PhD Dissertation Defense Announcement
Mechanical & Aerospace Engineering Department
University of Texas at Arlington

Analysis and Detection of Cyber Attacks in Multi-Vehicle Systems Using Macroscopic Models

By: Abhishek Kashyap

Thesis Advisor: Dr. Animesh Chakravarthy

1 PM, Thursday, 13 June 2024

Woolf Hall, 413

Abstract

The study of potential cyber-attacks in different domains is an active area of research. Given that systems are becoming more and more interconnected, cyber physical systems that operate infrastructure and/or plants can make these assets more vulnerable and open to different attack vectors. The primary focus of this research is the modeling, analysis, and detection of cyber-attacks on platoons of autonomous cars and swarms of UAVs.

In this work, we consider scenarios wherein an attacker may hack into a subset of vehicles in a multi-vehicle system and make subtle modifications in their parameters. Due to the interconnected nature of the multi-vehicle system, these hacked vehicles (referred to as malicious vehicles) are subsequently able to modify the behavior of the entire system. The multi-vehicle systems considered in this research include vehicle platoons on highway stretches, vehicles driving on interconnected road networks, as well as flying UAV swarms. The heterogeneous two species (normal and malicious vehicles) multi-vehicle systems are modeled using macroscopic PDE (Partial Differential Equation) models. Such models can describe collective phenomena such as the evolution of high-density regions as well as the propagation of traffic waves in multi-vehicle systems in a computationally efficient manner. These models are subsequently analyzed using both analytical and machine learning techniques such as Gaussian Process Regression (GPR) methods, to detect the occurrence of malicious attacks, and quantify the number and distribution of malicious vehicles in the multi-vehicle system. These analyses are verified and supported by non-linear PDE simulations.