VirginiaTech
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series, 2013

National Capital Region

Bayesian Nonparametric Learning for Network Security

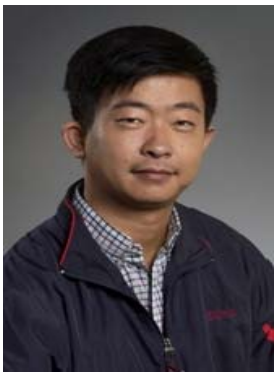
Speaker: Prof. Zhu Han
University of Houston

Tuesday, March 5, 2013
1:00PM- 2:00PM, NVC T3

Abstract

An insider attack is a notoriously difficult problem in security, since the adversaries possess valid keying materials and thus can easily pass the crypto-based security checks. Classification of device finger prints is to supplement the traditional crypto-based solutions with unique, unforgeable, and robust credentials extracted from the inherent properties of network nodes; hence effectively countering the insider attack. The classification technique based on Bayesian inference is an important and popular topic of machine learning. Classical classification methods normally assume the number of classes is known, leading to difficulties in model selecting. The methods can be easily under fitting or over fitting. Bayesian nonparametric learning/classification, on the other hand, does not assume any prior knowledge on the number of classes or hidden processes. Instead, the number of classes is assumed to be infinite and only a limited number of classes are observed. As more data are observed, the number of classes can vary. This advanced property, based on the Infinite Gaussian Mixture Model, overcomes the difficulties in the model selection task in classical approaches, and approaches several performance bounds. Three possible security applications will also be described: Masquerade attack, Sybil attack, and Primary User Emulation attack in cognitive radio networks. The algorithm is also implemented in a GNU Radio USRP2 prototype. Finally, this Bayesian nonparametric learning can be employed to other scenarios such as social networks and smart grid networks. The theoretical extension is also elaborated.

Biography



Zhu Han received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, in 1999 and 2003, respectively. From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an assistant professor in Boise State University, Idaho. Currently, he is an associate Professor in Electrical and Computer Engineering Department at University of Houston, Texas. His research interests include security, wireless resource allocation and management, wireless communications and networking, game theory, and wireless multimedia. Dr. Han is an NSF CAREER award recipient 2010, together with another 5 NSF award, 1 DOD award, and 3 other awards since joining University of Houston 2008. Dr. Han has 6 conference best paper awards (IEEE ICC09, Wiopt 09, WCSP 12, two IEEE WCNC 12, and IEEE Smartgridcom 12), and winner of IEEE Fred W. Ellersick Prize 2011.