UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD.CSCI Seminar

Monday November 16 2020 at 1:00PM on Teams (To view please email hassan.khan@uoguelph.ca)

Resisting Adversarial Attacks on AI-Based Network Traffic Classification Systems

Dennis Xu

Advisor: Dr. Hassan Khan
Co-Advisor: Radu Muresan (Engineering)
Advisory Committee: Dr. Andrew Hamilton-Wright
Advisory Committee: Dr. Xiaodong Lin

ABSTRACT:

With the increased Internet connectivity and the adoption of network-based services, there has been an explosive growth in the amount of network traffic that is generated. This increased traffic requires traffic classification in many use cases including network traffic shaping, malware classification, and censoring illegitimate content. Accurate traffic classification is crucial for these systems to work properly but adversarial attackers find new ways to mislead traffic classification systems. Although traditional AI-based systems are effective in aforementioned use cases, they may not operate against sophisticated adversarial attacks. Adversarial attackers are well aware of the defense systems in place and can evade them in many ways. It is important for researchers and vendors of such systems to assess how their systems behave against adversarial attacks. My research aims to build tools and techniques that assists researchers and vendors of AI-systems to build systems that are able to resist adversarial attacks.