TEMPLE UNIVERSITY®

Summer 2019 Colloquium

Center for Networked Computing
Department of Computer and Information Sciences

Toward a Game-Theoretic Foundation for Cyber Deception

Quanyan Zhu
New York University

Wednesday, July 10, 3:00PM, SERC 306

Abstract:. Deceptive and anti-deceptive technologies have been developed for various specific applications. But there is a significant need for a general, holistic, and quantitative framework of deception. Game theory provides an ideal set of tools to develop such a framework of deception. In particular, game theory captures the strategic and self-interested nature of attackers and defenders in cybersecurity. Additionally, control theory can be used to quantify the physical impact of attack and defense strategies. In this talk, we present an overview of game-theoretic models and design mechanisms for deception and counter-deception. The talk aims to provide a taxonomy of deception and counter-deception and understand how they can be conceptualized, quantified, and designed or mitigated. This talk presents diverse methodologies from game theory that includes games of incomplete information, dynamic games, mechanism design theory to offer a modern theoretic underpinning of cyber deception.

Bio: Quanyan Zhu received B. Eng. in Honors Electrical Engineering with distinction from McGill University in 2006, M.A.Sc. from the University of Toronto in 2008, and Ph.D. from the University of Illinois at Urbana-Champaign (UIUC) in 2013. After stints at Princeton University, he is currently an assistant professor at the Department of Electrical and Computer Engineering, New York University. He is a recipient of many awards including NSF CAREER Award, NYU Goddard Junior Faculty Fellowship, NSERC Postdoctoral Fellowship (PDF), NSERC Canada Graduate Scholarship (CGS), and Mavis Future Faculty Fellowships. He spearheaded and chaired INFOCOM Workshop on Communications and Control on Smart Energy Systems (CCSES), and Midwest Workshop on Control and Game Theory (WCGT). His current research interests include resilient and secure interdependent critical infrastructures, Internet of Things, cyber-physical systems, game theory, machine learning, network optimization, and control. He is a recipient of best paper awards at 5th International Conference on Resilient Control Systems and 18th International Conference on Information Fusion. He has served as the general chair of the 7th Conference on Decision and Game Theory for Security (GameSec) in 2016, the 9th International Conference on NETwork Games, COntrol and OPtimisation (NETGCOOP) in 2018, and the 5th International Conference on Artificial Intelligence and Security (ICAIS 2019) in 2019. His current research is supported by NSF, DoD, DOE, DHS, DOT, and DARPA.