Computer Science Seminar

A Scheduling Formulation for a Cybersecurity Game with Applications in Adaptive Machine Learning

Nourhan Sakr-Ph.D. Student at Data Science Institute at Columbia University

November 12, 2018
10:00 - 10:50 am
209 Computer Science Building



National security and economy highly depend on the safe and secure operation of a wide range of networked computing and control systems. We need reliable security techniques to protect systems subject to attacks by intelligent, adaptable and well-resourced adversaries. Moving Target Defenses (MTD) is one category of mitigations that use diversity, randomization, and change to make exploiting vulnerabilities more costly for an adversary without having to find and remove all flaws from a system. The motivation behind PLADD (Probabilistic Learning Attacker, Dynamic Defender) is to study the essential characteristics of MTD strategies in cyber systems via a high-level gametheoretical model. Our optimization-based analysis attacks the challenge of modeling and analyzing the dynamics of when a learning model should be adjusted in a non-stationary interactive environment. Using stochastic programming, we express PLADD in the language of scheduling theory, yet in an unconventional way. We analyze theoretical aspects and prove NP-hardness and are currently developing approximation algorithms. Introducing this rather unconventional scheduling problem is not only promising for purposes of analyzing PLADD and thus MTD value, but also pioneering as it proposes a novel class of scheduling problems. Another interpretation fits PLADD to machine learning (ML) algorithms with unique build and adaptation costs. We provide insights into learning the strategies of an adaptive ML algorithm and guide its optimization. We apply PLADD to real classification data from Sandia, emphasizing how a scheduling formulation may be used to serve ML problems.

Bio: Nouri is a Ph.D. student at Columbia University working under the supervision of Cliff Stein at the Data Science Institute. Her research lies at the intersection of data science, combinatorial optimization and algorithms where she leverages connections between the three fields to (re-)design data-driven algorithms that efficiently solve fundamental and real-world social or industrial challenges. Additionally, she seeks real-data to confirm the theory she develops in her work and drive the design of her algorithms.

Nouri accumulated industrial experience via her collaborations and internships at places like Google, Amazon, Microsoft, Sandia National Labs, and Graham Windham, where she addresses problems like adaptive ML in cyber security, dynamic inventory allocation, foster care matching, etc.Prior to joining Columbia, she received her double degree in Computer Science and Actuarial Science from the American University in Cairo and her Masters in Actuarial Science from the University of Waterloo in Canada.

MISSOURI S&T