THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

Research Seminar

Towards Adversarial Robustness of Graphical Models

Dr Kai Zhou
Postdoctoral Research Associate
Department of Computer Science and Engineering
Washington University in St. Louis
USA

Date : 21 January 2020 (Tuesday)
Time : 11:15 a.m. - 12:15 p.m.
Venue : Room PQ703, 7/Floor, Core P, Mong Man Wai Building, The Hong Kong Polytechnic University

▶ Abstract

Data in various domains are naturally represented as graphs, with nodes representing objects and edges indicating relations among them. Sophisticated intelligent systems (or graphical models) are designed to extract valuable knowledge from graph data. In the real world, however, structural attacks that modify the input graph structure can fool the graphical models and make the extracted knowledge undependable. In this talk, I will introduce state-of-the-art attacks and defenses on graphical models through three instances in different application domains: social network analysis, collective classification, and graph representation learning. Specifically, I will talk about several approaches, such as game-theoretical modeling, robust optimization, and randomized smoothing, to achieve adversarial robustness of graphical models.

▶ About the Speaker

Dr Kai Zhou is currently a postdoctoral research associate in the Department of Computer Science and Engineering at Washington University in St. Louis. He obtained a B.S. from Shanghai Jiao Tong University in 2013, and a Ph.D. in the Department of Electrical and Computer Engineering at Michigan State University in 2018. His research interest centers around data security and privacy in a broad spectrum of application domains, such as mobile cloud computing, social network analysis, and machine learning. Representative topics of his recent research include secure and verifiable computation, adversarial robustness of learning systems, and game-theoretical modeling.

ALL are welcome!

Enquiries : Department of Computing
Email : comp.enquiry@polyu.edu.hk
Tel : 3400 3145