

1. Record Nr.	UNISA996465353503316
Autore	Zhu Quanyan
Titolo	Cross-layer design for secure and resilient cyber-physical systems : a decision and game theoretic approach // Quanyan Zhu, Zhiheng Xu
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2020] Â©2020
ISBN	3-030-60251-6
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XVII, 212 p.)
Collana	Advances in Information Security ; ; Volume 81
Disciplina	005.8
Soggetti	Computer networks - Security measures Computer security Cooperating objects (Computer systems)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Part I Motivation and Framework -- 1 Introduction -- 1.1 Cyber-Physical Systems and Smart Cities -- 1.2 New Challenges in CPS -- 1.3 Overview and Related Works -- 1.4 Outline of the book -- 2 Cross-Layer Framework for CPSs -- 2.1 Introduction to Cross-Layer Design -- 2.2 Cross-Layer Design: Connecting Cryptography and Control Theory -- 2.3 Cross-Layer Design: Connecting Game Theory with Control Theory -- 2.4 Cross-Layer Design under Incomplete Information -- 2.5 Conclusions -- Part II Secure Outsourcing Computations of CPS -- 3 New Architecture: Cloud-Enabled CPS -- 3.1 Promising Applications of CE-CPSs -- 3.1.1 Cloud-Enabled Robotics -- 3.1.2 Cloud-Enabled Smart Grids -- 3.1.3 Cloud-Enabled Transport Systems -- 3.1.4 Cloud-Enabled Manufacturing -- 3.2 New Security Requirements of CE-CPSs -- 3.3 Conclusion -- 4 Secure and Resilient Design of Cloud-Enabled CPS -- 4.1 New Challenges and Proposed Solutions of CE-CPS -- 4.2 Problem Statements -- 4.3 System Dynamics and MPC Algorithm -- 4.4 The Standard form of Quadratic Problem -- 4.4.1 Cloud Attack Models -- 4.4.2 The Framework of the proposed mechanism -- 4.5 Confidentiality and Integrity -- 4.5.1 Encryption Methods -- 4.5.2 Verification Methods -- 4.6 Availability Issues -- 4.6.1 Switching Mode Mechanism -- 4.6.2 Buer Mode and Switching Condition -- 4.6.3 The Local Controller for the Safe Mode -- 4 4.7 Analysis and Experiments

-- 4.8 Conclusions and Notes -- 5 Secure Data Assimilation of Cloud Sensor Networks -- 5.1 Introduction to CE-LSNs -- 5.2 Problem Formulation -- 5.2.1 System Model and the Outsourcing Kalman Filter -- 5.2.2 Challenges and Design Objectives -- 5.3 The Secure Outsourcing Data Assimilation -- 5.3.1 The Additive Homomorphic Encryption -- 5.3.2 The Homomorphic Observer -- 5.3.3 Customized Encryption for Outsourcing Computation -- 5.4 Analysis of the Efficiency and Security -- 5.4.1 Efficiency Analysis -- 5.4.2 Security Analysis -- 5.5 Analysis of Quantization Errors -- 5.6 Experimental Results -- 5.6.1 The Output of the Encrypted Information -- 5.6.2 The Impact of the Quantization Errors -- 5.7 Conclusions and Notes -- Part III Game-Theoretic Approach for CPS -- 6 Review of Game Theory -- 6.1 Introduction to Game Theory -- 6.2 Two-Person Zero-Sum Game Model -- 6.2.1 Formulation of the Zero-sum Game -- 6.3 Stackelberg Game Model -- 6.3.1 Formulation of the Stackelberg Game -- 6.3.2 Security Design based on Stackelberg Game -- 6.4 FlipIt Game Model -- 6.4.1 Formulation of FlipIt Game -- 6.4.2 Analysis of the FlipIt Game -- 6.5 Signaling Game with Evidence -- 6.6 Conclusion and Notes -- 7 A Game-Theoretic Approach to Secure Control of 3D Printers -- 7.1 New Challenges in Networked 3D Printers -- 7.2 Problem Formulation -- 7.2.1 The Dynamic Model of 3D Printing Systems -- 7.2.2 Physical Zero-Sum Game Framework -- 7.2.3 A Cyber-Physical Attack Model for 3D-printing Systems -- 7.2.4 The Cyber FlipIt Game Model -- 7.2.5 A Cyber-physical Stackelberg Game Model -- 7.3 Analysis of the Cyber-Physical Games -- 7.3.1 Analysis of the Physical Zero-Sum Game Equilibrium -- 7.3.2 Analysis of the Cyber FlipIt Game Equilibrium -- 7.3.3 Analysis of the Cyber-Physical Stackelberg Game Equilibrium -- 7.4 Numerical Results -- 7.5 Conclusion and Notes -- 8 A Game Framework to Secure Control of CBTC Systems -- 8.1 Introduction to CBTC systems -- 8.2 Problem Formulation -- 8.2.1 The Physical Model of a Train System -- 8.2.2 Communication Model and Attack Model -- 8.3 Estimation Approach and Security Criterion -- 8.3.1 Physical Estimation Problem -- 8.3.2 Security Criterion for CBTC System -- 8.4 The Stochastic Game-Theoretic Framework -- 8.4.1 Cyber Zero-Sum Game -- 8.4.2 Analyzing the Equilibrium of the Game -- 8.4.3 Special Case Study: Two-Channel Game -- 8.4.4 Inter-dependency Between Physical and Cyber Layers -- 8.5 Experimental Results -- 8.5.1 The Results of Cyber Layer -- 8.5.2 The Results of Physical Layer -- 8.6 Conclusions and Notes -- 9 Secure Estimation of CPS with a Digital Twin -- 9.1 Using Digital Twin to Enhance Security Level in CPS -- 9.2 System Modelling and Characterization -- 9.2.1 System Model and Control Problem of a CPS -- 9.2.2 Kalman Filter Problem -- 9.2.3 Stealthy Estimation Attack -- 9.2.4 Digital Twin for the CPS -- 9.2.5 General Setup of Signaling Game with Evidence -- 9.3 Equilibrium Results of the Cyber SGE -- 9.3.1 SGE Setup for the CPSs -- 9.3.2 Best Response of the Players and a PBNE of the SGE -- 9.3.3 Estimated Loss Under the Stealthy Attack -- 9.4 Simulation Results -- 9.4.1 Experimental Setup -- 9.5 Conclusions and Notes -- 10 Introduction to Partially Observed MDPs -- 10.1 Preliminaries of POMDPs -- 10.1.1 Definition of a POMDP -- 10.1.2 Belief State Formulation of a POMDP -- 10.1.3 Stochastic Dynamic Programming -- 10.2 Algorithms for Infinite Horizon POMDPs -- 10.2.1 Piecewise Linear Property of POMDPs -- 10.2.2 Algorithms based on Markov Partition -- 10.3 Conclusions and Notes -- 11 Secure and Resilient Control of ROSs -- 11.1 New Challenges in Networked ROSs -- 11.2 Problem Formulation -- 11.2.1 The Outline of the Proposed Mechanism -- 11.2.2 The Physical Dynamics of a ROS agent -- 11.2.3 Attack Model: Data-Integrity Attack -- 11.2.4 The Lightweight MAC and the Estimated Delay -- 11.2.5

Physical-Aware Design of the Key Length -- 11.2.6 Cyber States and Cyber Actions -- 11.2.7 Stochastic Cyber Markov Decision Process -- 11.3 Cyber POMDP Formulation for ROSs -- 11.3.1 Basic Setups of the Cyber POMDP -- 11.3.2 Main Results of Cyber POMDP -- 11.3.3 Special Case of the Cyber POMDP -- 11.4 Experimental Results -- 11.4.1 Part I: Physical Performance -- 11.4.2 Part II: Cyber Performance -- 11.5 Conclusions and Notes -- Part IV Discussion of the Future Work -- 12 Future Work in Security Design of CPSs -- 12.1 Research Directions: Advanced Attack Models -- 12.1.1 Man-in-the-Middle Attack -- 12.1.2 Compromised-Key Attack -- 12.2 Research Directions: Data-Availability Issues in CPSs -- 12.2.1 Safe-Mode Mechanism -- 12.2.2 Availability of a Partially Compromised System -- 12.3 Conclusions -- Part V Appendix -- A Basics of Optimization -- A.1 Optimality conditions for unconstrained problems -- A.2 Optimality conditions for constrained problems -- B Basics of Linear-Quadratic Optimal Control -- B.1 Finite-Time Optimal Control Problem Formulation -- B.2 Infinite Horizon Optimal Control Problem Formulation -- B.3 Principle of Optimality -- B.4 Finite-Time Linear-Quadratic Optimal Control -- B.5 Infinite-Time Linear-Quadratic Optimal Control -- References -- Index.

---

## Sommario/riassunto

This book introduces a cross-layer design to achieve security and resilience for CPSs (Cyber-Physical Systems). The authors interconnect various technical tools and methods to capture the different properties between cyber and physical layers. Part II of this book bridges the gap between cryptography and control-theoretic tools. It develops a bespoke crypto-control framework to address security and resiliency in control and estimation problems where the outsourcing of computations is possible. Part III of this book bridges the gap between game theory and control theory and develops interdependent impact-aware security defense strategies and cyber-aware resilient control strategies. With the rapid development of smart cities, there is a growing need to integrate the physical systems, ranging from large-scale infrastructures to small embedded systems, with networked communications. The integration of the physical and cyber systems forms Cyber-Physical Systems (CPSs), enabling the use of digital information and control technologies to improve the monitoring, operation, and planning of the systems. Despite these advantages, they are vulnerable to cyber-physical attacks, which aim to damage the physical layer through the cyber network. This book also uses case studies from autonomous systems, communication-based train control systems, cyber manufacturing, and robotic systems to illustrate the proposed methodologies. These case studies aim to motivate readers to adopt a cross-layer system perspective toward security and resilience issues of large and complex systems and develop domain-specific solutions to address CPS challenges. A comprehensive suite of solutions to a broad range of technical challenges in secure and resilient control systems are described in this book (many of the findings in this book are useful to anyone working in cybersecurity). Researchers, professors, and advanced-level students working in computer science and engineering will find this book useful as a reference or secondary text. Industry professionals and military workers interested in cybersecurity will also want to purchase this book.

---