Cyberphysical Security in Networked Control Systems

The integration of cyber and physical components is becoming widespread, leading to a rapidly growing field of cyberphysical systems (CPSs), which builds on related work within the area of dynamic data-driven applications systems [1], [2]. CPSs typically combine continuous physical systems, sensors and actuators, communication networks, software, autonomy, and control, and, as such, there are numerous unique technical and systems-level challenges in obtaining the desired levels of performance (with assurances). These challenges include the need for new architectural models, the quantification and handling of the uncertainty in systems that combine continuous and discrete components,

Digital Object Identifier 10.1109/MCS.2014.2364693
Date of publication: 19 January 2015

Contributors

Henrik Sandberg by the Columbia River, outside of Portland, Oregon.

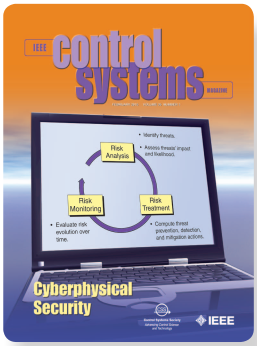
Karl H. Johansson testing wireless connectivity for a cyberphysical system. Photograph courtesy of Jann Lipka.

Saurabh Amin at the Hoover Dam.

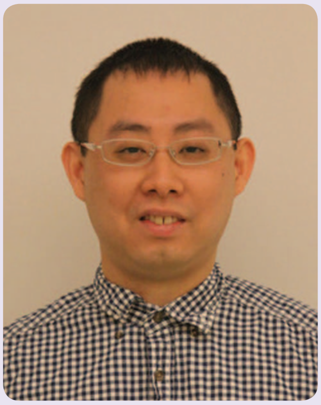
André Teixeira at the Mutianyu Great Wall of China.

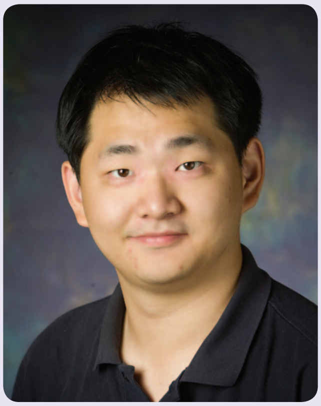
and that traditional real-time performance guarantees are insufficient for the large-scale CPS [1]. Further challenges include the safety and security of networked systems, which is the topic of this special issue. If these challenges can be addressed, then the techniques developed are likely to have a large impact in many domains, including environmental monitoring, manufacturing, health care, and transportation.

The special issue includes an introduction by the issue's organizers Henrik Sandberg, Saurabh Amin, and Karl Henrik Johansson, which motivates the main problem, namely that many control systems operate using relatively open networks to transmit sensor data and actuation commands, which makes them vulnerable to attack. While previous research in the control field has addressed the impact of time delays or lost messages as part of these communication networks, the main issues here are how much damage can a "bad actor" do by injecting malicious signals or commands into the networked system and what can be done to mitigate that damage. A key argument in the article is that the feedback control loop inherent to these CPSs poses new challenges for cybersecurity systems, and thus new analysis and synthesis tools based on control theory, game theory, and network optimization are required.


IEEE
control systems
MAGAZINE
FEBRUARY 2015 VOLUME 35 NUMBER 1
Risk Analysis
Risk Monitoring
Risk Treatment
• Identify threats.
• Assess threats' impact and likelihood.
• Evaluate risk evolution over time.
• Compute threat prevention, detection, and mitigation actions.
Cyberphysical Security
CSS
Control Systems Society
Advancing Control Science and Technology
IEEE

There are six features in this issue, the first of which is "Secure Control Systems: A Quantitative Risk Management Approach," by André Teixeira, Kin Cheong Sou, Henrik Sandberg, and Karl Henrik Johansson. The article addresses threats to networked control systems (NCSs) at both the cyber and physical layers. The article defines three security properties of information technology systems, considers different adversary


Kin Cheong Sou in the lab at KTH Royal Institute of Technology.


Quanyan Zhu.

Tamer Başar.

Galina A. Schwartz next to Cory Hall at the University of California Berkeley.

Alvaro A. Cárdenas in front of some islands of Colombia.

models with various assumptions on the available resources and information, and then defines a defense methodology based on a risk management framework. The technique is based on the notion of a security index that can be computed to identify elements in a system that are vulnerable to attack. An interesting aspect of the article is that the framework is demonstrated on multiple bus-network benchmark problems.

The second feature is "Game-Theoretic Methods for Robustness, Security, and Resilience of Cyberphysical Control Systems: Games-in-Games Principle for Optimal Cross-Layer Resilient Control Systems" by Quanyan Zhu and Tamer Başar. This article addresses the need for resilience (ability to recover online after an adversarial event) in an NCS since no desirable control system exhibits perfect robustness (tolerance to known range of uncertain parameters) or security (the ability of a system to be protected from malicious events). Since game theory has been successfully applied to the robustness and security problems, it is presented as a natural solution to the design of resilient control systems. The result is two coupled games—the cybersystem game and the physical system game—the combined solution of which is shown to yield a natural balance between security, resilience, and robustness in the overall system.

The third feature article, "Game-Theoretic Models of Electricity Theft Detection in Smart Utility Networks: Providing New Capabilities with Advanced Metering Infrastructure" by Saurabh Amin, Galina A. Schwartz, Alvaro A. Cárdenas, and S. Shankar Sastry, addresses the issue of theft in smart grids and techniques to combat it using advanced metering infrastructure. The authors develop a game-theoretic model of the situation faced by energy distributors when interacting with both good and bad actors. The framework enables the design of the optimal policies for the distributors (under some mild assumptions) yielding key insights on the best investment strategy to be used to combat theft.

Shankar Sastry in a classroom at the University of California, Berkeley.

Yilin Mo enjoying nature at Zion National Park in Utah.

Roy S. Smith climbing in Switzerland.

To illustrate the magnitude of the potential vulnerability of an NCS, the feature article "Covert Misappropriation of Networked Control Systems: Presenting a Feedback Structure" by Roy S. Smith presents a feedback structure that enables an attacker to take over control of a system while remaining hidden from the control and supervisor. The article demonstrates that, even if the covert agent's knowledge of the plant is not perfect, it is possible to set up the system so that the effect on the measured plant output of any nominal controller control signal is the same whether or not a covert controller is operating. This greatly hinders the nominal controller's ability to detect covert actions through probing signals (watermarks) or signal analysis.

The feature "Physical Authentication of Control System: Designing Watermarked Control Inputs to Detect Counterfeit Sensor Outputs" by Yilin Mo, Sean Weerakkody, and Bruno Sinopoli continues a similar investigation by determining what can be done with physical watermarking to authenticate the correct operation of a control system. As an example, the approach considers adding noisy watermarks to a standard linear-quadratic-Gaussian controller. The results determine the performance degradation associated with adding the signal, provide an optimal detector to determine if the system is under attack, and then give a formulation of the optimal watermark signal to be used.

The final feature of the issue is "Control-Theoretic Methods for Cyberphysical Security: Geometric Principles for Optimal Cross-Layer Resilient Control Systems" by Fabio Pasqualetti, Florian Dörfler, and Francesco Bullo. The article points out that, although there have been many papers on fault detection, isolation, and recovery, these have typically considered accidental faults. CPSs, however, suffer from specific vulnerabilities (that is, intentional and unforeseen attacks on the NCS) that do not affect classical systems and for which appropriate detection and identification techniques need to

Sean Weerakkody taking a hike in Gaithersburg, Maryland.

Bruno Sinopoli wakeboarding while on vacation.

Fabio Pasqualetti.

Florian Dörfler.

Francesco Bullo.

be developed. This article considers examples of attacks against power systems and water networks, and it provides a framework for a rigorous study of the detectability and identifiability of attacks and for the design of monitors and attack-remedy schemes.

"From the Editor" discusses the need for benchmarks to enable better comparison of new techniques to the state of the art. In the "President's Message," Elena Valcher discusses peer review. "CSS News" is a notice to members of the IEEE Control Systems Society (CSS) of the process by which petitions are made for nominees for the CSS Board of Governors. "Feedback" has comments from members of the control community on past editorials published in *IEEE Control Systems Magazine*. "Awards" recognizes the 2014 recipients of the control systems awards offered by the IEEE and the CSS.

"Conference Reports" has a summary of the 33rd Chinese Control Conference, held in Nanjing, Jiangsu Province, China, July 28–30, 2014. A preview is provided for the 2015 American Control Conference, which will be held in Chicago, Illinois, July 1–3, 2015.

Among the regular columns, "25 Years Ago" revisits some architectures for controlling cascade control systems. "Conference Calendar" lists upcoming conferences sponsored or cosponsored by the CSS. "Book Announcements" provides summaries of books recently published in the control field. "Random Inputs" considers some conflicting definitions that arise in the control field.

REFERENCES

[1] Cyber-Physical Systems Program Solicitation NSF 14-542 (2014, Nov. 20). [Online]. Available: http://www.nsf.gov/pubs/2014/nsf14542/nsf14542.htm

[2] Dynamic data-driven application systems. (2014, Nov. 20). [Online]. Available: http://www.dddas.org/

Jonathan P. How

Control in Flight

This invention relates to the field of automatic control of aircraft in flight, and more particularly to presettable means for controlling a number of the characteristics of flight of the craft so that they have desired conditions in each of a substantially unlimited number of portions of an extended flight. It is of course well known in the field of aircraft control to maintain at desired values various flight characteristics of a dirigible craft: heading, airspeed, altitude, position relative to a desired ground track, and pitch and roll attitudes are some of the flight characteristics with respect to which such control has in the past been exercised. It is also true that previous means have been developed for controlling certain of these and other characteristics according to successive desired overall states of the craft in successive portions of a long flight, automatic means being provided for substituting one set of controls for another as the craft passes from one portion of the flight to the next. … The inventive contribution herein centers about control of an aircraft in accordance with perforations in a record strip. A field of such perforations is provided having a portion for the control of each of the several variables under consideration, and a succession of such fields are punched into the strip for sequential control of those variables as the strip is advanced. Control of the flight of a craft in accordance with "punched card" techniques is entirely new in the field of aircraft engineering, and comprises a major object of the invention.

—Oscar Hugo Schuck, "Automatic Flight Control Apparatus,"
U.S. Patent #2,751,541, June 1956