DEPARTMENT OF MECHANICAL ENGINEERING COLLOQUIUM

UNIVERSITY OF CALIFORNIA
UC RIVERSIDE

The Department of Mechanical Engineering

PRESENTS

Vaibhav Katewa , Ph.D.

Post-Doctoral Scholar, Pasqualetti Lab
Department of Mechanical Engineering
University of California, Riverside

Friday, April 13 2018
WCH Room 205/206
11:10-12:00PM

Security and Privacy in Cyber-Physical Systems

Abstract:

Cyber-Physical Systems (CPS) are engineered systems resulting from a seamless integration between physical processes and cyber technologies such as communication networks and computational hardware. This tight integration exposes the CPS to a variety of attacks, both on the physical and cyber components, which can result in significant performance degradation. Further, CPS usually consist of multiple agents that collaborate and share information with each other, thus making them vulnerable to privacy breach and leakage of confidential data. This talk will focus on the need, design and analysis of security and privacy mechanisms in CPS.

In the first part of the talk, we will present a security problem for real-time resource-constrained autonomous systems (for example, a UAV), which can reserve only limited computational resources and time for security and control purposes. In such scenarios, the control and security tasks usually compete with each other for limited resources and there exists a trade-off between security and control performance. We characterize the optimal trade-off and identify attack regimes in which the system should prefer control tasks over security tasks, and vice-versa.

The second part will focus on privacy in cooperative dynamical multi-agent CPS. We present a noise adding differentially private mechanism to preserve the privacy of agents' state over time, and analyze the effect of the privacy mechanism on the system performance. Next, we show that a fundamental trade-off exists between privacy and cooperation level, and it is beneficial for the agents to reduce cooperation if they want to be more private.

About the Speaker:

Vaibhav Katewa is a postdoctoral scholar in the department of Mechanical Engineering at UCR since January 2017, where he is working with Dr. Fabio Pasqualetti. He received his M.S. and Ph.D. degrees from University of Notre Dame in 2012 and 2016, and his Bachelors degree from Indian Institute of Technology - Kanpur in 2007, all in Electrical Engineering. His research interests include design and analysis of security and privacy methods for cyber-physical systems and complex networks, decentralized and sparse feedback control, and protocol design for networked control systems.