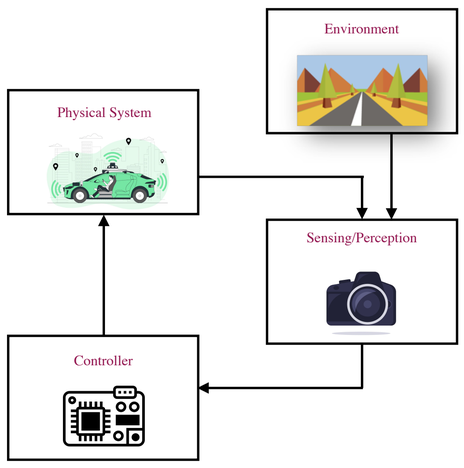
SHF: Small: Scalable Formal Verification of ANN controlled Cyber-Physical Systems

PI: Scott DeLoach (Former PI: Pavithra Prabhakar)
Postdoc: Lipsy Gupta, Kansas State University

Award Abstract # 2008957

Learning-based components in CPS

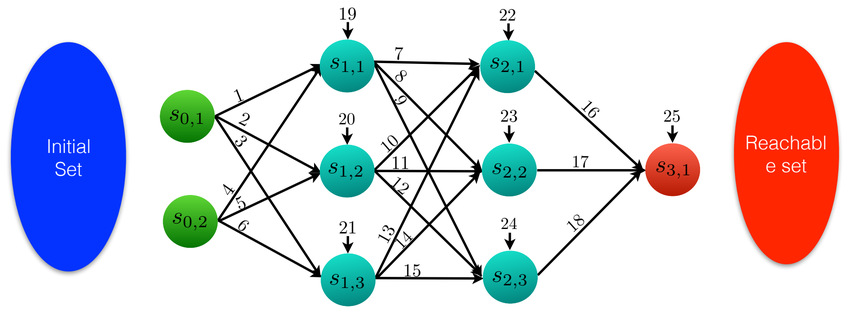
Today, CPS are increasingly being deployed in dynamic and uncertain environments, are expected to operate over long time horizons with quick response time and make decisions autonomously.



- Learning-based components such as artificial neural networks (NN) deployed for control and perception
- Autonomous driving: Image-based perception to compute distance to neighboring vehicles for control
- Airborne Collision Avoidance System: ACAS Xu, a neural network controller that is more computation and memory efficient
- Safety is a challenge!

Reachable Set Computation Problem

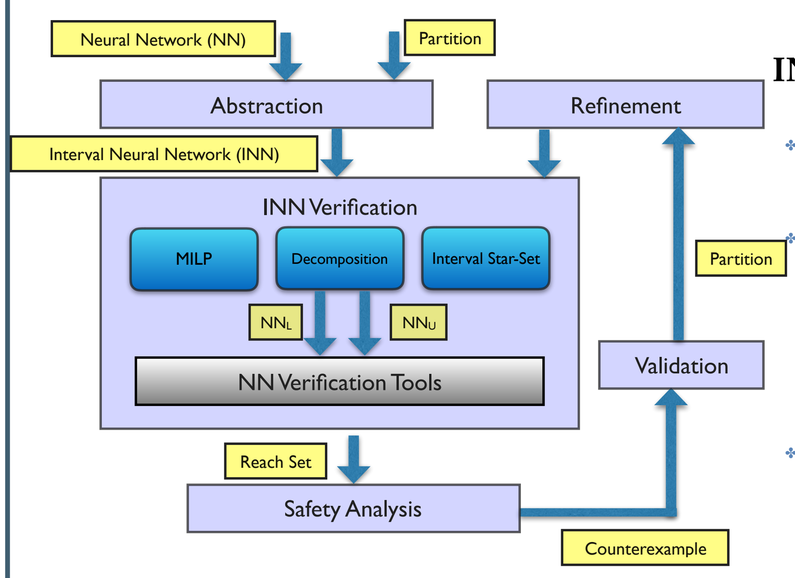
The crux of safety analysis lies in computing the reachable set, that is, the set of all outputs values given a set of input values



Given a neural network $\mathcal{T}$, and a set of values I for the input layer, compute a range of values $[v_{min}, v_{max}]$ for the corresponding values of an output node.

Challenge: Controller is a highly non-linear complex function represented by a deep neural network!

Abstraction-based Verification

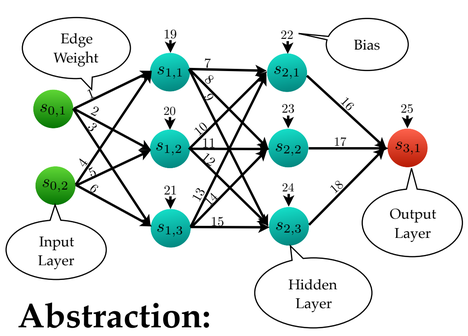


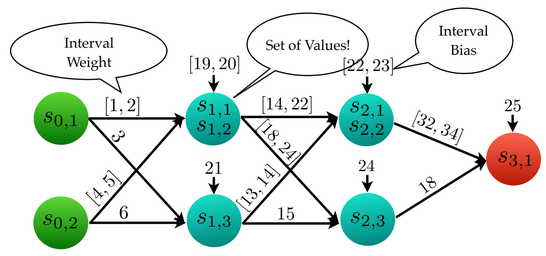
INN Verification Methods:

- **MILP-based approach:** Extend MILP encoding for NN to INN
- **Star set-based symbolic approach:** Novel data structure-Interval star-sets; can compute linear transformation and intersection with half-space
- **Decomposition-based approach:** Reduce INN verification to NN verification using upper and lower bound NNs

Interval Neural Network (INN)

- Extends a neural network with "interval" weights and biases
- The value at a node is computed nondeterministically by choosing some value for the weight and biases from their corresponding intervals



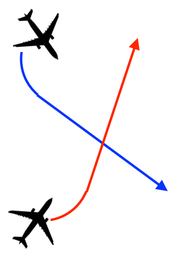


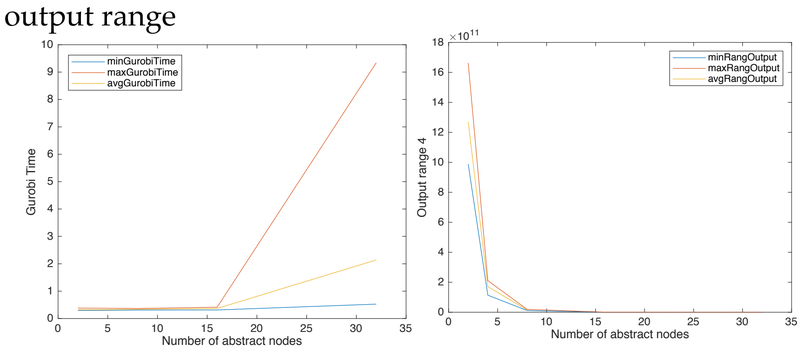
Abstraction:

- Partition nodes of a layer and merge to form an abstract node
- Approximate weights by convex hull of edge weight multiplied by number of nodes in the source
- Approximate biases by intervals corresponding to convex hulls of biases of nodes being merged

Case Study

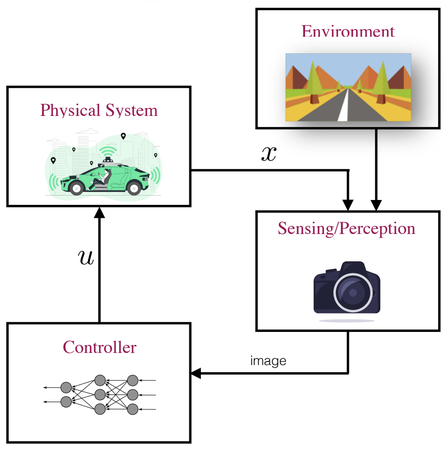
- **ACAS Xu Benchmark:** Aircraft Collision Avoidance System (ACAS); NN with 6 hidden layers and 50 neurons/layer; has large look up tables
- Abstraction algorithm implemented in Python with Gurobi as the backend MILP solver
- Evaluate the trade-off between the granularity of abstraction and verification time and precision of the computed output range
- MILP solving time increases more drastically than abstraction/encoding time
- Precision improves with the increase in the number of abstract nodes
- The times and precision vary based on the partitioning of the nodes for a fixed number of abstract nodes





Camera-based Perception

- Mathematically capture the camera model and rendering phenomenon on canvas
- Symbolic analysis: Propagate system states through the closed-loop
  - A novel notion of invariant regions for propagation through the camera model
- Scalable analysis: Notion of *interval images* for scalable verification



Publications:

- *Star based Reachability Analysis of Interval Neural Networks. V. Bondalakunta and P. Prabhakar:* ***CDC'23***
- *Abstraction-based Safety Analysis of Linear Dynamical Systems with Neural Network Controllers. R. Lal and P. Prabhakar:* ***CDC'23***
- *Bisimulations for Neural Network Reduction. P. Prabhakar:* ***VMCAI'22***
- *Verification of Camera-Based Autonomous Systems: Habeeb P, N Deka, D D'Souza, K Lodaya, P Prabhakar.* ***IEEE TCADICS, 2023***
- *Safety Verification of Closed-loop Control System with Anytime Perception. L. Gupta, J. C. Choton, P. Prabhakar,* ***ICRA'24***

Add Your Logo and/or project info here

Award ID#: 2008957