Guest Editorial Special Issue on Secure Control of Cyber-Physical Systems

THE integration of computation, communication, and control units has led to the birth and rapid development of a new generation of engineering systems, the cyber-physical systems (CPSs), which have been increasingly used in fields ranging from aerospace, automobile, industrial process control to energy, healthcare, manufacturing, and transportation, where secure operation is one of the key concerns. These CPSs are often distributed in nature with a hierarchical structure, and likely to be attacked due to diverse motivations, such as economic reasons (e.g., reducing or not paying electricity charge), or terrorism (e.g., threatening people by controlling electricity and other life-critical resources).

By exploiting the sensing, networking, and computation capabilities, the new generation CPSs is able to connect the cyber space and the physical space in an unprecedented manner. However, such connections also provide rich opportunities for adversaries to launch potential malicious attacks.

Secure data transmission is typically taken for granted in early research in CPSs. The control and systems community has played an important role in the analysis and design of CPSs, addressing issues related to data imperfection and its effect on closed-loop system performance. The assumed data imperfection models, such as packet drops, delays, quantization, etc., however, are inadequate to characterize the possibility that the communicated data may not be the true data collected by sensors or calculated by controllers, and may instead have been modified by attackers. In July 2010, the report of Stuxnet, a control system malware targeting Supervisory Control and Data Acquisition systems in power grids, has raised new questions and research challenges of secure control of CPSs.

The classical defense approaches, such as secure detection, estimation, and robust control, aim to identify system abnormities and design strategies under the assumption that these system abnormalities under certain types of malicious attacks are either benign or random. However, different from randomly taking attack actions, smart attackers can design strategies specifically to exploit vulnerabilities of the CPSs. Some recent works investigated how to detect and identify attack actions against the consensus algorithm in power systems and wireless control networks, respectively. These methods, however, rely on the assumption that the system model is noise-free. In a noisy environment, it is much harder to detect and identify the malicious behavior since it may be indistinguishable from the environmental noise. As a result, these approaches should be rethought to guarantee CPS security requirements in more general scenarios.

Security of CPS has recently attracted a lot of interest in the control community. The Annual Conference on High Confidence Networked Systems has been held as part of CPSWeek since 2012, and focuses on the design of more secure, dependable, and trustworthy CPSs. One session of ACM/IEEE International Conference on Cyber-Physical Systems has concentrated on the security and safety of CPS. Security was also an important topic in the 2013 International Workshop on CPS. Furthermore, an increasing number of research achievements about this topic have appeared in the recent IEEE Conferences on Decision and Control, American Control Conferences, etc. Thus, we feel that it is important and timely to publish a special issue to emphasize the importance of secure control theory in CPSs analysis and design, which encompass both system theory and important applications. Such a special issue is expected to link the practical challenges and requirements with the most recent theoretical advances in this emerging research area. This is the first special issue in a major control journal to offer a systematic study of secure CPSs that includes secure detection, estimation, and control. Beyond covering the state-of-the-art, it also aspires to motivate the control systems community to make more contributions in the area of CPS security.

The main topics of the special issue include intrusion detection, secure state estimation and control in CPS analysis, design, and applications.

In response to the call for papers for this special issue, we received 46 submissions from all regions. Among these submissions, after an initial screening by the editorial board members, 3 were considered to be "out of scope" and the remaining 43 papers were sent to at least three independent reviewers. All of these papers have undergone a very rigorous peer-review process. As a final result, we selected 11 full papers for this special issue.

The accepted papers in this issue can be broadly classified in the following three main categories, which are as follows: 1) Secure control, 2) secure state estimation, and 3) other applications.

Papers in category 1) mainly consider various different attack scenarios involving the analysis and design of closed-loop control systems. Specifically, Weerakkody *et al*. characterize perfect attackabilitity for the secure design of distributed control systems using a graph theoretic approach. Liu *et al*. consider dynamic state recovery for CPSs under switching location attacks. Dolk *et al*. study event-triggered control systems subject

Digital Object Identifier 10.1109/TCNS.2017.2667233

to DoS attacks. Miao *et al*. study coding strategies for securing CPSs against stealthy data integrity attacks. Finally, Gupta *et al*. propose a dynamic game formulation with asymmetric information when considering cyber attacks.

Papers in category 2) consider remote state estimation applications, where either the sensor or the network are subject to various cyber attacks. The paper by Guo *et al*. considers optimal linear integrity attacks for remote state estimation. Pajic *et al*. study attack-resilient state estimation for noisy dynamic systems, and Mishra *et al*. consider secure state estimation in the presence of arbitrary sensor attacks.

Papers in category 3) consider cyber attacks in other application areas such as networking or power networks. The paper by Ponniah *et al*. presents a clean-slate approach to secure ad-hoc wireless networking. Shelar and Amin provide a security assessment of electricity distribution networks under DER node compromise attacks, and Wang *et al*. study differential privacy in linear distributed control systems via entropy minimizing mechanisms.

We would like to mention that this special issue only attempts to provide a snapshot of the CPS security from a control perspective. Due to the standard page limits, we could only include a rather small number of papers. As a result, despite our best efforts, its coverage is by no means complete nor even is comprehensive.

Finally, we would like to take this opportunity to thank all of the authors for their submission and contributions. We would also like to thank many individuals who helped review the papers timely and professionally and provided many excellent suggestions. The Editorial Assistant Denise Joseph provided valuable assistance. Last, but not least, we are grateful to the Editor-in-Chief, Ioannis Ch. Paschalidis, for providing us this great opportunity to put together this special issue.

PENG CHENG, *Guest Editor*
Zhejiang University
Hangzhou 310027, China

LING SHI, *Guest Editor*
Hong Kong University of Science and Technology
Kowloon, Hong Kong

BRUNO SINOPOLI, *Guest Editor*
Carnegie Mellon University
Pittsburgh, PA 15213 USA

Peng Cheng received the B.E. degree in automation and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2004 and 2009, respectively.

He is curently a Professor in the College of Control Science and Engineering, Zhejiang University. His research interests include networked sensing and control, cyber-physical systems, and control system security.

Dr. Cheng serves as an Associate Editor of IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS, *Wireless Networks*, and *International Journal of Communication Systems*. He has served as the guest editor of IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS, and IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSINGOVER NETWORKS. He served as the tpc Co-Chair of IEEE IOV 2016, local arrangement Co-Chair for ACM MobiHoc 2015, and the publicity Co-Chair for IEEE MASS 2013.

Ling Shi received the B.S. degree in electrical and electronic engineering from Hong Kong University of Science and Technology, Kowloon, Hong Kong, in 2002, and the Ph.D. degree in control and dynamical systems from California Institute of Technology, Pasadena, CA, USA, in 2008.

He is currently an Associate Professor in the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology. His research interests include cyber-physical systems security, networked control systems, sensor scheduling, and event-based state estimation.

Dr. Shi has been serving as a subject editor for *International Journal of Robust and Nonlinear Control* since 2015, an Associate Editor for IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS since 2016, and an Associate Editor for IEEE CONTROL SYSTEMS LETTERS since 2017. He also served as an Associate Editor for a special issue on Secure Control of Cyber Physical Systems in the IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS in 2015–2017.

Bruno Sinopoli received the Dr. Eng. degree in electrical engineering from the University of Padova, Padova, Italy, in 1998, and the M.S. and Ph.D. degrees in electrical engineering from the University of California at Berkeley, Berkeley, CA, USA, in 2003 and 2005, respectively.

After a Postdoctoral position at Stanford University, Stanford, CA, USA, he joined the faculty at Carnegie Mellon University, Pittsburgh, PA, USA, where he is an Assistant Professor in the Department of Electrical and Computer Engineering with courtesy appointments in Mechanical Engineering and in the Robotics Institute. His research interests include networked embedded control systems, distributed estimation and control over wireless sensor-actuator networks, and cyber-physical systems security.

Dr. Sinopoli received the 2006 Eli Jury Award for outstanding research achievement in the areas of systems, communications, control and signal processing at University of California at Berkeley and the NSF Career award in 2010.