

Smart Living Faculty Candidate Seminar

Towards the Design of Cyber-Physical-Human Systems from Security and Behavioral Viewpoints

Dr. Venkata Sriram Siddhardh Nadendla

University of Illinois at Urbana-Champaign

Abstract: Smart living is a modern outlook to infrastructure design where people and technology interact with each other strategically in order to improve the social and economic well-being of those who live, work, or travel within it. This novel viewpoint offers unprecedented opportunities to develop “smart” cyber-physical-human systems so that system agents (humans/machines) can effectively interact over a secure platform and make able decisions so that the overall system operates at optimum social-welfare. However, the challenging task lies in the design and analysis of such mechanisms due to the presence of uncertainties, adversaries and/or strategic agents with non-aligned motives, behavioral preferences and cognitive biases. In this talk, I will address two fundamental settings in cyber-physical-human systems, namely, (i) security in distributed detection networks, and (ii) strategic information transmission (SIT) in human-system interaction.

In the first part of the talk, I will present a brief overview of my work on secure distributed detection in the presence of eavesdropping, Byzantine (data-falsification) and jamming attacks. Specifically, I will focus on the design and analysis of distributed detection in the presence of Byzantine attacks in greater detail. In the second part of the talk, I will consider a persuasive human-human/machine interaction in a point-to-point communication setting, where the human agents are modeled using prospect theory. I will present a detailed analysis regarding the effects of subjective biases on the encoding/decoding strategies within the framework of Stackelberg SIT games under Gaussian and exponential test channels. Lastly, I will conclude the talk by discussing future directions in the strategic design and analysis of communication systems, statistical inference and machine learning frameworks within the context of cyber-physical-human systems and smart living.

Bio: Venkata Sriram Siddhardh Nadendla received his BE degree in Electronics and Communication Engineering from SCSVMV University (India), MS degree in Electrical Engineering from Louisiana State University and PhD in Electrical and Computer Engineering from Syracuse University. He worked as a research intern at ANDRO Computational Solutions, LLC, Rome, NY in the summers of 2013 and 2014. Currently, he is a postdoctoral research associate at Coordinated Science Laboratory, University of Illinois at Urbana-Champaign. His research interests broadly span the field of cyber-physical-human systems, with special focus on topics such as statistical inference and machine learning, communications and information theory, security, network economics and behavioral decision theory.

Date: April 4, 2018

Time: :10:00 am

209 Computer Science Building

