THE OHIO STATE UNIVERSITY
COLLEGE OF ENGINEERING

Securing Autonomous Systems

ECE 5555

Credit Hours:
3.00

Course Levels:
Undergraduate (1000-5000 level)
Graduate (5000-8000 level)

Course Components:
Lecture

Course Description:
The course covers different security measures for safeguarding against cyberattacks, detecting cyberattacks, and mitigating the effects of cyberattacks on autonomous control systems.

Prerequisites and Co-requisites:
Prereq: 3050 and 3551; or Grad standing in Engineering, Math, or Statistics.

Course Goals / Objectives:
- Familiarity with deriving mathematical models of typical engineering systems to be controlled
- Master various cyberattack detection algorithms that can be launched on autonomous control systems
- Be competent in deriving algorithms that defend against cyberattacks in autonomous control systems
- Apply knowledge gained in mathematics, statistics, physical sciences, and engineering courses to derive algorithms that defend against cyberattacks in autonomous control systems
- Exposure to implementation of secure control algorithms using Simulink or hardware testbeds (e.g., Arduino, Raspberry Pi, or microcontrollers)

Course Topics:

- Introduction to closed loop control systems, state space model in discrete time, and hierarchical control systems
- Control architecture and challenges in complex autonomous systems
- Review of statistical concepts, mean, covariance, law of large numbers, classification and regression
- Review of vulnerabilities in control systems; passive, active, and proactive measures for security
- Attack detection, signature based anomaly detection, change detection, dynamic watermarking, digital twin technology
- Attack mitigation through active interventions

Designation:

Required
Elective