University of Pittsburgh | School of Computing and Information

## Proposal Defense

***Doctor of Philosophy in Information Science***

"**Physics and AI Driven Anomaly Detection in Cyber Physical Systems**" by **Faris Alotibi**

**Date:** November 29, 2022
**Time:** 08:30AM – 10:30AM
**Place:** Virtual

**Committee:**

- Dr. David Tipper, Professor, Department of Informatics and Networked Systems, School of Computing and Information (Advisor)
- Dr. James Joshi, Professor, Department of Informatics and Networked Systems, School of Computing and Information
- Dr. Mai Abdelhakim, Assistant Professor, Department of Electrical and Computer Engineering, Swanson School of Engineering
- Dr. Amy Babay, Assistant Professor, Department of Informatics and Networked Systems, School of Computing and Information

**Abstract:**

Organizations across various sectors are moving rapidly to digitization. Various applications in cyber physical systems (CPSs) emerged from interconnectivity such as smart cities, autonomous vehicles, smart grid, and smart homes, utilizing advance capabilities of internet of things (IoTs), cloud computing, and machine learning. Interconnectivity also becomes a critical component in industrial systems such as smart manufacturing and production, smart oil and gas distribution grid, smart electric power grid, etc. These critical infrastructures and systems rely their operations on industrial IoTs and learning-enabled components to handle the uncertainty and variability of the environment and increase the level of autonomy of making effective operational decisions. The prosperity and benefits of systems interconnectivity demand the fulfillment of functional requirements such as interoperability of communication and technology, efficiency and reliability, and real time communication. Systems need to integrate with various communication technologies and standards, process and analyze shared data efficiently, ensure the integrity and accuracy of exchanged data, and execute their processes with tolerable delay. This creates enormous attack vectors targeting both physical and cyber components. Protection of systems interconnection and validation of communicated data against cyber and physical attacks become highly critical due to the massive consequences of disruption or malfunction the attacks pose to critical systems.

In this dissertation, we tackle one of the prominent attacks in the CPS space, namely false data injection attack (FDIA). FDIA is an attack executed to maliciously influence decisions, that is CPSs operational decisions such as opening a valve, changing wind turbines configurations, charging/discharging energy storage system battery, or coordinating autonomous vehicles driving. We focus on the development of anomaly detection techniques to protect CPSs from this emerging threat. The anomaly detection mechanisms leverage both physics of CPSs and AI to improve their detection capability as well as the CPSs ability to mitigate the impact of FDIA on their operations.