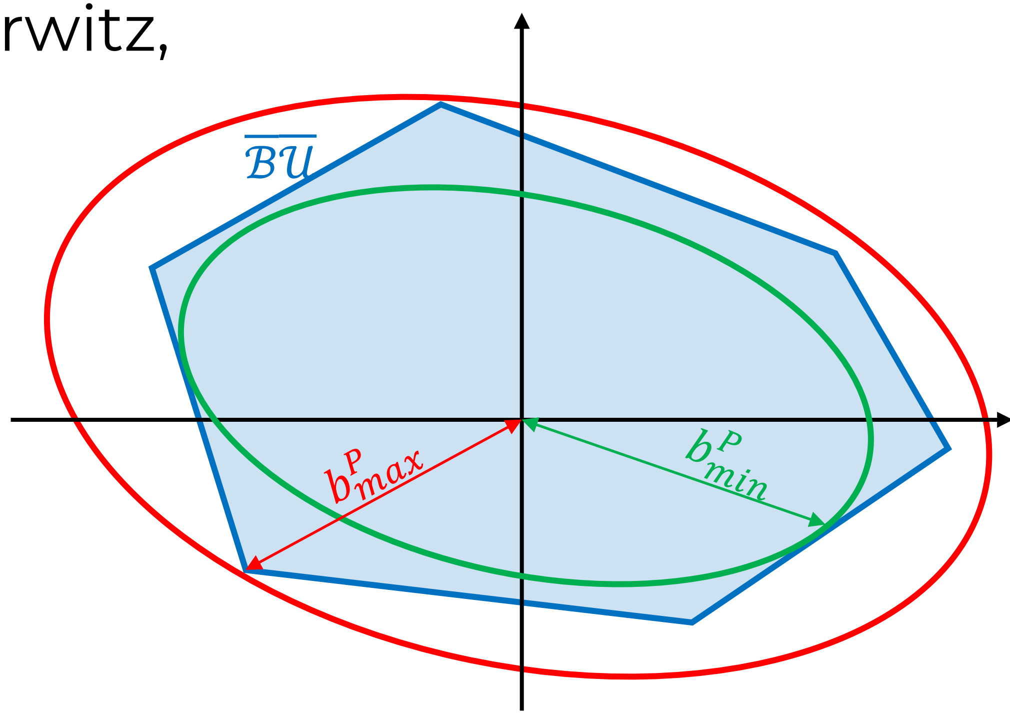
Quantitative resilience of linear systems

If $\dot{x}(t) = Ax(t) + \bar{B}\bar{u}(t)$ is controllable and A is Hurwitz,

then $T_N^*(x_0) \geq 2\,\frac{\lambda_{min}^P}{\lambda_{max}^Q}\,ln\left(1 + \frac{\lambda_{max}^Q \|x_0\|_P}{2\lambda_{min}^P b_{max}^P}\right)$,

$P \succ 0, \quad Q \succ 0, \quad PA + A^\top P = -Q, \quad \|x\|_P^2 = x^\top P x$

and $\quad b_{max}^P = \max\{\|\bar{B}\bar{u}\|_P : \bar{u} \in \bar{\mathcal{U}}\}$.



If $\bar{B}$ is full-rank, $T_N^*(x_0) \leq 2\,\frac{\lambda_{max}^P}{\lambda_{min}^Q}\,ln\left(1 + \frac{\lambda_{min}^Q \|x_0\|_P}{2\lambda_{max}^P b_{min}^P}\right)$,

with $b_{min}^P = \min\{\|\bar{B}\bar{u}\|_P : \bar{u} \in \partial\bar{\mathcal{U}}\}$.

J.-B. Bouvier and M. Ornik, “Quantitative Resilience of Linear Systems”, European Control Conference 2022.

Quantitative resilience of linear systems

If $\dot{x}(t) = Ax(t) + Bu(t) + Cw(t)$ is resiliently stabilizable, then

$$2\,\frac{\lambda_{min}^{P}}{\lambda_{max}^{Q}}\,ln\left(1 + \frac{\lambda_{max}^{Q}||x_0||_P}{2\lambda_{min}^{P} z_{max}^{P}}\right) \leq T_M^*(x_0) \leq 2\,\frac{\lambda_{max}^{P}}{\lambda_{min}^{Q}}\,ln\left(1 + \frac{\lambda_{min}^{Q}||x_0||_P}{2\lambda_{max}^{P} z_{min}^{P}}\right),$$

$$min\left(\frac{\lambda_{min}^{P}\lambda_{min}^{Q}}{\lambda_{max}^{P}\lambda_{max}^{Q}}, \frac{z_{min}^{P}}{b_{max}^{P}}\right) \leq r_q \leq min\left(\frac{\lambda_{max}^{P}\lambda_{max}^{Q}}{\lambda_{min}^{P}\lambda_{min}^{Q}}, \frac{z_{max}^{P}}{b_{min}^{P}}\right),$$

with $z_{min}^{P} = min\{\|z\|_P : z \in \partial\mathcal{Z}\}$, $z_{max}^{P} = max\{\|z\|_P : z \in \mathcal{Z}\}$ and $r_q = \inf\limits_{x_0 \in \mathbb{R}^n} \frac{T_N^*(x_0)}{T_M^*(x_0)}.$

J.-B. Bouvier and M. Ornik, "Quantitative Resilience of Linear Systems", European Control Conference 2022.

Outline

I. Linear systems with bounded energy
   A. Resilient reachability
   B. Resilience of driftless systems
   C. Control synthesis

II. Linear systems with bounded amplitude
   A. Resilient reachability
   B. Quantitative resilience of driftless systems
   C. Quantitative resilience of linear systems

III. Latest contributions to resilience theory
   A. Extensions of resilience theory
   B. Resilience of an orbital inspection mission
   C. Resilience of linear networks

Extensions of resilience theory

Limiting assumptions:

- the nominal mission is to reach a target $\mathcal{T}$,
- the controller $u(t)$ has immediate knowledge of the undesirable input $w(t)$,
- the nominal dynamics are linear: $\dot{x}(t) = Ax(t) + \bar{B}\bar{u}(t)$.

Resilient trajectory tracking

Malfunctioning system $\dot{x}(t) = Ax(t) + Bu(t) + Cw(t)$ with $x(0) = x_0$, $u(t) \in \mathcal{U}$, $w(t) \in \mathcal{W}$ and $\mathcal{Z} = B\mathcal{U} \ominus (-C\mathcal{W})$.

Reference trajectory: $\dot{x}_{ref}(t) = Ax_{ref}(t) + z_{ref}(t)$ with $z_{ref}(t) \in \mathcal{Z}_{ref}$.

Initial error correction:

$$\dot{y}(t) = Ay(t) + z_\varepsilon(t), \qquad y(0) = x_0 - x_{ref}(0), \qquad z_\varepsilon(t) \in \mathcal{Z}_\varepsilon \qquad (1.\varepsilon)$$

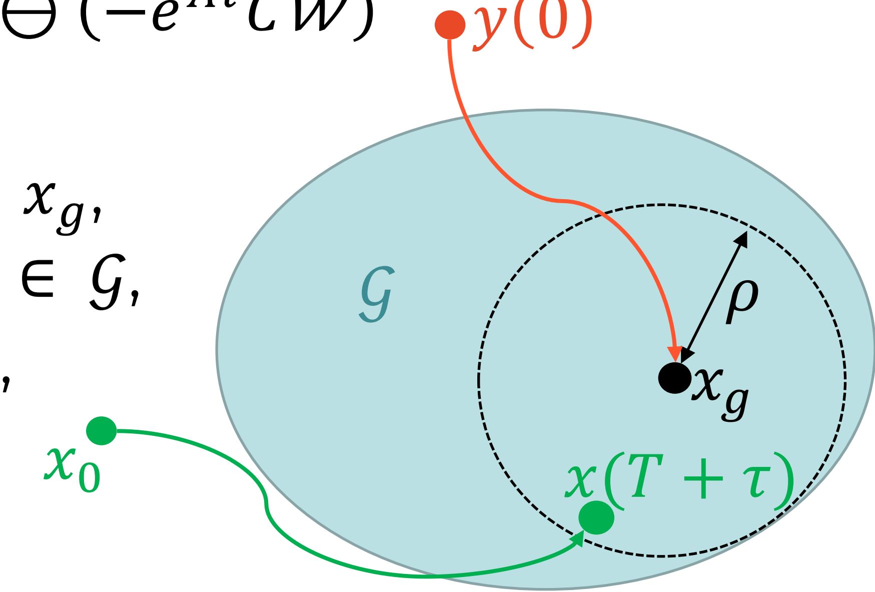
If $\mathcal{Z}_{ref} \oplus \mathcal{Z}_\varepsilon \subseteq \mathcal{Z}$ and $(1.\varepsilon)$ is stabilizable in a time t_f, then for all w, there exists u_w such that $x(t) = x_{ref}(t)$ for all $t \geq t_f$.

Resilience despite actuation delay

Actuation delay $\tau > 0$ such that $\dot{x}(t) = Ax(t) + Bu(t, x(t-\tau), w(t-\tau)) + Cw(t)$
with $x(0) = x_0,\ u(t) \in \mathcal{U},\ w(t) \in \mathcal{W}.$

$\dot{y}(t) = Ay(t) + z(t) \qquad y(0) = e^{A\tau}x_0 \qquad z(t) \in \mathcal{Z}_\tau = B\mathcal{U} \ominus (-e^{A\tau}C\mathcal{W})$

If there is $x_g \in \mathcal{G}$ such that $\mathbb{B}(x_g, \rho) \subseteq \mathcal{G}$ and $y(T) = x_g$,
then for all $w \in \mathcal{W}$ there is $u \in \mathcal{U}$ such that $x(T+\tau) \in \mathcal{G}$,
with $\rho = \frac{c}{\mu(A)}\left(e^{\mu(A)\tau} - 1\right),\quad c = max\{\|Cw\| : w \in \mathcal{W}\},$
and $\mu(A) = max\left\{\lambda\left(\frac{A+A^\top}{2}\right)\right\}.$



Resilience despite actuation delay

Actuation delay $\tau > 0$ such that $\dot{x}(t) = Ax(t) + Bu(t, x(t-\tau), w(t-\tau)) + Cw(t)$ with $x(0) = x_0,\ u(t) \in \mathcal{U},\ w(t) \in \mathcal{W}$.

Reference trajectory: $\dot{x}_{ref}(t) = Ax_{ref}(t) + z_{ref}(t)$ with $z_{ref}(t) \in \mathcal{Z}_{ref}$.

$$\dot{y}(t) = Ay(t) + z_\varepsilon(t), \qquad y(0) = e^{A\tau}\left(x_0 - x_{ref}(0)\right), \qquad z_\varepsilon(t) \in \mathcal{Z}_\varepsilon \qquad (2.\varepsilon)$$

If $\mathcal{Z}_{ref} \oplus \mathcal{Z}_\varepsilon \subseteq \mathcal{Z}_\tau$ and $(2.\varepsilon)$ is stabilizable in a time t_f, then $\|x(t) - x_{ref}(t)\| \leq \rho$ for all $t \geq t_f$.

Resilience of nonlinear systems

$$\dot{x}(t) = f(t, x(t)) + g(t, x(t))(Bu(t) + Cw(t)), \quad x(0) = x_0, \quad u(t) \in \mathcal{U}, \quad w(t) \in \mathcal{W} \tag{1}$$

$$\dot{x}(t) = f(t, x(t)) + g\big(t, x(t)\big)\, z(t), \quad x(0) = x_0, \quad z(t) \in \mathcal{Z} = B\mathcal{U} \ominus (-C\mathcal{W}) \tag{2}$$

Sufficient condition for resilience:

If x_{goal} is reachable in a time T by (2),
then x_{goal} is resiliently reachable in time T by (1).

The reverse implication is much more difficult.

Outline

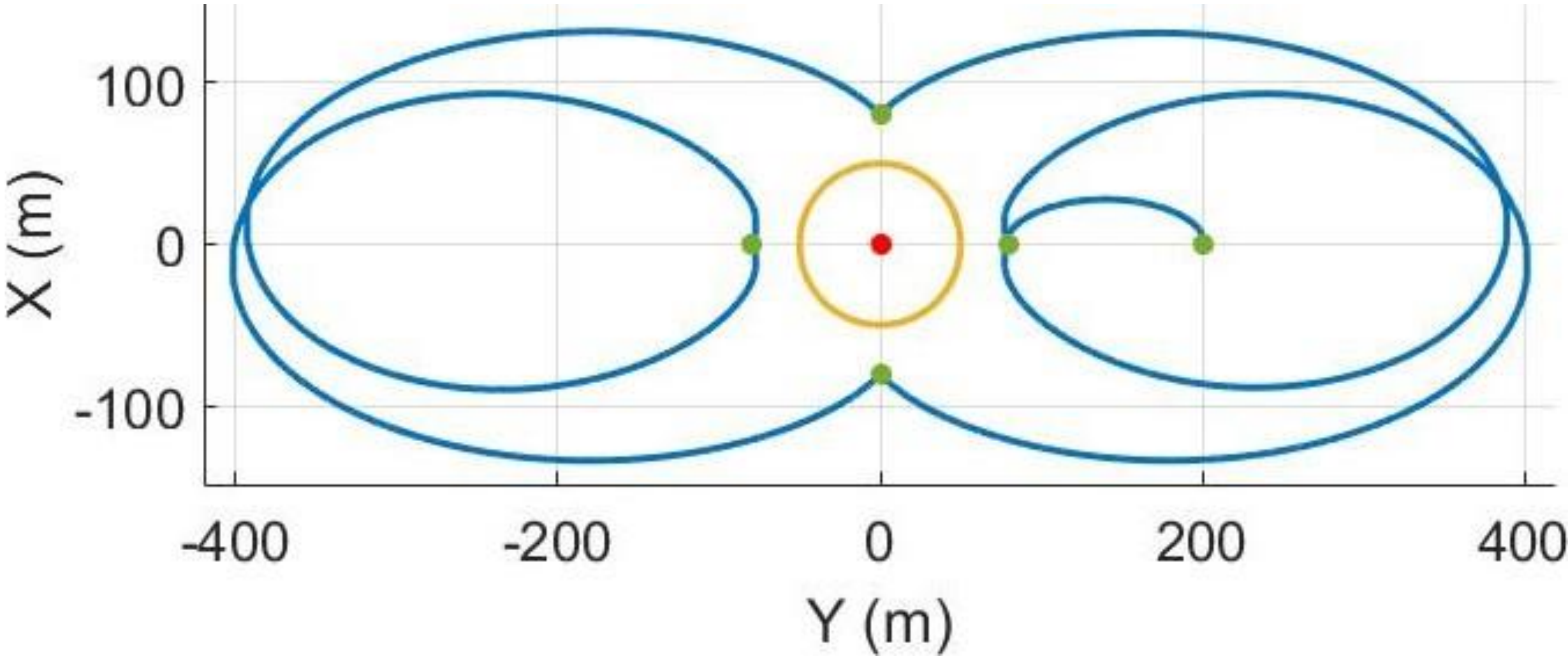
I. Linear systems with bounded energy
   A. Resilient reachability
   B. Resilience of driftless systems
   C. Control synthesis

II. Linear systems with bounded amplitude
   A. Resilient reachability
   B. Quantitative resilience of driftless systems
   C. Quantitative resilience of linear systems

III. Latest contributions to resilience theory
   A. Extensions of resilience theory
   B. Resilience of an orbital inspection mission
   C. Resilience of linear networks

Resilience of an orbital inspection mission

- Target satellite (red)
- Four holding points at 80m (green)
- Fuel optimal inspection trajectory (blue)
- Keep-out sphere (KOS) of radius 50m (yellow)



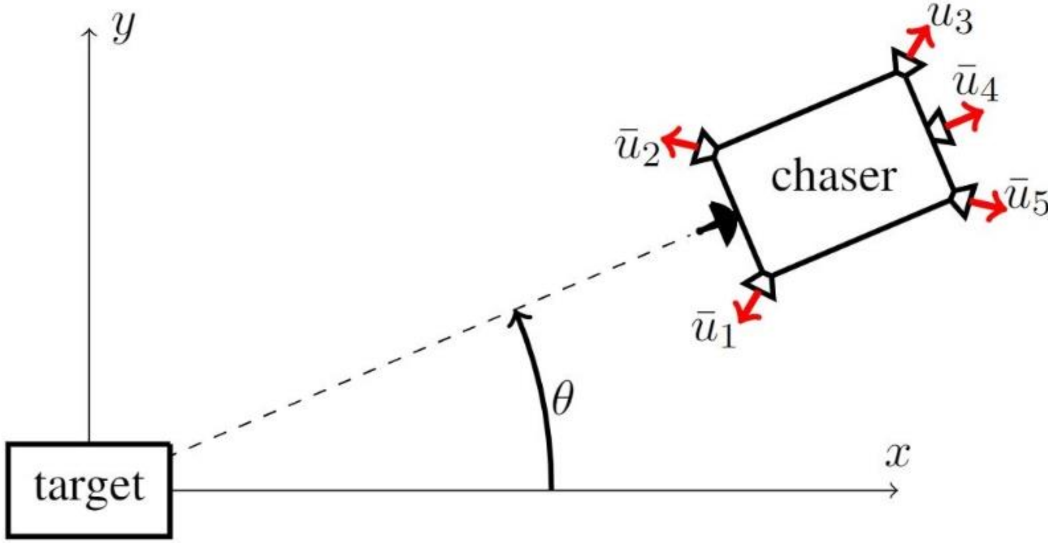
M. Vavrina et al., "Safe rendezvous trajectory design for the Restore-L mission," 29th AAS/AIAA Space Flight Mechanics Meeting, 2019.
N. Ortolano et al., "Autonomous optimal trajectory planning for orbital rendezvous, satellite inspection, and final approach based on convex optimization," Journal of the Astronautical Sciences, 2021.

Nominal Clohessy-Wiltshire dynamics

$$\dot{X}(t) = AX(t) + rR_\theta(t)\bar{B}\bar{u}(t), \qquad X = \begin{bmatrix} x \\ y \\ \dot{x} \\ \dot{y} \end{bmatrix},$$

$$\bar{u}_i(t) \in [0, 1]$$

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 3\Omega^2 & 0 & 0 & 2\Omega \\ 0 & 0 & -2\Omega & 0 \end{bmatrix} \quad \bar{B} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & -\sqrt{2} & -1 \\ 1 & -1 & -1 & 0 & 1 \end{bmatrix}$$



Camera of the chaser always pointing at the target.

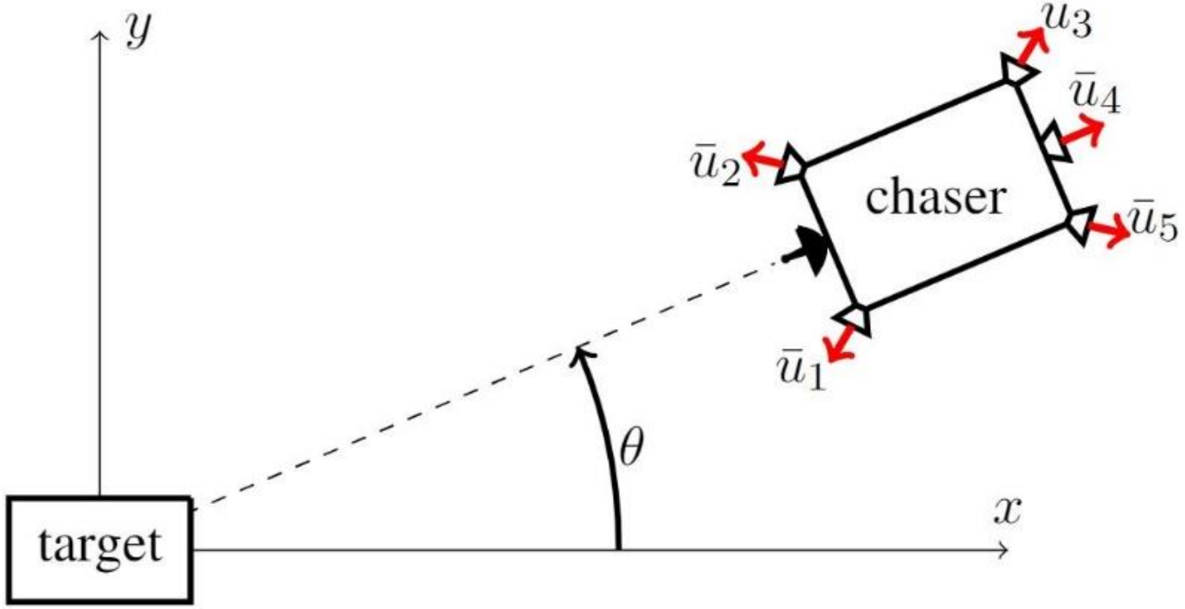
Ω mean orbital rate, r thrust-to-mass ratio, $R_\theta(t)$ rotation matrix.

J.-B. Bouvier et al., *“Resilience of orbital inspections to partial loss of control authority over the chaser satellite,”* AAS/AIAA Astrodynamics Specialist Conference, 2022.

Malfunctioning dynamics

After the loss of control authority over thruster no.4 and actuation delay τ:

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad C = \begin{bmatrix} 0 \\ 0 \\ -\sqrt{2} \\ 0 \end{bmatrix}$$

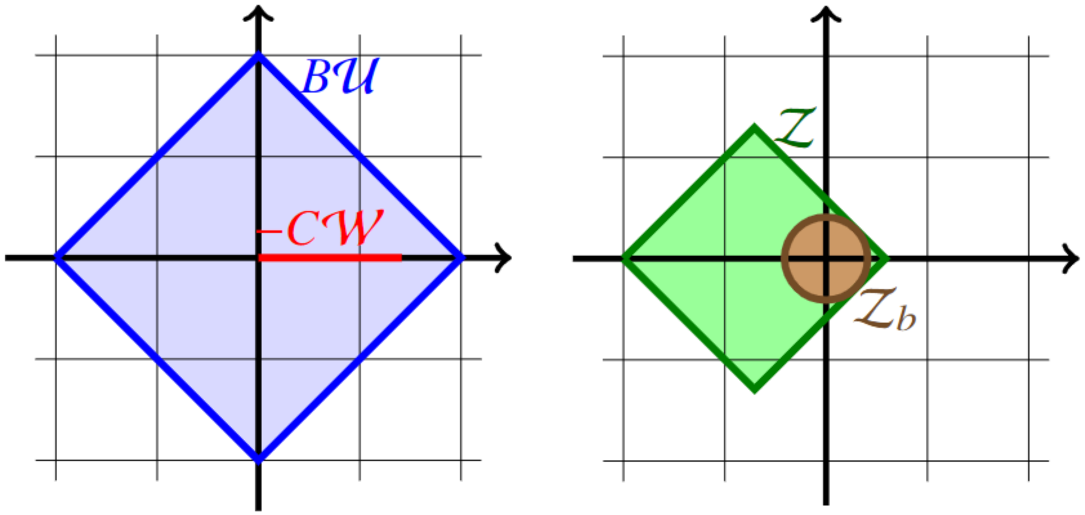


$$\dot{X}(t) = AX(t) + rR_\theta(t)Bu(t, X(t-\tau), w(t-\tau)) + rR_\theta(t)Cw(t),$$

$$u_i(t) \in [0,1], \qquad w(t) \in [0,1]$$

J.-B. Bouvier et al., “*Resilience of orbital inspections to partial loss of control authority over the chaser satellite,*” AAS/AIAA Astrodynamics Specialist Conference, 2022.

Spacecraft resilience



controlled inputs

undesirable inputs

$$(1) \quad \begin{cases} \dot{X}(t) = AX(t) + rR_\theta(t)Bu(t) + rR_\theta(t)Cw(t) \\ X(0) = X_0, \quad u(t) \in \mathcal{U}, \quad w(t) \in \mathcal{W} \end{cases}$$

effective inputs

$$(2) \quad \begin{cases} \dot{X}(t) = AX(t) + rR_\theta(t)z(t) \\ X(0) = X_0, \quad z(t) \in \mathcal{Z} \end{cases}$$

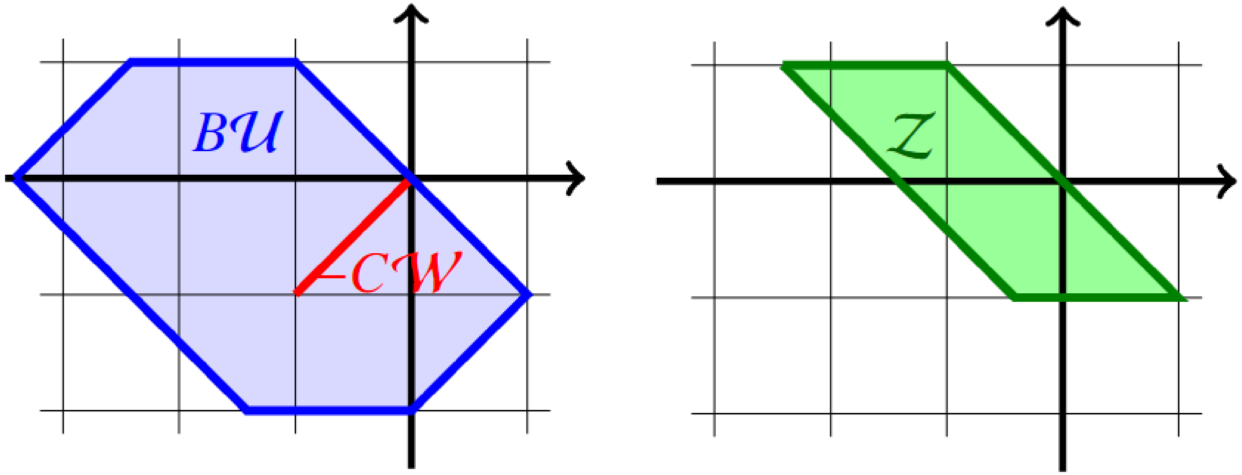
Polygons $B\mathcal{U}$ (blue), $-C\mathcal{W}$ (red), their Minkowski difference $\mathcal{Z}$ (green) and the largest ball $\mathcal{Z}_b$ (brown) centered on 0 in $\mathcal{Z}$.

$$(3) \quad \begin{cases} \dot{X}(t) = AX(t) + r\hat{B}z(t) \\ X(0) = X_0, \quad z(t) \in \mathcal{Z}_b \end{cases}$$

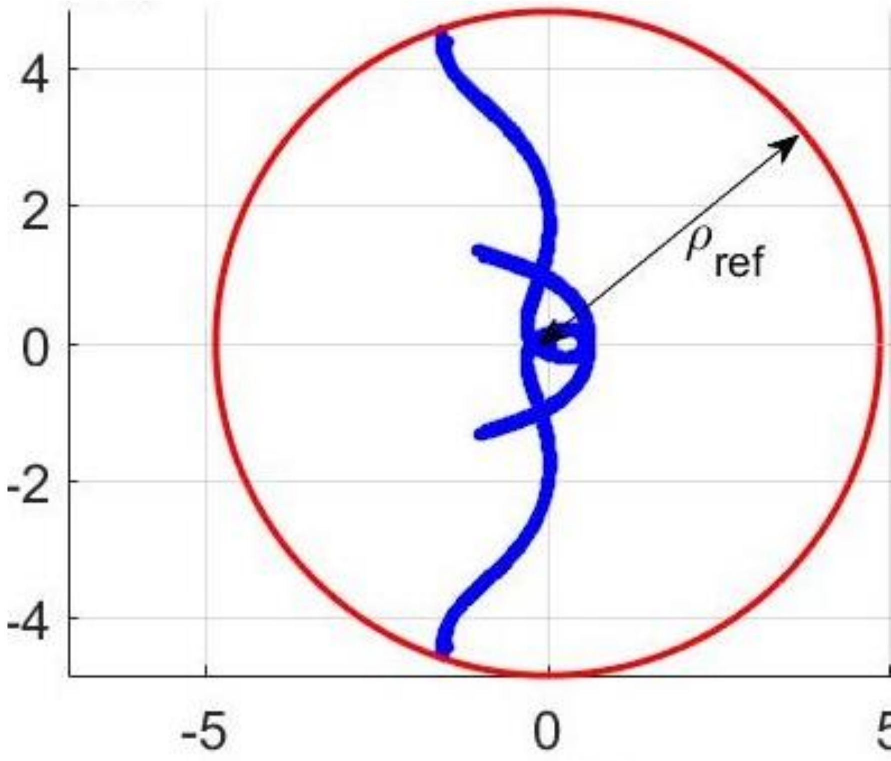
$$\mathcal{Z} = B\mathcal{U} \ominus (-C\mathcal{W}) = \{z \in B\mathcal{U} : z - Cw \in B\mathcal{U} \text{ for all } w \in \mathcal{W}\}$$

Spacecraft resilience

After the loss of thruster no. 1, the set of effective inputs $\mathcal{Z}$ (green) does not surround the origin.



The spacecraft can only track $\mathcal{T}_{ref}$ after the loss of thruster no. 4



Effective inputs on the reference trajectory $\mathcal{T}_{ref}$.

Controller design

At time t controller $u(t)$ has only access to $w(t-\tau)$ and $X(t-\tau)$.

To estimate $X(t)$, we use the Léchappé state predictor:

$$X_p(t) = e^{A\tau}X(t-\tau) + \int_{t-\tau}^{t} e^{A(t-s)} r R_\theta(s)\big(Bu(s) + Cw(s-\tau)\big)\, ds.$$

We prove that controller

$$Bu(t) = -Cw(t-\tau) + R_\theta^{-1}(t) z_{ref}(t) + R_\theta^{-1}(t)\, BK\big(X_{ref}(t) - X_p(t)\big)$$

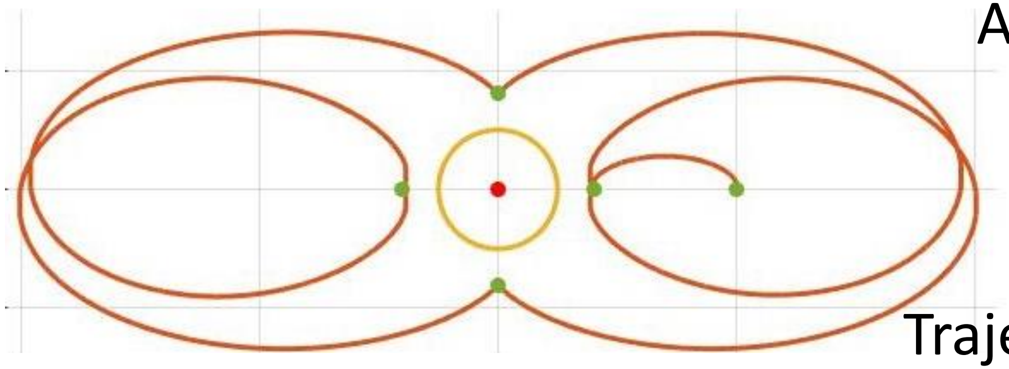
guarantees resilient tracking

$$\left\|X(t) - X_{ref}(t)\right\| \leq max\big(\left\|X(0) - X_{ref}(0)\right\|, \varepsilon\big).$$

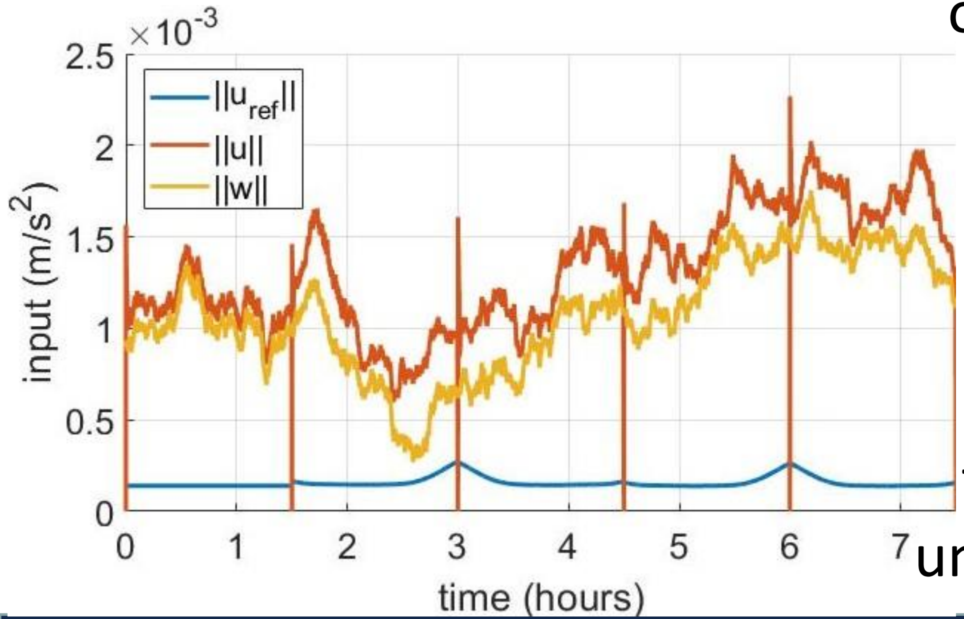
V. Léchappé et al., "New predictive scheme for the control of LTI systems with input delay and unknown disturbances," Automatica, 2015.

Numerical simulation

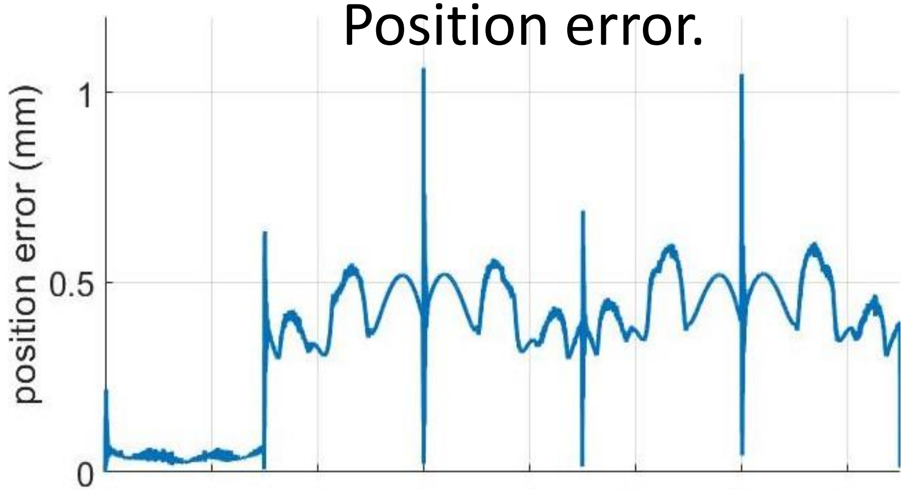
Actuation delay $\tau = 0.2s$



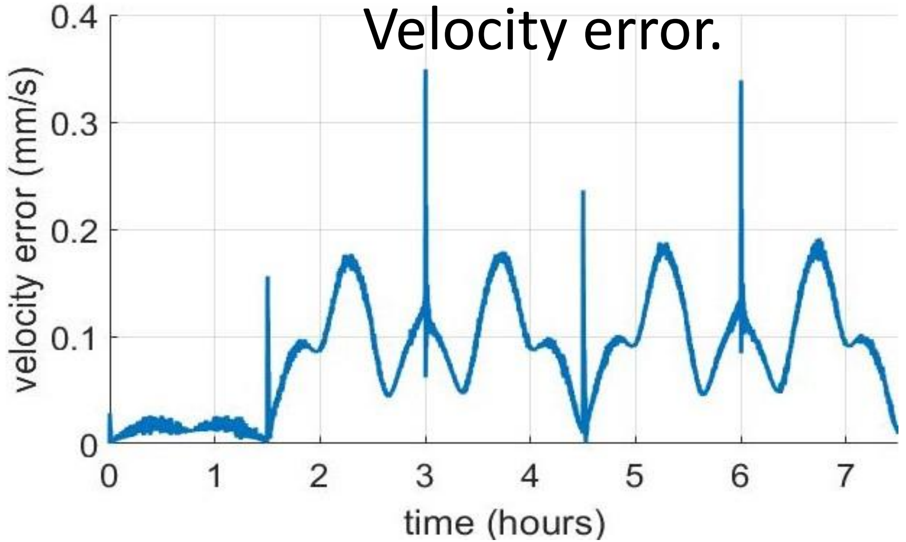
Trajectory tracking (red) of the reference (blue).



Reference thrust (blue), tracking thrust (red) and undesirable thrust (orange).

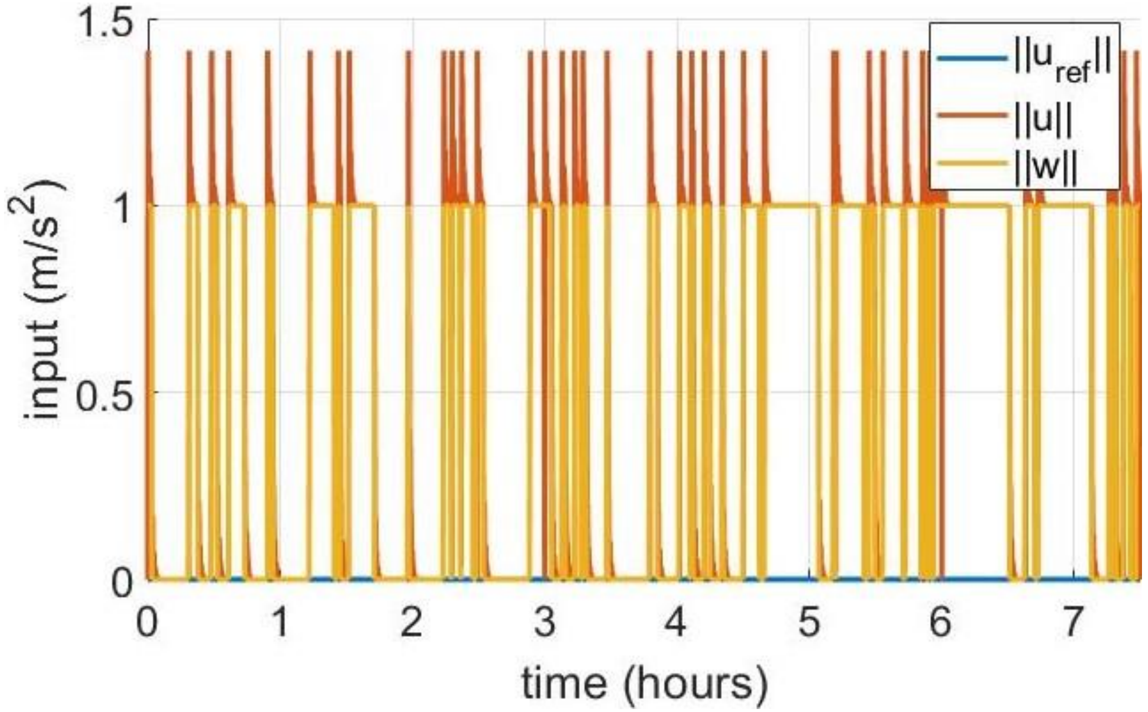


Position error.



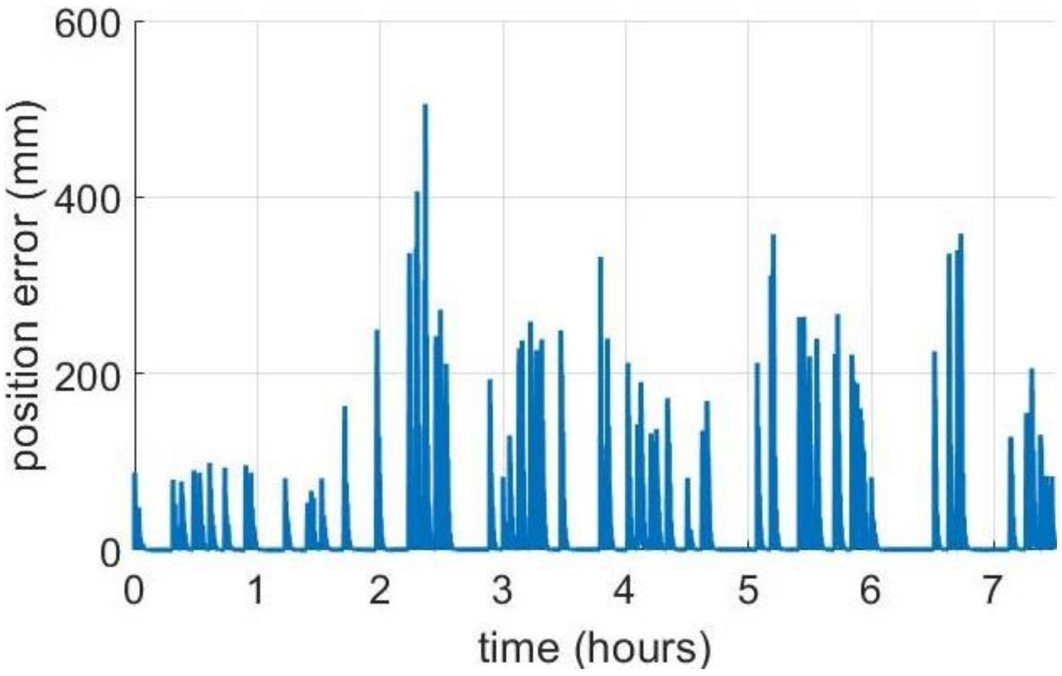
Velocity error.

Numerical simulation



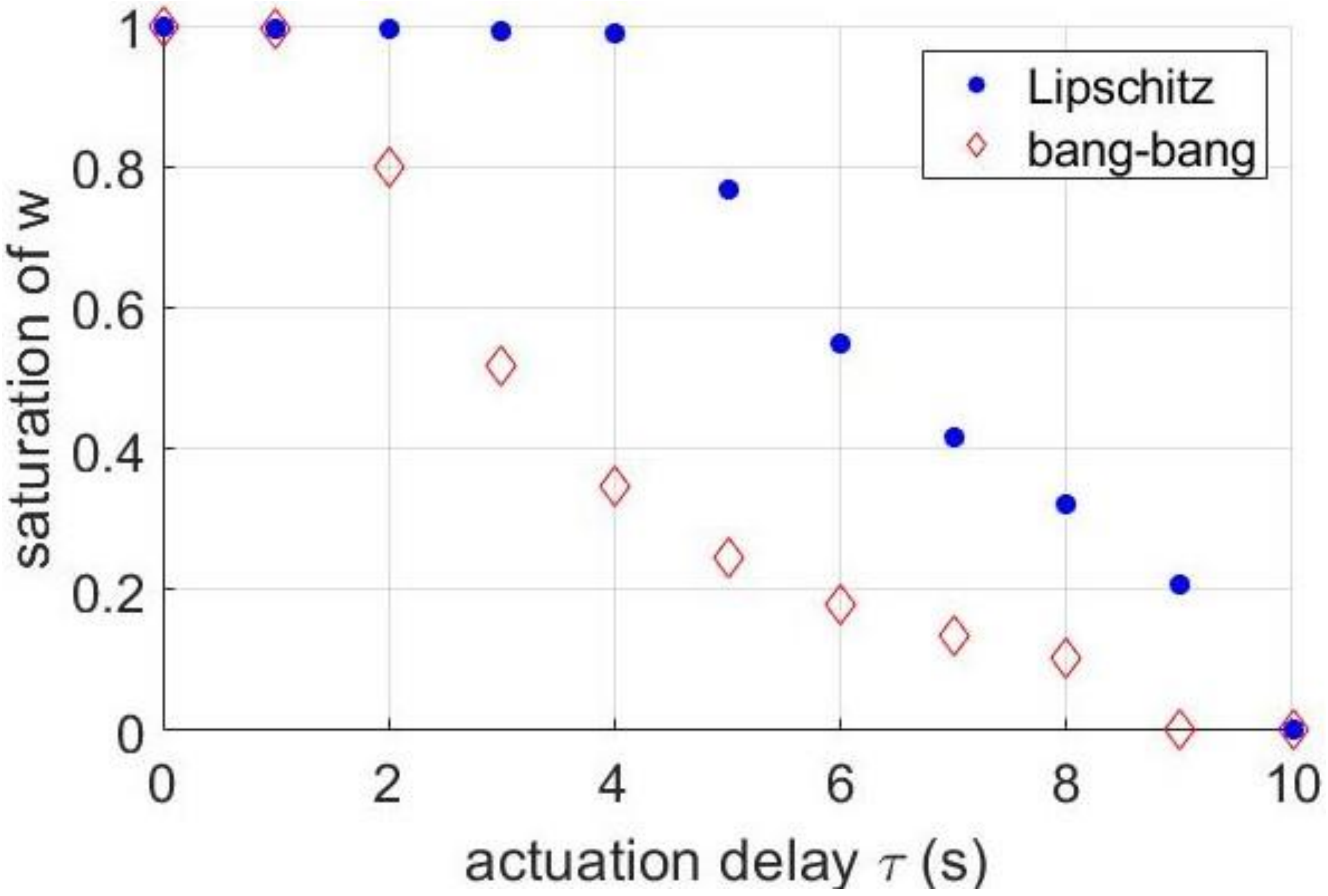
Thrust magnitude on the tracking trajectory (red), the reference (blue), and the undesirable thrust (orange).

Scenario: $w(t) \in [0,1]$ is bang-bang, actuation delay $\tau = 1s$.



Position tracking error

Summary of the simulations



With a given actuation delay τ, how much undesirable thrust w can the tracking handle?

Outline

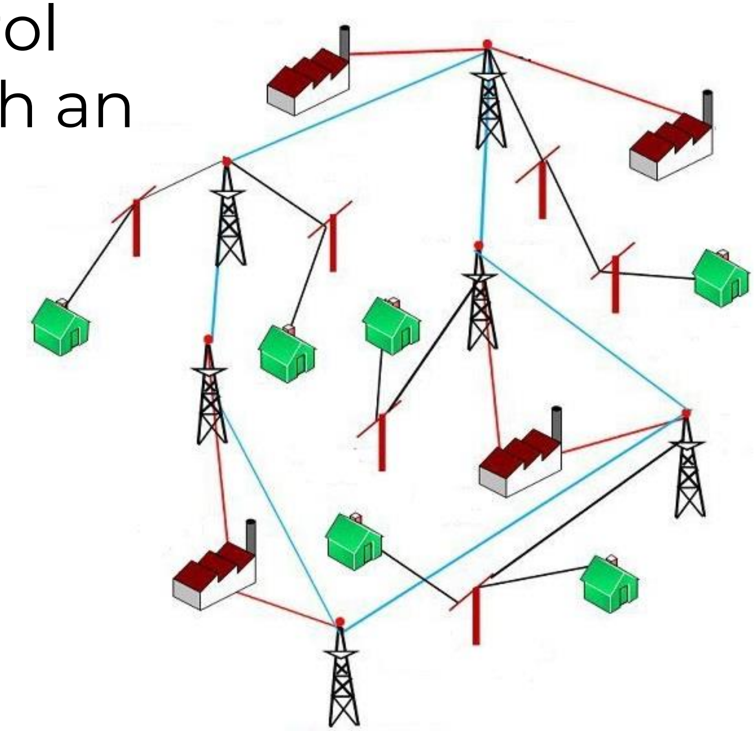
I. Linear systems with bounded energy
   A. Resilient reachability
   B. Resilience of driftless systems
   C. Control synthesis

II. Linear systems with bounded amplitude
   A. Resilient reachability
   B. Quantitative resilience of driftless systems
   C. Quantitative resilience of linear systems

III. Latest contributions to resilience theory
   A. Extensions of resilience theory
   B. Resilience of an orbital inspection mission
   C. Resilience of linear networks

Resilience of linear networks

A cyberattack on an electric grid causes a loss of control over a power generator. Is the network resilient to such an attack?



Nominal dynamics at node $i \in [\![1, N]\!]$

$\dot{x}_i(t) = A_i x_i(t) + \bar{B}_i \bar{u}_i(t) + \sum D_{i,k} x_k(t).$

After a loss of control authority in node N,

$\dot{x}_N(t) = A_N x_N(t) + B_N u_N(t) + C_N w_N(t) + \sum D_{N,k} x_k(t).$

Can we still drive all the x_i to 0?

Framework

Network $\dot{X}(t) = (A + D)X(t) + \bar{B}\bar{u}(t) \quad + D_{-,N}x_N(t)$

Malfunctioning node $\dot{x}_N(t) = \quad A_N x_N(t) \quad + B_N u_N(t) + D_{N,-}X(t) \; + C_N w_N(t)$

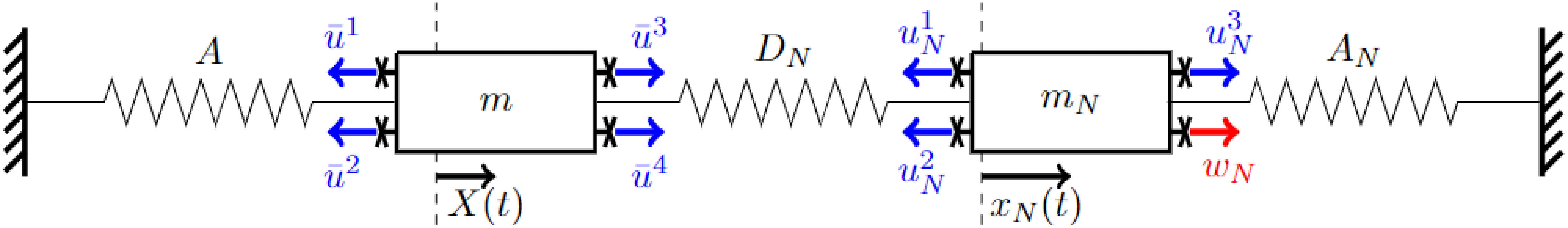
$$X(t) = \begin{bmatrix} x_1(t) \\ \vdots \\ x_{N-1}(t) \end{bmatrix} \qquad A = \begin{bmatrix} A_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A_{N-1} \end{bmatrix} \qquad \bar{u}(t) = \begin{bmatrix} \bar{u}_1(t) \\ \vdots \\ \bar{u}_{N-1}(t) \end{bmatrix} \qquad \bar{B} = \begin{bmatrix} \bar{B}_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \bar{B}_{N-1} \end{bmatrix}$$

$$D = \begin{bmatrix} 0 & D_{1,2} & \dots & D_{1,N-1} \\ D_{2,1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & D_{N-2,N-1} \\ D_{N-1,1} & \dots & D_{N-1,N-2} & 0 \end{bmatrix} \begin{bmatrix} D_{1,N} \\ \vdots \\ D_{N-2,N} \\ D_{N-1,N} \end{bmatrix} = D_{-,N}$$

$$D_{N,-} = \begin{bmatrix} D_{N,1} & \dots & D_{N,N-2} & D_{N,N-1} \end{bmatrix} \quad 0$$

Resilient node

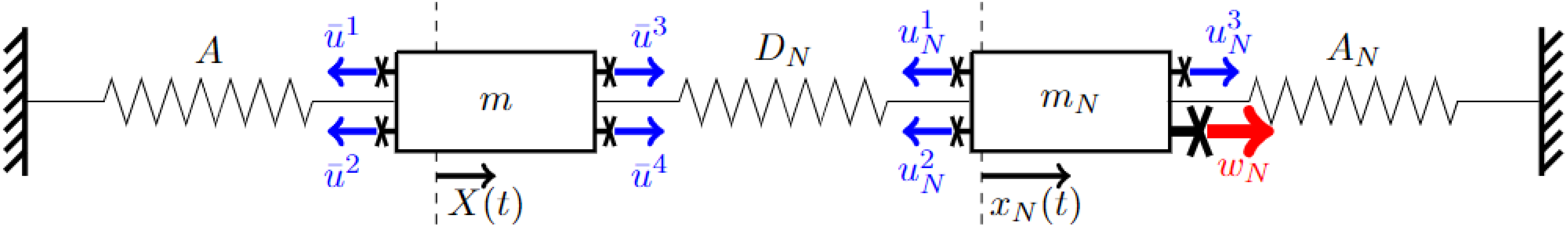
If the isolated malfunctioning node is resilient, i.e.,
if $\dot{x}_N(t) = A_N x_N(t) + B_N u_N(t) + C_N w_N(t)$ is resilient
and the initial network was controllable,
then the network is resilient.



Toy example: two submarines connected with springs.

Non-resilient node

Non-resilience: $C_N \mathcal{W}_N \not\subseteq B_N \mathcal{U}_N$, i.e., some w_N cannot be counteracted.
Then, x_N cannot be resiliently driven to 0 by u_N.
To prevent x_N from diverging, we assume that A_N is Hurwitz.



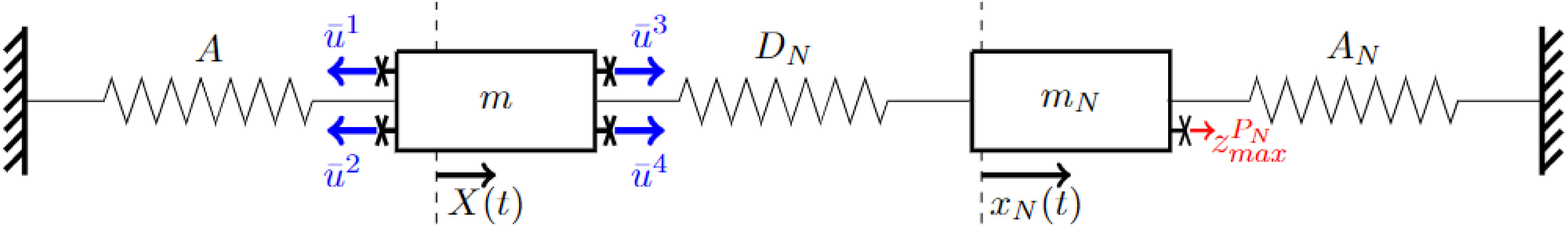
Non-resilient node

If A_N is Hurwitz, then

$$\|x_N(T)\|_{P_N} \leq e^{-\alpha_N T}\left(\|x_N(0)\|_{P_N} + \int_0^T e^{\alpha_N t}\left(z_{max}^{P_N} + \left\|D_{N,-}X(t)\right\|_{P_N}\right) dt\right),$$

with $P_N \succ 0$ such that $A_N^\top P_N + P_N A_N = -Q_N \prec 0$, $\alpha_N = \frac{\lambda_{min}^{Q_N}}{2\lambda_{max}^{P_N}} > 0$,

and $z_{max}^{P_N} = \max\{\min\{\|C_N w_N + B_N u_N\|_P : u_N \in \mathcal{U}_N\} : w_N \in \mathcal{W}_N\} > 0.$

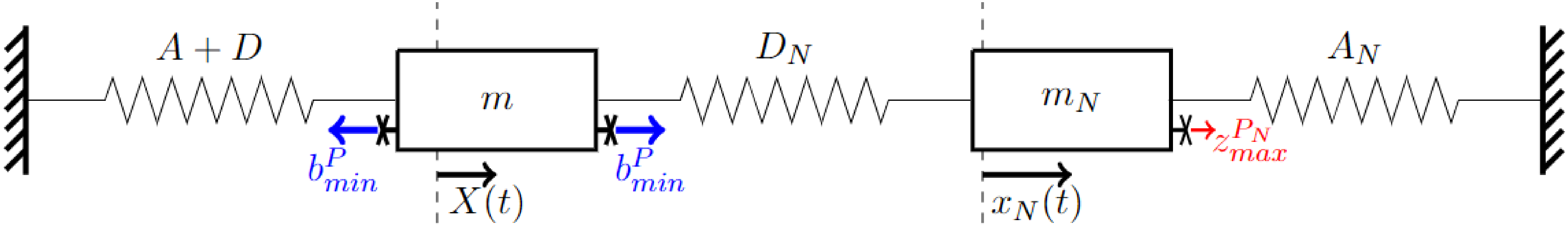


Impact of a non-resilient node

If A_N and $A + D$ are Hurwitz and $\bar{B}$ is full rank, then

$$\|X(t)\|_P \leq \frac{\gamma z_{max}^{P_N} - \alpha_N b_{min}^P}{\alpha\alpha_N - \gamma\gamma_N} + h_1 e^{(r_1 - \alpha_N)t} + h_2 e^{(r_2 - \alpha_N)t},$$

where $b_{min}^P = \min\{\|\bar{B}\bar{u}\|_P : \bar{u} \in \partial\bar{\mathcal{U}}\} > 0$ is the minimal guaranteed control.



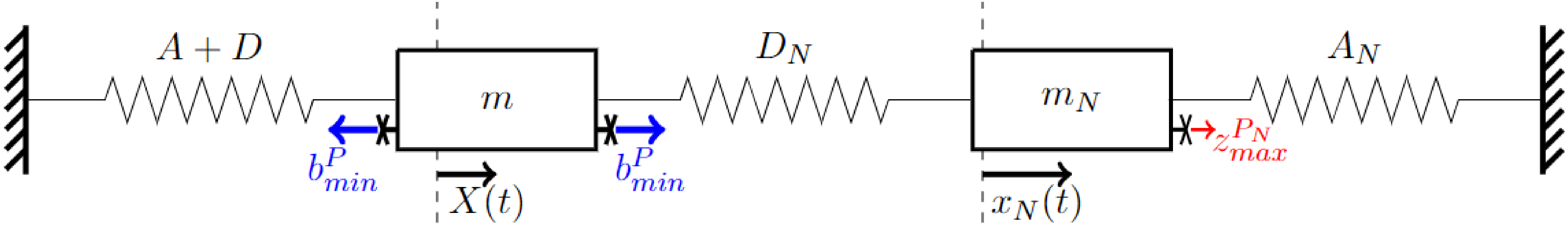
Impact of a non-resilient node

If A_N and $A + D$ are Hurwitz, $\bar{B}$ is full rank, $\alpha\alpha_N \geq \gamma\gamma_N$ and $\gamma z_{max}^{P_N} < \alpha_N b_{min}^P$, then the network X is stabilizable in finite time.

$\alpha = \dfrac{\lambda_{min}^Q}{2\lambda_{max}^P}$ internal stability, $\gamma = \|D_{-,N}\|_P \sqrt{\dfrac{\lambda_{max}^P}{\lambda_{min}^{P_N}}}$ coupling strength,

$b_{min}^P = \min\{\|\bar{B}\bar{u}\|_P : \bar{u} \in \partial\bar{\mathcal{U}}\}$ minimal guaranteed control,

$z_{max}^{P_N} = \max\{\min\{\|C_N w_N + B_N u_N\|_P : u_N \in \mathcal{U}_N\} : w_N \in \mathcal{W}_N\}$ worst undesirable input.



Conclusion

- We established analytical conditions to verify whether autonomous systems are resilient to a loss of authority over some of their actuators.

- We quantified the resilience of these systems by comparing the minimal reach times for the initial and the malfunctioning systems.

- We extended resilience theory to encompass trajectory tracking, actuation delay and nonlinear dynamics.

- We applied these extensions to an orbital inspection mission.

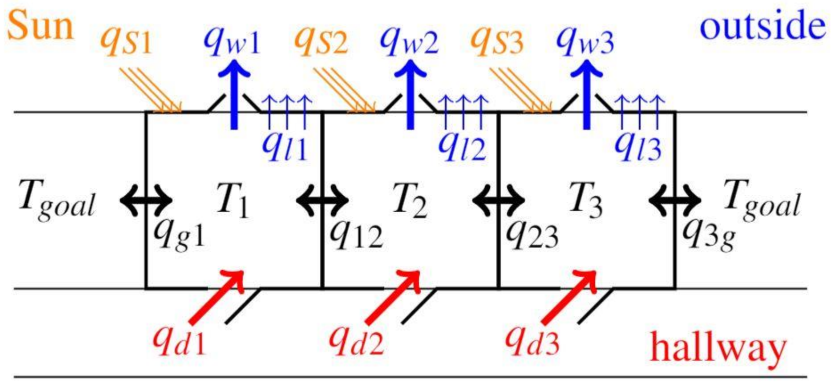
- We derived partial resilience conditions for linear networks.

Thank you for your attention

References

- J.-B. Bouvier and M. Ornik, “*Resilient reachability for linear systems,*” in 21st IFAC World Congress, 2020, pp. 4409–4414.
- J.-B. Bouvier, K. Xu, and M. Ornik, “*Quantitative resilience of linear driftless systems,*” in SIAM Conference on Control and its Applications, 2021, pp. 32–39.
- J.-B. Bouvier and M. Ornik, “*Quantitative resilience of linear systems,*” in 20th European Control Conference, 2022, pp. 485–490.
- J.-B. Bouvier, H. Panag, R. Woollands, and M. Ornik, “*Resilience of orbital inspections to partial loss of control authority over the chaser satellite,*” in 2022 AAS/AIAA Astrodynamics Specialist Conference, 2022.
- J.-B. Bouvier and M. Ornik, “*Designing resilient linear systems,*” IEEE Transactions on Automatic Control, vol. 67, no. 9, pp. 4832–4837, 2022.
- J.-B. Bouvier and M. Ornik, “*The maximax minimax quotient theorem,*” Journal of Optimization Theory and Applications, vol. 192, pp. 1084–1101, 2022.
- J.-B. Bouvier and M. Ornik, “*Resilience of linear systems to partial loss of control authority,*” Automatica, vol. 152, pp. 110985, 2023.
- J.-B. Bouvier, K. Xu, and M. Ornik, “*Quantitative resilience of generalized integrators,*” IEEE Transactions on Automatic Control, 2023.

Bounding quantitative resilience



Actuators:

- Central heating/AC $q_h \ - q_{AC}$
- Door/window of each room $q_d \ - q_w$
- Sunshades/heat loss of each room $q_S \ - q_l$

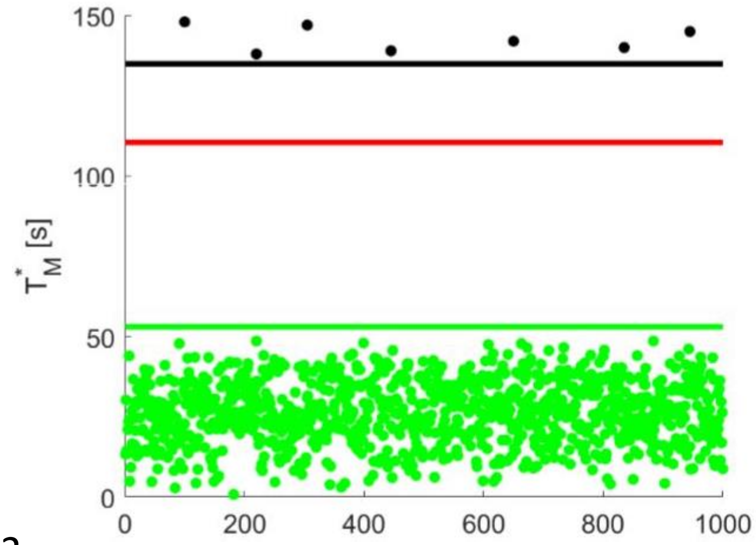
Objective: $\mathrm{T}_1 = \mathrm{T}_2 = \mathrm{T}_3 = \mathrm{T}_{\mathrm{goal}}$

$x = T \ - T_{goal}$ $\quad$ $x_0 = (0.8°C \quad 0.7°C \quad 0.9°C)$

$35.5s \leq T_N^*(x_0) = 42.5s \leq 54.1s$ $\qquad$ $53s \leq T_M^*(x_0) = 110.5s \leq 135s$

Worst-case time increase by a factor $\frac{T_M^*(x_0)}{T_N^*(x_0)} = 2.6 \leq 3.8$ for this x_0.

$0.097 \leq r_q \leq 2.79$ yields a worst-case time increase by a factor $\frac{1}{0.097} = 10.3$ over all x_0.



J.-B. Bouvier and M. Ornik, Quantitative Resilience of Linear Systems, European Control Conference 2022

Quantitative Resilience Framework

Maximize $\dot{x}(t)$? Maximize $\langle \dot{x}(t), x_{goal} - x(t) \rangle$? Assume that w is constant ? Assume that w is the worst bang-bang input?

.

“Target Function Approach to Linear Pursuit Problems” by W. Borgest and P. Varaiya

Closed-loop capture: controller $u^*(t)$ only knows $w^*([0, t])$. For time optimal, only general technique is to solve Isaac’s main equation: differential game equivalent of HJB equation (usually intractable PDE). Give sub-optimal solutions
Such a T_M^* cannot be compared with time-optimal T_N^*

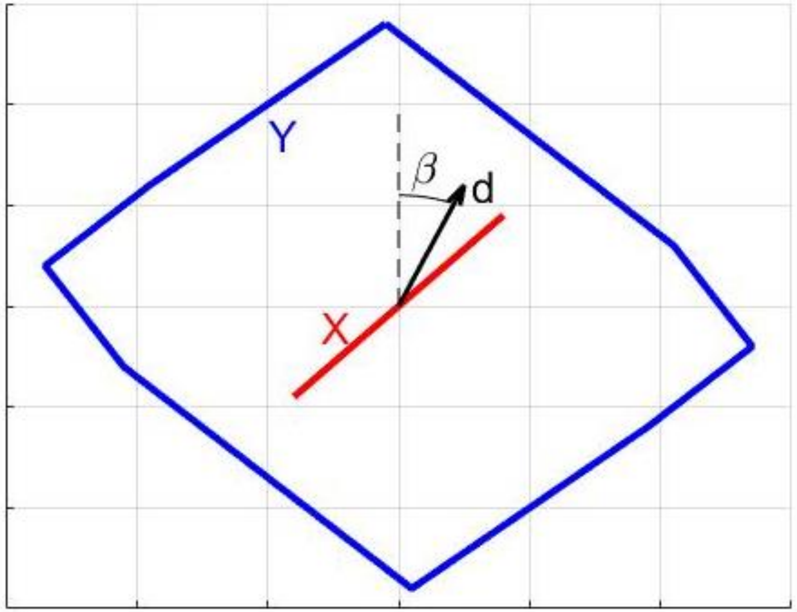
Open-loop capture: controller knows w^* in advance

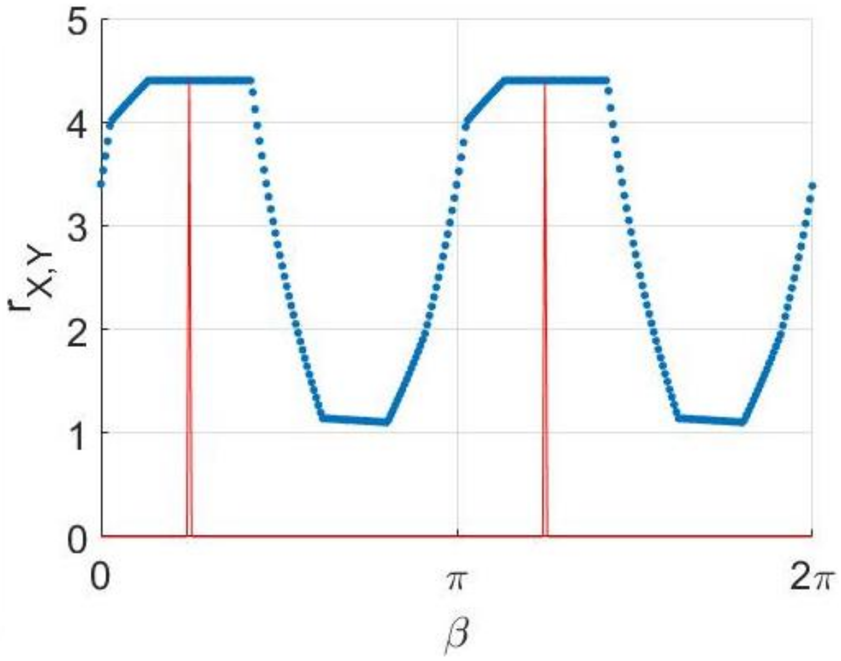
The Maximax Minimax Quotient Theorem

$$r_{X,Y}(d) = \frac{\max\limits_{x\,\in\,X,\,y\,\in\,Y}\{\|x+y\| : x+y \in \mathbb{R}^+ d\,\}}{\min\limits_{x\,\in\,X}\left\{\max\limits_{y\,\in\,Y}\{\|x+y\| : x+y \in \mathbb{R}^+ d\,\}\right\}} \quad for\ \ d \in \mathbb{R}^n, \qquad \|d\| = 1.$$

If X and Y are two symmetric polytopes in $\mathbb{R}^n$ with $X \subset Y^\circ$, $\partial X = \{-x, x\}$ and $\dim Y = n$, then $\max\limits_{\|d\|=1} r_{X,Y}(d) = r_{X,Y}(x)$.

https://www.youtube.com/watch?v=rjKzHyDJX40





J.-B. Bouvier and M. Ornik, “The Maximax Minimax Quotient Theorem”, Journal of Optimization Theory and Applications, 2022.

Quantitative resilience of driftless systems

System $\dot{x}(t) = \bar{B}\bar{u}(t)$ is resilient to the loss of a single column C if and only if it is controllable, $r(C) \in (0,1]$ and $r(-C) \in (0,1]$,

where $r(C) = \frac{w^{min}+\alpha^+}{w^{max}+\alpha^+}$, $r(-C) = \frac{w^{max}-\alpha^-}{w^{min}-\alpha^-}$, $\alpha^\pm = \max\limits_{u\,\in\,\mathcal{U}}\{\alpha : Bu = \pm\alpha C\}$ and $\mathcal{W} = [w^{min}, w^{max}]$.

If system $\dot{x}(t) = \bar{B}\bar{u}(t)$ is resilient to the loss of a single column C, then $r_q = min\{r(C), r(-C)\}$.

J.-B. Bouvier, K. Xu and M. Ornik, "Quantitative resilience of linear driftless systems", SIAM Conference on Control and its Applications, 2021.

Quantitative resilience of driftless systems

$\dot{x}^{(k)}(t) = \bar{B}\bar{u}(t) \qquad \bar{u} \in \bar{U}_\infty \qquad x(0) = x_0 \qquad x^{(l)}(0) = 0$ for $l \in [\![1,\ k-1]\!]$.

Nominal reach time $T^*_{k,N}(d) = \inf\limits_{\bar{u} \in \bar{U}_\infty} \{T : x(T) - x_0 = d\}$.

$\dot{x}^{(k)}(t) = Bu(t) + Cw(t) \qquad u \in U_\infty \qquad w \in W_\infty \qquad x(0) = x_0 \qquad x^{(l)}(0) = 0$ for $l \in [\![1,\ k-1]\!]$.

Malfunctioning reach time $T^*_{k,M}(d) = \sup\limits_{w \in W_\infty} \left\{ \inf\limits_{u \in U_\infty} \{T : x(T) - x_0 = d\} \right\}$.

If $\dot{x} = \bar{B}\bar{u}$ is controllable, so is $\dot{x}^{(k)} = \bar{B}\bar{u}$ and $T^*_{k,N}(d) = \sqrt[k]{k!\,T^*_N(d)}$.

If $\dot{x} = Bu + Cw$ is resilient, so is $\dot{x}^{(k)} = Bu + Cw$ and $T^*_{k,M}(d) = \sqrt[k]{k!\,T^*_M(d)}$.

Then, $r_{k,q} = \inf\limits_{d \in \mathbb{R}^n} \dfrac{T^*_{k,N}(d)}{T^*_{k,M}(d)} = \sqrt[k]{r_q}$. For a resilient system, $r_q \in (0,1]$, so $r_{k,q} \geq r_q$.

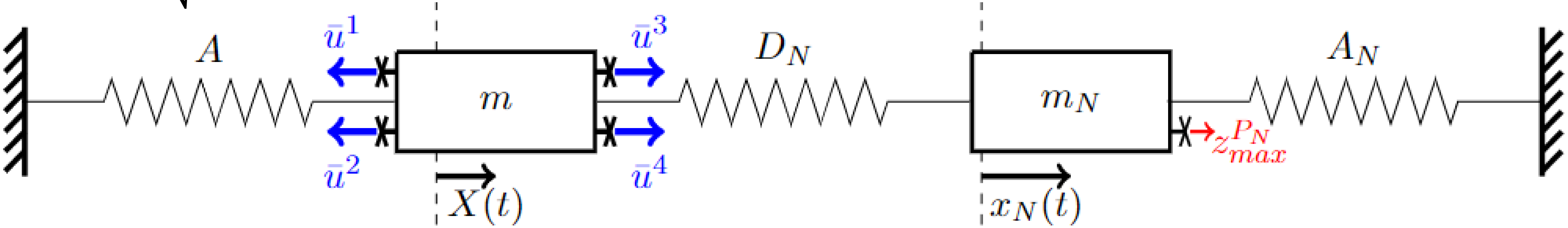
J.-B. Bouvier, K. Xu and M. Ornik, “Quantitative resilience of generalized integrators”, IEEE Transactions on Automatic Control, 2023.

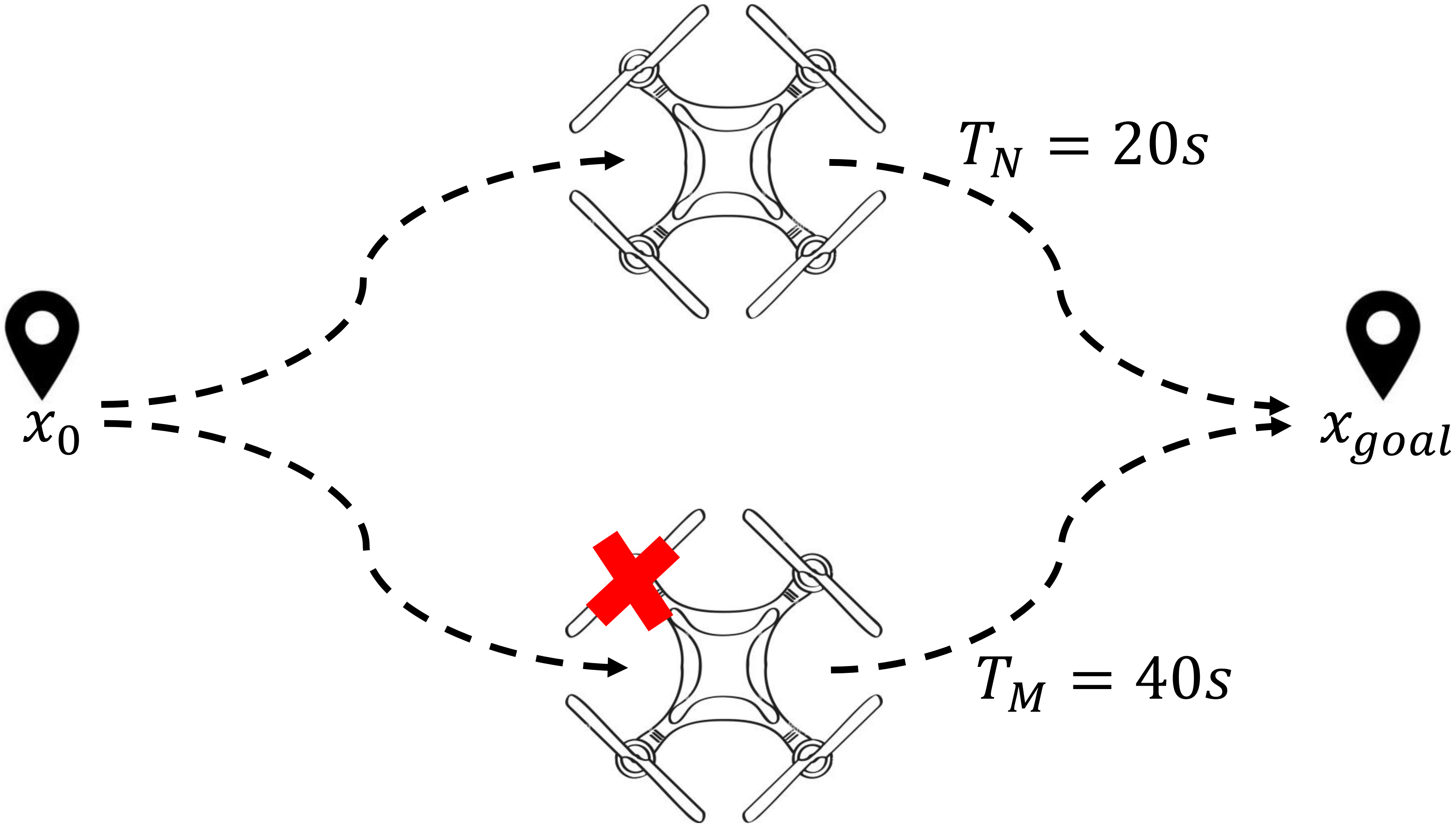
Non-resilient node

If $A + D$ is Hurwitz and $\bar{B}$ is full rank,

$$\|X(t)\|_P \leq \frac{\gamma z_{max}^{P_N} - \alpha_N b_{min}^P}{\alpha\alpha_N - \gamma\gamma_N} + h_1 e^{(r_1 - \alpha_N)t} + h_2 e^{(r_2 - \alpha_N)t}$$

with $P \succ 0$ such that $(A+D)^\top P + P(A+D) = -Q \prec 0$, $\alpha = \frac{\lambda_{min}^Q}{2\lambda_{max}^P}$, $\gamma = \left\|D_{-,N}\right\|_P \sqrt{\frac{\lambda_{max}^P}{\lambda_{min}^{P_N}}}$, $\gamma_N = \left\|D_{N,-}\right\|_P \sqrt{\frac{\lambda_{max}^{P_N}}{\lambda_{min}^P}}$ and $b_{min}^P = \min\{\|\bar{B}\bar{u}\|_P : \bar{u} \in \partial\bar{\mathcal{U}}\}$.




$T_N = 20s$
x_0
x_{goal}
$T_M = 40s$