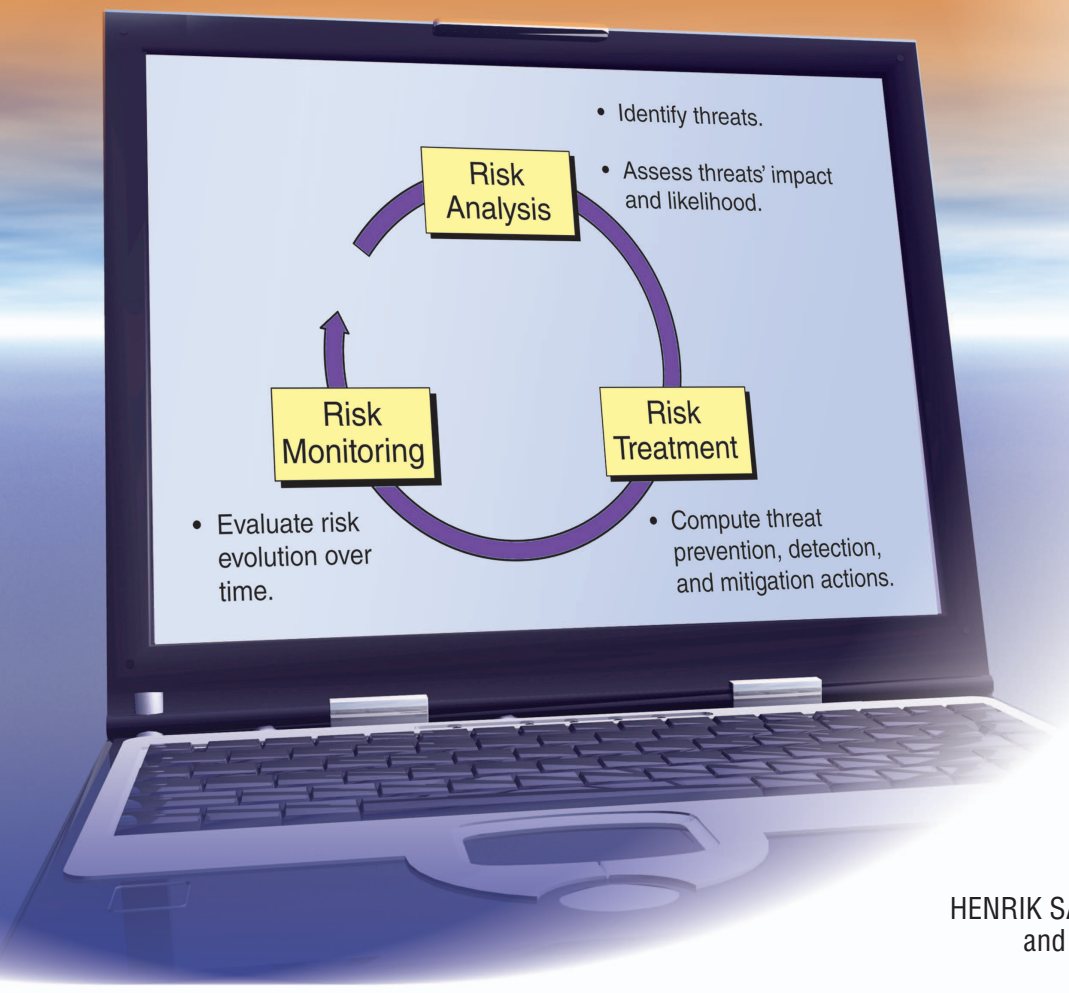

HENRIK SANDBERG, SAURABH AMIN, and KARL HENRIK JOHANSSON

Cyberphysical Security in Networked Control Systems

AN INTRODUCTION TO THE ISSUE

This special issue provides an introduction to cyberphysical security of networked control systems (NCSs) 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. The security of NCSs naturally depends on the integration 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. The six articles that constitute this special issue approach cyberphysical security from a variety of perspectives, including control theory, optimization, and game theory. They cover a range of topics such as models of attack and defense, risk assessment,

Digital Object Identifier 10.1109/MCS.2014.2364708
Date of publication: 19 January 2015

1066-033X/15©2015IEEE

NCS applications range from large-scale industrial applications to critical infrastructures such as water, transportation, and electricity networks.

attack detection and identification, and secure control design. A common theme among these contributions is an emphasis on the development of a principled approach to cyberphysical security of NCS.

A justified first question for this special issue is whether NCS security can be handled simply with information technology (IT) and network security solutions. After all, NCSs are applications typically built on Internet Protocol (IP)-based networks. However, feedback loops inherent to NCSs and the coupling to the physical environment impose fundamentally new challenges for cybersecurity tools. NCSs 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 cyberworld. 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, NCSs 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.

One concrete example is an incident from 2010 that is now well known, namely when 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 highlights the potential threats to control systems. Indeed, the articles in this special issue motivate their problem formulations using Stuxnet and other known attacks to control systems by malicious insiders or external hackers.

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 the desired level of defense against malicious insiders and computer hackers who target NCSs. We therefore argue for the need to develop a new set of analysis and synthesis tools drawing on control theory, game theory, and network optimization. Below is a brief overview of the topics that are covered in this issue.

The article by Teixeira, Sou, Sandberg, and Johansson develops a quantitative approach to security risk management in NCSs. First, the article summarizes the architecture of NCSs and models the adversary's objectives and constraints. Specifically, the adversary model includes the attack policy or mechanism as well as the resources available for violating NCS security and the adversary's knowledge of the system dynamics. Next, the article presents quantitative tools for the assessment and management of security risks to static and dynamic systems, with particular focus on stealthy deception attacks. For static systems, the proposed risk-assessment approach quantifies the likelihood of threats by posing the problem of finding minimum resource stealthy attacks. For dynamic systems, both impact and the likelihood of threats are considered by posing a multiobjective optimization problem that finds minimum-resource, maximum-impact stealthy attacks. Third, the applicability of these tools is explained by using examples of large-scale electric power systems and a wireless quadruple-tank test bed. Technological solutions for mitigating security risks are also discussed.

A complementary approach to assessing security NCS risks and improving their survivability in the face of strategic adversaries is to use game-theoretic tools. Two of the articles in this special issue present game-theoretic formulations to address security and resilience issues in NCS.

The article by Zhu and Başar presents a game-theoretic framework to analyze and improve the resilience of NCSs in the face of attacks. The framework builds on a hybrid dynamic model that models the evolution of the cybersystem as a discrete-time Markov model and combines it with continuous-time dynamics of the underlying controlled physical system. Two zero-sum games are introduced. First, a zero-sum differential game is used for robust control design

The security of NCSs naturally depends on the integration of cyber and physical dynamics and on different ways in which they are affected by the actions of human decision makers.

at the physical system level. Next, a stochastic zero-sum game between attacker and network operator is used for design of security strategies at the cyber level. A security strategy at the cyber (upper) level influences the optimal control strategy at the physical (lower) level, and in turn the design of security strategy at upper level must account for the optimal control strategy at the lower level. This two-level framework enables understanding the resilience and security aspects arising from cyberphysical interactions. Specifically, the article uses this framework to illustrate the tradeoff in allocating resources for improving the level of security of the cybersystem versus increasing control effort to ensure resilience.

The article by Amin, Schwartz, Cárdenas, and Sastry investigates energy theft in smart utility networks using techniques from game theory and detection theory. The game-theoretic model considers pricing and investment decisions by a distribution utility when it serves a population of strategic customers, and a fraction of customers are fraudulent. Each fraudulent customer chooses to steal electricity after accounting for the probability of fraud detection and the amount of fine that they pay if detected. The probabilistic rate of successful detection depends on the distributor's implementation of a diagnostic scheme and increases with level of investment made by the distributor monitoring fraud. The distributor (leader) chooses the level of investment, the price per unit quantity of billed electricity, and the fine schedule. The customers (followers) make their choices after they learn the distributor's decision. For specific assumptions on customer utilities and a distributor's profit function, this leader-follower game is used to compute equilibrium customer and a distributor choices. For two environments, namely an unregulated monopoly and the case of perfect competition, the results provide an estimate of the extent of stealing for different levels of investment (high versus low). These results point toward the need for creating regulatory measures to incentivize investments in security and fraud monitoring.

The aforementioned two articles on game-theoretic tools focus on modeling interactions between strategic entities (attacker and defender) for NCS security. The three articles mentioned below use techniques from systems and control theory to study fundamental limitations in detectability and identifiability of attacks on NCSs and to design attack-resilient NCSs for a range of applications.

The article by Smith poses the question whether signal-based attack detection techniques are sufficient to detect an attacker with sufficient resources and a certain level of knowledge of the physical system's dynamics. The attack model considered in the article is covert misappropriation of the system. Fundamental limits of detection for both linear and nonlinear system dynamics are studied. The main conclusion is that a resourceful covert agent can easily hide its actions from a nominal controller. The more knowledge that the covert agent has about the system dynamics, and the more linear the system is, the harder it will be to detect the misappropriation of the control system. The article also introduces two concrete examples to study the response of misappropriated NCSs.

The article by Mo, Weerakkody, and Sinopoli presents a new secure control scheme, called physical watermarking, to authenticate the correct operation of a control system. This scheme aims to expand and complement the effectiveness of traditional authentication schemes in computer security. The main idea behind physical watermarking is to use the ability to recognize irregularities in the dynamics of a system for intrusion-detection and attack-resilient control design. First, the article considers a class of replay attacks and shows that classical methods in estimation and failure detection in linear systems are not resilient to replay attacks. Second, an authenticating watermarked input is designed that can be superimposed on the classical linear-quadratic-Gaussian optimal input, thus providing improved detection at the expense of control performance. The watermarked input maximizes a relaxed version of the expected Kullback-Leibler divergence between the distributions of the compromised and healthy residue vector, while satisfying a constraint on the control performance. The authors generalize previously known results, where only independent and identically distributed Gaussian processes were considered. Simulation results provide insights on how false alarm rate and increased system costs affect the asymptotic detection performance.

The last article, by Pasqualetti, Dörfler, and Bullo, uses the framework of descriptor systems (subject to unknown inputs altering states and measurements) to model attacks on, and faults in, cyberphysical systems. This framework is used to model various attacks to NCSs, such as stealth, replay, covert, and false-data injection. It also provides the means to study the impact of successful attacks. Fundamental limitations of

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

detectability and identifiability of attacks are studied from system-theoretic and graph-theoretic viewpoints. Here, classical results from geometric control theory and its application to fault detection and isolation prove especially useful. The problem of designing monitors, such as bad-data detectors, is investigated. In particular, necessary and sufficient conditions are stated for the complete attack-detection monitor as well as the complete attack-identification monitor. Illustrative examples are drawn from power and water network domains.

AUTHOR INFORMATION

Henrik Sandberg received the M.Sc. degree in engineering physics and the Ph.D. degree in automatic control from Lund University, Sweden, in 1999 and 2004, respectively. He is an associate professor with the Automatic Control Laboratory, KTH Royal Institute of Technology, Stockholm, Sweden. From 2005 to 2007, he was a post-doctoral scholar with the California Institute of Technology, Pasadena. In 2013, he was a visiting scholar at the Laboratory for Information and Decision Systems at the Massachusetts Institute of Technology, Cambridge, United States. He has also held visiting appointments with the Australian National University and the University of Melbourne, Australia. His current research interests include secure networked control, power systems, model reduction, and fundamental limitations in control. He was a recipient of the Best Student Paper Award from the IEEE Conference on Decision and Control in 2004 and an Ingvar Carlsson Award from the Swedish Foundation for Strategic Research in 2007. He is currently an associate editor of *Automatica*.

Saurabh Amin (amins@mit.edu) is an assistant professor in the Department of Civil and Environmental Engineering at the Massachusetts Institute of Technology. His research focuses on the design and implementation of high-confidence network control algorithms for infrastructure systems. He works on robust diagnostics and control problems that involve using networked systems to facilitate the monitoring and control of large-scale critical infrastructures, including transportation, water, and energy distribution systems. He also studies the effect of security attacks and random faults on the survivability of networked systems and designs incentive-compatible control mechanisms to reduce network risks. He received his Ph.D. in systems engineering from the University of California, Berkeley (2011), his M.S. in transportation engineering from the University of Texas at Austin (2004), and his B.Tech. in civil engineering from the Indian Institute of Technology, Roorkee (2002). He can be contacted at 77 Massachusetts Avenue, 1-241, Massachusetts Institute of Technology, Cambridge, MA 02139 USA.

Karl Henrik Johansson is director of the KTH ACCESS Linnaeus Centre and professor at the School of Electrical Engineering, Royal Institute of Technology, Sweden. He is a Wallenberg Scholar and has held a six-year senior researcher position with the Swedish Research Council. He is director of the Stockholm Strategic Research Area ICT The Next Generation. He received M.Sc. and Ph.D. degrees in electrical engineering from Lund University. He has held visiting positions at the University of California, Berkeley (1998–2000) and the California Institute of Technology (2006–2007). His research interests are in networked control systems; hybrid and embedded systems; and applications in transportation, energy, and automation systems. He has been a member of the IEEE Control Systems Society Board of Governors and chair of the IFAC Technical Committee on Networked Systems. He has been on the editorial boards of several journals, including *Automatica*, *IEEE Transactions on Automatic Control*, and *IET Control Theory and Applications*. He is currently on the editorial board of *IEEE Transactions on Control of Network Systems* and the *European Journal of Control*. He has been a guest editor for special issues, including the 2011 issue on wireless sensor and actuator networks in *IEEE Transactions on Automatic Control*. He was the general chair of the ACM/IEEE Cyber-Physical Systems Week 2010 in Stockholm and IPC chair of many conferences. He has served on the executive committees of several European research projects in the area of networked embedded systems. In 2009, he received the Best Paper Award of the IEEE International Conference on Mobile Adhoc and Sensor Systems. In 2009, he was also appointed as a Wallenberg Scholar as one of the first ten scholars from all sciences, by the Knut and Alice Wallenberg Foundation. He was awarded an Individual Grant for the Advancement of Research Leaders from the Swedish Foundation for Strategic Research in 2005. He received the triennial Young Author Prize from IFAC in 1996 and the Peccei Award from the International Institute of System Analysis, Austria, in 1993. He received Young Researcher Awards from Scania in 1996 and from Ericsson in 1998 and 1999. He is a Fellow of the IEEE.