CPS – Breakthrough: Development of Novel Architectures for Control and Diagnosis of Safety-Critical Complex Cyber-Physical Systems

Stéphane Lafortune and Necmiye Ozay Department of EECS, University of Michigan

Overall Objective:

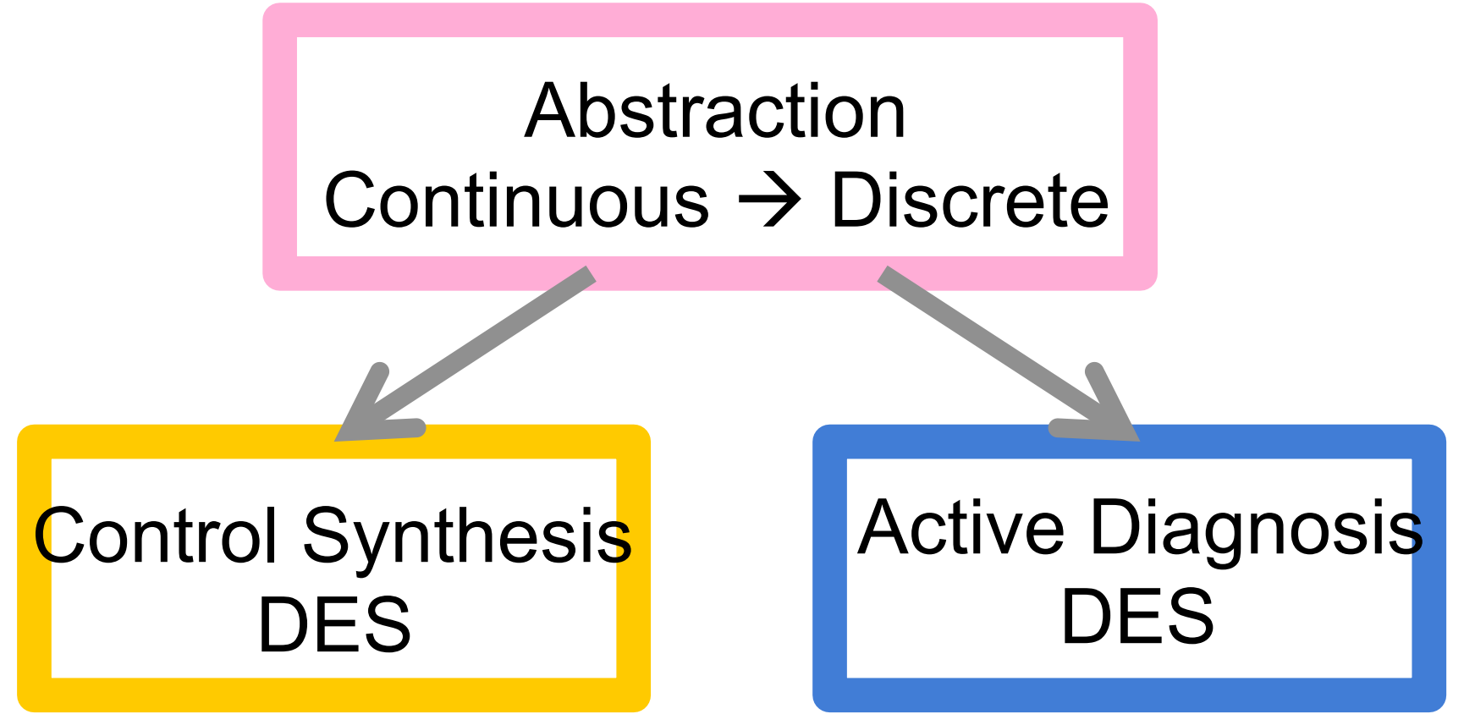
•Scalability of formal methods for synthesis of provably-correct controllers

•Development of abstraction techniques that lift CPS design problem to synthesis problem on discrete state system

•Combination of control and sensor activation

•Synthesis for resilience and adaptivity

•Consideration of the distributed features of the system at synthesis step and at implementation step



Abstraction
Continuous → Discrete

Control Synthesis
DES

Active Diagnosis
DES

Project Start Date: January 2015

Project Website:

https://wiki.eecs.umich.edu/complexcps/

Participants:

• Graduate Students: Xiang Yin (PhD graduate 2017), Yun Jae Cho (MS graduate 2016), Yunus Sahin, Romulo Meira Goes

• Undergraduate Students: Hector Dominguez, Dylan Lawton, Nicholas Recker, Stanley Smith, Siyuan Shen, Andrew Wagenmaker, Gregory Willett, Ryan Wunderly

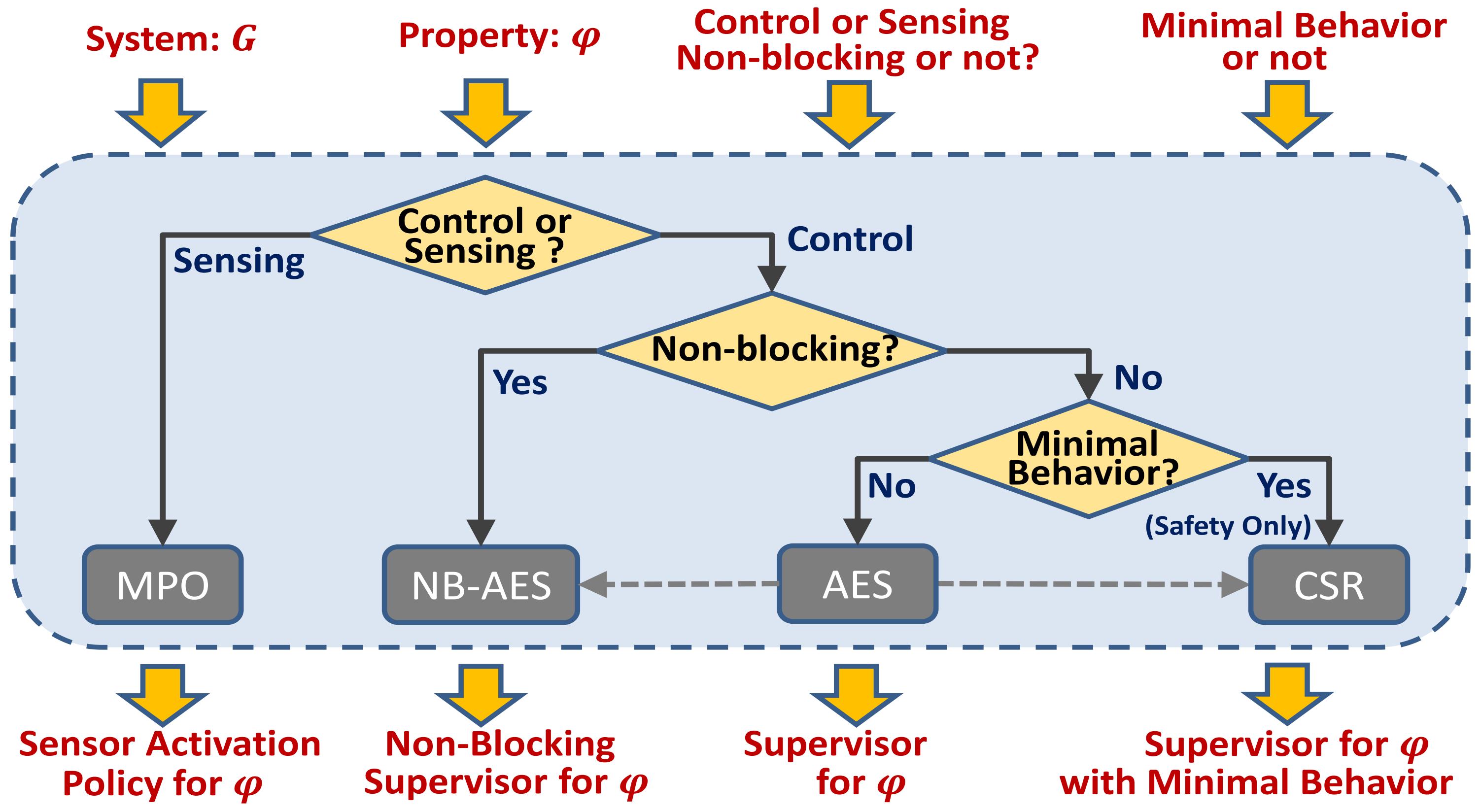
Industrial Collaborators:

• UTC Aerospace Systems (UTAS)

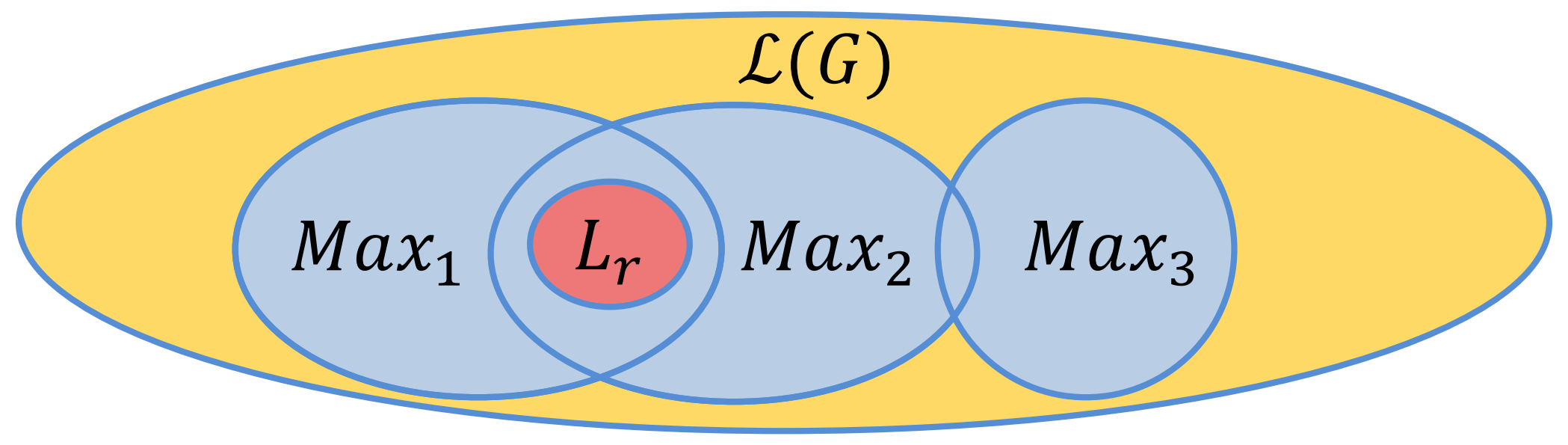
• Ford Motor Company

Recent Results:

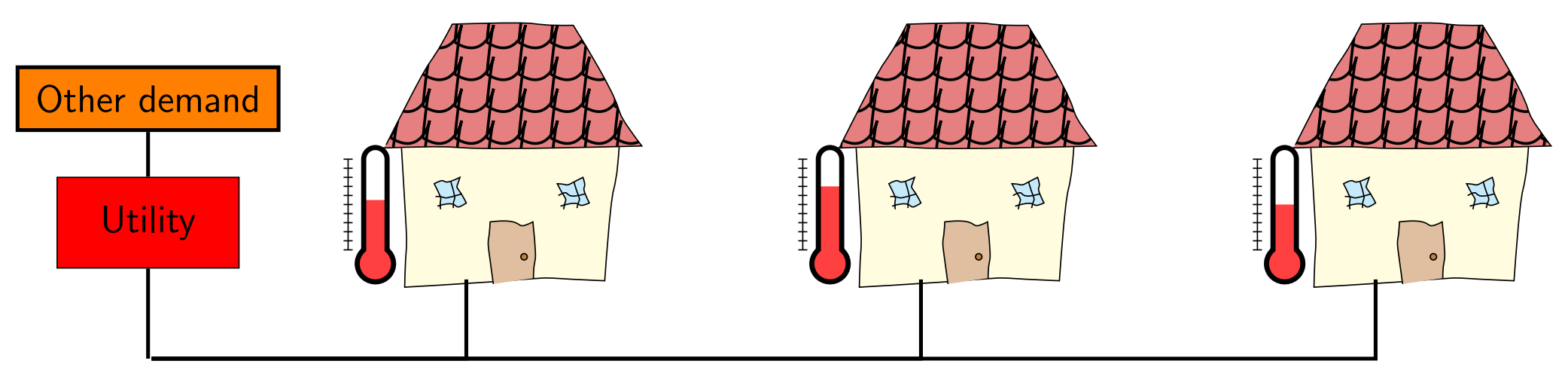
- Uniform Synthesis Methodology at the Discrete Level
  - ➢ Controller synthesis: for safety, non-blockingness, maximal permissiveness, and minimal behavior
  - ➢ Synthesis of sensor activation policies: for information-state based properties, such as diagnosability, opacity
  - ➢ Solves synthesis problems that had remained open for a long time, using a game approach on suitable discrete transition structures: MPO and [NB-]AES
  - ➢ Implemented in Software Tool: DPO-SYNT https://gitlab.eecs.umich.edu/M-DES-tools/DPO-SYNT
  - ➢ PhD dissertation of Xiang Yin (2017)

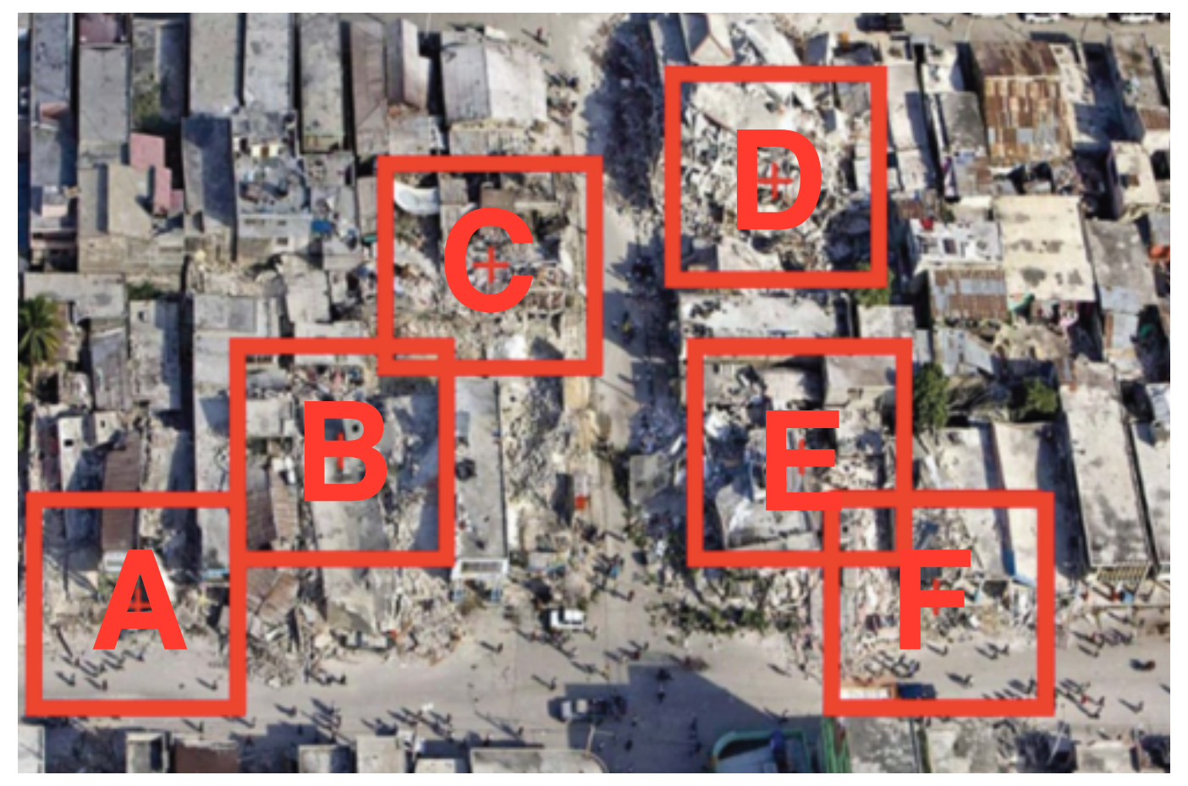


Use minimal required behavior at synthesis time to select local maximal solution



- Massively Scalable Synthesis at the Continuous Level
  - ➢ Structural properties: large # of systems, small # of classes; counting constraints (sufficiently many/not too many); identity of individual systems is not important



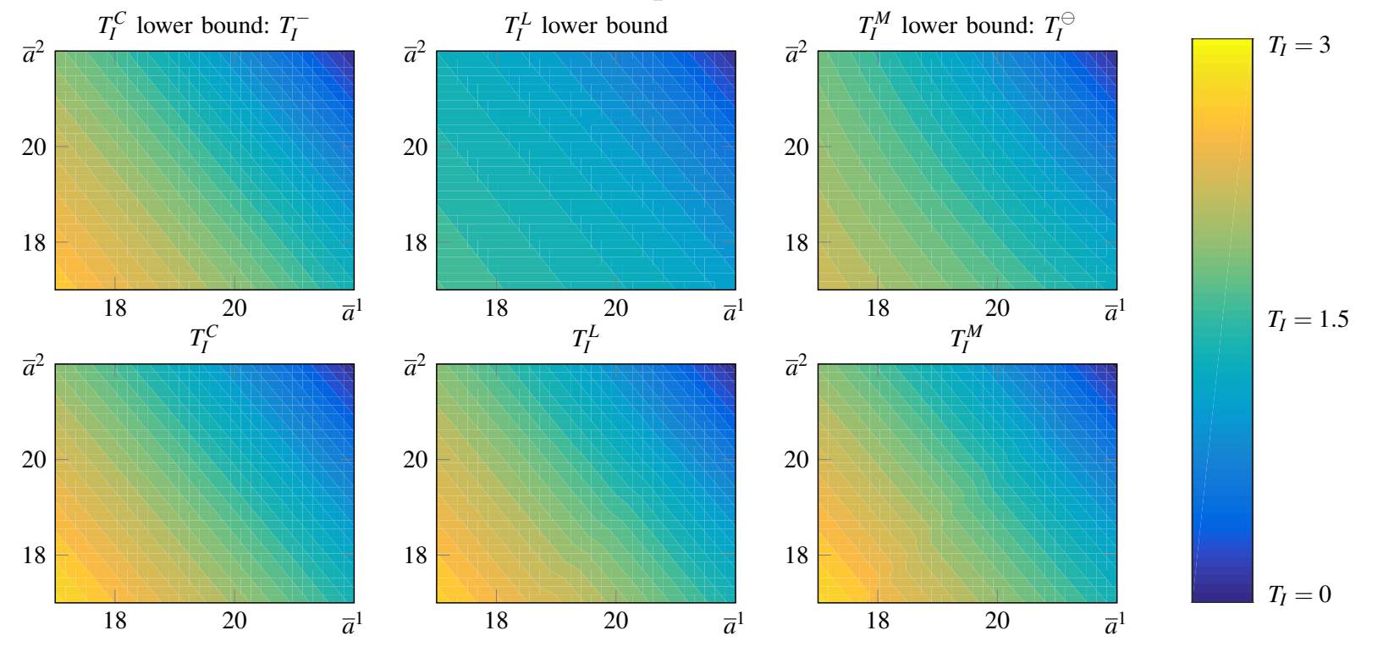


Applications: thermostatically controlled load coordination; multi-agent emergency response

  - ➢ Exploits symmetry (permutation invariance) in dynamics and specifications
    - ➢ extensions to near symmetric case
    - ➢ works across scales (10 to 10K or more systems)
    - ➢ robustness to asynchrony, agents entering and exiting the group
  - ➢ A new logic (counting Linear Temporal Logic) to capture multi-agent coordination specifications

- Time of invariance: a time-based abstraction
  - ➢ Time of invariance: a timing abstraction that measures the time to constraint violation when constraint violation is unavoidable. Associated synthesis techniques for large scale switched systems. Dual to time-optimal control.

Efficiently computable relaxations for time of invariance for heterogeneous collections of switched systems



T_I^C lower bound: T_I^-
T_I^L lower bound
T_I^M lower bound: $T_I^\ominus$
T_I^C
T_I^L
T_I^M
$\bar{a}^2$
$\bar{a}^1$
$T_I = 3$
$T_I = 1.5$
$T_I = 0$