VirginiaTech
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
1872

Computer Science Seminar Series, 2014
National Capital Region

Cyber-Security Using Statistical Learning

Speaker: Prof. Harry Wechsler

George Mason University
Friday, March 21, 2014
1:00PM- 2:00PM, NVC 325

Abstract

The challenges addressed are related to developing and deploying robust cyber-security applications that can operate under adversarial conditions, e.g., uncontrolled settings (for the purpose of interoperability) and incomplete / masquerading information (to cope with denial and deception). Examples of such applications include spam, phishing, and fraud detection; covert time channels (CTC); deliberate poor annotation for training; and active authentication and continuous re-authentication to counter identity theft and insider threats / exfiltration faced by information and control systems. Similar to biometrics, we seek for cognitive footprints that integrate appearance, behavior, and emotional and cognitive / intent state, all aware of and driven by context.

The methods discussed are characteristic of statistical learning and link analysis, in general, and adversarial and consensus learning, collective classification, and (filter-type and collaborative) recommender systems, in particular. Novel solutions, which merge all encompassing (appearance, behavior, and state) biometrics, probabilistic natural language processing (NLP) / Conditional Random Fields (CRF) and Latent Dirichlet Allocation (LDA)/, are proposed. The ultimate challenge is that of autonomic computing, which is characterized by SELF healing, configuration, protection, and optimization.

Biography

Harry Wechsler is a Professor in the Department of Computer Science at George Mason University. His research area is active authentication, adversarial and consensus learning, biometrics, change and anomaly detection, cyber security (spam, fraud, and phishing detection), data fusion, identity management, interoperability, performance evaluation, and re-identification. He authored 3 books, published over 300 scientific papers, and has 7 patents (together with his doctoral students). He is a Fellow of IEEE and IAPR (Int. Assoc. for Pattern Recognition). More information about the speaker can be found at: **http://cs.gmu.edu/~wechsler/biosketch-wechsler.pdf**