Specification and Verification of Timed Systems

Joseph Sifakis (VERIMAG, France)

We present a survey of recent results on the specification and verification of timed systems. Three different classes of formalisms are considered: Algebraic formalisms including operators that allow to express timing constraints like delays, timeouts, watchdogs. These formalisms can be considered as timed process algebras whose the most realistic representatives are the timed extensions of the Lotos language. Transition based formalisms which can be considered as extensions of automata or Petri nets with timing constraints. This class includes timed Petri nets and extensions of automata with continuous variables measuring the time elapsed such as timed automata and hybrid automata. Logical formalisms which are languages of the formulas of a logic with operators expressing timing constraints. Representatives of these formalisms are real-time temporal logics that are extensions of temporal logics with quantitative time and the Calculus of Durations. We show that as in the untimed case, all these formalisms admit a general common model: labeled transition systems with timed transitions. The existence of a common semantic framework allows a comparison of the classes. We focus on two particular problems: The translation of algebraic languages into transition based ones. This is a central problem for the compilation of algebraic timed languages into an executable model and it raises problems of compositionality, efficiency and optimality of the generated model. The verification by comparison of two transition-based descriptions or by comparison of a transition based description against a logical specification. We conclude by discussing issues concerning the applicability of the existing results and approaches and by pointing out some interesting research directions.