The advances in wireless technologies have led to autonomous deployments of various wireless networks. As these networks must co-exist, it is important that all transmitters and receivers are aware of their radio frequency (RF) surroundings so that they can learn and adapt their transmission and reception parameters to best suit their needs. To this end, machine learning techniques have become popular as they can learn, analyze and even predict the RF signals and associated parameters that characterize the RF environment.

In this dissertation, we address some of the fundamental challenges on how to effectively apply different learning techniques in the RF domain. In the presence of adversaries, malicious activities such as jamming, and spoofing are inevitable which render most machine learning techniques ineffective. To facilitate learning in such settings, we propose an adversarial learning-based approach to detect unauthorized exploitation of RF spectrum. First, we show the applicability of existing machine learning algorithms in the RF domain. We design and implement three recurrent neural networks using different types of cell models for fingerprinting RF transmitters. Next, we focus on securing transmissions on dynamic spectrum access network where primary user emulation (PUE) attacks can pose a significant threat. We present a generative adversarial net (GAN) based solution to counter such PUE attacks. Ultimately, we propose recurrent neural network models which are able to accurately predict the primary users' activities in DSA networks so that the secondary users can opportunistically access the shared spectrum. We implement the proposed learning models on testbeds consisting of Universal Software Radio Peripherals (USRPs) working as Software Defined Radios (SDRs). Results reveal significant accuracy gains in accurately characterizing RF transmitters- thereby demonstrating the potential of our models for real world deployments.

Major: Computer Science

Educational Career:
Bachelor's of Information Technology, BS, 2009, Indian Institute of Engineering Science and Technology, Shibpur, India
Master's of Information Technology, MS, 2011, Indian Institute of Engineering Science and Technology, Shibpur, India
Master's of Computer Science, MS, 2018, University of Central Florida, Orlando, FL, USA

Committee in Charge:
Mainak Chatterjee, Chair, Computer Science
Nazanin Rahnavard, Computer Science
Cliff Zou, Computer Science
Qipeng Phil Zheng, Industrial Engineering & Management Systems

Approved for distribution by Mainak Chatterjee, Committee Chair, on September 25, 2019.

The public is welcome to attend.