Recent Results in Resilient CPS Design using Passivity and Dissipativity

Current Research by Panos Antsaklis' Group at Notre Dame:
Hasan Zakeri
Yang Yan
Etika Agarwal

Control Systems and the Quest for Autonomy
28th October, 2018

Overview

- System Level
  - Local Passivity (and indices) of Nonlinear Systems
  - Adaptation Methods Based on Experimental Passivity Indices
- Connection Level
  - Security Design for Data Injection Attack
  - Design Strategy over Imperfect Network
- Interconnection Level
  - Applications to Network of Microgrids
  - Compositional Control of Large-Scale Systems

Overview

- **System Level**
  - Local Passivity (and indices) of Nonlinear Systems
  - Adaptation Methods Based on Experimental Passivity Indices
- **Connection Level**
  - Security Design for Data Injection Attack
  - Design Strategy over Imperfect Network
- **Interconnection Level**
  - Applications to Network of Microgrids
  - Compositional Control of Large-Scale Systems

Local Passivity Indices of Nonlinear Systems

- Behaviors of nonlinear systems change in different regions
- Examples: stability, controllability, and even uniqueness and existence
- Even systems that are passive around one equilibrium and non-passive around another
- Limited course of action in most physical systems bounded control input
- Controllers and feedback loops “tame” the system to operate around an equilibrium
- Solution: studying IO properties (particularly passivity indices) with respect to regions of state space and known bounds on input signal
- New definitions for passivity indices with respect to restrictions on the state and input spaces

Example

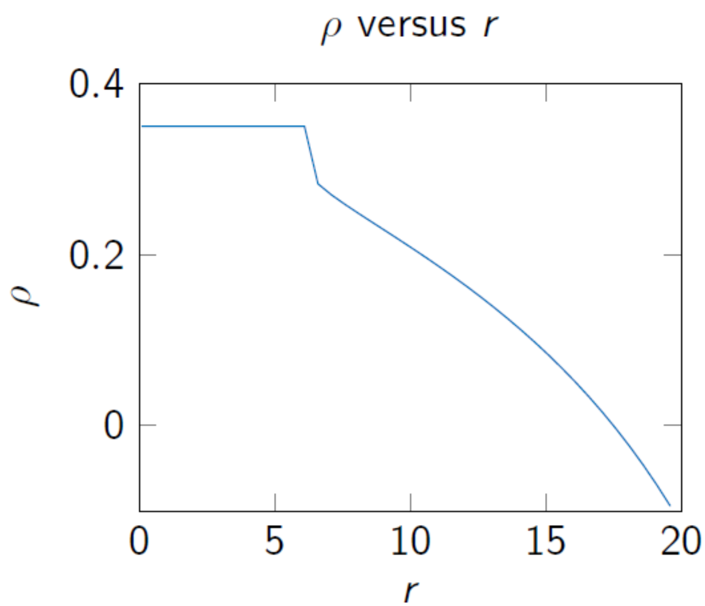
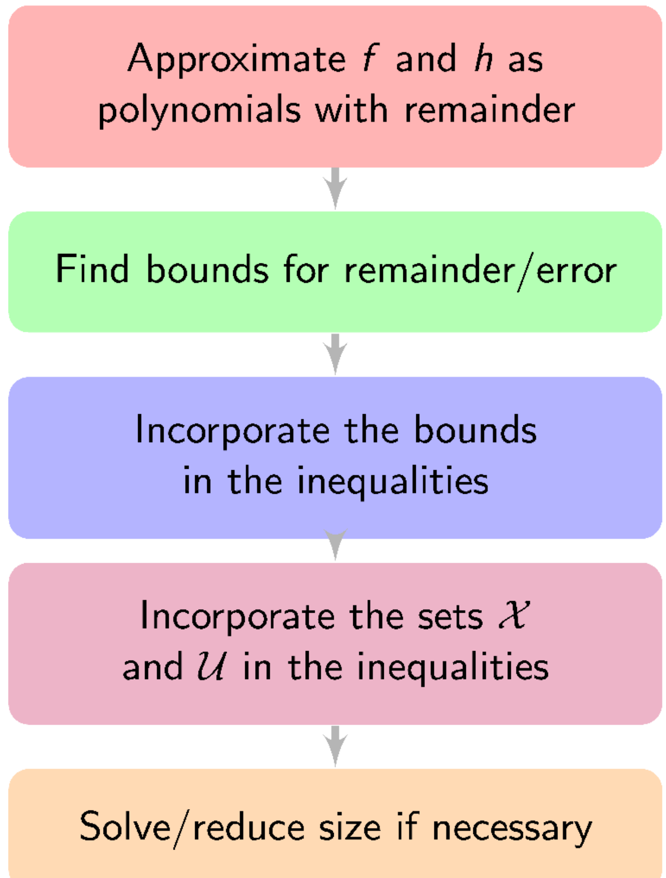


Figure: OFP index ρ, for $X = \{\, x \mid \|x\|_2^2 \leq r \,\}$

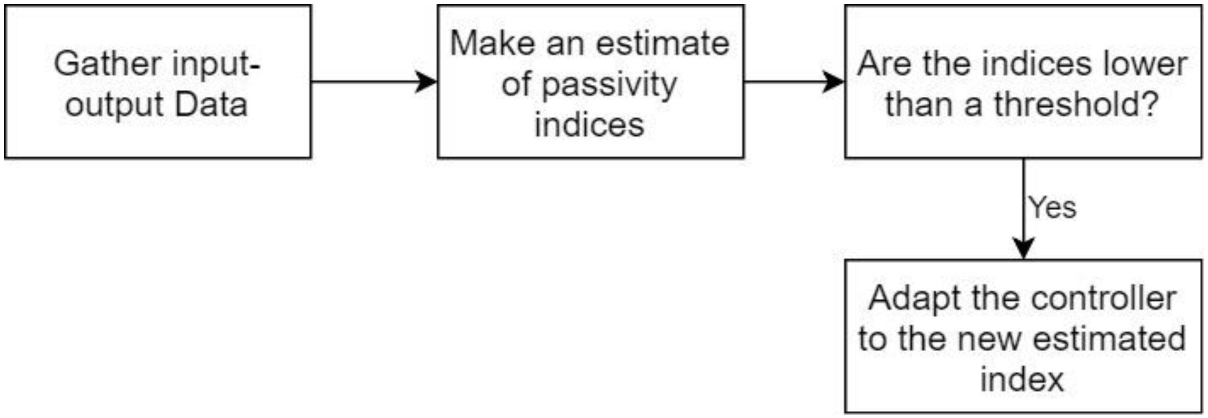
For an example nonlinear system

Approximate Methods For Passivity Indices



Adaptation Method Based on Experimental Passivity Indices

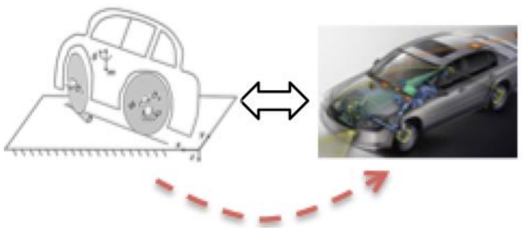
- Experimental passivity indices of the system (with respect to current input)
- A measure of failure in the system (data-driven, no model)
- Adaptive method to mitigate any shortage with changing the controller



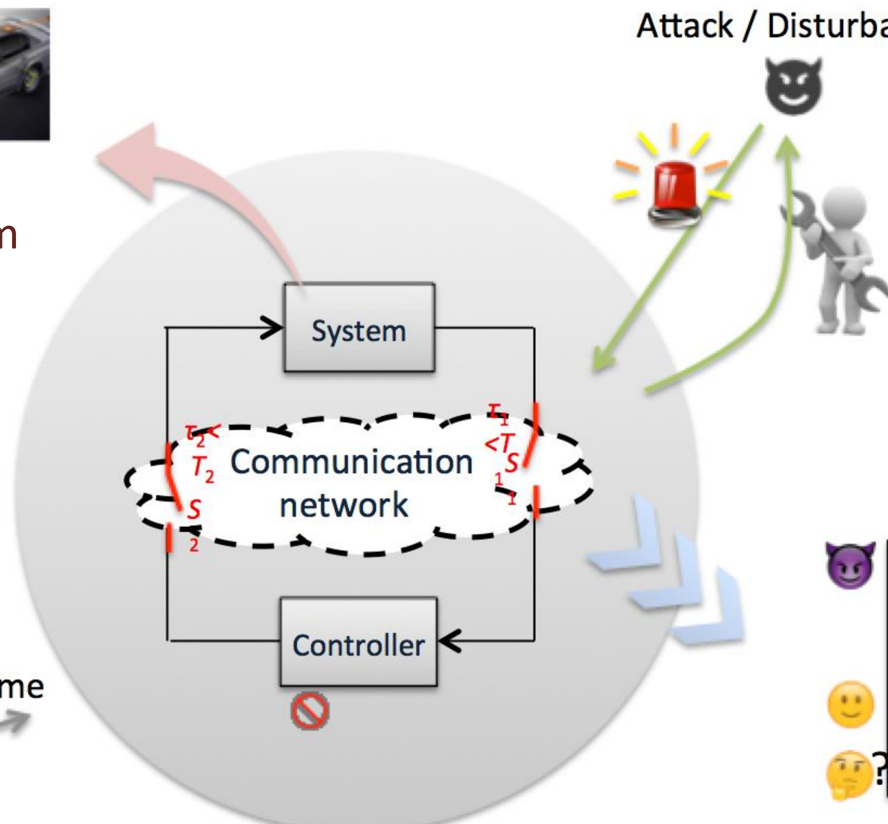
Overview

- **System Level**
  - Local Passivity (and indices) of Nonlinear Systems
  - Adaptation Methods Based on Experimental Passivity Indices
- **Connection Level**
  - Security Design for Data Injection Attack
  - Design Strategy over Imperfect Network
- **Interconnection Level**
  - Applications to Network of Microgrids
  - Compositional Control of Large-Scale Systems

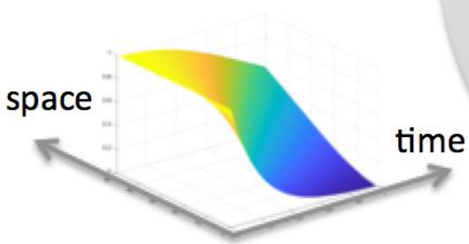
Challenge in Connection Level



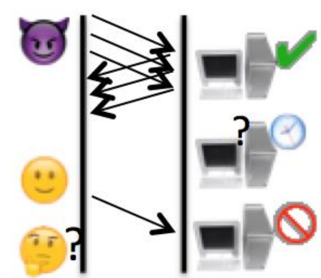
Analyze behavior from its approximation considering model discrepancies



Design a joint disturbance monitor and robust controller framework facing uncertainties and adversarial attacks

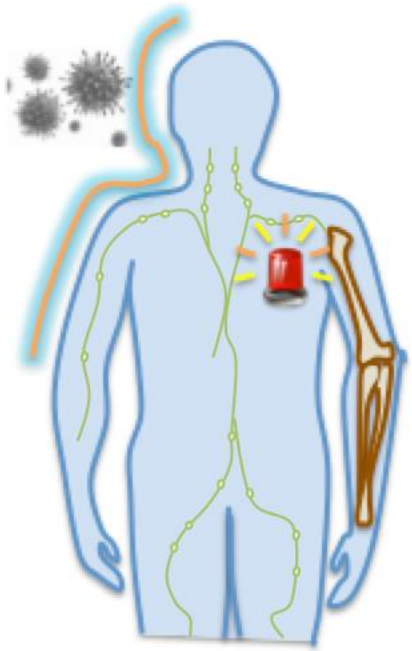


Analyze energy dissipation under a digital control framework for high-dimensional systems



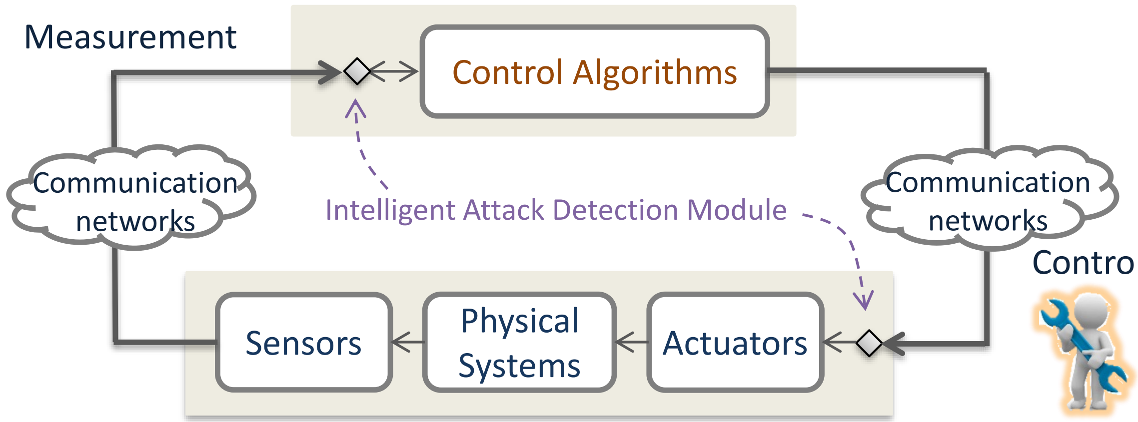
Preserve passivity and stability properties over imperfect communication networks

Joint Disturbance Observer and Controller Design



The **immune system** (from the Latin work immunis, meaning: "untouched") protects the body like a guardian from harmful influences from the environment and is essential for survival*.

* U.S. National Library of Medicine, "Immune System". https://www.ncbi.nlm.nih.gov/pubmedhealth/.



Y. Yan, P. Antsaklis and V. Gupta, "A resilient design for cyber physical systems under attack," *2017 American Control Conference* (*ACC*), Seattle, WA, 2017, pp.4418-4423.

Joint Disturbance Observer and Controller Design

Attack Monitor:

Internal state variable →

$$\dot{\varepsilon} = -l(x)\varepsilon + l(x)(-Ax - Bu - \rho(x))$$

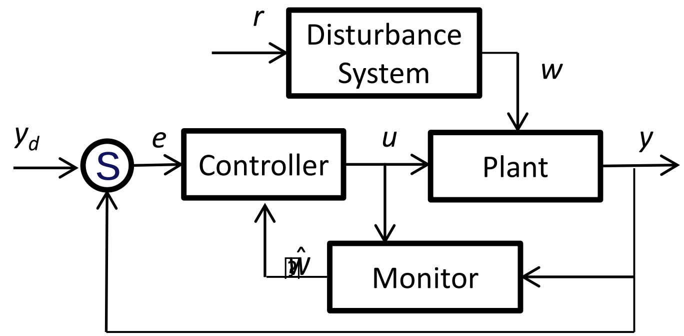
$$\hat{w} = \varepsilon + \rho(x)$$

$$\frac{d}{dt}\rho(x) = l(x)\dot{x}$$

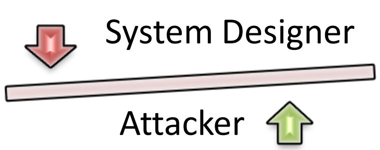
Output of the detection filter

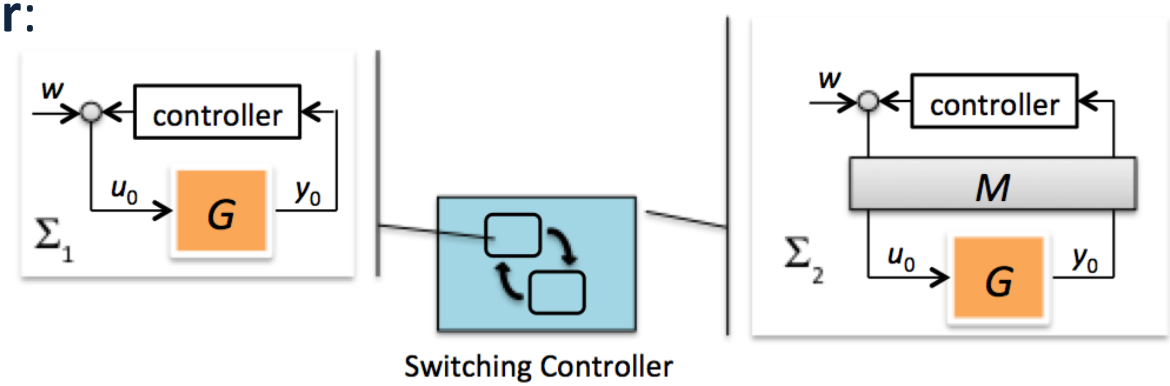
Detection filter gain

Nonlinear function to be designed



Switching the controller:



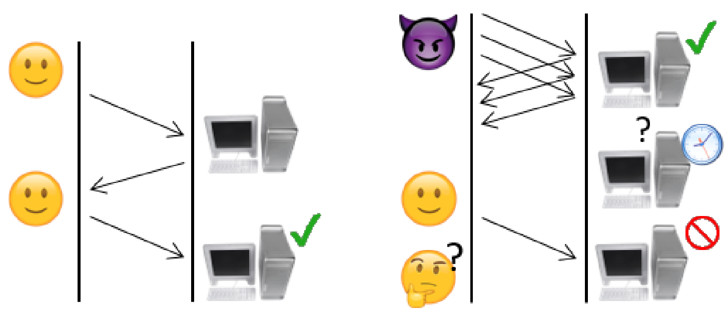


LMI of stable performance under attack ⇨ Design passivation linear transformation M

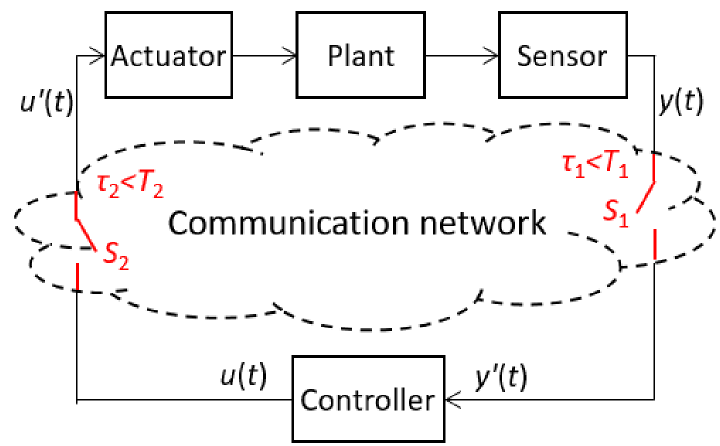
Self-Triggered Strategy under DoS Attack

A **denial-of-service (DoS attack)** is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet*.

* “Understanding Denial-of-Service Attacks”. *US-CERT*. https://www.us-cert.gov/ncas/tips/ST04-015 Retrieved Dec 8th 2017.



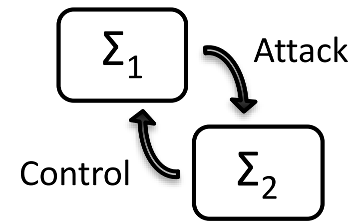
Normal connection　　Under DoS attack



Y. Yan, M. Xia, A. Rahnama and P. Antsaklis, “A passivity-based self-triggered strategy for cyber physical systems under denial-of-service attack,” *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, Melbourne, VIC, 2017, pp. 6072-6088.

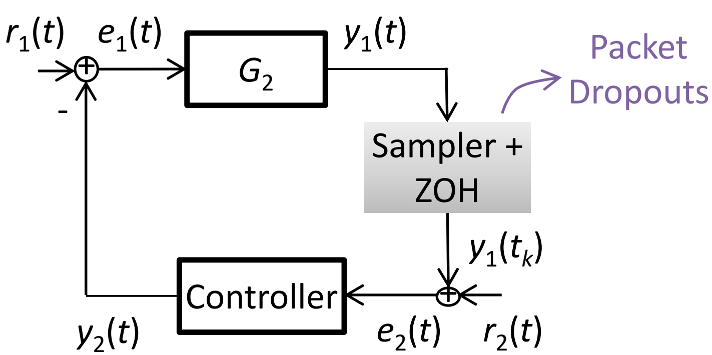
Self-Triggered Strategy under DoS Attack

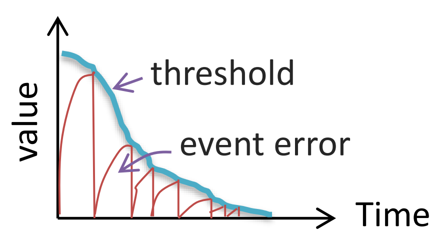
Attack : communication through the network is not ideal

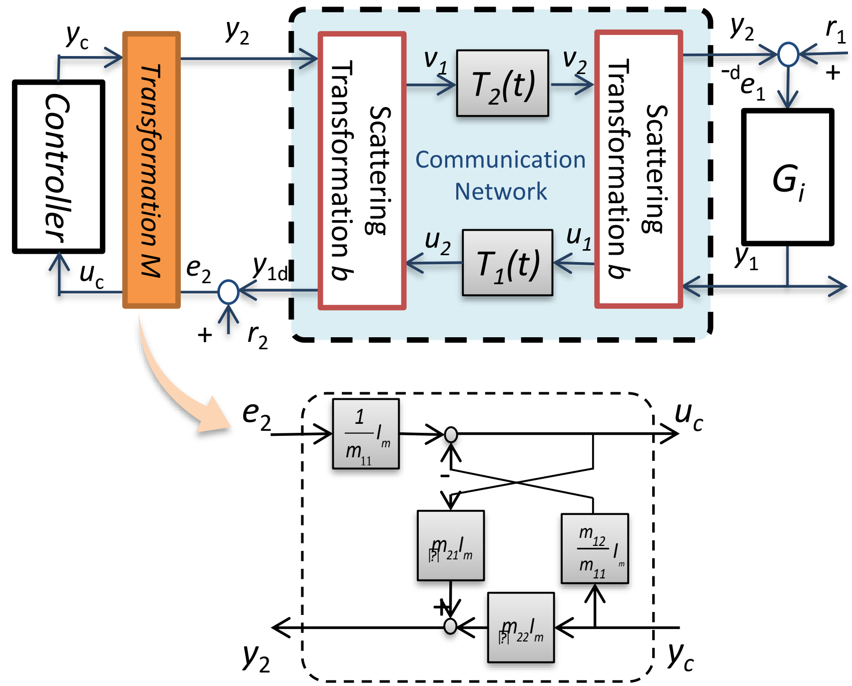


Objective :

- Maximum tolerable length of attack
- Switching strategy



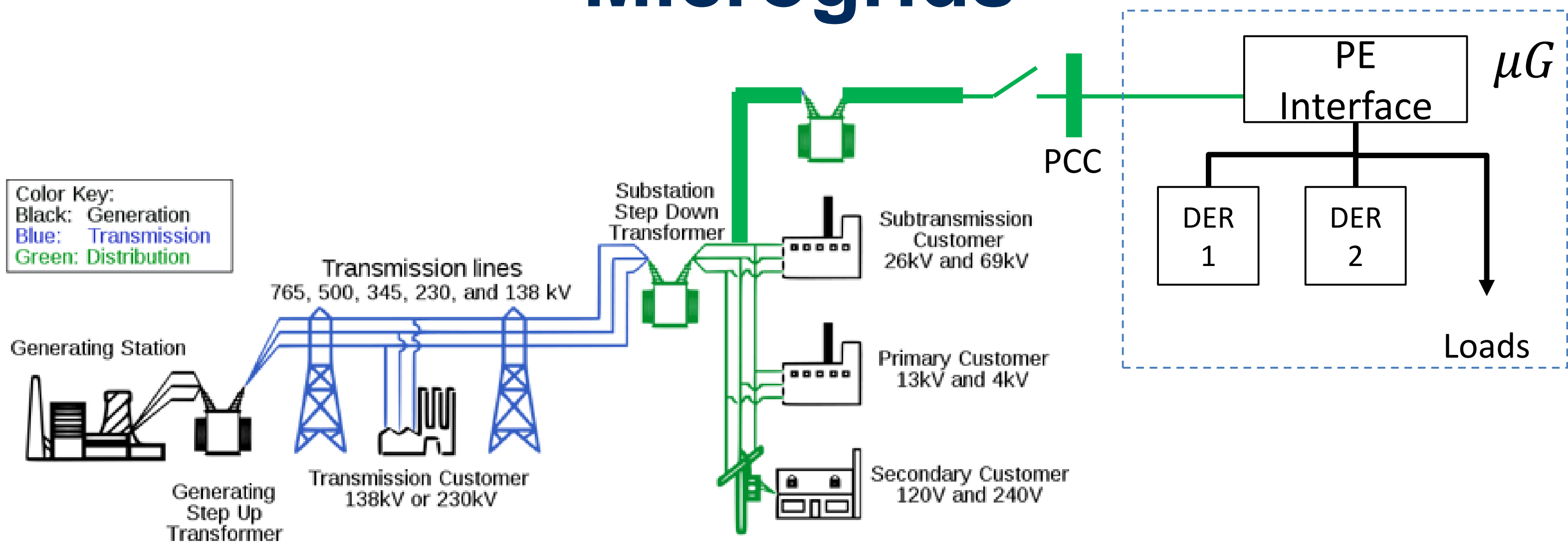




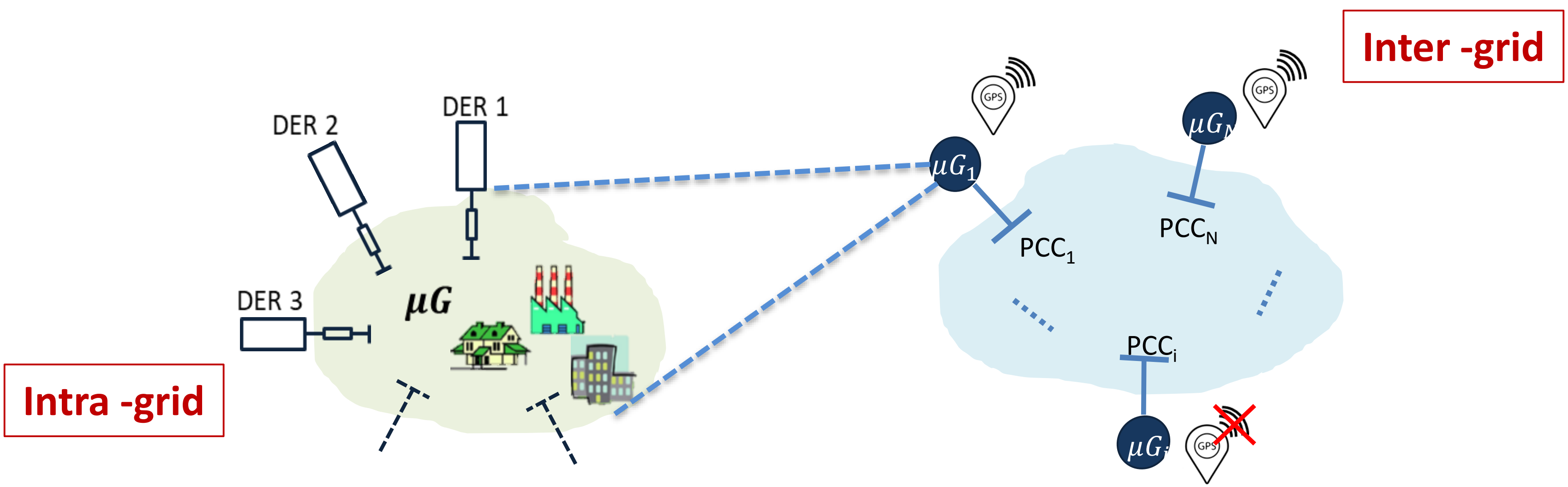
Overview

- **System Level**
  - Local Passivity (and indices) of Nonlinear Systems
  - Adaptation Methods Based on Experimental Passivity Indices
- **Connection Level**
  - Security Design for Data Injection Attack
  - Design Strategy over Imperfect Network
- **Interconnection Level**
  - Applications to Network of Microgrids
  - Compositional Control of Large-Scale Systems

Microgrids

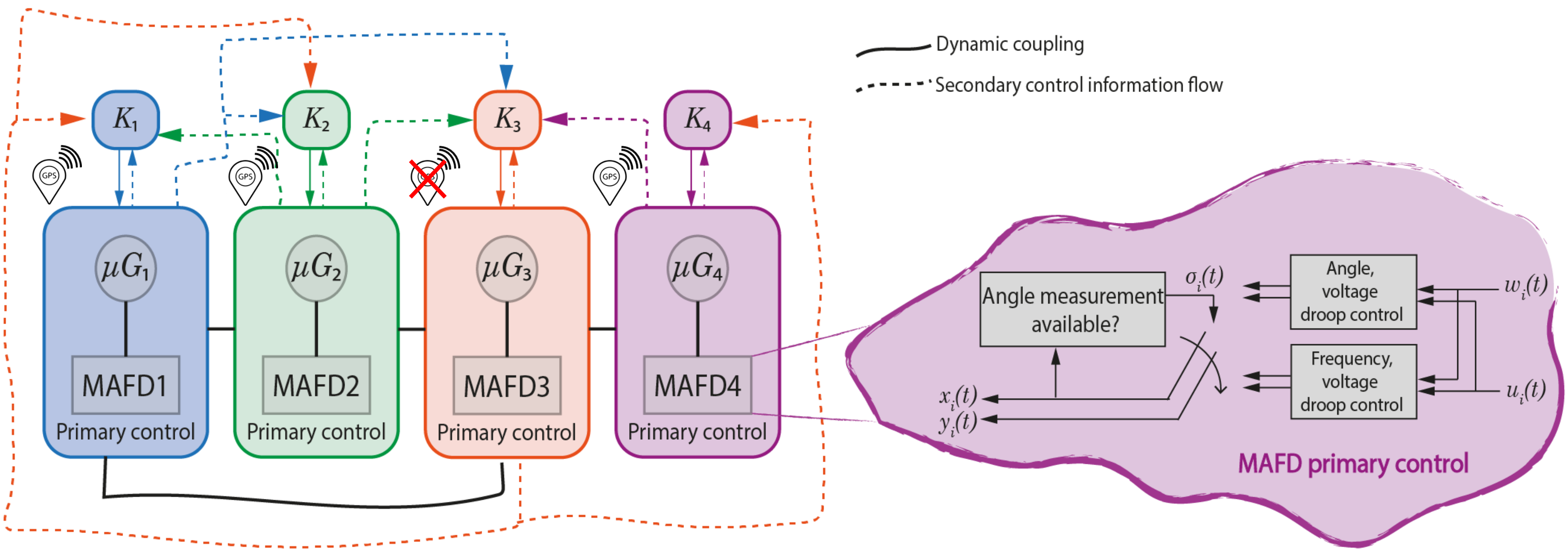


Color Key:
Black: Generation
Blue: Transmission
Green: Distribution
Generating Station
Generating Step Up Transformer
Transmission lines
765, 500, 345, 230, and 138 kV
Transmission Customer
138kV or 230kV
Substation Step Down Transformer
Subtransmission Customer
26kV and 69kV
Primary Customer
13kV and 4kV
Secondary Customer
120V and 240V
PCC
PE Interface
μG
DER 1
DER 2
Loads



Inter -grid
Intra -grid
DER 1
DER 2
DER 3
μG
μG_1
μG_N
PCC_1
PCC_N
PCC_i
GPS

Distributed Mixed Voltage Angle and Frequency Droop Control of Microgrid Interconnections with Loss of Distribution-PMU Measurements



D-MAFD

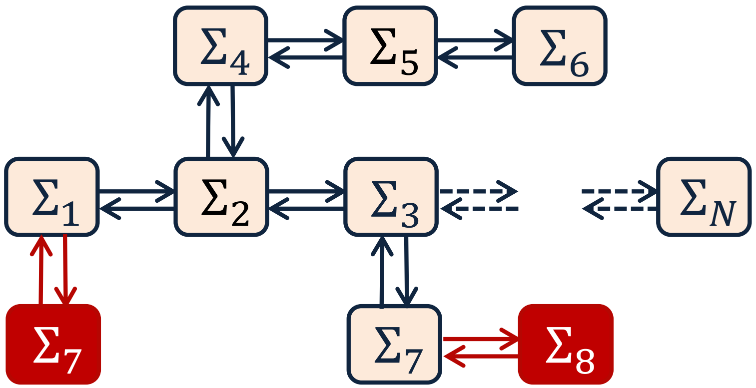
- Passivity under loss of PMU-measurement
- Robustness to topology changes

Next question – How do we facilitate ad-hoc connections of microgrids?

S. Sivaranjani*, E. Agarwal*, L. Xie, V. Gupta, and P. J. Antsaklis, "Distributed mixed voltage angle and frequency droop control of microgrid interconnections with loss of distribution-PMU measurements," submitted to IEEE Transactions on Smart Grid, arXiv:1810.09132, Oct 2018.

Compositional Control of Large-Scale Systems

"We refer to a system as large-scale if it is more appropriate to consider the system as an interconnection of small sub-systems than dealing with it as a whole"

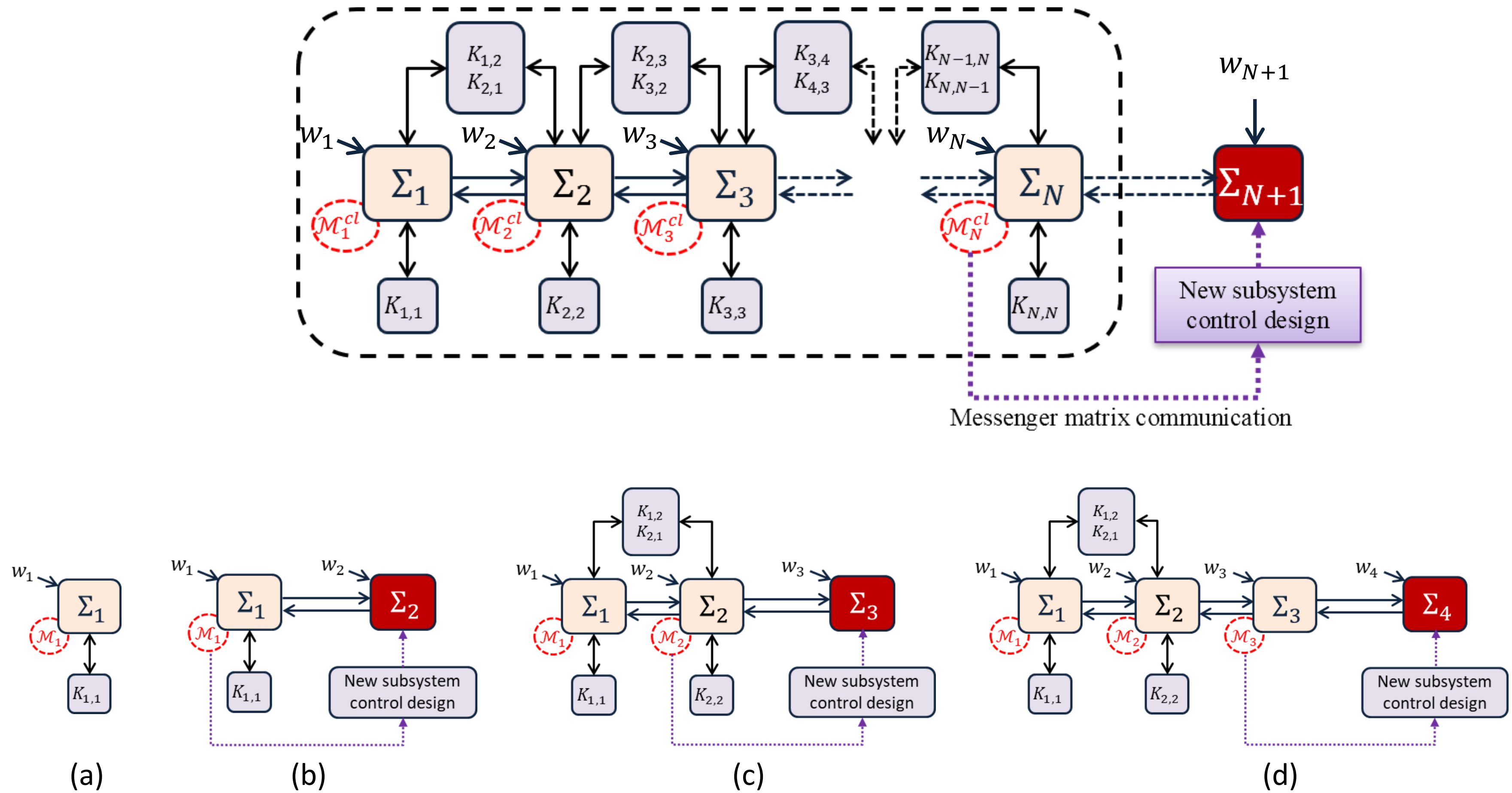


Objective:

Develop an algorithm to guarantee passivity of a dynamically growing interconnection, such that the addition of new subsystems does not require redesigning the pre- existing local controllers in the network.

- Distributed verification of passivity using equivalent analysis on passivity of individual subsystems and coupling at individual interconnections.
- Local synthesis of individual sub-system level controllers, with no direct knowledge of the dynamics of other subsystems, for passivity guarantees on large-scale system.

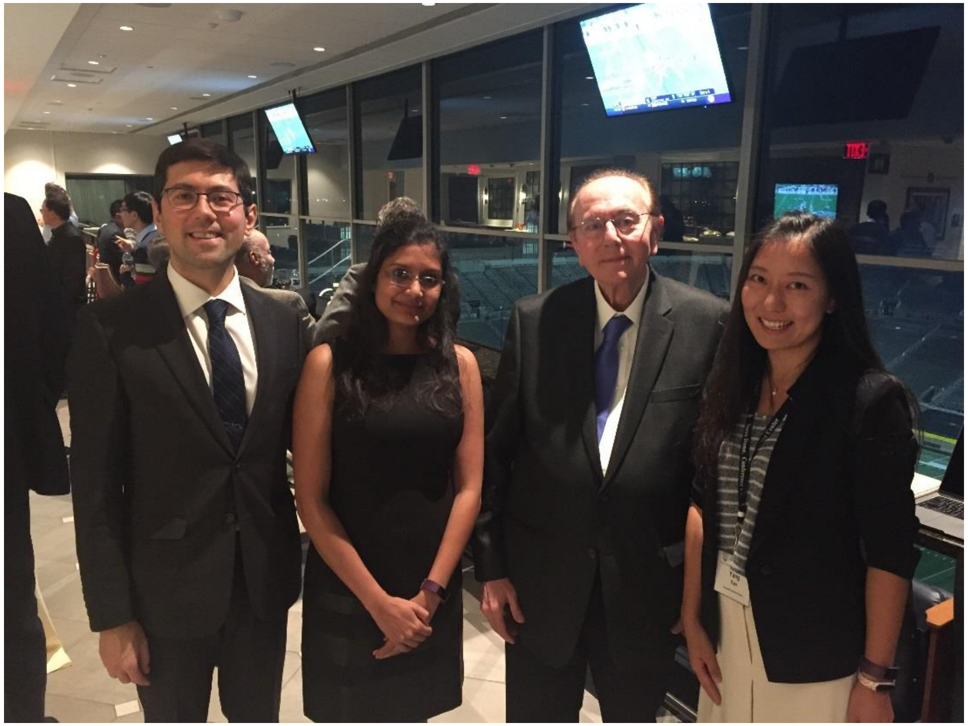
Sequential Synthesis of Distributed Controllers for Cascade Interconnected Systems



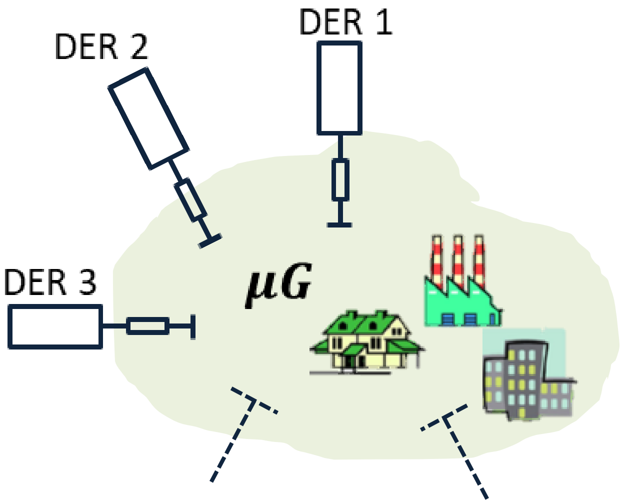
E. Agarwal*, S. Sivaranjani*, V. Gupta, P. J. Antsaklis, “Sequential synthesis of distributed controllers for cascade interconnected systems,” submitted to American Control Conference, 2019, pre-print: goo.gl/JTCV6z.

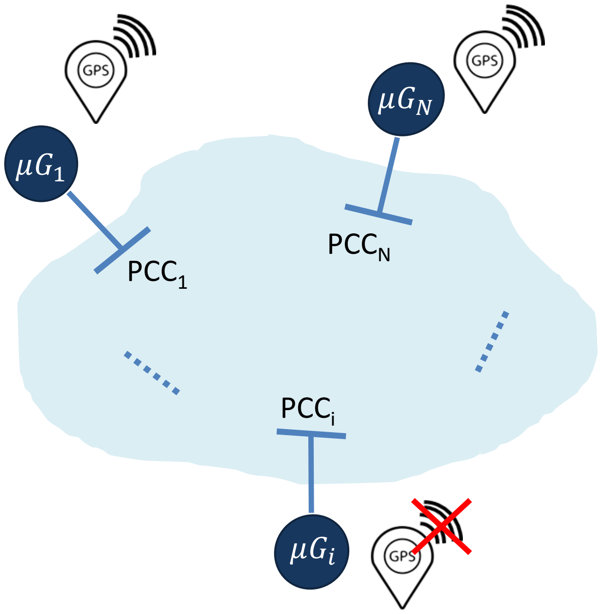
Thank You

For always being there for us, and for all your mentorship



Microgrids





Intra -grid

Stability with respect to small disturbances

Robustness to generation-load mismatch

Information and network limitations

Inter -grid

PMU-measurement loss

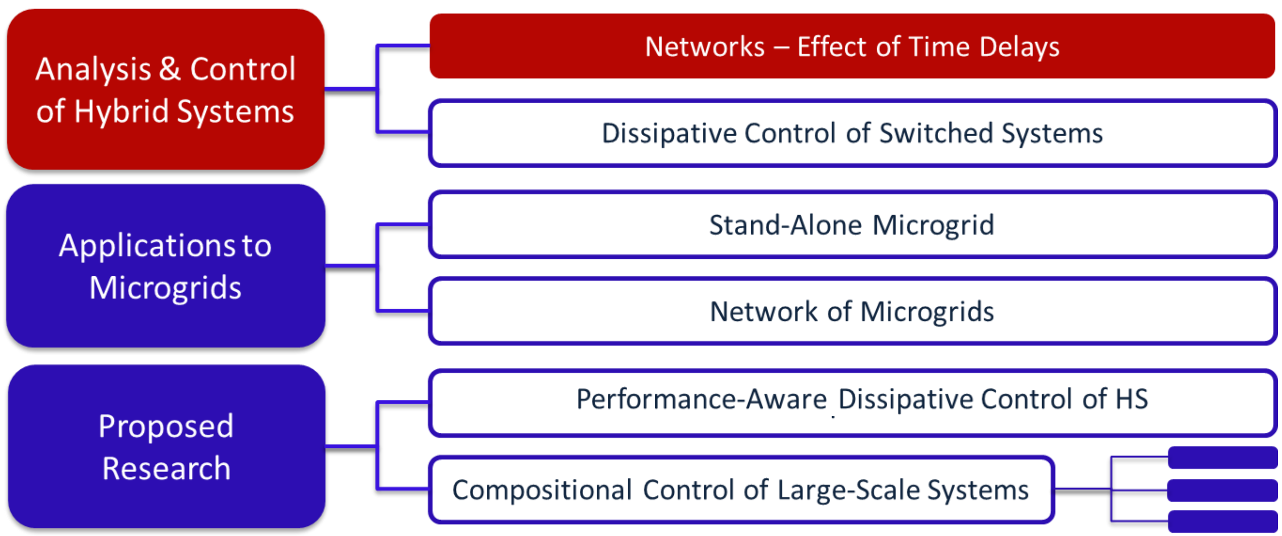
Robustness to topology changes

Facilitate ad-hoc connections of microgrids

Dissipativity of Networks of Hybrid Systems

E. Agarwal, M. J. McCourt, and P. J. Antsaklis, "Dissipativity of hybrid systems: Feedback interconnections and networks," in American Control Conference (ACC), 2016. IEEE, 2016, pp. 6060-6065.

E. Agarwal, M. J. McCourt, and P. J. Antsaklis, "Dissipativity of finite and hybrid automata: An overview," in Control and Automation (MED), 2017 25th Mediterranean Conference on. IEEE, 2017, pp. 1176-1182.

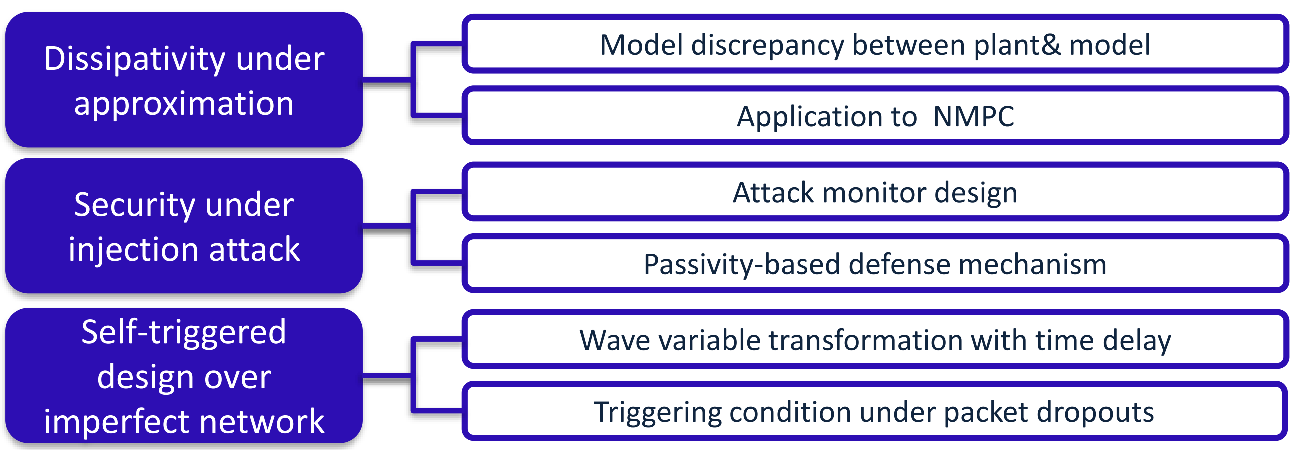


Resilient Design for Connection Level

Yang Yan and Panos Antsaklis, “Stabilizing Nonlinear Model Predictive Control Scheme Based on Passivity and Dissipativity,” *2016 American Control Conference* (*ACC*), Boston, MA, 2016, pp.76-81.

Y. Yan, P. Antsaklis and V. Gupta, “A resilient design for cyber physical systems under attack,” *2017 American Control Conference* (*ACC*), Seattle, WA, 2017, pp.4418-4423.

Y. Yan, M. Xia, A. Rahnama and P. Antsaklis, “A passivity-based self-triggered strategy for cyber physical systems under denial-of-service attack,” *2017 IEEE* 56^{th} *Annual Conference on Decision and Control (CDC)*, Melbourne, VIC, 2017, pp. 6072-6088.



Dissipativity

The system (1) is said to be dissipative with respect to the supply rate $\omega(w(t), y(t))$, if there exists a positive definite function $V(x)$: $\mathbb{R}^n \longrightarrow \mathbb{R}^+$ with $V(0) = 0$, called the storage function, such that

$$\int_{t_0}^{t_1} \omega\big(w(t), y(t)\big)dt \geq V\big(x(t_1)\big) - V\big(x(t_0)\big)$$

holds, for all $w \in \mathbb{R}^m$, and all $t_1 \geq t_0 \geq 0$, where $x(t_1)$ is the state at time t_1 resulting from the initial condition $x(t_0)$ and input $w(\cdot)$.

Dissipativity

The system (1) is said to be dissipative with respect to the supply rate $\omega(w(t), y(t))$, if there exists a positive definite function $V(x)$: $\mathbb{R}^n \longrightarrow \mathbb{R}^+$ with $V(0) = 0$, called the storage function, such that

$$\int_{t_0}^{t_1} \omega\big(w(t), y(t)\big)dt \geq V\big(x(t_1)\big) - V\big(x(t_0)\big)$$

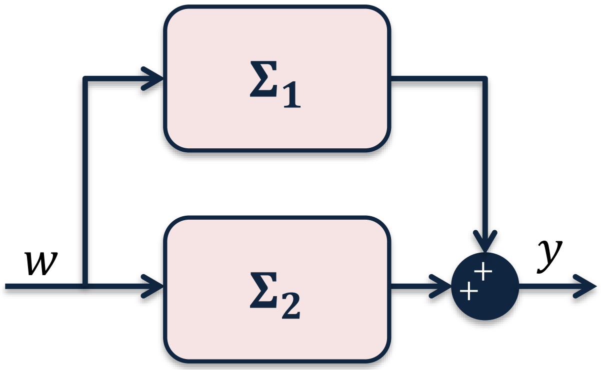
holds, for all $w \in \mathbb{R}^m$, and all $t_1 \geq t_0 \geq 0$, where $x(t_1)$ is the state at time t_1 resulting from the initial condition $x(t_0)$ and input $w(\cdot)$.

Dissipativity

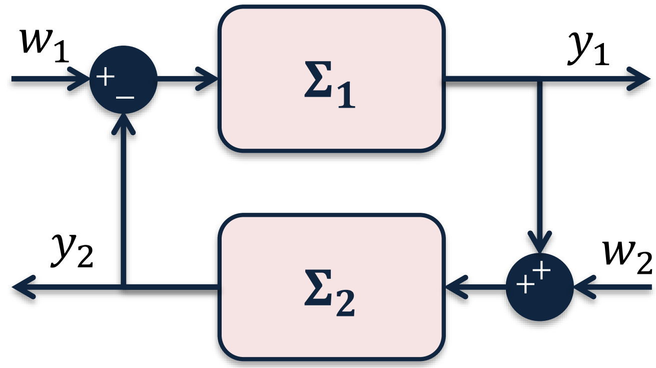
Supply rate	Dissipativity
	– Dissipativity
	Passivity
	State Strict Passivity;
	Input Feed-Forward Passivity (IFP); ISP if
	Output Feedback Passivity (OFP); OSP if
	Finite Gain stability,

Passivity, ISP, OSP	Lyapunov Stability
State Strict Passivity	Asymptotic stability
– Dissipativity,	Finite Gain Stability
OSP	Finite Gain Stability

Dissipativity



$\mathbf{\Sigma_1}$ - Passive/ISP
$\mathbf{\Sigma_2}$ - Passive/ISP



$\mathbf{\Sigma_1}$ - QSR dissipative
$\mathbf{\Sigma_2}$ - QSR dissipative

Passivity, ISP, OSP	Lyapunov Stability
State Strict Passivity	Asymptotic stability
– Dissipativity,	Finite Gain Stability
OSP	Finite Gain Stability

Cyber-Physical Systems

[1]CPS are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components.

Large scale interconnection – Compositional design tools






[1]http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286