Chapter 1
Overview

Masoud Abbaszadeh and Ali Zemouche

The increasing sophistication and severity of intelligently designed cyber-attacks warrants new theoretical and technological developments beyond current detection, estimation, and control methodologies. On the other hand, cyber-physical systems are dramatically changing, incorporating new elements such as the Internet of Things (IoT) connectivity and distributed intelligence into the perspective. This transformation further expands the digital footprint of these systems, hence making them susceptible to cyber-attacks and other safety and security issues. Advanced targeted attacks against control systems have increased in the past years with evidence of high risks related to zero-day and replay attacks. In order to tackle this threat, we need advances in detection, feedback control, and estimation with built-in resilience to cyber-attacks, to maintain system integrity and reliability at all times, by providing uninterrupted, equipment-safe, and controlled operation.

This book is intended to cover some of the latest theory and technology advancements for detection and protection against cyber-attacks in cyber-physical systems. This is a very important emerging field and a very active multidisciplinary research and technology development area. The book covers some of the latest problems and research on cyber-physical security and resilience, and highlights active research directions and solutions that are currently pursued in academia and industry. The topics comprise of a blend of new theoretical results on resilient estimation and control combined with machine learning techniques, as well as important application areas such as industrial control systems, power generation and distribution,

M. Abbaszadeh (✉)
GE Research, Niskayuna, NY, USA
e-mail: masoud@ualberta.net

A. Zemouche
CRAN CNR-UMR 7039, IUT Henri Poincaré de Longwy, Université de Lorraine, Cosnes-et-Romain, France
e-mail: ali.zemouche@univ-lorraine.fr

M. Abbaszadeh and A. Zemouche (eds.), *Security and Resilience in Cyber-Physical Systems*, https://doi.org/10.1007/978-3-030-97166-3_1

autonomous systems, wireless communication networks, and chemical plants. The book comprises of a collection of chapters from well-known researchers in academia, and industrial research labs providing a comprehensive perspective of some of the latest advancements and prospects of cyber-physical security and resilience.

The book is structured as follows. It starts with an introductory chapter on cyber-physical security and resilience (Chap. 2), and continues with chapters containing theoretical results on attack detection and situational awareness, resilient estimation, and control, with case studies on power generation, transmission and distribution, sensor networks, cooperative tracking, and autonomous vehicles (Chaps. 3–11). Then, it moves to application-oriented chapters on wastewater treatment plants, oil refinery, and wireless communication networks (Chaps. 12–14). A fundamental trade-off study of stealthiness–distortion is offered in Chap. 3. This is an important topic and sets foundations for future work in this emerging space. Chapter 4 is dedicated to predictive situational awareness in which an anomaly detection and forecasting framework is proposed, combining elements from estimation theory and machine learning. Chapter 5 provides a resilient observer design solution using a concurrent learning approach, while a framework for detection of advanced persistent threats is presented in Chap. 6. Chapters 7–10 are focused on secure and resilient estimation from different perspectives. Chapter 7 addresses the resilient state estimation and attack mitigation problems for switched linear systems with stochastic and set-membership uncertainties. Chapter 8 is on state and attack estimation for nonlinear fuzzy systems with delayed measurements. Chapter 9 establishes the notion of secure estimation under imperfect attack detection and isolation decisions and studies the fundamental couplings between those decisions and the estimation problem, characterizing closed-form decision rules. Chapter 10, addresses cyber-attack reconstruction using higher-order sliding mode observers and sparse recovery methods. Chapter 11 is on resilient cooperative control over networks to achieve consensus tracking under input constraints and communication restraints. Chapter 12 is on resilient distributed estimation, addressing the resilience of wastewater treatment plants against natural disasters. A distributed attack detection algorithm is proposed in Chap. 13 for crude oil distillation columns. Chapter 14 is on resilient estimation in optical wireless communication networks for cooperative robot autonomy under actuator faults and noise jamming. The titles and abstracts of the chapters are in the following.

Chapter 2. Introduction to Cyber-Physical Security and Resilience: This chapter describes the fundamentals of the cyber-physical security and resilience approaches as well as some of the current research directions, and provides a survey of latest results in attack detection, isolation, resilient estimation and resilient control. It also makes distinctions between cyber-physical security versus adjoining and seemingly related applications such as fault detection, and data communications and network security (a.k.a, cyber-security).

Chapter 3. Fundamental Stealthiness–Distortion Tradeoffs in Cyber-Physical Systems: In this chapter, we analyze the fundamental stealthiness–distortion tradeoffs of linear Gaussian open-loop dynamical systems and (closed-loop) feedback control systems under data injection attacks using a power spectral analysis,, whereas the Kullback–Leibler (KL) divergence is employed as the stealthiness measure. Par-

ticularly, we obtain explicit formulas in terms of power spectra that characterize analytically the stealthiness–distortion trade-offs as well as the properties of the worst-case attacks. Furthermore, it is seen in general that the attacker only needs to know the input–output behaviors of the systems in order to carry out the worst-case attacks.

Chapter 4. Predictive Situation Awareness and Anomaly Forecasting in Cyber-Physical Systems: A new feature-based situation awareness and forecasting framework is presented for rapid detection and early warning of abnormalities in cyber-physical systems. The abnormalities may refer to intelligent cyber-attacks or naturally occurring faults and failures. Techniques presented here are aimed at protecting against unauthorized intrusions as well as fault prevention. Time series signals from system monitoring nodes are converted to features using feature discovery techniques. The feature behavior for each monitoring node is characterized in the form of decision boundaries, separating normal and abnormal space with operating data collected from the plant or by running virtual models of the plant. A set of ensemble state-space models are constructed for representing feature evolution in time domain, where the ensembles are selected using Gaussian Mixture Model (GMM) clustering. The forecasted outputs are anticipated time evolution of features, computed by applying an adaptive Kalman predictor to each ensemble model. The overall features forecast is then obtained through dynamic ensemble averaging. This is done by projecting evolution of feature vector to future times. This projection can be performed either in a receding horizon or a committed horizon fashion. The feature forecasts are compared to the decision boundary to estimate if/when the feature vectors will cross the boundary. The decision boundary is a high-dimensional manifold in the feature space learned by a neural network. The training of the neural network is based on labeled data provided either through simulation of the system digital twin or by capturing historical field data. In this chapter, we also establish a framework for situation awareness, discussing the different components to achieve full situation awareness and showing the interactions between the attack detection, isolation, and prediction modules at the system level. Simulation results in a high-fidelity GE gas turbine platform show the effectiveness of our approach for forecasting abnormalities, which can be used for protecting physical assets from abnormalities due to cyber-intrusion or natural faults.

Chapter 5. Resilient Observer Design for Cyber-Physical Systems with Data-Driven Measurement Pruning: Resilient observer design for Cyber-Physical Systems (CPS) in the presence of adversarial false data injection attacks (FDIA) is an active area of research. Existing state-of-the-art algorithms tend to break down as more and more knowledge of the system is built into the attack model; also as the percentage of attacked nodes increases. From the view of optimization theory, the problem is often cast as a classical error correction problem for which a theoretical limit of 50% has been established as the maximum percentage attacked nodes for which state recovery is guaranteed. Beyond this limit, the performance of ℓ_1-minimization-based schemes, for instance, deteriorates rapidly. Similar performance degradation occurs for other types of resilient observers beyond certain percentages of attacked nodes. In order to increase the corresponding percentage of attacked nodes for which state

recoveries can be guaranteed, researchers have begun to incorporate prior information into the underlying resilient observer design framework. For the most pragmatic cases, this prior information is often obtained through a data-driven machine learning process. Existing results have shown a strong positive correlation between the maximum attacked percentages that can be tolerated and the accuracy of the data-driven model. Motivated by these results, this chapter examines the case for *pruning algorithms* designed to improve the *Positive Prediction Value* (PPV) of the resulting prior information, given stochastic uncertainty characteristics of the underlying machine learning model. Theoretical quantification of the achievable improvement is given. Simulation results show that the pruning algorithm significantly increases the maximum correctable percentage of attacked nodes, even for machine learning model whose prediction power is comparable to the random flip of a coin.

Chapter 6. Framework for Detecting APTs Based on Steps Analysis and Correlation: An advanced persistent threat, (APT), is an attack that uses multiple attack behavior to penetrate a system, to achieve specifically targeted and highly valuable goals within a system. This type of attack has presented an increasing concern for cyber-security and business continuity. The resource availability, integrity, and confidentiality of the operational cyber-physical systems' (CPS) state and control are highly impacted by the safety and security measures adopted. In this study, we propose a framework based on deep APT steps analysis and correlation, abbreviated as "APT-DASAC", for securing industrial control systems (ICSs) against APTs. This approach takes into consideration the distributed and multi-level nature of ICS architecture, and reflects on multi-step APT attack lifecycle. We validated the framework with three case studies: (i) network transactions between a remote terminal unit (RTU) and a master control unit (MTU) within a supervisory control and data acquisition (SCADA) gas pipeline control system, (ii) a case study of command and response injection attacks, and (iii) a scenario based on network traffic containing hybrid of the real modern normal and the contemporary synthesized attack activities of the network traffic. Based on the achieved result, we show that the proposed approach achieves a significant attacks detection capability and demonstrates that attack detection techniques that performed very well in one application domain may not yield the same result in another. Hence, robustness and resilience of operational CPS state or any system and performance are determined by the security measures in place, which is specific to the application system and domain.

Chapter 7. Resilient State Estimation and Attack Mitigation in Cyber-Physical Systems: Smart and Cyber-Physical Systems (CPS), e.g., power and traffic networks and smart homes, are becoming increasingly ubiquitous as they offer new opportunities for improved performance and functionalities. However, these often safety-critical systems have also recently become the target of cyber- or physical attacks. This chapter contributes to the area of CPS security from the perspective of leveraging the knowledge of physical system dynamics as an additional "sensor" to mitigate the effects of false data injection attacks on actuator and sensor signals as well as attacks on the switching mechanisms, e.g., circuit breakers, on the state estimation and control algorithms in these systems, in order to ensure continued safety, reliability and integrity of systems despite attacks. Specifically, we consider

physical models with switched linear dynamics subject to two classes of uncertainties: (a) stochastic uncertainty (aleatoric), i.e., with (unbounded) stochastic process and measurement noise signals and (b) set-membership uncertainty (epistemic), i.e., with distribution-free bounded-norm process and measurement disturbances. In both settings, we model the system under attack as a hidden-mode switched linear system with unknown inputs (attacks) and propose multiple-model inference algorithms to perform attack-resilient state estimation with stability and optimality guarantees. Moreover, we characterize fundamental limitations to resilient state estimation (e.g., upper bound on the number of tolerable signal attacks) and discuss the topics of attack detection, identification, and mitigation under this framework. Simulation examples of switching and false data injection attacks on a benchmark system and an IEEE 68-bus test system show the efficacy of our approach to recover resilient state estimates as well as to identify and mitigate the attacks in the presence of stochastic and set-membership uncertainties.

Chapter 8. State and Attacks Estimation for Nonlinear Takagi–Sugeno Multiple Models Systems with Delayed Measurements: In the following contribution, a state and attacks estimation for nonlinear Takagi–Sugeno Systems with variable time-delay measurements is proposed. Based on the sector nonlinearity approach, sufficient conditions in term of Linear Matrix Inequalities ($LMIs$) formulation are given for the observer design. It is demonstrated that, despite the presence of cyber-attack (i.e., data deception attacks on both actuators and sensors), and the delayed measurements, the proposed observer is quite efficient and ensures the asymptotic convergence of the estimation errors with an $\mathscr{L}_2$ attenuation constraint.

Chapter 9. Secure Estimation under Model Uncertainty: The increasing scale and widespread deployment of cyber-physical systems for novel applications leave them vulnerable to malicious intrusions and potential failures. Therefore, the performance of a cyber-physical system hinges on both the successful detection and elimination of malicious behavior. More importantly, the robustness of inference algorithms in making high-quality inference decisions even under active malicious behaviors is instrumental to making reliable decisions. This chapter focuses on the robustness of state estimates in complex networks . In such systems, state estimation is the key inference task at the core of monitoring and decision-making. One key challenge when facing malicious attacks is uncertainty in the true underlying statistical model of the data collected. Such uncertainty can be an outcome of a variety of adversarial behaviors, such as false data injection attacks, denial of service (DoS) attacks, and causative attacks . In all such scenarios, the estimation algorithms operate under a distorted statistical model with respect to what they expect. Therefore, forming estimates under malicious attacks involves an additional decision pertinent to the presence of an attack and isolating the true statistical model. This chapter introduces new notions of secure estimation under the knowledge that imperfect detection and isolation decisions induce a coupling between the desired estimation performance and the auxiliary necessary detection and isolation decisions. The fundamental interplay among the different decisions involved is established and closed-form decision rules are provided.

Chapter 10. Resilient Control of Nonlinear Cyber-Physical Systems: Higher-Order Sliding Mode Differentiation and Sparse Recovery-based Approaches: In this chapter, we focus on a cyber-attack reconstruction and secure state estimation to facilitate the resilient control of nonlinear cyber-physical systems under sensor and/or actuator attacks. The Sliding Mode Observation/Differentiation (SMO/D) techniques, which can handle systems of arbitrary relative degree perturbed by bounded attacks of arbitrary shape, are used for online reconstruction of the attacks and secure state estimation in CPSs under attacks. The Sparse Recovery (SR) algorithm is also employed to reconstruct the stealth sensor attacks to the unprotected sensors. Next, the corrupted measurements and states are to be cleaned up online in order to prevent the attack propagation to the CPS via the feedback control signal. The case study based on the US Western Electricity Coordinating Council (WECC) power network under attack is considered. The power network performance degradation as a result of cyber-attacks to actuators and/or sensors is observed. The proposed SMO/D and SR algorithms and methodologies are applied to recover the performance of the attacked WECC power network. Simulation results illustrate the efficacy of the proposed approaches.

Chapter 11. Resilient Cooperative Control of Input Constrained Networked Cyber-Physical Systems: This chapter mainly studies the resilient cooperative control methods for Networked Cyber-Physical Systems (NCPS) subject to input saturation constraints. First, input constrained asymptotic consensus tracking problems for high-order triangular form NCPS are investigated. Sliding mode control methods are employed to achieve robust consensus tracking under input saturation and bounded input disturbances. Both the cases of static leader and dynamic leader are considered. Observer-based distributed controllers are further designed to reduce the relative state measurement requirement between the systems. Then, input constrained robust finite-time consensus tracking problems for high-order triangular form NCPS are studied. A switching control strategy is proposed which is shown to achieve consensus tracking in finite time under the input saturation constraint. Both the cases with relative state measurement and only relative output measurement are handled. The proposed control strategies are novel in that they are resilient to both the control input constraints, the unknown external disturbances and the possible digital communication restraints. Numerical simulation is performed and an application to the vehicle platoon control problem is given to illustrate the effectiveness of the proposed control strategies.

Chapter 12. Optimal Subsystem Decomposition and Resilient Distributed State Estimation for Wastewater Treatment Plants: In this work, an optimal subsystem decomposition algorithm is proposed based on the community discovery algorithm with weighted network graph and is applied to a benchmark wastewater treatment plants (WWTP) system. With the obtained subsystems, a resilient distributed state estimation method is further investigated to deal with the natural disasters (storm and rain) and the unreliable communication networks. The nodes of information graph theory are introduced to represent the state, input and output variables of the WWTP system. By defining a sensitivity of an edge, a weighted directed graph of WWTP system is constructed. The nodes are connected by weighted edges

with the weight reflecting the strength of the connection between nodes. The weighted network graph can reflect both the connectivity and connection strength of the system. The community structure discovery algorithm is used to divide all variables into subsystem groups, such that the interaction between groups is strong. Then, the subsystem decomposition of complex process system is obtained. The optimal subsystem decomposition method is validated by designing a resilient distributed state estimation for WWTP system with unreliable communication networks. An information compensation strategy is proposed to coordinate the sub-estimators. Comparative study is carried out for the subsystem decomposition by physical structure and unweighted network-based method. The results show that the subsystem decomposition and distributed state estimation scheme improves the resiliency of the system, compared to a centralized scheme applied to the whole system.

Chapter 13. Cyber-Attack Detection for a Crude Oil Distillation Column: Industrial control systems are recently being interfaced to the cyber-domain as computing, communication, and electronics technologies continue to evolve giving rise to what is known as Cyber-Physical Systems (CPSs). Integration of cyber-domain makes these plants vulnerable to cyber-threats and hence it is indispensable to address the cyber-security of these systems. The huge worldwide demand for crude oil can make them a lucrative target for cyber-intrusions. In this chapter, a continuous binary Distillation Column (DC) plant is considered as a CPS and a distributed attack detection algorithm is proposed to enhance its security. In order to demonstrate the real-time performance of attack detection algorithm, a hybrid Hardware-In-the-Loop (HIL) testbed is developed where the DC plant is simulated in real time inside PC and the controllers as well as the detection algorithms are implemented inside Siemens PLC. Finally, the real-time performance of the developed attack detection algorithm is validated through several attack scenarios.

Chapter 14. A Resilient Nonlinear Observer for Light-Emitting Diode Optical Wireless Communication under Actuator Fault and Noise Jamming: Optical wireless communication is emerging as a low-power, low-cost, and high data rate alternative to acoustic and radio-frequency communications in several short to medium-range applications. However, it requires a close-to-line-of-sight link between the transmitter and the receiver. Indeed, a severe misalignment can lead to intolerable signal fades and can significantly degrade system performance. Despite recent efforts to establish a line-of-sight (LOS) between transmitter and receiver by improving system designs and active alignment, maintaining a perfect LOS between the two sides despite the robot's mobility remain a challenging task for cooperative autonomy. On the other hand, the optical wireless communication system is often hampered by noise jamming on the optical communication channel that reduces the system capacity of the wireless optical mobile networks. Additionally, a situation of an occurrence of actuator failures can occur due to malfunctions or high instantaneous torques of the actuator mechanism flexible on the receiver orientation. To address this problem, we propose a novel extended state switched-gain discrete-time nonlinear observer to simultaneously estimate the actuator fault and the optical communication system's state variables subject to noise jamming attack. Furthermore, Lyapunov function-based analysis is used to design the proposed unknown switched-gain input

observer in each piecewise monotonic region of the optical communication model output functions and ensures global stability of the extended error system. Numerical simulation results are then provided to demonstrate the validity and effectiveness of the proposed extended switched-gain state observer subject to noise jamming attack on the optical communication link.