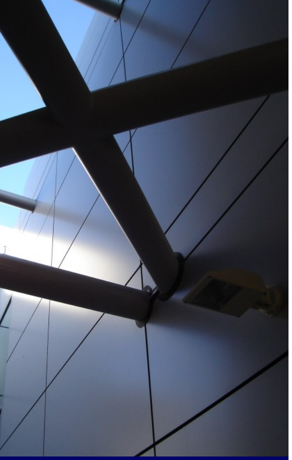

MECHANICAL ENGINEERING

*The Department of Mechanical Engineering presents:*

# *The Master's Dissertation Defense of:*

# *Yin-Chen Liu*

**Monday, May 15, 2017**
**12PM, Bourns Hall A265**

## RSSI-aided Trajectory Planning Against GNSS Spoofing

Master of Science, Graduate Program in Mechanical Engineering
University of California, Riverside, May 2017
Dr. Fabio Pasqualetti, Chairperson

Global Navigation Satellite System (GNSS) is widely adopted in most applications requiring autonomous navigation, as it provides accurate measurements of a robot's position with limited hardware and computation requirements. Yet, recent studies and real world incidents have demonstrated that GNSS readings can be easily corrupted, for instance, by jamming the receiver unit or spoofing the transmitted measurements via unauthorized GNSS transmissions. In the presence of attacks, success of autonomous navigation is not guaranteed in most scenarios. In this paper we put forth the idea of planning a robot's trajectory and exploiting additional sensors to account and limit the effect of attacks against autonomous robots. In particular, we consider a robot equipped with a GNSS sensor and a Radio Signal Strength Indicator (RSSI) antenna, which provides the robot with an estimate of its distance to a radio station. We consider an attacker capable of arbitrarily spoofing the GNSS measurements and altering the robot's input commands. We analytically characterize the class of undetectable attacks, that is, the attack signals that alter the robot's nominal trajectory and that produce GNSS and RSSI measurements compatible with the robot's nominal trajectory. We quantify the largest perturbation induced by an undetectable attack, and we show how the robot's nominal trajectory should be designed to guarantee secure navigation in the presence of attacks. We illustrate our results through several numerical examples and experiments.