ELECTRICAL & COMPUTER ENGINEERING

Systems and Control Seminar

A Stochastic Control Approach to Dynamic Defense of Large-Scale Cyber Networks

Erik Miehling

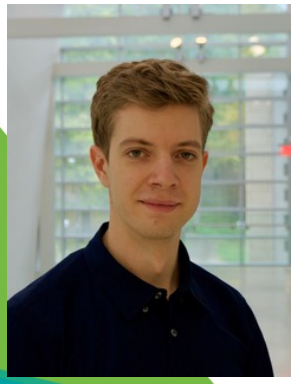
Electrical and Computer Engineering
University of Michigan at Ann Arbor

November 2, 2017, 2pm-3pm, ECE 118

ABSTRACT

The ubiquity of security breaches in modern times necessitates the development of systems that are able to automatically detect and react to attacks, with the goal of preventing the attacker from reaching its goal. In this talk, I will present a stochastic control approach to the design of a such a system. The model is built upon the notion of a dependency graph which describes how the attacker can use its current set of capabilities to perform exploits and gain further capabilities. The defender does not perfectly observe the capabilities of the attacker at any given time and must infer them from noisy security alerts (generated by an intrusion detection system). The resulting problem of choosing defense actions that strike a trade-off between mitigation of the attacker's progression and minimization of the negative impact to availability is formulated as a partially observable Markov decision process (POMDP). Unfortunately, due to the scale of the defense problem, obtaining an optimal solution is computationally intractable. As a result, we make of use an online solution method, termed the partially observable Monte-Carlo planning (POMCP) algorithm. The algorithm samples future possible scenarios from the current belief in order to select actions, avoiding the state-space explosion problem.

SPEAKER BIOGRAPHY



Erik Miehling is currently a PhD Candidate in the Electrical and Computer Engineering department at the University of Michigan where he works with Demosthenis Teneketzis. Previously, he received a B.A.Sc. and M.A.Sc., both in Electrical and Computer Engineering, from the University of British Columbia in Vancouver, Canada. He has contributed to a diverse set of fields including radar resource management, power systems and markets, and cyber security. His research interests lie in the theory of stochastic control, optimization, graphs, and microeconomics, with a focus on applying these tools to dynamic problems over networked systems under imperfect information.

EMPOWER.CONNECT.ENGINEER.