MASTER THESIS

Title: Secure Control Systems

Problem Description

Cyber-physical systems (CPSs) represent a large class of networked control systems such as smart cities, autonomous systems, transportation networks, and power systems. However, the trend towards increased usage of open-standard communication protocols among control systems has made them vulnerable to online cyber-attacks. Such cyber-attacks can negatively affect the operation of CPS and receive significant media coverage. For instance, in 2015, the Ukrainian power distribution company reported power outages to $80,000$ customers for 3 hours as a result of a foreign cyber-attacker.

A pictorial representation of a CPS with a cyber-attack is shown in Figure 1. Here, the communication channels are prone to cyber-attacks which makes it harder for the CPS to calculate and apply the control input reliably. For this reason, there has been an increased research interest for the security of CPS[1].

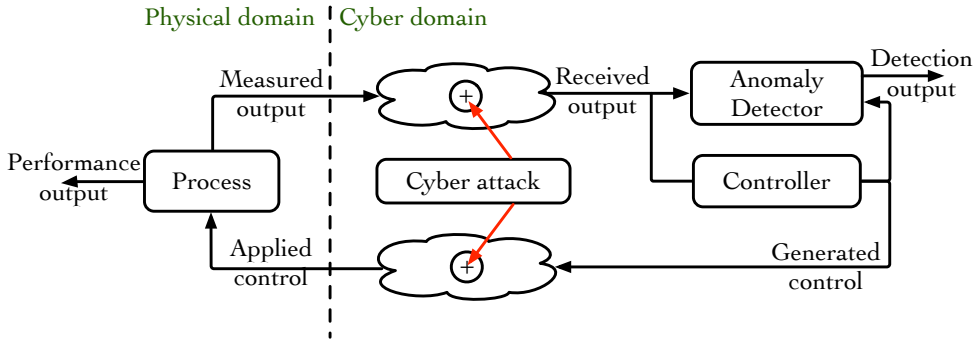

Figure 1: Depiction of Cyber-attack

There are different types of cyber-attacks such as replay attacks, denial of service attacks, eavesdropping attacks, bias injection attacks, and zero dynamics attacks. This project will focus on (a) worst-case impact assessment, and/or (b) system design for minimizing the worst-case impact of cyber-attacks on CPS. Some relevant literature on: attack modeling[2], attack impact assessment[3], and design for lowered attack impact[4].

Who we are looking for:

1. We are looking for highly motivated students, with a research-oriented attitude. A research-oriented attitude implies students are willing to tackle challenging research tasks, driven mostly by the pleasure of researching problems of fundamental nature where theory plays a bigger role than applications.
2. The goal of the project can be realigned to match the interest of the student. For more research topics on security on control systems, see a list of related publications **here** (`https://www.andre-teixeira.eu/publications.html`).
3. Together with us, the student if interested will be requested to write a scientific paper of 6/8 pages of which the student will be the main author.
4. Expected background: Basics of control theory, linear algebra, programming (MATLab), convex optimization.

For students interested in this thesis project, please contact Sribalaji C. Anand (`sribalaji.anand@angstrom.uu.se`) or André M. H. Teixeira (`andre.teixeira@it.uu.se`) for further information.

[1] Michelle S Chong, Henrik Sandberg, and André MH Teixeira. "A tutorial introduction to security and privacy for cyber-physical systems". In: *2019 18th European Control Conference (ECC)*. IEEE. 2019, pp. 968–978.

[2] André Teixeira et al. "A secure control framework for resource-limited adversaries". In: *Automatica* 51 (2015), pp. 135–148.

[3] André Teixeira, Henrik Sandberg, and Karl H Johansson. "Strategic stealthy attacks: the output-to-output ℓ_2-gain". In: *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE. 2015, pp. 2582–2587.

[4] Sribalaji C Anand and André MH Teixeira. "Joint controller and detector design against data injection attacks on actuators". In: *IFAC-PapersOnLine* 53.2 (2020), pp. 7439–7445.