Electrical & Computer ENGINEERING

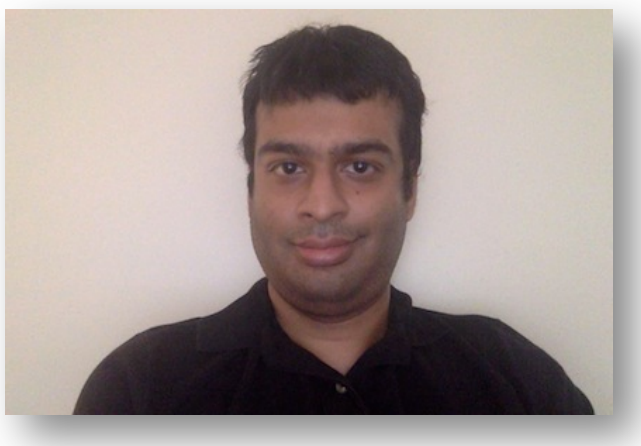
ENERGY AND INFORMATION SEMINAR

eis.ece.cmu.edu

Mon, April 7

Porter Hall
Room B34
12:30 p.m.

Detecting Integrity Attacks on Control Systems Using Physical Watermarking



Sean Weerakkody is a second year Ph.D. student at Carnegie Mellon University. He received BS degrees in Mathematics and Electrical Engineering from the University of Maryland, College Park in 2012. His research interests lie in the area of secure cyber physical systems and estimation in sensor networks.

Sean Weerakkody
PhD Student
Carnegie Mellon University

Detecting Integrity Attacks on Control Systems using Physical Watermarking

In this presentation, I will consider the problem of securing control systems from integrity attacks using system theoretic techniques. In an integrity attack, an adversary alters sensor measurements and/or inputs to the system. Integrity attacks can be constructed to mimic system dynamics under normal operation, while physically causing damage to the system. In this work, I will consider an adversary with knowledge of the system model and the capability to bypass traditional cyber security techniques protecting the integrity of sensor measurements. The adversary uses this knowledge and capability to create and inject false sensor outputs into the system to deceive the system operator. To cause physical damage, the attacker also inserts a destabilizing input into the plant.

To counter such an adversary, we propose injecting a secret physical watermark or noisy input to the system, added on top of the optimal control signal. The actual physical output of the system is correlated to the watermark or input in general through the dynamics of the system. As such, if the system is operating under normal conditions, the system operator should be able to detect the presence of the watermark in the sensor outputs. However, if the sensor outputs are manufactured by an attacker who does not know the noisy input, the watermark and artificial measurements should be independent. This approach is conceptually similar to challenge response authentication schemes in traditional cyber security where the watermark serves as the challenge, while the measurements serve as the response. In addition to introducing this approach, I will discuss the design of these watermarking inputs in the class of stationary Gaussian signals as well as the choice of detector in the case of perfect secrecy, where the attacker has no access to the systems true control inputs or sensor outputs. I will then extend these results to the case where the attack can eavesdrop on a subset of sensors and actuators and provide results and conclusions.

ECE Energy and Information Seminar Hosts

Pulkit Grover <pulkit@cmu.edu>
Marija Ilic <milic@ece.cmu.edu>
Soummya Kar <soummyak@ece.cmu.edu>
José Moura <moura@ece.cmu.edu>
Rohit Negi <negi@ece.cmu.edu>
Aswin Sankaranarayanan <saswin@ece.cmu.edu>

Student Coordinator

June Zhang <junez@andrew.cmu.edu>

Electrical & Computer ENGINEERING

Carnegie Mellon University