Synchronous Neural Networks for Cyber-Physical Systems

Abstract:

*Cyber-physical systems (CPS), such as autonomous vehicles or smart power grids, use interactive machine learning modules for decision making. Current design approaches use multiple machine learning modules, often using Artificial Neural Networks (ANNs), to achieve the desired functionality. Current approaches to verification and validation of these ANNs are generally either very difficult, time consuming and/or not fully reliable. A key feature missing is related to the use of ANNs in real-time systems, which demand the capability of worst-case analysis.*

*In this thesis we introduce Synchronous Neural Networks (SNNs) as a new approach to the safe use of ANNs in CPS. SNNs provide synchronous semantics to ANNs. This enables real-time operation and facilitates static timing analysis of individual ANNs. We define these SNNs the Esterel synchronous language. We then use a time predictable platform called T-CREST, which facilitates static timing analysis.*

*We propose Meta Neural Networks (MNNs) as a framework for the systematic composition of SNNs. This enables compositional system design using multiple SNNs and other synchronous functional components, while maintaining the synchronous semantics of the system. Synchronous MNNs allow for the creation of causal, deterministic, predictable controllers for CPS.*

*Misclassification is a major issue with input perturbation in ANNs. We combine MNNs with Run-time Enforcers (RE), which enforce a set of desired policies by transforming inputs and outputs suitably. The proposed solution is able to effectively deal with many misclassifications.*

*Finally, we propose a tool that extends the ANN-library Keras to give it a MNN description capability. We then automatically generate synchronous C code, which is shown to perform even better than our earlier MNN implementation using Esterel.*

*We have developed several CPS examples that range from an energy storage system for charging electric vehicles, to a traffic sign detection system for autonomous vehicles. These results show that the implemented MNNs can meet real-time, safety critical deadlines. Composing MNNs of multiple SNNs and RE provide an increase in the safety of autonomous vehicles, where the MNNs not only increase classification accuracy of the environment, but also detect misclassifications and allow the system to respond safely to these misclassifications.*