Security and Limitations of Cyber-Physical Systems

[Draft, 2015-06-15]

Henrik Sandberg and André Teixeira, KTH

Intensive PhD course, Linköping University, August 24-26, 2015

Background

This short course provides an introduction to cyber-physical security of networked control systems (NCS), and summarizes recent progress in applying fundamentals of systems theory and decision sciences to this new and increasingly promising area. NCS applications range from large-scale industrial applications to critical infrastructures such as water, transportation, and electricity networks. Their security naturally depends on the integrations of cyber and physical dynamics, and on different ways in which they are affected by the actions of human decision makers. Thus, problems in this area lie at the intersection of control systems and computer security.

A first justified question to answer in this course is if it is at all necessary to focus on security for *control systems*. Is it not enough to say that IT and network security solutions will also address control system security? After all, NCS are applications typically built on IP-based networks. However, the inherent feedback in NCS and the coupling to the physical environment impose completely new challenges for cyber-security tools. NCS highlight special feedback characteristics of control systems that have implications on the underlying physical dynamics. On one hand, the traditional IT security focuses on the protection of information in the cyber world. On the other hand, classical control theory focuses on the attenuation of disturbances and uncertainties in the physical world. This separation was natural for many practical applications, such as traditionally hard-wired supervisory control and data acquisition (SCADA) systems. However, the separation at the design stages of IT security tools and control-theoretic implementations is no longer permissible. Indeed, NCS are vulnerable to remote access over IP-based communication networks, software flaws and hardware malfunctions of off-the-shelf IT devices, and the presence of a large number of field devices used for sensing and actuation. In such a networked environment, the cyber and physical components become interconnected and hence, their security is interdependent. A concrete example is a now well-known incident in 2010: The advanced computer worm *Stuxnet* infected industrial control systems that supposedly had strategic value to certain nation states. While there are no confirmed reports about the actual impact of the attack, the incident certainly highlights the potential threats to control systems.

Incorporating traditional IT security in control designs, such as encryption of certain communication channels, is important; however, it is only a partial solution to NCS security concerns. Even if certain communication channels have been encrypted, malicious data or actions can enter due to unauthorized access to NCS components, which can result in undesirable behaviors of the controlled physical plant. Furthermore, many encryption solutions will likely introduce time delay in the feedback loop, which usually deteriorates control system performance. Therefore, traditional IT security cannot completely provide desired level of defense against malicious insiders and computer hackers who target NCS. Fault-tolerant control methods can be used to detect and attenuate the consequences of attacks on NCSs, since these attacks affect the physical behavior of the system similar to faults. However, there are substantial conceptual and technical differences between the fault-tolerant and resilient control frameworks that motivate the need for specific theories and methodologies to address security issues in control systems. Cyber-attacks and faults have inherently distinct characteristics, which pose different challenges. Faults are considered as physical events that affect the system behavior, where simultaneous events are assumed to be non-colluding, i.e., the events do not act in a coordinated way. On the other hand, cyber-attacks may be performed over a significant number of attack points in a coordinated fashion. Moreover, faults do not have an intent or objective to fulfill, as opposed to cyber-attacks that do have a malicious intent. We are therefore

arguing for the need to develop a new set of analysis and synthesis tools based on control theory, game theory, and network optimization.

Next follows a brief overview of the topics that are covered in this short course.

Course Goals and Structure

The PhD course consists of four lectures (about 2 x 45 minutes each), and accompanying turn-in exercises. The goal of the course is to introduce and survey some recent results in security and fundamental limitations of cyber-physical systems. To fully appreciate the course, a good knowledge of multivariable control theory (cf. Glad and Ljung: Control Theory, Taylor & Francis, 2000) is required.

Tentative schedule:

- **Lecture 1: Introduction**. Fundamentals of cybersecurity, problem formulation, motivating examples, security metrics

- **Lecture 2: Attack analysis and impact**. Modeling framework, classes of NCS attack scenarios (denial-of-service, stealth, replay, covert, bias), impact analysis

- **Lecture 3: Defense strategies**. Risk management, watermarking, model perturbations, anomaly detectors

- **Lecture 4: Cyber-physical limitations**. Information-constrained optimal control, information-theoretic bounds on control performance, physical realization of controllers

Literature:

The course content is based on recent articles, such as:

- Yilin Mo, Sean Weerakkody, Bruno Sinopoli: “Physical Authentication of Control Systems”. IEEE Control Systems Magazine, vol. 35, no. 1, pp. 93-109, February 2015.

- Fabio Pasqualetti, Florian Dörfler, Francesco Bullo: “Attack Detection and Identification in Cyber-Physical Systems”. IEEE Transactions on Automatic Control, 58(11):2715-2729, 2013.

- Henrik Sandberg, Jean-Charles Delvenne, Nigel J. Newton, Sanjoy K. Mitter: "Maximum work extraction and implementation costs for nonequilibrium Maxwell's demons". Physical Review E, 90, 042119, 2014.

- Roy Smith: “Covert Misappropriation of Networked Control Systems”. IEEE Control Systems Magazine, vol. 35, no. 1, pp. 82-92, February 2015.

- André Teixeira, Iman Shames, Henrik Sandberg, Karl Henrik Johansson: "A Secure Control Framework for Resource-Limited Adversaries". Automatica, 51, pp. 135-148, January 2015.

- André Teixeira, Kin Cheong Sou, Henrik Sandberg, Karl Henrik Johansson: "Secure Control Systems: A Quantitative Risk Management Approach". IEEE Control Systems Magazine, 35:1, pp. 24-45, February 2015.