Subject: Cyber-security of CPS: Detection methods and Resiliency

Prof. Heidar Ali Talebi

Amir Kabir University of Technology

Abstract:

Currently, the control of physical systems no longer relies on conventional methods, and all processes can be connected and controlled via communication links. The integration and coordination of cyber and physical components give rise to systems known as cyber-physical systems (CPSs) which have numerous applications in real-life and industries, including but not limited to mobility and transportation, health-care, smart homes, and smart-grids.

Unfortunately, CPSs are vulnerable to cyber-attacks. An attacker can penetrate the communication links and disrupt system performance. In recent years, there has been an emergence of several types of attacks aimed at compromising CPSs. These attacks, namely Denial-of-Service (DoS), Replay, Zero dynamic, and Covert attacks, have resulted in significant financial and human repercussions. An illustrative instance is the Stuxnet malware, which inflicted significant harm on Iran's nuclear infrastructure, resulting in a substantial setback of their nuclear program for a duration of two years.

Detecting cyber-attacks is a challenging research area. Certain cyber-attacks have the ability to elude detection strategies that are based on conventional signal monitoring, thereby enabling the attacker to inflict damage onto a system without raising suspicion. Therefore, novel detection algorithms must be investigated such as watermarking algorithms, zero dynamic detection, KL-divergence metrics, AI-powered detection algorithms and etc. Moreover, to maintain the performance of the CPSs against cyber-attacks and enhance their resiliency, it is imperative to adopt countermeasure tactics on CPSs. With this regard, the resilient control approaches can be classified into three categories: I) graph-based methods, including W-MSR and reputation algorithms, II) model-based methods, encompassing robust and adaptive control techniques, and III) encryption-based methods, involving the utilization of semi-homomorphic encryptions.

In this talk, we start by reviewing the key concepts in the field of CPS and cyber-security of CPS along with introducing common types of cyber-attacks and their attack strategies. Afterwards, we discuss some instances of detection algorithms for CPSs. Finally, the different resilient control strategies will be presented for enhancing the security of CPSs.