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 Could-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 Condentiality and Integrity -- 4.5.1 Encryption Methods -- 4.5.2 Verication 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

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 Innite Horizon Optimal Control Problem Formulation -- B.3 Principle of Optimality -- B.4 Finite-Time Linear-Quadratic Optimal Control -- B.5 Innite-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.