Air Force Office of Scientific Research

Windows on Science

Hosting faculty and students from the Universidad de los Andes and UC Santa Cruz

Located at the Griffiss Institute – Executive Board Room

Agenda for Tuesday 23 June, 2019

9:00AM – Introductions and equipment setup

9:30AM – "Dynamic Data and Information Processing – Introduction and Welcome" – Dr. Erik Blasch, Air Force Office of Scientific Research

10:00AM – "DDDAS Anomaly Detection and Response for Autonomous Systems" – Dr. lvaro A. Cardenas, Associate Professor, UC Santa Cruz

The talks will focus on how to leverage the DDDAS paradigm for attack detection and attack response in autonomous systems. We will show our results on applying these concepts to control systems, and our ongoing work for attack detection and response in autonomous vehicles, UAVs, and multi-agent systems. In more detail, attack detection, isolation and reconfiguration are necessary to maintain a control system safe, even in the presence of attacks. In this work, we exploit some tools from fault-tolerant control systems and analyze them under a security framework leveraging the insights from Dynamic Data Driven Applications Systems (DDDAS). In particular, we propose DDDAS Anomaly Isolation and Response (DDDAS-AIR), an architecture for secure autonomous systems that relies on virtual sensors to help us reconfigure the sensors in order to mitigate the impact of the attack.

11:00 AM – "Dynamic Data Integration for Resilience to Sensor Attacks in Multi-agent Systems" – Mr. Luis Burbano. MS Student, Universidad de los Andes

This talk shows how to apply the DDDAS paradigm to attack detection and response in autonomous robotic systems.

12:00PM – Lunch break

2:00PM – "Mitigating Attacks on Industrial Control Systems" - Mr. Luis Francisco Combita, PhD Student, Universidad de los Andes

This talk is about the design and implementation of a mechanism that helps to mitigate sensor attacks on industrial control systems. The proposed architecture uses analytical redundancy, i.e., additional data about the system operation is obtained from a dynamical model of the system. The information obtained from the model is compared with the information from the system sensors, using a mechanism which is based on the simultaneous use of a Kalman filter and a set of optimal disturbances decoupling observers. Results show the effectiveness of the presented mechanism to mitigate attacks on industrial control systems. This mechanism is evaluated on two

typical testbeds the three and the four tanks systems. Finally, some conclusions and ideas for future work are given.

2:30 PM – "Leveraging Software-Defined Networking for Data-Driven Reconfiguration of Control Systems to Survive Attacks" – Dr. Sandra Rueda, Associate Professor, Universidad de los Andes

Most of the literature on cyber-physical systems security focuses on attack prevention and detection, however, there is very little work on how to automatically respond to detected attacks; most responses are manual or are hardwired with a fixed response that cannot be dynamically configured. In this presentation we show how software-defined networks (SDNs) and network function virtualization (NFV) technologies can help us in implementing DDDAS-inspired attack response systems.

3:00 PM – "Human-Allied Artificial Intelligence for Learning to Act in Complex Stochastic Environments" – Dr. Sriraam Natarajan, Associate Professor. UT Dallas

Statistical Relational AI (StaRAI) Models combine the powerful formalisms of probability theory and first-order logic to handle uncertainty in large, complex problems. While they provide a very effective representation paradigm due to their succinctness and parameter sharing, efficient learning is a significant problem in these models. Using these StaRAI models as the fundamental building blocks, I will present a layered approach for learning in complex dynamic environments: starting with entity resolution, then proceeding to relation extraction, then performing temporal event modeling and finally learning to act. In each of these layers, I will demonstrate how to effectively leverage domain expertise for learning efficient models. The ideas combine probabilistic models, relational models, graph theory, deep networks and reinforcement learning methods to achieve the broader goal of Human-Allied AI.

Location and Teleconference Information

Meeting Location

Griffiss institute
Executive Board Room
725 Daedalian Dr.
Rome, NY 13441
https://www.griffissinstitute.org/

Teleconference Line

For Tuesday 23 June

Dial-in Number: (712) 451-0011
Access Code: 411884