TEXAS TECH UNIVERSITY
Edward E. Whitacre Jr.
College of Engineering™
Computer Science

**"Robustness of Neural Networks to Parameter Quantization"**

Ariful Islam, Ph.D.
Tuesday, September 24, 2019at 3:30 p.m.
Electrical and Computer Engineering, Room 101

**Abstract**
Quantization, a commonly used technique to reduce the memory footprint of a neural network for edge computing, entails reducing the precision of the floating-point representation used for the parameters of the network. The impact of such rounding-off errors on the overall performance of the neural network is estimated using testing, which is not exhaustive and thus cannot be used to guarantee the safety of the model. In this talk, I will present a framework based on Satisfiability Modulo Theory (SMT) solvers to quantify the robustness of neural networks to parameter perturbation. To this end, I will introduce notions of local and global robustness that capture the deviation in the confidence of class assignments due to parameter quantization.
The robustness notions are then cast as instances of SMT problems and solved automatically using solvers, such as dReal. I will demonstrate this framework on simple Multi-Layer Perceptrons (MLP) that perform binary classification. In addition to quantifying the robustness, I will also show that Rectified Linear Unit activation results in higher robustness than linear activations for our MLPs.

**Bio**
Md Ariful Islam is an assistant professor in the department of computer science at Texas Tech University since 2018. Before joining at Tech, he was a postdoctoral fellow in the department of Computer Science at Carnegie Mellon University. His research interest lies in the intersection of Cyber-Physical Systems (CPSs), such as medical devices and autonomous vehicles, formal methods, and control theory. Specifically, he is working on developing tools and techniques for the verification and control of CPSs by leveraging techniques from formal methods and control theory. His research has been published in numerous reputed journals and conferences, including Nonlinear Analysis: Hybrid Systems (NAHS), Theoretical Computer Science (TCS), Decision and Control (CDC), Computer Aided Verification (CAV), Hybrid Systems: Computation and Control (HSCC) and so on. He earned his PhD from the department of Computer Science at Stony Brook University in 2015. He completed his bachelor's degree in computer science and Engineering from Bangladesh University of Engineering and Technology.