Time & Location: June 22, 2018 at 1:00 PM in HEC 438
Title: Security of Autonomous Systems under Physical Attacks: With application to Self-Driving Cars

The drive to achieve trustworthy autonomous cyber-physical systems (CPS), which can attain goals independently in the presence of significant uncertainties and for long periods of time without any human intervention, has always been enticing. Many advances have occurred in this direction. However, technological challenges still exist and particularly in terms of decision making under uncertainty. In CPS, uncertainties can arise from the operating environment and adversarial attacks. Consequently, human beings lack trust in these systems and hesitate to use them for day-to-day use.

In this dissertation, we develop algorithms to enhance trust by mitigating physical attacks targeting the integrity and security of sensing units of CPS. Sensors are responsible for gathering data of the physical processes and lack of measures for securing their information can enable malicious attackers to cause life-threatening situations. This serves as a motivation for developing attack resilient solutions.

Among various security solutions, attention has been recently paid toward developing system-level countermeasures to prevent CPS from attack. Along this direction, we develop an active and multiple passive algorithm to detect attacks such as Denial of Service (DoS), False Data Injection (FDI) and minimize their effect on the internal state estimates of the system. We analyze the asymptotic performance of the estimator and provide conditions for resilience of the state estimate.

We also design novel distributed estimators based on l1 norm optimization, which can recursively estimate states within an error bound without restricting the number of agents (of the distributed system) that can be compromised. Again, we analyze the resiliency and asymptotic properties of the estimator.

Finally, we make preliminary effort to formally verify the control system of the autonomous CPS using the statistical model checking approach. It is done to ensure that a real-time and resource constrained CPS, with controllers and security solutions, adheres to strict timing constrains.

Major: Computer Engineering

Educational Career:
Bachelor's of Electronics and Communication, BS, 2007, Visvesvaraya Technological University
Master's of Electrical Engineering, MS, 2011, University of Central Florida

Committee in Charge:
Yier Jin, Chair, Electrical and Computer Engineering
Kalpathy Sundaram, Co-Chair, Electrical and Computer Engineering
Ronald Demara, Department of Electrical and Computer Engineering
Teng Zhang, Department of Mathematics
Shaojie Zhang, Department of Electrical and Computer Engineering

Approved for distribution by Yier Jin, Committee Chair, on March 26, 2018.

The public is welcome to attend.