August 4, 2020

BLOC: A Game-Theoretic Approach to Orchestrate CPS with Check Blocks against Cyber Attacks

Cybersecurity Lecture Series

Mina Guirguis is a Professor of Computer Science at Texas State University.

Link to more information/paper.

Cyber-Physical Systems (CPS) will be core to most emerging computing systems. A myriad of activities in our lives will rely on the correct operation of these systems, from transportation and energy domains, to manufacturing and healthcare. Securing CPS against cyber-attacks, however, is challenging due to the wide range of possible attacks — from stealthy ones that seek to manipulate control and measurement signals to malware that infects host machines that control the physical process. This has prompted the research community to develop targeted methods that protect and check the run-time operation of the CPS. Since protecting signals and checking for errors result in performance penalties, they must be performed within the delay bounds dictated by the control loop. Due to the large number of potential checks that can be performed, coupled with various degrees of their effectiveness to detect a wide range of attacks, strategic assignment of these checks in the control loop is a critical endeavor. In this talk, I will present a coherent runtime framework — which we coin BLOC — for orchestrating the CPS with check blocks to secure them against cyber-attacks. BLOC capitalizes on game theoretical techniques to enable the defender to find an optimal randomized use of check blocks to secure the CPS while abiding to the control-loop delay constraints. In the first

part of the talk, I will present a Stackelberg game model for stateless blocks and a Markov game model for stateful ones and derive optimal policies that minimize the worst-case damage from rational adversaries. In the second part of the talk, I will present a Deep Reinforcement Learning framework that solves for optimal/sub-optimal assignments of check blocks against the explosion in the size of the state/action spaces. I will present results obtained from extensive simulations as well as real instantiations of CPS.