Collaborative Systems

Andre Scedrov, University of Pennsylvania, USA

We discuss a model of collaboration, introduced in a joint work with Kanovich and Rowe, in which the participants are unwilling to share all their information with each other, but some information sharing is unavoidable when achieving a common goal. The need to share information and the desire to keep it confidential are two competing notions which affect the outcome of a collaboration. Our model is based on the notion of a plan which originates in the AI literature. We also consider an extension of the model which allows for updates of values with fresh ones, such as updating a password.

All the players inside our system, including potential adversaries, have similar capabilities. They have bounded storage capacity, that is, they can only remember a bounded number of facts. This is technically imposed by allowing only the so-called balanced actions, that is, actions that have the same number of facts in their pre and post conditions. We investigate the complexity of the planning problem, whether the players can reach a goal while avoiding certain critical configurations along the way. We show that this problem is PSPACE-complete. The complexity is lowered to NP-completeness for the class of so-called progressing collaborative systems, intended to describe administrative processes, which normally have a progressing nature: once an item in an activity to-do list is checked, that activity is not repeated.

As an application we turn to network security protocol analysis and demonstrate that when an adversary has enough storage capacity, then many known protocol anomalies can also occur in the presence of a bounded memory intruder. We believe that precisely this is a theoretical reason for the successful use in the past years of model checkers in security protocol verification. In particular, the known anomalies arise for bounded memory protocols, where there is only a bounded number of concurrent sessions and the honest participants of the protocol cannot generate an unbounded number of facts nor an unbounded number of fresh values. This led us to the question of whether it is possible to infer an upper-bound on the memory required by the adversary to carry out an anomaly from the memory restrictions of the bounded protocol. We answer this question negatively. This is joint work with Max Kanovich, Tajana Ban Kirigin, and Vivek Nigam.