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 NNs in real-time systems, which demand the capability of worst-case analysis.*

*A new approach to verifiable ANNs is proposed using the synchronous paradigm to introduce Synchronous Neural Networks (SNNs). Logical time is allocated to the operations of the SNNs, providing sound compositional primitives. This enables the composition of interacting ANNs to ensure causality and determinism.*

*In this thesis we introduce SNNs as a new approach to the safe use of ANNs in CPS. Their synchronous semantics enable periodic real-time operation and facilitate static timing analysis of individual SNNs. Additionally, 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 safe, functional components. The combination of SNNs and Runtime Enforcement (RE), which enforce a set of desired policies by transforming inputs and outputs suitably, is proposed as an effective solution to deal with misclassifications and avoid safety violations as a result.*

*Finally, we propose a tool that extends Keras to give it a MNN description capability. We then automatically generate C code, which are shown to perform even better than our earlier MNN implementations using Esterel. Initially, MNNs for this thesis were implemented in Esterel for the design of synchronous systems, while subsequent MNNs were implemented using this tool. We demonstrate the efficacy of our approach by developing CPS with MNN controllers; ranging from MNNs with 5 neurons to MNNs with 10,000+ neurons.*