CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

from the viewpoint of close-loop

Edited by

Peng Cheng • Heng Zhang • Jiming Chen

CRC Press
Taylor & Francis Group

CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

from the viewpoint of close-loop

This page intentionally left blank

CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

from the viewpoint of close-loop

Edited by

Peng Cheng

Heng Zhang

Jiming Chen

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20160301

International Standard Book Number-13: 978-1-4987-3474-5 (eBook - PDF)

Contents

Preface . . . . . **vii**

Contributors . . . . . **ix**

SECTION I: SECURE STATE ESTIMATION **1**

1 A Game-Theoretic Approach to Jamming Attacks on Remote State Estimation in Cyber-Physical Systems **3**
Yuzhe Li, Ling Shi, Peng Cheng, Jiming Chen, and Daniel E. Quevedo

2 Secure State Estimation against Stealthy Attack **31**
Yilin Mo

3 Secure State Estimation in Industrial Control Systems **57**
Arash Mohammadi and Konstantinos N. Plataniotis

SECTION II: RESILIENT CONTROL THEORY **95**

4 Optimal Denial-of-Service Attack Policy against Wireless Industrial Control Systems **97**
Heng Zhang, Peng Cheng, Ling Shi, and Jiming Chen

5 Behavior Rule Specification-Based False Data Injection Detection Technique for Smart Grid **119**
Beibei Li, Rongxing Lu, and Haiyong Bao

6 Hierarchical Architectures of Resilient Control Systems: Concepts, Metrics, and Design Principles 151
Quanyan Zhu, Dong Wei, and Kun Ji

7 Topology Control in Secure Wireless Sensors Networks 183
Jun Zhao

8 Resilient Distributed Control in Cyber-Physical Energy Systems 225
Wente Zeng and Mo-Yuen Chow

SECTION III: SECURITY ISSUES IN APPLICATION FIELDS 251

9 Distributed Resilient Control of Operator-Vehicle Networks under Cyber Attacks 253
Minghui Zhu and Sonia Martínez

10 Privacy-Preserving Data Access Control in the Smart Grid 285
Kan Yang, Xiaohua Jia, and Xuemin (Sherman) Shen

Preface

By exploiting sensing, networking, and computation capabilities, the new-generation industrial control systems are able to better connect cyber space and the physical process in close-loop than ever before. However, such connections have also provided rich opportunities for adversaries to perform potential malicious attacks.

There has been extensive research on security issues from the viewpoint of networks and communication, and the secure defending approaches mainly consider how to guarantee network performance. Considerable efforts have been devoted to the design of secure defending approaches against malicious attacks with communication technologies. For example, channel hopping is often used to maintain network performance, for example, throughput, in a jamming attack environment.

Such network performance rarely considers the operation of physical plants without the features of automatic control or feedback. However, industrial control systems are characterized by feedback control and aim to optimize the system control performances, such as reducing state estimation errors, improving the stability of unstable plants, and enhancing the robustness against uncertainties and noise. Thus, it is equivalent or even more important to protect the system control performance while studying the cyber-security issues in industrial control systems. For example, when the communication of system entities is under a jamming attack, different from the existing design, such as the channel hopping algorithm, the secure state estimation and control algorithms may be better configured by exploiting the feedback information as well as the dynamics of the physical plants. As a result, it is of great research interest to develop novel theories and technologies from the viewpoint of close-loop in order to protect the industrial control system performance under various cyber and physical attacks.

Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop is the first comprehensive and updated book on cyber security from the

viewpoint of close-loop. This book provides a comprehensive technical guide on up-to-date secure defending theories and technologies, novel design, and systematic understanding of secure architecture and some practical applications. Specifically, it consists of 10 chapters, which are divided into three parts. The first part, consisting of Chapters 1 through 3, extensively introduces secure state estimation technologies, providing a systematic presentation on the latest progress in security issues regarding state estimation. The second part, composed of five chapters, focuses on the design of secure feedback control technologies in industrial control systems, showing its extraordinary difference from that of traditional secure defending approaches from the viewpoint of network and communication. The third part, with two chapters, elaborates on the systematic secure control architecture and algorithms for various concrete application scenarios.

This book has the following salient features:

1. Provides an extensive introduction to state-of-the-art cyber security theories and technologies from the viewpoint of close-loop
2. Identifies the quantitative characteristics of typical cyber attacks and analyzes the attack decision mechanisms in closed-loop industrial systems in depth
3. Proposes novel intrusion detection mechanisms against cyber attacks in industrial control systems
4. Presents a systematic understanding of the secure architectural design for industrial control systems
5. Addresses secure control approaches against cyber attacks for the representative applications in industrial control systems

This book provides detailed descriptions on attack model and strategy analysis, intrusion detection, secure state estimation and control, game theory in closed-loop systems, and various cyber-security applications. We expect the book to be favorable to those who are interested in secure theories and technologies for industrial control systems.

We would like to thank all the contributors of each chapter for their expertise and cooperation, and efforts invested, without which we would not have such an excellent book. Specially, we highly appreciate the support, patience, and professionalism of Ruijun He and Kathryn Everett from the very beginning to the final publication of the book. Last but not least, we are grateful for our families and friends for their constant encouragement and understanding throughout this project.

Peng Cheng
Heng Zhang
Jiming Chen

Contributors

Haiyong Bao
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore

Jiming Chen
College of Control Science and Technology
Zhejiang University
Zhejiang, China

Peng Cheng
College of Control Science and Technology
Zhejiang University
Hangzhou, China

Mo-Yuen Chow
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, North Carolina, USA

Kun Ji
Corporate Technology
Siemens Corporation
Princeton, New Jersey, USA

Xiaohua Jia
Department of Computer Science
City University of Hong Kong
Kowloon Tong, Hong Kong, China

Beibei Li
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore

Yuzhe Li
Department of Electronic and Computer Engineering
Hong Kong University of Science and Technology
Kowloon, Hong Kong, China

Rongxing Lu
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore

Sonia Martínez
Department of Mechanical and Aerospace Engineering
University of California
San Diego, California, USA

Yilin Mo
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore

Arash Mohammadi
Department of Electrical and Computer Engineering
University of Toronto
Toronto, Ontario, Canada

Konstantinos N. Plataniotis
Department of Electrical and Computer Engineering
University of Toronto
Toronto, Ontario, Canada

Daniel E. Quevedo
Department of Electrical Engineering
University of Paderborn
North Rhine-Westphalia, Germany

Xuemin (Sherman) Shen
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, Canada

Ling Shi
Department of Electronic and Computer Engineering
Hong Kong University of Science and Technology
Kowloon, Hong Kong, China

Dong Wei
Corporate Technology
Siemens Corporation
Princeton, New Jersey, USA

Kan Yang
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, Canada

Wente Zeng
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, North Carolina, USA

Heng Zhang
College of Control Science and Technology
Zhejiang University
Hangzhou, China

Jun Zhao
CyLab and Department of Electrical and Computer Engineering
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA

Minghui Zhu
Department of Electrical Engineering
Pennsylvania State University
University Park, Pennsylvania, USA

Quanyan Zhu
Department of Electrical and Computer Engineering
New York University
New York, New York, USA

I SECURE STATE ESTIMATION

This page intentionally left blank

Chapter 1

A Game-Theoretic Approach to Jamming Attacks on Remote State Estimation in Cyber-Physical Systems

Yuzhe Li
Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology

Ling Shi
Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology

Peng Cheng
College of Control Science and Technology, Zhejiang University

Jiming Chen
College of Control Science and Technology, Zhejiang University

Daniel E. Quevedo
Department of Electrical Engineering, University of Paderborn

CONTENTS

1.1 Introduction 4
1.2 Problem Setup 7
1.2.1 Local State Estimation 8
1.2.2 Communication Channel 9
1.2.3 Estimation Process 10
1.2.4 Main Problem 11
1.3 Game-Theoretic Framework 13
1.3.1 Nash Equilibrium 13
1.3.2 Existence of the Nash Equilibrium 15
1.3.3 Finding the Nash Equilibrium 16
1.4 Dynamic Update Based on Online Information 17
1.5 Relaxation: Average Energy Constraints 17
1.5.1 Constraint-Relaxed Problem Formulation 18
1.5.2 Markov Chain Model 20
1.5.3 Comparison and Analysis 23
1.6 Multisensor Scenario 25
1.6.1 Multiple Sensor Formulation 25
1.6.2 Constraint-Relaxed Game Formulation 26
1.7 Conclusion 27
References 27

We consider security issues in remote state estimation of cyber-physical systems in this chapter. We first investigate the single-sensor case. A sensor node communicates with a remote estimator through a wireless channel that may be jammed by an external attacker. The interactive decision-making process of when to send and when to attack is studied when the sensor and the attacker are both subject to energy constraints. We formulate a game-theoretic framework and prove that the optimal strategies for both sides constitute a Nash equilibrium of this zero-sum game. To tackle the computational complexity issues, we present a constraint-relaxed problem and provide corresponding solutions using Markov chain theory. Under a constraint-relaxed formulation, taking the multisensor data fusion into consideration, the problem for the multiple sensors case is also studied.

1.1 Introduction

Cyber-physical systems (CPS) are systems that integrate sensing, control, communication, computation, and physical process. Typical CPS usually consist of a group of networked agents, including sensors, actuators, control processing units, and communication devices [27] (Figure 1.1), which have a wide spectrum of applications in areas such as aerospace, smart grids, civil infrastructure, and transportation. Significant advances in terms of efficiency, reliability, adaptability, and autonomy of engineered systems have been brought by the rapid development of CPS in recent years.

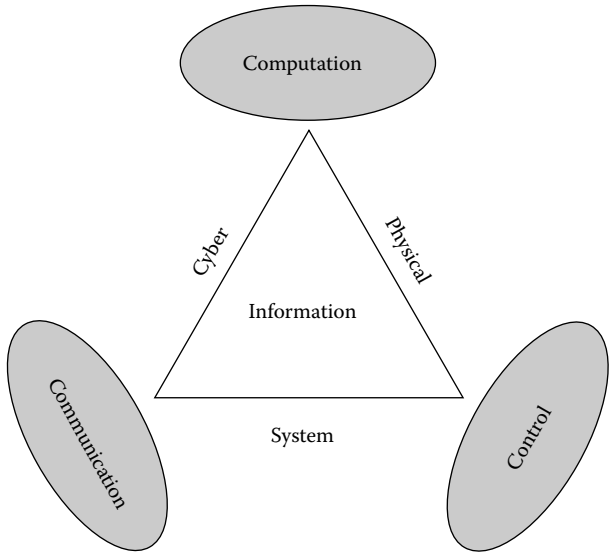

Figure 1.1: Architecture of cyber-physical systems.

Due to the increasing connection of CPS to many safety-critical applications, high risks of cyber attacks by adversaries around the globe have arisen. For example, the future electric power grids, that is, the smart grids, will be the largest and most complex CPS. Since grid operation and communication are mainly through a shared network, such systems are quite vulnerable to cyber-security threats. Any severe attack on the national power grids may have a significant impact on the environment, national economy, or national security or even the loss of human life [25]. Therefore, designing CPS taking into account security issues is of fundamental importance to ensure their safe operation, which has been a hot research area in recent years. Two possible types of attacks on CPS have been studied by Cardenas et al. [10]: denial-of-service (DoS) attacks and deception attacks, which correspond to the traditional security goals of *availability* and *integrity*, respectively. The DoS attack blocks the exchange of information, including sensor measurement data or control inputs, between each part of the CPS, while the integrity attack focuses on the integrity of the data by modifying the data packets. Other works in the literature that have dealt with specific types of attacks include DoS attacks [3, 11, 38, 39], false data injection attacks [23, 24], integrity attacks [27], and replay attacks [26]. Liu et al. [23] studied a new class of attacks on state estimation schemes in electric power grids, namely, false data injection attacks. Given the knowledge of the configuration and parameters of the power system, the attacker can launch such attacks to inject arbitrary errors into certain state variables without triggering the existing bad measurement detection

alarm. Mo and Sinopoli [27] described the CPS model as a discrete linear time-invariant system running a Kalman filter, an LQG controller, and a χ^2 failure detector, which is under integrity attacks. The authors presented a quantitative index of the system resilience by investigating the set of nondetectable adversary's attack strategies and the corresponding state estimation error under certain attacks.

Though some fundamental frameworks have been proposed in existing literature, such as [3, 11, 39], they have focused only on one side, that is, either the attacker or the defender. If attackers have knowledge of system parameters, however, both parties (defender and attacker) will be involved in an interactive decision-making process. Each side chooses the optimal action based on all the information it has, including the understanding and prediction of the actions its opponent may take. To study such a situation, one requires a more comprehensive description of CPS security, which goes beyond a static one-sided analysis. In this chapter, we adopt a game-theoretic approach that provides an alternative way to handle these interactive decision issues.

Game theory is the study of mathematical models of conflict and cooperation between intelligent rational decision makers, that is, interactive decision theory [13]. While game theory was originally used for studying economic systems, it has since developed into a wide range of applications [2, 6, 8]. The work [19] studied the zero-sum game on multiple-input multiple-output (MIMO) Gaussian Rayleigh fading channels where both the jammer and the encoder are subject to power constraints. Gupta et al. [14] considered a dynamic game between a controller for a discrete-time linear time-invariant (LTI) plant and an attacker who could jam the communication between the controller and the plant. The equilibrium control and jamming strategies for both players were provided. The work [30] investigated existing results for enhancing network security under the game-theoretic framework and provided a classification of recent results based on the types of corresponding games. Agah et al. [1] formulated a cooperative game between sensor nodes in mobile wireless sensor networks and showed that through cooperation between two nodes the data communication between them will be more reliable.

In the work described in [21], the communication channels for transmitting system state information from a sensor to a remote controller can be partly jammed by a jammer. Multiple channels can be chosen to avoid the attack. The payoff function of the stochastic game investigated in [21] is in quadratic form, consisting of the weighted sum of the norms of the system state and action vector with discount factors. This objective (also used in [14]) and the assumption of noiseless sensor measurements, however, are not suitable for remote estimation scenarios, where the overall estimation quality is critical with trade-off to the energy constraints. A preliminary version of parts of this chapter (see [22]) investigated the jamming game in CPS, which studied the case where the data packet from the sensor always arrives at the remote estimator successfully without attack

and drops under attack. To better describe the practical communication process, here we consider a more practical communication model that embeds [22] as a special case. Furthermore, as the computational complexity issue for solving the optimal solution is significant in [22], we propose a constraint-relaxed problem formulation and provide corresponding closed-form expressions that significantly reduce the calculation. Note that [14, 21, 22] only investigated the single-sensor case, which is not typical in general CPS, where many applications are dealing with sensor networks. We also consider the jamming game between the attacker and multiple sensors, which is a more interesting and practical challenge in CPS.

The remainder of this chapter is organized as follows. Section 1.2 presents the system model and states the main problem of interest. Section 2.3 presents some game theory preliminaries and studies the optimal strategies for both sides. Section 2.4 provides the dynamic updating algorithm. Section 2.5 provides a constraint-relaxed problem formulation that reduces the computational complexity. The multisensor case is considered in Section 1.6. Section 1.7 draws the conclusions.

Notations: $\mathbb{Z}$ denotes the set of all integers and $\mathbb{N}$ the positive integers. $\mathbb{R}$ is the set of real numbers. $\mathbb{R}^n$ is the n-dimensional Euclidean space. $\mathbb{S}_+^n$ (and $\mathbb{S}_{++}^n$) is the set of $n \times n$ positive semi-definite matrices (and positive definite matrices). When $X \in \mathbb{S}_+^n$ (and $\mathbb{S}_{++}^n$), we write $X \geqslant 0$ (and $X > 0$). $X \geqslant Y$ if $X - Y \in \mathbb{S}_+^n$. $\mathrm{Tr}(\cdot)$ is the trace of a matrix. The superscript $'$ stands for transposition. For functions f, f_1, f_2 with appropriate domains, $f_1 f_2(x)$ stands for the function composition $f_1\big(f_2(x)\big)$, and $f^n(x) \triangleq f\big(f^{n-1}(x)\big)$, where $n \in \mathbb{N}$ and $f^0(x) \triangleq x$. δ_{ij} is the discrete-time Dirac delta function; that is, δ_{ij} equals 1 when $i = j$ and 0 otherwise. The notation $\mathbb{P}[\cdot]$ refers to probability and $\mathbb{E}[\cdot]$ to expectation.

1.2 Problem Setup

Consider a general discrete linear time-invariant (LTI) process of the form

$$x_{k+1} = Ax_k + w_k,$$

$$y_k = Cx_k + v_k,$$

where $k \in \mathbb{N}$, $x_k \in \mathbb{R}^{n_x}$ is the process state vector at time k, $y_k \in \mathbb{R}^{n_y}$ is the measurement taken by the sensor, and $w_k \in \mathbb{R}^{n_x}$ and $v_k \in \mathbb{R}^{n_y}$ are zero-mean independent and identically distributed (i.i.d.) Gaussian noises with $\mathbb{E}[w_k w_j'] = \delta_{kj} Q$ ($Q \geqslant 0$), $\mathbb{E}[v_k v_j'] = \delta_{kj} R$ ($R > 0$), and $\mathbb{E}[w_k v_j'] = 0 \; \forall j, k \in \mathbb{N}$. The initial state x_0 is a zero-mean Gaussian random vector with covariance $\Pi_0 \geqslant 0$ and is uncorrelated with w_k and v_k. The pair (A, C) is assumed to be observable and $(A, Q^{1/2})$ is controllable.

1.2.1 Local State Estimation

Our interest lies in security of remote state estimation as depicted in Figure 1.2. In CPS, sensors are typically equipped with onboard processors [17]. These capabilities can be used to improve system performance significantly. At each time k, the sensor first locally estimates the state x_k based on all the measurements it collects up to time k and then transmits its local estimate to the remote estimator. Denote $\hat{x}_k^s$ and P_k^s as the sensor's local minimum mean-squared error (MMSE) estimate of the state x_k and the corresponding error covariance, which are given by

$$\begin{aligned}\hat{x}_k^s &= \mathbb{E}[x_k|y_1,y_2,...,y_k],\\ \hat{P}_k^s &= \mathbb{E}[(x_k-\hat{x}_k^s)(x_k-\hat{x}_k^s)'|y_1,y_2,...,y_k]\end{aligned}$$

and can be calculated by a Kalman filter as follows:

$$\begin{aligned}\hat{x}_{k|k-1}^s &= A\hat{x}_{k-1}^s,\\ 9K_k^s &= P_{k|k-1}^s C'[CP_{k|k-1}^s C'+R]^{-1},\\ \hat{x}_k^s &= A\hat{x}_{k-1}^s + K_k^s(y_k - C\hat{x}_{k|k-1}^s),\\ P_k^s &= (I-K_k^s C)P_{k|k-1}^s,\end{aligned}$$

where the recursion starts from $\hat{x}_0^s = 0$ and $P_0^s = \Pi_0 \geqslant 0$.

For notational ease, we introduce the functions $h, \tilde{g} : \mathbb{S}_+^n \to \mathbb{S}_+^n$ as

$$\begin{aligned}h(X) &\triangleq AXA' + Q,\\ \tilde{g}(X) &\triangleq X - XC'[CXC'+R]^{-1}CX,\\ h^k(X) &\triangleq \underbrace{h\circ h\circ\cdots\circ h\circ h}_{k \text{ times}}(X).\end{aligned}$$

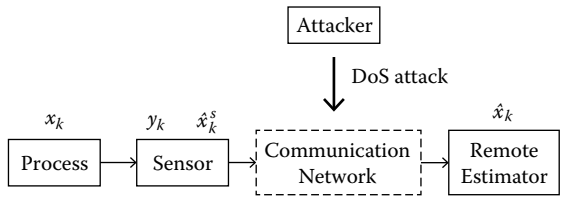

Figure 1.2: The communication network is jammed by a malicious attacker. This affects remote estimation performance.

It is well known that under suitable conditions the estimation error covariance of the Kalman filter converges to a unique value from any initial condition (proved in [36]); thus, the local estimation error covariance P_k^s will converge to a steady state. Without loss of generality (similar assumptions can be found in works such as [22, 32]), we assume that the Kalman filter at the sensor side has entered the steady state and simplify our subsequent discussion by setting

$$P_k^s = \overline{P},\ k \geqslant 1, \tag{1.1}$$

where $\overline{P}$ is the steady-state error covariance given in [36], which is the unique positive semidefinite solution of $\tilde{g} \circ h(X) = X$. For convenience, we also assume that the remote estimator's error covariance is $\overline{P}$ before the process starts, that is,

$$P_0 = \overline{P}. \tag{1.2}$$

The error covariance $\overline{P}$ has the following property:

Lemma 1.1
(see [34].) For $0 \leqslant t_1 \leqslant t_2$, the following inequality holds:

$$h^{t_1}(\overline{P}) \leqslant h^{t_2}(\overline{P}).$$

In addition, if $t_1 < t_2$, then

$$\mathrm{Tr}\left(h^{t_1}(\overline{P})\right) < \mathrm{Tr}\left(h^{t_2}(\overline{P})\right).$$

1.2.2 Communication Channel

Denial-of-service (DoS) attacks are the most reachable attack pattern for the attacker [38] since the communication between sensors and remote estimators in CPS is mainly through a wired or wireless network. Typical DoS attacks can jam the communication between components in CPS and degrade the overall system performance [3, 11, 39]. In this chapter, we assume the attacker to be capable of conducting a DoS attack on the server to jam the communication channel between the sensor and the remote estimator, therefore worsening the system performance (see Figure 1.2).

Energy constraint is a natural concern for both sensors and attackers in practice, which affects the remote estimation performance and attacking policies [5,7,20,29,35]. To encompass energy limitations, we will assume that within a time horizon T, the sensor can send data packets at most $M \leqslant T$ times to the remote estimator, while the attacker can launch jamming attacks at most $N \leqslant T$ times.

Denote

$$\theta_S \triangleq \{\gamma_1, \gamma_2, ..., \gamma_T\} \tag{1.3}$$