CoCo Seminar Series
Fall 2019

Topology Switching for Secure Networked Control Systems

Yanbing Mao
PhD candidate, Electrical and Computer Engineering, Binghamton University

Wednesday September 18, 2019 11:00am-12:00pm
Engineering Building T-1 (Multipurpose Room)

Security concerns regarding the networked systems, see e.g., power networks and social networks, pose a formidable threat to their wide deployment. The ``networked" aspect exacerbates the difficulty of securing these multi-agent systems since centralized measurement (sensing) and control are not feasible, and hence require the development of decentralized approaches, which are inherently prone to attacks. Particularly, a special class of ``stealthy" attacks, namely the ``zero-dynamics attack" (ZDA), poses a significant security challenge. The main idea behind ZDA is to hide the attack signal in the null-space of the state-space representation of the control system so that it cannot be detected by applying conventional detection methods on the observation signal (hence, the name "stealthy"). In this talk, I will first present our proposed defense strategy of strategic topology switching that relies on a naive attacker to detect ZDA. Lately, I will present the realistic ZDA variations where the attacker is aware of this topology-switching strategy, and hence employs the following policies to avoid detection: (i) ``pause (update and resume) attack" before (after) topology switching to evade detection; (ii) cooperate with a concurrent stealthy topology attack that alters network topology at switching times, such that the original ZDA is feasible under the corrupted topology. We systematically study the proposed ZDA variations, and then develop defense strategies against them under the realistic assumption that the defender has no knowledge of attack starting, pausing, and resuming times and the number of misbehaving agents. Particularly, we characterize conditions for detectability of the proposed ZDA variations, in terms of the network topologies to be maintained, the set of agents to be monitored, and the measurements of the monitored agents that should be extracted, while simultaneously preserving the privacy of the states of the non-monitored agents. Finally, I will talk about the attack detection algorithm based on the Luenberger observer, using the characterized detectability conditions.

Yanbing Mao received the M.E. degree in Circuits & Systems from University of Electronic Science and Technology of China, Sichuan, China, in 2013. He is currently pursuing the Ph.D. degree at Binghamton University–-SUNY, NY, USA. His research interests include security and privacy of networked cyber-physical systems and (mis)-information spread in social networks. http://coco.binghamton.edu/