Notice and Invitation
Oral Defense of Doctoral Dissertation
The Volgenau School of Engineering, George Mason University

Monireh Dabaghchian
Bachelor of Science, University of Tabriz, 2006
Master of Science, University of Tabriz, 2009

Security and Intelligence Measure in Online Machine Learning-based Dynamic Spectrum Sharing Networks

Monday, July 1, 2019, 10:00 am
ENGR 3507
All are invited to attend.

Committee
Dr. Kai Zeng, Chair
Dr. Zhi Tian
Dr. Brian Mark
Dr. Jie Xu

Abstract
Cognitive radio (CR) is considered as a key enabling technology for dynamic spectrum access to improve spectrum efficiency. This dissertation studies the two aspects of spectrum sharing networks: Security and intelligence capabilities. In the first part, we consider a primary user emulation (PUE) attacker that can send falsified primary user signals and prevent the secondary user from utilizing the available channel. The best attacking strategies that an attacker can apply have not been well studied. In this thesis, for the first time, we study optimal PUE attack strategies by formulating an online learning problem where the attacker needs to dynamically decide the attacking channel in each time slot based on its attacking experience. We propose online learning-based attacking strategies based on the attacker's observation capabilities. Through our analysis, we show that with no observation within the attacking slot, the attacker loses on the regret order, and with the observation of at least one channel, there is a significant improvement on the attacking performance. Observation of multiple channels does not give additional benefit to the attacker (only a constant scaling) though it gives insight on the number of observations required to achieve the minimum constant factor. Our proposed algorithms are optimal. In the second part of the dissertation, we study the intelligence capabilities of Cognitive radios. Although the CR concept was invented with the core idea of realizing "cognition", the research on measuring CR cognition capabilities and intelligence is largely open. Deriving the intelligence capabilities of CR not only can lead to the development of new CR technologies, but also makes it possible to better configure the networks by integrating CRs with different intelligence capabilities in a more cost-efficient way. In this work, for the first time, we propose a data-driven methodology to quantitatively analyze the intelligence factors of the CR with learning capabilities. We present a case study consisting of sixty-three different types of CRs. Based on our methodology, we analyze the intelligence capabilities of the CRs through extensive simulations. Four intelligence capabilities are identified for the CRs through our analysis, which comply with the nature of the tested algorithms.