Computer Science Seminar

Artificial Intelligence Approaches for Wickedly Hard National Security Problems

Dr. Daniel Tauritz, Missouri S&T

January 28, 2019
10:00 - 10:50 am
209 Computer Science Building

Many national security problems are wickedly hard in that they map to computational problem classes which are intractable. This seminar aims to illuminate how artificial intelligence approaches can be created to address these problems and produce useful solutions. In particular, two promising approaches will be discussed, namely (I) computational game theory employing coevolutionary algorithms for identifying high-consequence adversarial strategies and corresponding defense strategies, and (II) hyper-heuristics employing evolutionary computation for the automated design of algorithms tailored for high-performance on targeted problem classes.

The first approach will be illustrated with the Coevolving Attacker and Defender Strategies for Large Infrastructure Networks (CEADS-LIN) project funded by Los Alamos National Laboratory (LANL) via the LANL/S&T Cyber Security Sciences Institute (CSSI) [https://web.mst.edu/~tauritzd/CSSI/]. This project focuses on coevolving attacker & defender strategies for enterprise computer networks. A proof of concept for operationalizing cyber security R&D from this project demonstrated in simulation that coevolution is capable of implementing a computational game theory solution for adversarial models of network security. Currently a high-fidelity emulation framework with intelligent attacker and defender agents is being developed with as end goal to provide a fully automated solution for identifying high-impact attacks and corresponding defenses.

The second approach will be illustrated with the Scalable Automated Tailoring of SAT Solvers project funded by Sandia National Laboratories with supplemental funding from the Computer Research Association's Committee on the Status of Women in Computing Research (CRA-W), and with the Network Algorithm Generating Application (NAGA) project funded via CSSI. These projects show how hyper-heuristics can be employed to create algorithms targeting arbitrary but specific problem classes for repeated problem solving where high a priori computation costs can be amortized over many problem class instances.

Bio: Dr. Daniel Tauritz is an Associate Professor & Associate Chair in the Department of Computer Science at the Missouri University of Science and Technology (S&T), a University Contract Scientist for Sandia National Laboratories, a University Collaboration Scientist at Los Alamos National Laboratory (LANL), the founding director of S&T's Natural Computation Laboratory, and founding academic director of the LANL/S&T Cyber Security Sciences Institute. He received his Ph.D. in 2002 from Leiden University for Adaptive Information Filtering employing a novel type of evolutionary algorithm. His research interests focus on artificial intelligence approaches to complex real-world problem solving with an emphasis on national security problems in areas such as cyber security, cyber physical systems, critical infrastructure protection, and program understanding. He was granted a US patent for an artificially intelligent rule-based system to assist teams in becoming more effective by improving the communication process between team members.

MISSOURI S&T