samsi
NSF·Duke·NCSU·UNC

GDRR Program Opening Workshop
August 5-9, 2019

SPEAKER TITLES/ABSTRACT

Bowei Xi
Purdue University

“A Game Theoretic Approach for Adversarial Machine Learning â€” When Big Data Meets Cybersecurity”

Nowadays more and more data are gathered for detecting and preventing cyber attacks. Unique to the cybersecurity applications, learning models face active adversaries that try to deceive learning models and avoid being detected. The existence of such malicious adversaries motivates the development of robust learning techniques. Game theory offers a suitable framework to model the conflict between the adversaries and the defender. We develop a game theoretic framework to model the sequential actions of the adversaries and the defender, allowing players to maximize their own utilities. For supervised learning tasks, our adversarial support vector machine has a conservative decision boundary, whereas our robust deep neural network plays a random strategy inspired by the mixed equilibrium strategy. On the other hand, in real practice, labeling the data instances often requires costly and time consuming human expertise and becomes a significant bottleneck. Our novel grid based adversarial clustering algorithm is able to identify the high confidence normal regions and the overlapping areas inside a mixed cluster, and identify outliers which may be potential anomalies.