Abstractions for Scalable Verification of AI-enabled Cyber-Physical Systems

3.8.2026 - Pavithra Prabhakar | IMDEA Software Institute

11:00am 302-Mountain View and Zoom3 (https://zoom.us/j/3911012202, password:@s3).

Pavithra Prabhakar, *Professor, University of New Mexico*

Abstractions for Scalable Verification of AI-enabled Cyber-Physical Systems

Abstract:

AI-based components have become integral to Cyber-Physical Systems (CPS), enabling transformative functionalities across various domains including transportation, energy, and medicine. Specifically, machine learning components are now widely used for perception, control, and decision-making in safety-critical applications, necessitating rigorous verification methods to ensure safe deployment in real-world environments.

In this talk, we present a formal approach for verifying the safety of AI-enabled CPS. We focus on closed-loop systems that integrate dynamical models of physical processes with neural network-based perception and control modules. We explore two verification scenarios: (1) controllers implemented as neural networks, and (2) perception pipelines combining camera models with neural networks. A key challenge in both settings is the scalability of verification algorithms, particularly due to the large size of neural networks and the complexity introduced by image-based perception.

To address these challenges, we propose abstraction techniques that simplify system representations and make verification tractable. Specifically, we introduce two novel data structures: Interval Neural Networks, which provide abstract representations of neural network behaviors, and Interval Images, which serve as abstract symbolic representations of a set of images. We also present novel abstraction-refinement algorithms that efficiently search for small abstractions to prove system safety. Our experimental results demonstrate that these abstraction-refinement algorithms significantly improve scalability and efficiency by quickly identifying small abstractions to prove safety, enabling the analysis of complex, large-scale AI-enabled CPS.

We also discuss verification approaches for evolving neural networks and highlight ongoing work on stability analysis, refinement checking, compositional analysis, and related challenges.

https://software.imdea.org/events/invited-talks/2026/08-03