# Towards Timed Models for Cyber-Physical Security Protocols

Max Kanovich[*], Tajana Ban Kirigin[†], Vivek Nigam[‡], Andre Scedrov[§] and Carolyn Talcott[¶]
[*] Queen Mary, University of London, UK, Email: mik@dcs.qmul.ac.uk
[*] University College London, UCL-CS, UK, Email: m.kanovich@ucl.ac.uk
[†] University of Rijeka, HR, Email: bank@math.uniri.hr
[‡] Federal University of Paraíba, Brazil, Email: vivek.nigam@gmail.com
[§]University of Pennsylvania, USA, Email: scedrov@math.upenn.edu
[¶]SRI International, USA, Email: clt@csl.sri.com

***Abstract*—Many security protocols rely on the assumptions on the physical properties in which its protocol sessions will be carried out. For instance, Distance Bounding Protocols take into account the round trip time of messages and the transmission velocity to infer an upper bound of the distance between two agents. We classify such security protocols as cyber-physical. The key elements of such protocols are the use of cryptographic keys, nonces and time. This paper investigates timed models for the verification of such protocols. Firstly, we introduce a multiset rewriting framework with continuous time and fresh values. We demonstrate that in this framework one can specify distance bounding protocols and intruder models for cyber-physical security protocols that take into account the physical properties of the environment. We then investigate how the models with continuous time relate to models with discrete time in protocol verification and show that there is a difference between these models in exposing security flaws. This is done by proposing a protocol and demonstrating that there is no attack to this protocol when using the model with discrete time, but there is an attack when using the model with continuous time. For the important class of Bounded Memory Cyber-Physical Security Protocols with a Memory Bounded Intruder the reachability problem is PSPACE-complete if the size of terms is bounded.**