

# Discrete-Event Control to Keep Secrets Secret

Karen Rudie

Department of Electrical and Computer Engineering  
Queen's University

We show how systems that can be characterized by sequences of events can be modelled using finite automata, which are comparable to directed graphs. In this modeling paradigm, called *discrete-event systems*, we can disable or enable events as the system evolves to ensure that the controlled system has some properties. Traditionally, control has been used to ensure that the controlled system does not contain any sequences of events that are considered illegal. More recently, researchers have been interested in whether systems possess a property called *opacity*. A system satisfies opacity, or is *opaque*, if sequences of events that are considered secret (or that lead to a state that is considered secret) cannot be distinguished from non-secret event sequences (or non-secret states). We discuss recent work in which control is used ensure that a system is opaque to an adversary. This work has application in network security and in distributed systems in which autonomous agents may communicate to achieve some task but where it is desired that the communications are judiciously chosen so that secret information is not discernible to a hostile agent.

---