1. Record Nr. UNINA9910586588603321

Titolo	Security and resilience in cyber-physical systems : detection, estimation and control / / Masoud Abbaszadeh and Ali Zemouche, editors
Pubbl/distr/stampa	Cham, Switzerland : , : Springer Nature Switzerland AG, , [2022] ©2022
ISBN	3-030-97166-X
Descrizione fisica	1 online resource (383 pages)
Disciplina	344.0533
Soggetti	Computer security Cooperating objects (Computer systems)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Contents -- Contributors -- 1 Overview -- 2 Introduction to Cyber-Physical Security and Resilience -- 2.1 Introduction -- 2.2 Cyber-Physical Security and Resilience Functionality Overview -- 2.3 Cyber-Physical Security Versus Adjacent Fields -- 2.3.1 Cyber-Physical Security Versus Cyber-Security -- 2.3.2 Cyber-Physical Security Versus FDII -- 2.3.3 Cyber-Physical Security Versus Prognostics -- 2.4 Attack Detection, Isolation, and Identification -- 2.4.1 Model-Based ADII -- 2.4.2 Data-Driven ADII -- 2.5 Attack Resilience -- 2.6 Resilient Estimation -- 2.6.1 State of the Art on Resilient and Secure Estimation: A Glimpse on Existing Methods -- 2.7 Resilient Control -- 2.7.1 Centralized Secure Control -- 2.7.2 Distributed Secure Control -- 2.7.3 Resource-Aware Secure Control -- References -- 3 Fundamental Stealthiness-Distortion Trade-Offs in Cyber-Physical Systems -- 3.1 Introduction -- 3.2 Preliminaries -- 3.3 Stealthiness-Distortion Trade-Offs and Worst-Case Attacks -- 3.3.1 Open-Loop Dynamical Systems -- 3.3.2 Feedback Control Systems -- 3.4 Simulation -- 3.5 Conclusion -- References -- 4 Predictive Situation Awareness and Anomaly Forecasting in Cyber-Physical Systems -- 4.1 Introduction -- 4.2 Forecasting Framework -- 4.2.1 Digital Twin Simulation Platform -- 4.2.2 Anomaly Forecasting Approaches -- 4.2.3 Dimensionality Reduction -- 4.2.4 Forecasting Process -- 4.2.5 Feature Discovery -- 4.3 Ensemble Forecasting --

Recovery-Based Approaches -- 10.1 Introduction -- 10.2 Mathematical Modeling -- 10.2.1 Problem Statement -- 10.3 Preliminary: Sparse Recovering Algorithm -- 10.4 Attack Reconstruction When the Number of Potential Attacks is Greater Than the Number of Sensors -- 10.4.1 System Transformation.
10.4.2 Attack Reconstruction -- 10.5 Attack Reconstruction When the Number of Sensors is Greater Than the Number of Potential Sensor Attacks -- 10.5.1 State Attack Reconstruction -- 10.5.2 Sensor Attacks Reconstruction -- 10.6 Case Study: Cyber Attack Reconstruction in the US Western Electricity Coordinating Council Power System -- 10.6.1 Mathematical Model of Electrical Power Network -- 10.6.2 Transformation of DAE to ODE -- 10.6.3 Parameterization of Mathematical Model of Western Electricity Coordinating Council Power System -- 10.6.4 Reconstruction of Attacks via Sparse Recovery Algorithm: The Number of Potential Attacks is Greater Than the Number of Sensors -- 10.6.5 Reconstruction of Attacks and Estimation of States: The Number of Sensors is Greater Than the Number of Potential Sensor Attacks -- 10.7 Conclusions -- References -- 11 Resilient Cooperative Control of Input Constrained Networked Cyber-Physical Systems -- 11.1 Introduction -- 11.1.1 Notation -- 11.1.2 Preliminaries on Algebraic Graph Theory -- 11.1.3 Preliminaries on Finite-Time Stability -- 11.2 Input Constrained Robust Consensus Tracking for High-Order NCPS -- 11.2.1 Problem Formulation -- 11.2.2 Input Constrained Robust Consensus Tracking with a Static Leader -- 11.2.3 Input Constrained Robust Consensus Tracking with a Dynamic Leader -- 11.2.4 Output-Based Input Constrained Robust Consensus Tracking -- 11.3 Input Constrained Robust Finite-Time Consensus Tracking for High-Order NCPS -- 11.3.1 Problem Formulation -- 11.3.2 Input Constrained Robust Finite-Time Consensus Tracking with Relative State Measurements -- 11.3.3 Input Constrained Robust Finite-Time Consensus Tracking with Relative Output Measurements -- 11.4 Numerical Examples -- 11.4.1 Input Constrained Robust Consensus Tracking for High-Order NCPS.
11.4.2 Input Constrained Robust Finite-Time Consensus Tracking for High-Order NCPS -- 11.5 Conclusions -- References -- 12 Optimal Subsystem Decomposition and Resilient Distributed State Estimation for Wastewater Treatment Plants -- 12.1 Introduction -- 12.2 Model Description of Wastewater Treatment Plants -- 12.3 Subsystem Decomposition -- 12.4 Resilient Distributed State Estimator Design -- 12.5 Simulation -- 12.5.1 Subsystem Decomposition -- 12.5.2 Resilient Distributed State Estimator Design -- 12.6 Conclusion -- References -- 13 Cyber-Attack Detection for a Crude Oil Distillation Column -- 13.1 Introduction -- 13.1.1 Preliminary -- 13.1.2 Cyber-Security of Distillation Column -- 13.2 Distillation Column Design and Modeling -- 13.2.1 Plant Data -- 13.2.2 Distillation Column Design -- 13.2.3 Dynamic Model of the Distillation Column -- 13.2.4 Control of Distillation Column -- 13.3 Testbed Design -- 13.4 Attack Modeling -- 13.5 Attack Detection Algorithm -- 13.5.1 UKF Based Attack Detection -- 13.5.2 Detector Design -- 13.6 Results -- 13.6.1 Attack on Distillate Purity Measurement -- 13.6.2 Attack on Bottoms Impurity Measurement -- 13.6.3 Attack on Reflux Flow Rate -- 13.6.4 Attack Case Summary -- 13.7 Conclusion and Future Work -- References -- 14 A Resilient Nonlinear Observer for Light-Emitting Diode Optical Wireless Communication Under Actuator Fault and Noise Jamming -- 14.1 Introduction -- 14.2 LED-Based Optical Channel Modeling -- 14.2.1 System Setup -- 14.2.2 Luminous Flux Model -- 14.2.3 Model Calibration -- 14.2.4 State-Space and Output Measurement Equations -- 14.3 LED System Model Representation Under Actuator Fault and

Noise Jamming Attack -- 14.4 Resilient Observer-Based Tracking Control Design -- 14.4.1 Problem Formulation -- 14.4.2 Unknown Input Observer Design Method -- 14.4.3 Feasibility of (14.24) for Non-monotonic Outputs.
14.4.4 A Switched-Gain-Based Observer Solution.