A Risk Management Approach to Cyber-Physical Security in Networked Control Systems

Reports of cyber-attacks, such as Stuxnet, have shown their devastating consequences on digitally controlled systems supporting modern societies, and shed light on their modus operandi: first learn sensitive information about the system, then tamper the visible information so the attack is undetected, and meanwhile have significant impact on the physical system. Securing control systems against such complex attacks requires a systematic and thorough approach. Risk management is a fundamental approach to build security, which critically depends on the ability to characterize, analyze, and rank attack scenarios in terms of their risk (i.e., impact and likelihood). The security of the control system is then built by deploying mitigation schemes targeted at high-risk (high-impact, high-likelihood) scenarios.

In the first part of this lecture, we shall provide an overview of the recent work on secure networked control systems centered on the risk management framework and its main stages: scenario characterization, risk analysis, and risk mitigation. In particular, we shall consider malicious attacks on key security properties such as confidentiality, integrity, availability, and map different attack policies into important characteristics of the adversaries, namely their access to resources enabling the disclosure and disruption of data, and model information.

In the second part of the lecture, we discuss a specific mitigation scenario in a power system application. In response to a discovered vulnerability in a large network of controllable power loads, it is important to quickly distribute and install security patches to all units without risking system safety violations in the update process. We call such a problem the software update rollout problem. We present a mathematical framework for its modeling and solution in low-voltage distribution grids. First, it is shown that this problem can be understood as a multi-resource bin packing problem. Then several approximate and exact solution schemes are discussed. These schemes are then evaluated on benchmark networks of realistic size.

The lecture is mainly based on these references:

[1] Michelle S. Chong, Henrik Sandberg, André M.H. Teixeira: “A Tutorial Introduction to Security and Privacy for Cyber-Physical Systems”. 18th European Control Conference (ECC), Naples, Italy, 2019, pp. 968-978.

[2] Marcial Guerra de Medeiros, Kin Cheong Sou, Henrik Sandberg: “Minimum-time Secure Rollout of Software Updates for Controllable Power Loads”. Electric Power Systems Research, 189, 106797, Dec 2020.