STEVENS
INSTITUTE OF TECHNOLOGY
1870

Ph.D. DISSERTATION DEFENSE

Candidate:	Mohammad (Rayan) Bahrami
Degree:	Doctor of Philosophy
School/Department:	Charles V. Schaefer, Jr. School of Engineering & Science (SES), Department of Mechanical Engineering
Date:	Thursday, August 15th, 2024
Time/Location:	02:00 PM – 04:00 PM | **https://stevens.zoom.us/j/92935875311**
Title:	Multi-Robot Systems in Adversarial Settings: Adversary Detection, Resilient Coordination and Cooperation
Chairperson:	Dr. Hamid Jafarnejad Sani, Department of Mechanical Engineering, SES
Committee Members:	Dr. Brendan Englot, Department of Mechanical Engineering, SES Dr. Long Wang, Department of Mechanical Engineering, SES Dr. Yi Guo, Department of Electrical and Computer Engineering, SES

ABSTRACT

Networked autonomous mobile robots, such as unmanned aerial and ground vehicles, represent a burgeoning class of cyber-physical systems (CPS) within critical infrastructure sectors. This dissertation addresses the imperative to ensure the safe and secure cooperation of these systems in the face of adversarial challenges. Specifically, we consider a class of worst-case scenario vulnerabilities in the wireless communication networks of multi-robot systems and their perceptual sensing modalities, such as cameras. Such vulnerabilities can be adversarially exploited to compromise, severely and shortly, not only the system's operation but also information confidentiality, integrity, and availability while remaining stealthy (unnoticeable in the monitoring data) until a critical failure.

In the first part of this dissertation, we propose three principled algorithmic frameworks that allow for the detection and mitigation of adversarial attacks on multi-robot coordination with wireless communication. Our results extend the resilient consensus (coordination) of multi-agent (robot) systems to the case of time-varying communication topology with intermittent connections and provide theoretical stability and performance analysis in the continuous-time domain. We characterize control-theoretic and graph-theoretic conditions under which specific classes of adversarial attacks on the communication networks of the system exist. We develop theoretical conditions that determine the degree to which a multi-robot system maintains a certain level of communication-related performance in a cooperative task while enduring a specific number of adversarial/compromised robots in a given network. Finally, we develop decentralized and distributed attack detection frameworks that allow for resilient coordination of the remaining uncompromised robots.

In the second part of this dissertation, we present two open-source vision-enabled multi-quadrotor drone platforms, together with developed software packages, that allow for research and development on resilient cooperation of multi-drone systems and validation of the derived theoretical results through experimental studies. We also present a framework for perception-based multi-robot coordination subject to adversarial image attacks on their learned perception modules.

By providing principled algorithms and open-source software, this dissertation contributes to advancing the resilience and security of autonomous multi-robot systems in safety- and time-critical applications, with potential implications for enhancing operational safety across various sectors.