Thesis Defense

Computer Science Master's Program

"Optimal False Data Injection (FDI) in Simulated Cooperative Adaptive Cruise Control (CACC) Systems"

By **Lovro Dukic**

Abstract:

In the rapidly advancing field of autonomous vehicles, ensuring the security and reliability of self-driving systems is crucial. Autonomous vehicle systems, such as cooperative adaptive cruise control (CACC), must undergo significant research and testing before their integration into commercial intelligent transportation systems. CACC considers multiple vehicles in close proximity as a single entity, or platoon, with each vehicle equipped with a controller that uses sensor-based measurements and vehicle-to-vehicle (V2V) communication to control inter-vehicle spacing. While this system offers numerous potential benefits for traffic safety and efficiency, it is also susceptible to False Data Injection (FDI) attacks, which can cause the system to behave in potentially life-threatening ways. Testing these scenarios in the real world is infeasible due to expense, safety concerns, and the use of theoretical technologies.

This study presents an implementation of a vehicle platoon in a simulated environment where the vehicles' controllers were tuned to maintain desired inter-vehicle spacing. Various FDI signals were then implemented to demonstrate the feasibility of malicious attacks, including a novel parameterized sinusoidal FDI signal. Furthermore, acknowledging the necessity for future anomaly detection schemes and noise filtration, a theoretical optimal attack—generated using a model of the sinusoidal FDI attack and identification of optimal FDI values—was also evaluated.

Date: Thursday, June 13th, 2024
Time: 2:00 PM – 4:00 PM
Location: 14-232b
Committee: Dr. DeBruhl, Dr. Fang, Dr. Beard