Abstract

We are investigating the specification, design and verification of distributed systems that combine communications, computation and control in dynamic, uncertain and adversarial environments. Our goal is to develop methods and tools for designing control policies, specifying the properties of the resulting distributed embedded system and the physical environment, and proving that the specifications are met. In the area of hybrid systems, we have developed tools for analysis of periodically controlled hybrid automata (PCHAs) that allow us to prove stability for control systems that have slightly asynchronous controller execution (with bounds on the controller execution period). We have also developed a promising set of results in receding horizon temporal logic planning that allow automatic synthesis of complex dynamical systems which are guaranteed, by construction, to satisfy the desired properties even in the presence of adversary. The desired properties are expressed in the language of temporal logic and the resulting system consists of a discrete planner that plans, in the abstracted discrete domain, a set of transitions of the system to ensure the correct behaviors and a continuous controller that continuously implements the plan.