Seminar Series

Integrated Security, Performance, and Control of Networked Cyber-Physical Systems

Andrew Clark

Ph.D. Candidate, Network Security Lab, Department of Electrical Engineering
University of Washington - Seattle

Abstract

Cyber-physical systems (CPS) consist of physical systems tightly integrated with networked cyber devices in applications including energy, transportation, health, and manufacturing. Preventing attacks on CPS while preserving characteristics such as availability, robustness, and safety requires an integrated, scientific approach at the intersection of security, control, and networking. In this talk, I will describe such an approach for two areas of CPS control and security. First, I will consider the problem of selecting a set of leader nodes to steer a networked CPS towards a desired operating point. The choice of leader nodes impacts design metrics, such as robustness to environmental and adversarial noise, convergence rate of the dynamics, and controllability. I show that these metrics have a common mathematical structure that enables efficient leader selection with provable optimality, and describe connections to related problems in biological networks. Second, I will consider modeling and design of deception and moving target cyber defenses, which prevent an adversary from gathering information of the targeted system and hence reduce the effectiveness of attacks. I will present a control-theoretic methodology for achieving a desired trade-off between the security of the system and the performance, as measured by service disruptions to real users.

Biography of Speaker

Andrew Clark is currently a Ph.D. candidate in the Network Security Lab, Department of Electrical Engineering, at the University of Washington - Seattle. He received the BS degree in Electrical Engineering and the MS degree in Mathematics from the University of Michigan - Ann Arbor in 2007 and 2008, respectively. His research interests include performance and security of cyber-physical systems, modeling and design of adaptive and proactive network defenses, lightweight cryptography, and vulnerability metrics. He was co-author of the IEEE/IFIP William C. Carter award paper (2010) and the WiOpt Best Paper (2012), and was a finalist for the IEEE CDC 2012 Best Student Paper Award. He holds a patent on privacy-preserving constant time identification in RFID systems.