SimCenter Center of Excellence in Applied Computational Science and Engineering

presents

"Safety and Security Assurance in Autonomous Cyber-Physical Systems with Hyperproperties & Hybrid Automata"

Speaker:

Dr. Taylor Johnson

Vanderbilt University

October 19th, 2 p.m., UTC SimCenter Auditorium*

Networking | Light Refreshments | Seminar | Q & A

Public Invited

The ongoing renaissance in artificial intelligence (AI) has led to the advent of machine learning methods deployed within components for sensing, actuation, and control in safety-critical cyber-physical systems (CPS), and is enabling autonomy in such systems, such as autonomous vehicles and swarm robots. However, as demonstrated in part through recent accidents in semi-autonomous/autonomous CPS and by adversarial machine learning, ensuring such components operate reliably in all scenarios is extraordinarily challenging. We will define and discuss specifying desired behaviors (e.g., for safety, security, robustness, and stability) using hyperproperties, which are sets of properties, where properties are classically defined in formal methods as sets of traces, so hyperproperties are sets of sets of traces and are effective in describing security specifications, such as noninterference. In recent work, we have developed a real-time, real-valued temporal logic called hyperproperties for signal temporal logic (HyperSTL), which is useful for describing behaviors in autonomous CPS. We will discuss methods to falsify hyperproperties (i.e., to find sets of traces violating a hyperproperty) assuming only black-box models are available, as well as methods to formally verify hyperproperties (i.e., to establish all sets of traces satisfy a hyperproperty) when formal models, such as hybrid automata, are available. We will discuss the application of these approaches in several CPS, such as motor vehicles and swarm robots. We will conclude with some architectural solutions that enhance trust and safety assurance in autonomous CPS, building on supervisory control with the Simplex architecture, and will discuss future research directions for enhancing trust of machine learning components within CPS that we are exploring within recently started DARPA Assured Autonomy and NSA/DoD Science of Security Lablet projects.

Dr. Taylor T. Johnson is an Assistant Professor of Computer Engineering (CmpE), Computer Science (CS), and Electrical Engineering (EE) in the Department of Electrical Engineering and Computer Science (EECS) in the School of Engineering (VUSE) at Vanderbilt University (since August 2016), where he directs the Verification and Validation for Intelligent and Trustworthy Autonomy Laboratory (VeriVITAL) and is a Senior Research Scientist in the Institute for Software Integrated Systems (ISIS). Dr. Johnson serves as the President of a medical information technology startup firm, CelerFama, Inc., and as the Chief Technology Officer (CTO) of Verivital, LLC, both of which serve for technology transfer and commercialization of his research group's results to industry. Dr. Johnson was previously an Assistant Professor of Computer Science and Engineering (CSE) at the University of Texas at Arlington (September 2013 to August 2016). Dr. Johnson earned a PhD in Electrical and Computer Engineering (ECE) from the University of Illinois at Urbana-Champaign in 2013, where he worked in the Coordinated Science Laboratory with Prof. Sayan Mitra, and earlier earned an MSc in ECE at Illinois in 2010 and a BSEE from Rice University in 2008. Dr. Johnson has published over 70 papers on formal methods and their applications across cyber-physical systems (CPS) domains, such as power and energy, aerospace, automotive, transportation, biotechnology, and robotics, two of which were recognized with best paper awards, from the IEEE and IFIP, respectively, and one of which was awarded an ACM Best Software Repeatability Award. Dr. Johnson is a 2018 and 2016 recipient of the AFOSR Young Investigator Program (YIP) award, a 2015 recipient of the National Science Foundation (NSF) Computer and Information Science and Engineering (CISE) Research Initiation Initiative (CRII), and his research is / has been supported by AFOSR, ARO, AFRL, DARPA, NSA, NSF, the MathWorks, NVIDIA, ONR, Toyota, and USDOT. Dr. Johnson is a member of AAAS, ACM, AIAA, IEEE, and SAE, and is a TN Professional Engineer Intern (EiT).

**UTC SimCenter, Auditorium, 701 E. M.L. King Blvd., Chattanooga TN, 37403*

THE UNIVERSITY OF TENNESSEE
CHATTANOOGA