NJIT

Department of Computer Science

Machine Learning Enhanced Network Security

Michael J. DeLucia
U.S. Army Research Laboratory

Hosted by Cong Shi

Date: Thursday, February 9, 2023
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
WebEx Link: https://njit.webex.com/njit/j.php?MTID=mcbfa1defcd74ab07ee10f98fc0fd754c

http://cs.njit.edu/seminars

Abstract:
Increasingly cyber-attacks are sophisticated and occur rapidly, necessitating the use of machine learning techniques for detection at machine speed. However, the use of traditional machine learning techniques in cyber security requires subject matter expertise (i.e., network analysts) to extract relevant and distinctive features from the raw network traffic. Thus, we propose a novel machine learning algorithm for malicious network traffic detection using only the bytes of the raw network traffic. We also propose a transfer learning architecture to enable training and inference, respectively in a source and target network environment.

Furthermore, the use of machine learning within network detection, necessitates an understanding of an increased attack surface (i.e. adversarial machine learning). Accordingly, we depict the subtle distinctions of adversarial machine learning from a network detection point of view. Additionally, we present our contribution towards an initial defense for network detection classifiers against adversarial machine learning.

Bio:
Dr. Michael DeLucia is a computer scientist at the U.S. Army Research Laboratory (ARL). He graduated from the University of Delaware with a Ph.D. in Electrical and Computer Engineering focusing on research in machine learning detection of encrypted malicious activities and innovating Adversarial Machine Learning (AML) attacks and defenses within a network security context. He currently, leads research at the intersection of machine learning and network security. Dr. DeLucia has over 16 years of experience working in cyber security within the U.S. Department of the Army and graduated with a Bachelor's in Information Technology and Master's in Computer Science from the New Jersey Institute of Technology. Additionally, Dr. DeLucia teaches a special topics course in network security applied machine learning at the University of Delaware.