Chapter 2
Introduction to Cyber-Physical Security and Resilience

Masoud Abbaszadeh and Ali Zemouche

2.1 Introduction

Motivated by increasing demand for performance, availability, efficiency, and resilience, several sectors including energy, manufacturing, healthcare, and transportation have adopted latest advances in controls, automation, communications, and monitoring in the past decades, moving towards semi-autonomous or fully autonomous systems in some cases. The resulting integration of information, control, communication, and computation with physical systems, demands new methodologies for detailed systematic and modular analysis and synthesis of Cyber-Physical Systems (CPSs) as a means to realize the desired performance metrics of efficiency, sustainability, and safety (Dibaji et al. 2019). However, CPSs suffer from extendable vulnerabilities that are beyond classical networked systems due to the tight integration of cyber- and physical components. Sophisticated and malicious cyber-attacks continue to emerge to adversely impact CPS operation, resulting in performance degradation, service interruption, and system failure. Cyber-physical security provides a new line of defense at the physical domain layer (i.e., the process level) in addition to the network Information Technology (IT) and higher level Operational Technology (OT) solutions.

In the past few years, there has been tremendous research and development efforts in cyber-physical security and resilience. The forefront of these efforts is to develop theory and technology to detect and localize cyber-attacks, identify attack types, estimate, and reconstruct attacks, and to perform secure estimation and control under

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

A. Zemouche
CRAN - Nancy Automatic Research Center IUT Henri Poincaré de Longwy, University of Lorraine, Nancy, 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_2

attack. To this end, a variety of results have been proposed based on both model-based and data-driven methodologies (Abbaszadeh et al. 2018; Akowuah and Kong 2021; Alguttar et al. 2020; AlZubi et al. 2021; Ameli et al. 2018; An and Yang 2020; Ao et al. 2016; Azzam et al. 2021; Baniamerian et al. 2019; Brentan et al. 2017; Buason et al. 2019; Cao et al. 2020; Chen et al. 2021, 2016; Cómbita et al. 2020; Dibaji et al. 2018; Ding et al. 2020a, b, 2021, 2018; Dutta et al. 2021; Fang et al. 2020; Farivar et al. 2019; Ferrari and Teixeira 2017; Fillatre et al. 2017; Giraldo et al. 2018; Gu et al. 2020; Guan and Ge 2017; Han et al. 2021; Hendrickx et al. 2014; Housh and Ohar 2018; Humayed and Luo 2015; Humayed et al. 2017; Iwendi et al. 2021; Jahromi et al. 2021, 2019; Junejo and Goh 2016; Khan et al. 2020; Kim et al. 2021; Kozik et al. 2018; Krishnamurthy et al. 2014; Kumar et al. 2022; Lee et al. 2014; Li et al. 2021a, b, 2020; Loukas et al. 2019; Mestha et al. 2017; Narayanan et al. 2021; Noorizadeh et al. 2021; Olowononi et al. 2020; Orumwense and Abo-Al-Ez 2019; Paredes et al. 2021; Park et al. 2015, 2019; Pasqualetti et al. 2013; Pirani et al. 2021; Roy and Dey 2021; Sahoo et al. 2018; Semwal 2021; Shin et al. 2017; Su et al. 2020; Taheri et al. 2020; Tan et al. 2020; Teixeira et al. 2015; Tian et al. 2020; Tiwari et al. 2021; Tsiami and Makropoulos 2021; Valencia et al. 2019; Wang et al. 2021a, b, 2020; Wu et al. 2021; Xiong and Wu 2020; Yan et al. 2018, 2019; Ye et al. 2020; Zhang et al. 2021a, b, c, d, 2017; Zhang and Zhu 2020; Zhu et al. 2018).

Cyber-physical security technologies leverage dynamic models of the closed-loop control systems through utilization of first-principle or data-driven (e.g., system identification-based) modeling paradigms. This, in addition to utilizing historical operational data, enables realistic simulations of attack and fault scenarios, which, compared to normal operation data, are usually rare in the field. This in turn, enables utilization of both model-based and data-driven detectors, and in terms of data-driven detectors, enables exploiting both supervised and unsupervised machine learning approaches.

2.2 Cyber-Physical Security and Resilience Functionality Overview

Cyber-physical security and resilience generally consists of the following functionality modules:

- **Detection:** Determines if an attack has happened.
- **Isolation:** Determines what is under attack, in terms of sensor, actuator, or control nodes. It may also provide foundations for early warning generation at the system/subsystem/component level.
- **Identification:** Determines severity and impact of the attack (including attack type and magnitude), and backtracks the attack to find its source through attack forensics. It may also separate the source of the abnormality and distinguishes malicious attacks from naturally occurring faults/failures.

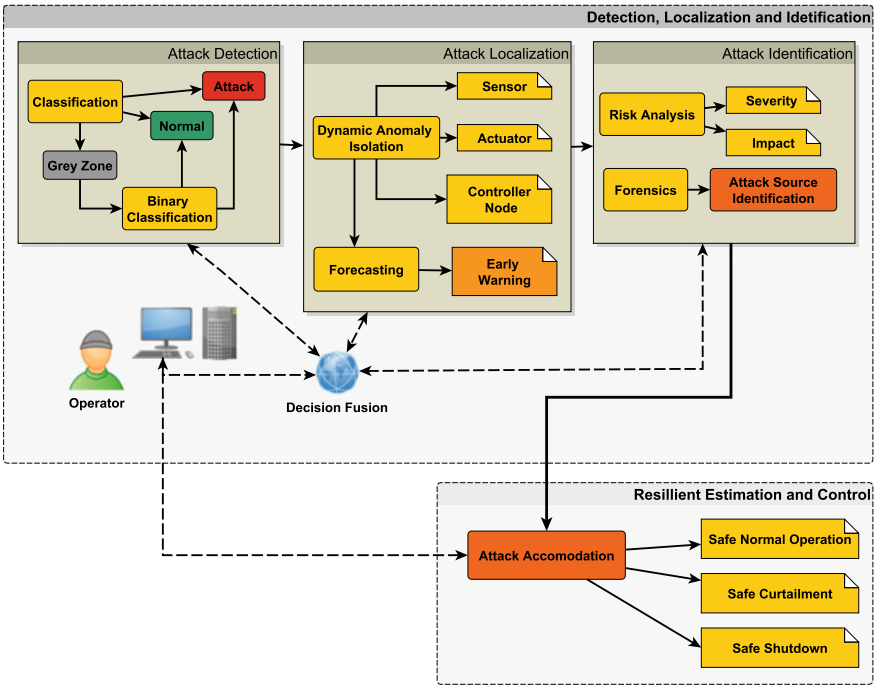

Fig. 2.1 Cyber-physical security & resilience functionality diagram

- **Resilience:** Maintains the integrity, operability, and availability of the system by accommodating (mitigating) the attack through resilient estimation and control, with/without a degraded performance (i.e., curtailment); or commands a controlled safe shutdown.

Figure 2.1 shows an example of a cyber-physical security system functionality diagram with modules as described above. The detection (and isolation) decisions may be made in one shot or in a two-step process, in which a second decision algorithm resolves the gray zones in the first decision. The system may be completely autonomous or with a human in the loop, in which case the operator may be in the loop for the whole process with the ability to override machine-made decisions. The system may also provide visual and/or textual status reports to the operator in real time through security user interfaces such as a Security Information and Event Management (SIEM) dashboard. Furthermore, to increase the decisions accuracy and speed, the detection and isolation decisions may be taken in parallel and fused with potential input from the operator.

Cyber-physical security goes beyond cyber-security, as it can provide an additional layer of defence. Attack neutralization through resilient estimation and control, helps providing the system with capabilities to overcome damage and continue operation when sensors or control signals are disrupted by adversarial threats.

Development of a cyber-physical security technology should follow a design philosophy that includes three main aspects:

1. ***Scalability:*** This is itself two-fold (a) to be organically expandable to large-scale systems, and (b) to be applicable to horizontal and cross-domain applications with reasonable system modeling/dataset generation, while the core algorithms and architecture remaining domain-agnostic.
2. ***Robustness:*** Ability to perform in high performance (in terms of requirements such as false positive and false negative rates, speed of detection, etc.) in the presence of model uncertainty, data value and label uncertainty, as well as system's operational and configuration/manufacturing variations.
3. ***Coherence:*** Having a unified architecture with modularity and flexibility to identify essential and optional modules and to fit into different application domains.

2.3 Cyber-Physical Security Versus Adjacent Fields

From the security perspective, cyber-physical security provides a new layer of defence against cyber-attacks, complementing the existing defence in the IT and higher level OT network security, and increasing the overall security posture of systems via a defence-in-depth strategy (Mosteiro-Sanchez et al. 2020). The focus of cyber-physical security is on the impact of the attack on the physical behavior of the system as opposed to monitoring data communications and network traffic. Furthermore, the attack resilience capability maintains safe operation and/or prevents system damage even at the presence of attacks which may go stealthy and undetected by the IT/OT network-layer security solutions. This increases the availability and integrity of the systems under protection.

2.3.1 Cyber-Physical Security Versus Cyber-Security

Although sounding similar, there are important distinctions between cyber-security and cyber-physical security. The IT layer cyber-security is concerned with data authenticity and integrity. Cyber-physical security, on the other hand, addresses the availability and reliability, in addition to the IT layer, and maintains system operability in an operational technology (OT) environment, at the *physical layer*. Therefore, mere access control, for example, does not help in the OT layer, e.g., the industrial communication bus in Supervisory Control, Data Acquisition (SCADA) systems or Distributed Control Systems (DCS), and physical layers. For example, in a data-only IT layer, it is possible to log out users or prevent their access to the network, but in the OT layer, operators should never be log out of the system during an emergency. Cyber-physical security complements IT and higher level OT cyber-security. While cyber-security tries to prevent a cyber-attack from happening at the first place,

cyber-physical security comes into play when an attacker has already bypassed the IT and higher level OT layers, and thus, an attack has already happened. Furthermore, a cyber-security solution detects an attack through anomalous activities in a communication data network, while cyber-physical security detects an attack by analyzing its impact on the physical behavior of the system. Additionally, cyber-security detects network attacks only, while cyber-physical security, due to its interaction with the physical world, can also detect physical attacks. Finally, cyber-security is often based on static analyses (in terms of system dynamics), while cyber-physical security is essentially based on physical dynamics of the system.

2.3.2 Cyber-Physical Security Versus FDII

A fault is a natural cause, while a cyber-attack is a malicious cause, often intelligently designed and targeted towards specific aspect(s) of a system. A fault is due to a component/system natural malfunction. Therefore, it is highly unlikely that multiple independent and unrelated faults happen simultaneously. A multi-fault scenario is most often a cascaded event started by a single fault. Fault Detection, Isolation, and Identification (FDII) methods cannot detect and isolate multiple simultaneous uncorrelated faults. A cyber-attack on the other hand, is artificially designed and can target multiple places of a system or even multiple systems as the same time without any system relations. Faults usually happen in the sensors, actuators, or some other hardware nodes, while a cyber-attack may happen in any hardware (e.g., sensor or actuator) or software (e.g., inside controller) node. Software faults are rare, especially in a certified code. For example, the probability of a software fault in an airworthy code certified by DO-178 aviation standard is less than 10^{-6} (RTCA 2011). There is yet no certification against a cyber-attack. FDI often works against a pre-determined set of system faults, identified through tools such as fault tree analysis (FTA) or Failure Mode and Effect Analysis (FMEA). A cyber-attack can very much go beyond specified or even known system faults. A cyber-attack can target or randomly activate a vulnerability even unknown to the system designers. Furthermore, FDI cannot detect stealthy attacks that keep the monitored signals within normal operational ranges.

2.3.3 Cyber-Physical Security Versus Prognostics

Prognostics concerns aspects like system ageing, estimation of the remaining useful life (RUL), life optimization, condition monitoring, and condition-based maintenance. These are all categorized under industrial asset performance management (APM). Prognostics provides a solution to the APM problem, which is quite different from what cyber-physical security is all about. Due to its mission, prognostics happens at time scales much slower than what is needed for cyber-physical security. Fast

response at the sampling rate of a real-time controller, as needed in cyber-physical security and resilience, is simply out of scope for prognostics. As a result, prognostics often uses steady-state or quasi-steady-state models. Cyber-physical security, on the other hand, often requires dynamic models of higher fidelity. In summary, prognostics is often a tool for gaining more financial benefit from an existing asset that would operate otherwise, anyway. However, cyber-physical security and resilience is about maintaining system operability at the first place, and therefore must enable the system to withstand and respond to existential threats.

2.4 Attack Detection, Isolation, and Identification

In this section, we provide a survey of some of the main and latest results on cyber-attack detection, isolation, and identification for cyber-physical systems.

A generic CPS architecture by considering the applications related to secure industrial control system (ICS) to explain the cyber resilience concepts is illustrated in Fig. 2.2, which is from the US DHS ICS-CERT recommended practice for defense-in-depth strategies (Dakhnovich et al. 2019; Homeland Security 2014), and based on the Purdue five-level model (Dakhnovich et al. 2019). An ICS is a set of electronic devices to monitor, control, and operate the behavior of interconnected systems. ICSs receive data from remote sensors measuring process variables, compare those values with desired values, and take necessary actions to drive (through actuators) or control the system to function at the required level of services (Galloway and Hancke 2013). Industrial networks are composed of specialized components and applications, such as programmable logic controllers (PLCs), SCADA systems, and DCS. There are other components of ICS such as remote terminal unit (RTU), intelligent electronic devices (IED), and phasor measurement units (PMU). Those devices communicate with the human–machine interface (HMI) located in the control network. With the rise of 5G and industrial IoT, the ICS architecture is becoming even more connected with lower level edge devices increasingly connected to each other and to the cloud, hence, expanding the attack surface and demanding for better cybersecurity solutions (Abosata et al. 2021). This increased connectivity and reduced latency have also enabled design of distributed architectures and distributed edge computing, creating both cybersecurity opportunities and challenges.

Cyber-attack detection is in general concerned with detecting a malicious cyber-incident in a system, while cyber-attack isolation is concerned with pinpointing specifics part(s) of the system that are under attack, and trying to trace back the entry point(s), and the root cause of the cyber-attack. Localizing the initial point(s) of cyber-incident is both critical and hard, in the sense that the attack may cause a series of cascaded events or propagate through the system, especially in feedback control systems. For cyber-physical systems, attack detection and isolation at the physical process level is based on monitoring the process variables such as sensor measurements and actuator commands in a control system. Several recent surveys on attack detection and isolation are available, covering the space from different

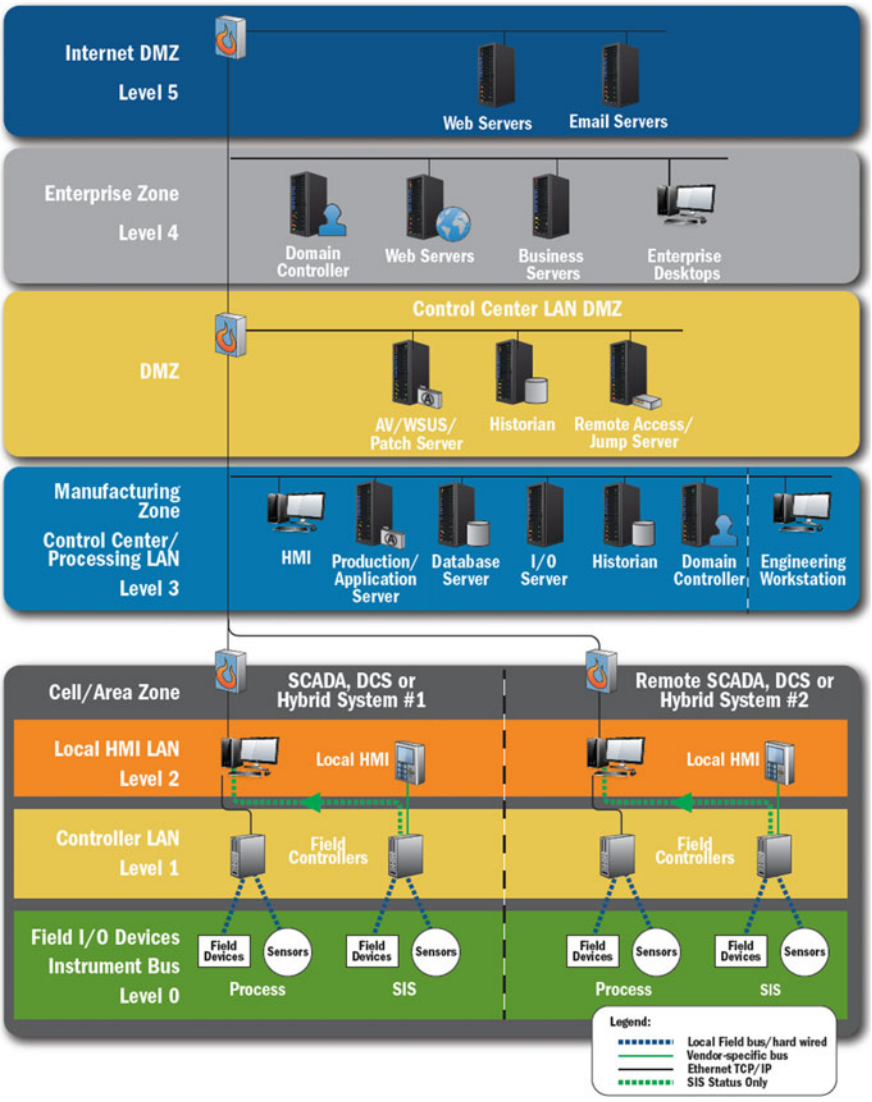

Fig. 2.2 Secure ICS architecture. Reproduced from (Dakhnovich et al. 2019), originally published under a CC BY 3.0 license, doi:10.1088/1757-899X/497/1/012006

perspectives and for different application domains including for general CPS (Ding et al. 2018; Giraldo et al. 2018; Humayed et al. 2017; Li et al. 2020; Tan et al. 2020), ICS (Zhang et al. 2021d), smart grid (Musleh et al. 2019; Peng et al. 2019), autonomous vehicles (Chowdhury et al. 2020; Grigorescu et al. 2020; Loukas et al. 2019) and energy systems (Orumwense and Abo-Al-Ez 2019).

Attack identification is concerned with providing additional insights about the nature of the attack, identifying the type of the attack, impact analysis and forensics (Long et al. 2005; Pasqualetti et al. 2013; Xuan and Naghnaeian 2021). Another important aspect of attack identification is to separate anomalies from novelties (e.g., environmental or operational changes) which can have process-level impacts, and hence, may be detected by attack detectors, and to distinguish cyber-attacks from naturally occurring faults or failures (Anwar et al. 2015; Pan et al. 2015). Attack detection, isolation, and identification (ADII) has similarities with FDII, but as mentioned before, also has major differences, especially for detecting and locating stealthy and coordinated attacks. Similar to other anomaly detection paradigms, ADII algorithms face fundamental design trade-offs among performance and robustness requirements such as false positive rate, false negative rate, and speed of detection (Ding et al. 2018; Li et al. 2020; Zhang et al. 2021d). Many of ADII algorithms are passive in the sense that they receive time-series data from sensors, actuators, and controller, without altering the system. These methods may not be effective against replay attacks. In a replay attack, the malware first records healthy system data during the normal operation, then injects malicious signals into sensors and/or actuators, while masking the real-time data to be sent to the HMI and replaying the prerecorded healthy data instead. Detection of replay attacks often requires active methods. To address this, dynamic physical watermarking methods are proposed (Porter et al. 2020; Satchidanandan and Kumar 2016, 2019). In these methods, carefully designed watermark signals are injected into the system on top of the control commands. The presence of the expected watermark fingerprints in the outputs, determines whether the system is uncompromised. These additional injections, however, may affect the control performance or reduce the stability margins. So, they need to be designed and implemented in a safe manner, through a trade-off optimization between attack detectability and control performance (Khazraei et al. 2017b, a).

The ADII algorithms may work stand-alone for monitoring and alarm generation, or may work in conjunction with an automatic attack mitigation and neutralization algorithm (Li et al. 2020; Mestha et al. 2017), or as part of a cyber-situational awareness system (Abbaszadeh et al. 2018; Chang et al. 2017; Pöyhönen et al. 2021. The ADII techniques can be categorized into two main categories: (i) model-based approaches and (ii) data-driven approaches. Next, we will provide an overview of some of the latest results in each category.

2.4.1 Model-Based ADII

Model-Based ADII utilizes a system model in the detection, isolation, and identification procedures. The model can be a simple encapsulation of domain knowledge of the system operation such as in traditional rule-based or expert systems, or can be a more formal dynamic system model, such as a state space model, developed using first-principles or system identification. Once such a model is available, an observer-based method is often used for attack detection and isolation. The most popular of such observers is the Kalman filter, providing an innovation signal between the measured outputs and the predicted outputs by the model. Detection and isolation procedures are mainly based on two threshold mechanisms over the innovation signal: (i) the chi-square distribution and (ii) the Cumulative Sum (CUSUM) (Ahmed et al. 2017; Housh and Ohar 2018; Sridhar and Govindarasu 2014). The CUSUM approach has the advantage to make a more robust decision based on a weighted sequential sum of the innovation signal as opposed to its instantaneous value, potentially reducing the false positives. However, it may induce a time delay in detecting cyber-events. The attack isolation is done mainly using two techniques, (i) a bank of observers (such as Kalman filters) running in parallel, each designed to be sensitive to a specific element of the innovation vector (Taheri et al. 2020; Ye et al. 2020; Zhang and Zhu 2020) and (ii) a hierarchical approach in which a hierarchy of detectors is designed to zoom in from the top system level into specific subsystems, components, or sensors/actuaros in a top-down manner (Karimipour and Leung 2019; Li et al. 2021a). Model-based attack identification mainly relies upon modeling different attack types and scenarios, and exploiting those attack models along with the system model (Azzam et al. 2021; Li et al. 2020; Park et al. 2019; Teixeira et al. 2015).

2.4.2 Data-Driven ADII

Many attacks detection algorithms available in the literature root back to fault detection techniques. Indeed, from the physical process perspective, cyber-attacks can be viewed as intelligent disturbances, which can affect the system in a malicious manner. To solve complex architectures of cyber-physical attacks, it is necessary to go beyond the traditional methods resulting from fault diagnosis. Novel and intelligent techniques are needed to deal with malicious attacks that appear nonlinearly in mathematical models. To this end, to avoid the need of conservative mathematical conditions, merging learning-based algorithms with standard control theory based techniques is gaining a lot of interest as a promising hybrid approach and a compelling solution.

In recent years, machine learning and deep learning methods have become popular in ADII Zhang et al. (2021c), Narayanan et al. (2021). Recent results for ICS and CPS include classification using statistical machine learning (Ameli et al. 2018; Lee et al. 2014), deep neural networks (Jahromi et al. 2021, 2019; Lee et al. 2014; Yan et al.

2018; Zhu et al. 2018), and pattern recognition (Brentan et al. 2017). Distributed machine learning methods are also proposed for large-scale systems including in IoT and edge computing (Guan and Ge 2017; Kozik et al. 2018). A challenge for adopting AI/ML techniques for CPS ADII is how to obtain the right training data sets, specially for supervised learning methods, and in particular for two-class learning, in which both normal and abnormal samples are required. To overcome this challenge, some researchers have proposed unsupervised learning methods, where no labeled data are required (Jahromi et al. 2019; Tiwari et al. 2021). Unsupervised machine learning methods have also been used in the past in anomaly and intrusion detection in communication and computer networks. However, these approaches need to go through an initial learning phase, often in-field, during which they tend to have a large false alarm rate. Their final accuracy is also often lower than those achieved by supervised learning methods. The alternative approach is to generate synthetic training data using a simulation platform of the system. To this end, digital twins have become a powerful tools to conduct controlled simulations, and to generate labeled data samples of both normal and abnormal classes, both for training and validation of the machine learning models (Abbaszadeh et al. 2018; Mestha et al. 2017; Yan et al. 2018). Digital twin simulations can be used together with available historical field data to address class imbalance (caused due to scarcity of abnormal data in the field), and also to generate data for complete coverage of normal operational and environmental conditions. Furthermore, intelligently designed experiments for digital twin simulations can reduce the need for large training datasets (Abbaszadeh et al. 2018; Yan et al. 2019).

Machine learning algorithms used for ADII are themselves susceptible to cyber-attacks, and hence, need to be secured via hardware and software protections. Robust and adversarial machine learning are active fields of research addressing the security and resilience of machine learning algorithms. A survey on secure and resilient machine learning for CPS security is given in (Olowononi et al. 2020). Besides, in order to be adopted in safety-critical and mission-critical systems, machine learning algorithms must exhibit trustworthiness, which includes certain level of explainability in a human-readable fashion. The explainability can, for example, include providing physical insights, outputting decision factors and their contributions to the overall decision, and giving decision confidence scores based on conformal prediction methods.

2.5 Attack Resilience

In this section, we provide an introduction to the notion of resilience, and a survey of some of the main results. Then in Sects. 2.6 and 2.7, we will cover some of the latest results on two major approaches towards achieving resilience for cyber-physical systems, namely, resilient estimation and resilient control.

Real-world attacks on control systems have in fact occurred in the past decade and have in some cases caused significant damage to the targeted physical processes.

One of the most popular examples is the attack on Maroochy Shire Council's sewage control system in Queensland, Australia, that happened in January 2000 Cardenas et al. (2008), Slay and Miller (2007). In this incident, an attacker managed to hack into some controllers that activate and deactivate valves causing flooding of the grounds of a hotel, a park, and a river with a million liters of sewage (Cardenas et al. 2008). Another well-known example of an attack launched on physical systems is the Stuxnet virus that targeted Siemens' supervisory control on an Iranian uranium enrichment plant targeting a commercially available PLC. Operating under a narrow set of conditions, the attackers were able to ensure the attack reached its intended recipient with limited fallout. They inserted a malware which would lie dormant in the system and go undetected (Falliere et al. 2018). This shows that even air-gapped systems are susceptible to cyber-espionage and -attack.

Given that the end-goal of CPS is a reliable and safe functioning at all times, cyber-physical resilience of CPS is a necessary requirement. It corresponds to the ability to withstand high-impact disturbances, which may occur due to either physical outages or cyber-causes, and to continue to deliver acceptable performance even under attack.

The term resilience is being discussed increasingly in the context of CPS lately, ranging from transportation (Ip and Wang 2011), power (Albasrawi et al. 2014; Zhu and Basar 2011), control systems (Rieger et al. 2009, 2013; Zhu and Basar 2011) as well as other types of systems such as ecological (Holling 1996, 1973) and biological (Kitano 2004). Resilience is often discussed concomitantly with other system-oriented notions such as robustness, reliability, and stability (Levin and Lubchenco 2008) and quite often used interchangeably with the term robustness. We argue however that these two terms are distinct. The reason is that resilience and robustness characterize fundamentally different system properties. The term robustness applies in the context of small bounded disturbances while resilience, in the context of extreme high-impact disturbances. Resilience of a CPS with respect to a class of extreme and high-impact disturbances, is the property that characterizes its ability to withstand and recover from this particular class of disturbances by being allowed to temporarily transit to a state where its performance is significantly degraded and returning within acceptable time to a state where certain minimal but critical performance criteria are met (Baros et al. 2017).

The National Academy of Sciences (NAS) (Cutter et al. 2013) defined resilience as the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events. The authors in Linkov et al. (2013) used the resilience definition provided by NAS to define a set of resilience metrics spread over four operational domains: physical, information, cognitive, and social. In another work (Linkov et al. 2013), the authors applied the previous resilience framework by Linkov et al. (2013) to develop and organize useful resilience metrics for cyber-systems. In Bruneau et al. (2003), the authors have proposed a conceptual framework initially to define seismic resilience, and later in Tierney and Bruneau (2007) the R4 framework for disaster resilience is introduced. It comprises robustness (ability of systems to function under degraded performance), redundancy (identification of substitute elements that satisfy functional requirements in event of significant per-

formance degradation), resourcefulness (initiate solutions by identifying resources based on prioritization of problems), and rapidity (ability to restore functionality in timely fashion).

The design of control and estimation algorithms that are resilient against faults and failures is certainly not a new problem. In fault-detection and identification Massoumnia et al. (1989), Blanke et al. (2006), the objective is to detect if one or more of the components of a system has failed. Traditionally, this is done by comparing the measurements of the sensors with an analytical model of the system and by forming the so-called residual signal. This residual signal is then analyzed (e.g., using signal processing techniques) in order to determine if a fault has occurred, however, in such algorithms there is in general one residual signal per failure mode and in some problems formulations, the number of failure modes can be very large and one cannot afford to generate and analyze a residual signal for each possible failure mode (Fawzi et al., 2014).

In another area, namely robust control (Zhou and Doyle 1998), one seeks to design control methods that are robust against disturbances in the model. However, these disturbances are mainly treated as natural disturbances to the system and are assumed to be bounded. This does not apply in the context of security since the disturbances will typically be adversarial and therefore cannot be assumed bounded which is also the case in stochastic control and estimation, where the disturbances are assumed to follow a certain probabilistic model, which we cannot adopt for CPSs.

Resilient or secure state estimation and control constitute effective and promising means for addressing various security-related issues of CPSs. The main objective is to keep an acceptable performance level of the CPS by resorting to different security countermeasures, including attack attenuation and mitigation, isolation, detection, and compensation. When an attack occurs, the developed secure estimation/control mechanisms possess certain capabilities to mitigate or counteract attack effects, or prevent CPSs from severe performance degradation and loss, or allow the system designers to make corrections and recover the system from any unsafe operation (Ding et al. 2020a).

Recently, there are several survey papers of security-oriented CPSs. For example, the recent progress of secure communication and control of smart grids under malicious cyber-attacks is reviewed in Peng et al. (2019), where different attack models and effects as well as security strategies are reviewed from IT protection and secure control-theoretic perspectives. A summary of detection methods of false data injection (FDI) attacks on smart grids is made in Musleh et al. (2019). The existing FDI attack detection algorithms in smart grids are classified into model-based types and data-driven types. From a systems and control perspective, the CPS security issue is evaluated in Dibaji et al. (2019), where some latest systems and control methods are reviewed and classified into prevention, resilience, detection, and isolation. An overview of security control and attack detection for industrial CPSs is conducted in Ding et al. (2018). An intensive discussion of adversarial attacks and their defenses is provided in Li et al. (2020) for sensor-based CPSs in the field of computer vision. Emerging techniques improving the safety and security of CPSs and IoT systems are

surveyed in Wolf and Serpanos (2017) from two aspects: (1) design time techniques verifying properties of subsystems and (2) runtime mechanisms helpful against both failures and attacks.

2.6 Resilient Estimation

This section is devoted to a general state of the art on available resilient and secure estimation algorithms in cyber-physical systems. Before recalling existing estimation methods, we give a general introduction to emphasize the importance of resilient and secure estimation, and explain what the software sensors have to face to ensure resilience and security of the estimation. State estimation plays an important role in better understanding the real-time dynamics of CPSs and executing some specific control tasks. These states can be reconstructed based on only measured yet possibly corrupted information from sensors. Different from traditional control systems, the tight integration of physical and cyber-components, and the occurrence of various malicious attacks pose nontrivial challenges to the performance analysis and the design of state estimators or filters. Vulnerability of cyber-physical systems may come from two kind of malicious attacks, namely cyber-attacks and physical attacks:

- *Cyber-attacks:* Cyber-attacks occur on the cyber-variables of the system. They may be due to a software virus or to a corruption in communication channels. The well-known Stuxnet malware is one of the relevant examples of cyber-attacks Mishra et al. (2016), Ferrari and Teixeira (2021, Chap. 7). The attackers exploited vulnerabilities of the system such as those running over SCADA devices (Fig. 2.2) to for example, inject false data in the sensor measurements gathered by the SCADA system.
- *Physical attacks:* Physical attacks (also called kinetic attacks) are intentional offensive actions which aim to get unauthorised access to physical assets such as infrastructure, hardware, or interconnection. Sensors are among the devices most exposed to this type of attack. This will have a direct and significant impact on any estimation algorithm using measurements issued from such sensors because, in addition to susceptible manipulations on the cyber-layer, sensor readings rely on physical layer properties that can be manipulated (Taormina et al. 2016). Examples of physical attacks include manipulating gyroscopes used to stabilize drones during formation flights, spoofing LiDAR sensors used in autonomous driving, manually deactivating the pump to disconnect the network from the reservoir in modern water distribution systems, and spoofing magnetic sensors used in several applications, like anti-lock braking systems in automotive.

In the following, we classify some existing secure state estimation approaches according to performance indicators and defense strategies against cyber-attacks.

2.6.1 State of the Art on Resilient and Secure Estimation: A Glimpse on Existing Methods

This section is dedicated to a short but complete overview of existing secure and resilient estimation methods. The overview is shared into two categories (Ding et al. 2020a), namely statistical methods and Lyapunov stability-based techniques.

2.6.1.1 Resilient Estimation Based on Statistical Methods

The statistical-based state estimation aims to select appropriate gain parameters to minimize estimation error variance, hence, the structured information of cyber-attacks, such as statistical information or boundedness information, is assumed to be known. Following this idea, the main focus is then placed on disclosing or offsetting the undesirable impact from compromised data generated by malicious attacks (Ding et al. 2020a. In Ma et al. (2017), an algorithm of variance-constrained filtering over sensor networks is proposed for discrete time-varying stochastic systems and by resorting to the recursive linear matrix inequality approach, a sufficient condition is established for the existence of the desired filter satisfying the pre-specified requirements on the estimation error variance. In the framework of Kalman filtering, a distributed filter with double gains is designed in Ding et al. (2017) which can be regarded as two weight matrices reflecting the different confidence levels of the information from itself and from neighboring nodes.

Estimators or filters can be integrated in some detection mechanisms to remove the compromised data generated by malicious attacks as much as possible. Benefiting from their favorable statistical characteristics, χ^2 detector and its variants are widely adopted. In light of such a detection rule, a critical attack probability is analyzed in Yang et al. (2019) where it is shown that when the considered probability is bigger than some critical value, the steady-state solution of estimation error covariance could exceed a preset value.

It is worth noting that the estimation performance can be properly warranted if the corrupted sensor is accurately detected and effectively isolated. For example, in Mishra et al. (2016) they have estimated the state of a noisy linear dynamical system when an unknown subset of sensors is arbitrarily corrupted by an adversary. They have proposed a secure state estimation algorithm, and derived optimal bounds on the achievable state estimation error given an upper bound on the number of attacked sensors. The proposed state estimator involves Kalman filters operating over subsets of sensors to search for a sensor subset which is reliable for state estimation. When the attack subset is properly identified, the performance of the developed algorithm does not exceed the one by the worst-case Kalman estimation. The optimal secure estimation is pursued in Shoukry et al. (2017) for attacks without restrictions on their statistical properties, boundedness, and time evolution in comparison with the sparse attacks. They have presented a novel algorithm that uses a satisfiability modulo theory approach to harness the complexity of secure state estimation.

2.6.1.2 Lyapunov Theory-Based Methods

Inspired by its mature approaches, an analysis of vulnerabilities of cyber-physical systems in the face of unforeseen failures and external attacks has received increasing attention in the recent years and some preliminary results have been published in literature, see, for instance, Ao et al. (2016), Pasqualetti et al. (2013). In Pasqualetti et al. (2013), the authors have characterized fundamental monitoring limitations from system-theoretic and graph-theoretic perspectives and a Luenberger-type detection filter is designed. Similarly, detectability of attacks is explored in Ao et al. (2016) in which detectability of attacks based on linear system theory is explored and some sufficient conditions of detecting state attacks and sensor attacks are established. Then, two adaptive sliding mode observers with online parameter estimation are designed to estimate state attacks and sensor attacks with uniformly bounded errors. A co-estimation of system states and attacks inspiration from fault-tolerant state reconstruction, as an alternative scheme, is investigated in Amin et al. (2012), Shoukry and Tabuada (2015). For instance, a scheme based on an unknown input observer is developed in Amin et al. (2012) to estimate the states of SCADA systems subject to stealthy deception attacks. In Fawzi et al. (2014), the secure state estimation problem is transformed into the solvability of an l_0 optimization issue and an ℓ_1/ℓ_r optimization issue in Liu et al. (2016), or the performance analysis problem of ℓ_2, $\mathscr{H}_2$, and $\mathscr{H}_\infty$ systems in Nakahira and Mo (2018) by virtue of the classical robust control, and fault detection and isolation methods.

Employing some artificial saturation constraint on state estimators is regarded as a promising security measure for constraining attacker capability and mitigating the impulsive outlier-like effects of cyber-attacks by attenuating the effects of these attack-incurred abnormal measurements using estimators with some saturated output rejection. For example, a saturated innovation update scheme is adopted in Chen et al. (2018) for distributed state estimators with an adaptive threshold of the saturation level, and in Sun et al. (2021) for stochastic nonlinear systems with a sector bounded condition on the saturation constraint. In Xie and Yang (2018), a saturated innovation scheme with an adaptive gain coefficient and a mode switch mechanism is developed, where the mismatched unknown inputs are suppressed by resorting to the well-known $\mathscr{L}_2$-gain attenuation property. Dynamic saturations with an adaptive rule are further developed in Alessandri and Zaccarian (2018); Casadei et al. (2019). It is noted that dynamic saturations with adaptive saturation levels enjoy more flexible attack attenuation capability and less estimation performance degradation.

2.7 Resilient Control

Besides the resilient state estimation above, CPSs also need to mitigate the threat from secret attackers via various control strategies. Compared with other control applications, security control techniques for CPSs are yet in their infancy, and few results can be found in literature Ding et al. (2018). There are two main lines of

research on secure control for CPSs under cyber-attacks, which are categorized as attack-tolerant control and attack-compensated control. The first category focuses on the design of a suitable control policy/law to tolerate unpredictable anomalies caused by attacks (Zhao et al. 2019). In Zhao et al. (2019), a novel observer-based PID controller is proposed and sufficient conditions are derived under which the exponentially mean square input-to-state stability is guaranteed and the desired security level is then achieved. An emphasis is then placed on examining the prescribed tolerance capability or pursuing the maximal tolerance capability for the controlled system, allowing further intervention actions to be made from the system designers. The second category deals with the design of preferable compensation schemes to prevent the system performance and stability from severe deterioration or even becoming unstable. For this purpose, it is essential to implement appropriate attack detection mechanisms to identify and locate the occurrence of cyber-attacks. With respect to networked control systems subject to various cyber-attacks, some preliminary and interesting results can be found in Dolk et al. (2016); Long et al. (2005); Zhang et al. (2016) for DoS attacks, in Amin et al. (2012), Ding et al. (2016a), Dolk et al. (2016), Ding et al. (2016b), Pang and Liu (2011), Pang et al. (2016) for deception attacks, and in Lee et al. (2014); Zhu and Martinez (2013) for replay attacks. The latest development of secure control is evaluated from three aspects: (1) centralized secure control; (2) distributed secure control; and (3) resource-aware secure control.

2.7.1 Centralized Secure Control

When CPSs are subjected to DoS attacks, they operate in an open-loop manner as the desired controller is not capable to receive any sensor data for feedback. To ensure the secure control for CPSs under such DoS attacks, switched system theory is deployed, allowing the system to operate in closed-loop mode during attack-free case and in open-loop mode otherwise. It is noteworthy, however, that the resulting system performance depends on the running duty cycle, which is commonly known as dwell time, between the two cases. Hence, the primary goal of secure control is to find the tolerant duration and/or attack frequency such that the desired system performance remains achievable. For example, a robustness measure against DoS attacks, which describes the tolerable maximum attack frequency and duration is investigated in De Persis and Tesi (2015), where an explicit characterization of the frequency and duration of DoS attacks under which closed-loop stability can be preserved is given. The obtained characterization is flexible enough so as to allow the designer to choose from several implementation options that can be used for trading-off performance versus communication resources. Such a robustness measure is further extended in Feng and Tesi (2017) by resorting to an impulsive controller based on a dynamic observer. A cyclic dwell-time switching strategy is proposed in Zhu and Zheng (2019) where an observer-based output feedback control problem for a class of cyber-physical systems with periodic (DoS) attacks is investigated; the attacks coexist both in the measurement and control channels in the network scenario.

By means of a cyclic piecewise linear Lyapunov function approach, the exponential stability and ℓ_2-gain analysis, and observer-based controller design are carried out for the augmented discrete-time cyclic switched system. Then, the desired observer and controller gains in piecewise linear form are determined simultaneously so as to ensure that the resulting closed-loop system is exponentially stable with a prescribed $\mathscr{H}_\infty$ performance index. Furthermore, a switching signal taking values in a finite set is employed to model the number of consecutive DoS attacks in Pessim and Lacerda (2020), where the corresponding stability criterion is derived by making use of a switching parameter-dependent Lyapunov function.

Adaptive detection of cyber-attacks offers an effective means to enhance the system's adaptation to malicious attacks. In An and Yang (2018), an adaptive switching logic is exploited to provide an online location of the real system mode via observing the variation of the traditional quadratic cost in the framework of linear quadratic control. A Kalman-based attack detector with an observation window of a given length is designed in Du et al. (2018) to remove the occurred deception attacks. When the noise level is below a threshold derived, the maximum allowable duration of deception attacks is obtained to maintain the exponential stability of the system. A common feature of the above detectors is that the duration of deception attacks is captured to describe their negative effects. Then, the maximum allowable duration threshold is examined to maintain the desired system stability.

Complete security of CPSs is generally difficult to be maintained from a control-oriented perspective. As a result, an alternative indicator, known as security in probability, is exploited (Ding et al. 2016c). A definition of security in probability is adopted to account for the transient dynamics of controlled systems. Then, a dynamic output feedback controller is designed such that the prescribed security in probability is guaranteed while obtaining an upper bound of the quadratic cost criterion and an original easy-solution scheme of desired controller gain is derived via the matrix inverse lemma.

2.7.2 Distributed Secure Control

In distributed CPSs, the subsystems are connected through communication links, which constitute a communication topology modeled by the Laplacian matrix (Chen and Shi 2017; Liu 2019). According to attack locations, the cyber-attacks in distributed CPSs are classified into two types: (1) intrasystem attacks and (2) intersystem attacks. As such, a critical concern is to design a suitable distributed secure controller to render the resulting closed-loop system survivable or recoverable from cyber-attacks by embedding attack model information (i.e., statistical or structured information). For example, in He et al. (2020) a distributed impulsive controller using a pinning strategy is redesigned, which ensures that mean square bounded synchronization is achieved in the presence of randomly occurring deception attacks, and in the presence of distributed DoS attacks, a control protocol guaranteeing scalability and robustness is proposed in Xu et al. (2019) for multi-agent systems under

event-triggered communication. On the other hand, the classical fault detection and estimation approaches provide a foundation to deal with the secure control issue of CPSs with an understanding of similarities of both mathematical descriptions and practical influences between faults and certain cyber-attacks. As in Modares et al. (2019); Moghadam and Modares (2018), a distributed state predictor is employed to estimate the existing attacks, and then a resilient controller is designed to guarantee robust performance and to adaptively compensate for the influence of attacks.

2.7.3 Resource-Aware Secure Control

In, the context of communication scheduling, it is apparent that cyber-attacks can result in a tremendous data sparsity issue because less sensor/control data is adopted for achieving feedback control. This further leads to some inherent and nontrivial challenges for performance analysis and secure control design of CPSs that are beyond the capacity of the existing results on stability analysis and controller design of event-based control systems without cyber-attacks.

The time series of data transmissions or updates under communication schedules become more complex due to the interference of malicious attacks, which poses a significant challenge for continuous-time physical systems. Under the assumption that the execution period and a uniform lower bound of sleeping periods are a priori known, a sufficient condition of exponential stability is derived in Hu et al. (2018) by using a piecewise Lyapunov functional along with a reconstructed state error-dependent switched system. An event-triggered scheduling and control co-design algorithm is developed in Peng et al. (2016) to obtain both the triggering parameter and the control gain. This event-triggered scheme is improved by integrating measurement variations with a minimal trigger sleeping interval in order to avoid the well-known Zeno behavior (Hu et al. 2019; Lu and Yang 2019). Then, under a sparse observability condition, an observer in a delta domain is designed in Gao et al. (2020) to estimate the system state under sensor and actuator attacks, and a self-triggered controller is designed via iterative analysis.

In the context of distributed secure control, there are considerable results reported for CPSs under event-triggered communication scheduling. In Ding et al. (2018), an observer-based event-triggering consensus control problem is investigated for a class of discrete-time multi-agent systems with lossy sensors and cyber-attacks. A novel distributed observer is proposed to estimate the relative full states and the estimated states are then used in the feedback protocol in order to achieve the overall consensus. An event-triggered mechanism with state-independent threshold is adopted to update the control input signals so as to reduce unnecessary data communications. In Feng and Hu (2019), two elaborate interval classifications are constructed by introducing the upper bound of adjacent event intervals under DoS attacks, their duration and their launching time, and then the switched system theory is employed to derive the consensus condition. It should be noted that the presence of cyber-attacks makes

the exclusion of Zeno behavior from the designed distributed event-triggered secure controllers generally difficult. This is because the interval of two consecutive data transmissions may not be that of two adjacent events invoked.

To mention a few, an event-triggered controller is designed in Dolk et al. (2016) to tolerate DoS attacks characterized by given frequency and duration properties. An optimal schedule of jamming attacks is proposed in Zhang et al. (2016) to maximize the linear quadratic Gaussian cost under energy constraints. An event-triggering consensus resilient-control with a state-independent threshold is discussed in Ding et al. (2016a) for discrete-time multi-agent systems with both lossy sensors and cyber-attacks.

Acknowledgements M. Abbaszadeh would like to thank GE Research for the partial support of this work. A. Zemouche would like to thank the ANR agency for the partial support of this work via the project ArtISMo ANR-20-CE48-0015.

References

M. Abbaszadeh, L.K. Mestha, W. Yan, Forecasting and early warning for adversarial targeting in industrial control systems, in *2018 IEEE Conference on Decision and Control (CDC)* (IEEE, 2018), pp. 7200–7205

N. Abosata, S. Al-Rubaye, G. Inalhan, C. Emmanouilidis, Internet of things for system integrity: a comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors **21**(11), 3654 (2021)

C.M. Ahmed, C. Murguia, J. Ruths, Model-based attack detection scheme for smart water distribution networks, in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, (2017), pp. 101–113

F. Akowuah, F. Kong, Real-time adaptive sensor attack detection in autonomous cyber-physical systems. in *IEEE 27th Real-Time and Embedded Technology and Applications Symposium (RTAS)* (IEEE, 2021), pp. 237–250

M.N. Albasrawi, N. Jarus, K.A. Joshi, S.S. Sarvestani, Analysis of reliability and resilience for smart grids, in *2014 IEEE 38th Annual Computer Software and Applications Conference (COMPSAC)* (IEEE, 2014)

A. Alessandri, L. Zaccarian, Stubborn state observers for linear time-invariant systems. Automatica **88**, 1–9 (2018)

A. Alguttar, S. Hussin, K. Alashik, R. Yildirim, An observation of intrusion detection techniques in cyber physical systems, *Avrupa Bilim ve Teknoloji Dergisi*, (2020), pp. 277–284

A.A. AlZubi, M. Al-Maitah, A. Alarifi, Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Comput. 1–14 (2021)

A. Ameli, A. Hooshyar, E.F. El-Saadany, A.M. Youssef, Attack detection and identification for automatic generation control systems. IEEE Trans. Power Syst. **33**(5), 4760–4774 (2018)

S. Amin, X. Litrico, S. Sastry, A.M. Bayen, Cyber security of water scada systems-part i: analysis and experimentation of stealthy deception attacks. IEEE Trans. Control Syst. Technol. **21**(5), 1963–1970 (2012)

L. An, G.-H. Yang, Secure distributed adaptive optimal coordination of nonlinear cyber-physical systems with attack diagnosis (2020). arXiv:2009.12739

L. An, G.-H. Yang, LQ secure control for cyber-physical systems against sparse sensor and actuator attacks. IEEE Trans. Control Netw. Syst. **6**(2), 833–841 (2018)

A. Anwar, A. N. Mahmood, Z. Shah, A data-driven approach to distinguish cyber-attacks from physical faults in a smart grid, in *Proceedings of the 24th ACM International on Conference on Information and Knowledge Management*, (2015), pp. 1811–1814

W. Ao, Y. Song, C. Wen, Adaptive cyber-physical system attack detection and reconstruction with application to power systems. IET Control Theory Appl. **10**(12), 1458–1468 (2016)

M. Azzam, L. Pasquale, G. Provan, B. Nuseibeh, Grounds for suspicion: Physics-based early warnings for stealthy attacks on industrial control systems, in *IEEE Transactions on Dependable and Secure Computing*, vol. 09, (2021), pp. 1–1

A. Baniamerian, K. Khorasani, N. Meskin, Determination of security index for linear cyber-physical systems subject to malicious cyber attacks, in *2019 IEEE 58th Conference on Decision and Control (CDC)* (IEEE, 2019), pp. 4507–4513

S. Baros, D. Shiltz, P. Jaipuria, A. Hussain, A. Annaswamy, Towards resilient cyber-physical energy systems (2017). https://core.ac.uk/download/pdf/83232958.pdf

M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki, *Diagnosis and Fault-Tolerant Control* (Springer, 2006)

B.M. Brentan, E. Campbell, G. Lima, D. Manzi, D. Ayala-Cabrera, M. Herrera, I. Montalvo, J. Izquierdo, E. Luvizotto Jr., On-line cyber attack detection in water networks through state forecasting and control by pattern recognition. World Environ. Water Res. Cong. **2017**, 583–592 (2017)

M. Bruneau, S. Chang, R. Eguchi, G. Lee, T. O'Rourke, A. Reinhorn, D.V. Winterfeldt, A framework to quantitatively assess and enhance the seismic resilience of communities. Earthq. Spectra **19**(4), 733–752 (2003)

P. Buason, H. Choi, A. Valdes, H.J. Liu, Cyber-physical systems of microgrids for electrical grid resiliency, in *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)* (IEEE, 2019), pp. 492–497

J. Cao, D. Wang, Z. Qu, M. Cui, P. Xu, K. Xue, K. Hu, A novel false data injection attack detection model of the cyber-physical power system. IEEE Access **8**, 95 109–95 125 (2020)

A. Cardenas, S. Amin, S. Sastry, Research challenges for the security of control systems, in *3rd conference on Hot topics in security* (ACM, 2008), pp. 1–6

G. Casadei, D. Astolfi, A. Alessandri, L. Zaccarian, Synchronization in networks of identical nonlinear systems via dynamic dead zones. IEEE Control Syst. Lett. **3**(3), 667–672 (2019)

E. Chang, F. Gottwalt, Y. Zhang, Cyber situational awareness for CPS, 5g and IOT, in *Frontiers in Electronic Technologies* (Springer, 2017), pp. 147–161

S. Chen, M. Wu, P. Wen, F. Xu, S. Wang, S. Zhao, A multimode anomaly detection method based on oc-elm for aircraft engine system. IEEE Access **9**, 28 842–28 855 (2021)

Y. Chen, Y. Shi, Distributed consensus of linear multiagent systems: Laplacian spectra-based method. IEEE Trans. Syst. Man Cybern.: Syst. **50**(2), 700–706 (2017)

Y. Chen, S. Kar, J.M. Moura, Dynamic attack detection in cyber-physical systems with side initial state information. IEEE Trans. Autom. Control **62**(9), 4618–4624 (2016)

Y. Chen, S. Kar, J.M. Moura, Resilient distributed estimation: sensor attacks. IEEE Trans. Autom. Control **64**(9), 3772–3779 (2018)

A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, R. Das, Attacks on self-driving cars and their countermeasures: a survey. IEEE Access **8**, 207 308–207 342 (2020)

L.F. Cómbita Alfonso et al., Intrusion response on cyber-physical control systems, Ph.D. dissertation, Uniandes (2020)

S.L. Cutter, J. Ahearn, B. Amadei, P. Crawford, E. Eide, G. Galloway, Disaster resilience: a national imperative. *Environment: Science and Policy for Sustainable Development*, vol. 55, no. 2, (2013), pp. 25–29

A. Dakhnovich, D. Moskvin, D. Zeghzda, An approach for providing industrial control system sustainability in the age of digital transformation, in *IOP Conference Series: Materials Science and Engineering*, vol. 497, no. 1. IOP Publishing, (2019), p. 012006

C. De Persis, P. Tesi, Input-to-state stabilizing control under denial-of-service. IEEE Trans. Autom. Control **60**(11), 2930–2944 (2015)

S.M. Dibaji, M. Pirani, A.M. Annaswamy, K.H. Johansson, A. Chakrabortty, Secure control of wide-area power systems: confidentiality and integrity threats, in *2018 IEEE Conference on Decision and Control (CDC)* (IEEE, 2018), pp. 7269–7274

S.M. Dibaji, M. Pirani, D.B. Flamholz, A.M. Annaswamy, K.H. Johansson, A. Chakrabortty, A systems and control perspective of CPS security. Ann. Rev. Control **47**, 394–411 (2019)

D. Ding, Q.-L. Han, X. Ge, J. Wang, Secure state estimation and control of cyber-physical systems: a survey. IEEE Trans. Syst. Man Cybern.: Syst. **51**(1), 176–190 (2020a)

D. Ding, Q.-L. Han, Z. Wang, X. Ge, Recursive filtering of distributed cyber-physical systems with attack detection. IEEE Trans. Syst. Man Cybern. (2020b)

S.X. Ding, L. Li, D. Zhao, C. Louen, T. Liu, Application of the unified control and detection framework to detecting stealthy integrity cyber-attacks on feedback control systems (2021), arXiv:2103.00210

D. Ding, Y. Shen, Y. Song, Y. Wang, Recursive state estimation for discrete time-varying stochastic nonlinear systems with randomly occurring deception attacks. Int. J. Gen. Syst. **45**(5), 548–560 (2016)

D. Ding, Z. Wang, G. Wei, F.E. Alsaadi, Event-based security control for discrete-time stochastic systems. IET Control TheoryAppl. **10**(15), 1808–1815 (2016)

D. Ding, Z. Wang, Q.-L. Han, G. Wei, Security control for discrete-time stochastic nonlinear systems subject to deception attacks. IEEE Trans. Syst. Man Cybern.: Syst. **48**(5), 779–789 (2016)

D. Ding, Z. Wang, D.W. Ho, G. Wei, Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks. Automatica **78**, 231–240 (2017)

D. Ding, Q.-L. Han, Y. Xiang, X. Ge, X.-M. Zhang, A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing **275**, 1674–1683 (2018)

V. Dolk, P. Tesi, C. De Persis, W. Heemels, Event-triggered control systems under denial-of-service attacks. IEEE Trans. Control Netw. Syst. **4**(1), 93–105 (2016)

D. Du, C. Zhang, H. Wang, X. Li, H. Hu, T. Yang, Stability analysis of token-based wireless networked control systems under deception attacks. Inf. Sci. **459**, 168–182 (2018)

A.K. Dutta, R. Negi, S.K. Shukla, Robust multivariate anomaly-based intrusion detection system for cyber-physical systems, in *International Symposium on Cyber Security Cryptography and Machine Learning* (Springer, 2021), pp. 86–93

N. Falliere, L. Murchu, E. Chien, W32. stuxnet dossier: syman-tec security response, 2018, technical Report, Symantec, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

C. Fang, Y. Qi, P. Cheng, W.X. Zheng, Optimal periodic watermarking schedule for replay attack detection in cyber-physical systems. Automatica **112**, 108698 (2020)

F. Farivar, M.S. Haghighi, A. Jolfaei, M. Alazab, Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial iot. IEEE Trans. Ind. Inf. **16**(4), 2716–2725 (2019)

H. Fawzi, P. Tabuada, S. Diggavi, Secure estimation and control for cyber-physical systems under adversarial attacks. IEEE Trans. Autom. control **59**(6), 1454–1467 (2014)

Z. Feng, G. Hu, Secure cooperative event-triggered control of linear multiagent systems under dos attacks. IEEE Trans. Control Syst. Technol. **28**(3), 741–752 (2019)

S. Feng, P. Tesi, Resilient control under denial-of-service: robust design. Automatica **79**, 42–51 (2017)

R.M. Ferrari, A.M. Teixeira, Detection and isolation of routing attacks through sensor watermarking, in *American Control Conference (ACC)*, vol. 2017 (IEEE, 2017), pp. 5436–5442

R.M. Ferrari, A.M. Teixeira, Safety, security, and privacy for cyber-physical systems (2021)

L. Fillatre, I. Nikiforov, P. Willett et al., Security of scada systems against cyber-physical attacks. IEEE Aerosp. Electron. Syst. Mag. **32**(5), 28–45 (2017)

B. Galloway, G. Hancke, Introduction to industrial control networks. Commun. Surv. Tutor. **15**(2), 860–880 (2013)

Y. Gao, G. Sun, J. Liu, Y. Shi, L. Wu, State estimation and self-triggered control of CPSS against joint sensor and actuator attacks. Automatica **113**(2020)

J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N.O. Tippenhauer, H. Sandberg, R. Candell, A survey of physics-based attack detection in cyber-physical systems. ACM Comput. Surv. (CSUR) **51**(4), 1–36 (2018)

S. Grigorescu, B. Trasnea, T. Cocias, G. Macesanu, A survey of deep learning techniques for autonomous driving. J. Field Robot. **37**(3), 362–386 (2020)

C.-Y. Gu, J.-W. Zhu, W.-A. Zhang, L. Yu, Sensor attack detection for cyber-physical systems based on frequency domain partition. IET Control Theory Appl. **14**(11), 1452–1466 (2020)

Y. Guan, X. Ge, Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. IEEE Trans. Signal Inf. Process. Over Netw. **4**(1), 48–59 (2017)

K. Han, Y. Duan, R. Jin, Z. Ma, H. Wang, W. Wu, B. Wang, X. Cai, Attack detection method based on bayesian hypothesis testing principle in CPS. Procedia Comput. Sci. **187**, 474–480 (2021)

W. He, Z. Mo, Q.-L. Han, F. Qian, Secure impulsive synchronization in lipschitz-type multi-agent systems subject to deception attacks. IEEE/CAA J. Automatica Sinica **7**(5), 1326–1334 (2020)

J.M. Hendrickx, K.H. Johansson, R.M. Jungers, H. Sandberg, K.C. Sou, Efficient computations of a security index for false data attacks in power networks. IEEE Trans. Autom. Control **59**(12), 3194–3208 (2014)

C.S. Holling, *Engineering Resilience Versus Ecological Ressilience* (National Academy Press, 1996), ch. 3, pp. 31–43

C.S. Holling, Resilience and stability of ecological systems. Ann. Rev. Ecol. Syst. **4**, 1–23 (1973)

M. Housh, Z. Ohar, Model-based approach for cyber-physical attack detection in water distribution systems. Water Res. **139**, 132–143 (2018)

S. Hu, D. Yue, X. Xie, X. Chen, X. Yin, Resilient event-triggered controller synthesis of networked control systems under periodic dos jamming attacks. IEEE Trans. Cybern. **49**(12), 4271–4281 (2018)

S. Hu, D. Yue, Q.-L. Han, X. Xie, X. Chen, C. Dou, Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks. IEEE Trans. Cybern. **50**(5), 1952–1964 (2019)

A. Humayed, B. Luo, Cyber-physical security for smart cars: taxonomy of vulnerabilities, threats, and attacks, in *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems*, (2015), pp. 252–253

A. Humayed, J. Lin, F. Li, B. Luo, Cyber-physical systems security-a survey. IEEE Int. Things J. **4**(6), 1802–1831 (2017)

W.H. Ip, D. Wang, Resilience and friability of transportation networks: evaluation, analysis and optimization. IEEE Syst. J. **5**(2), 189–198 (2011)

C. Iwendi, S.U. Rehman, A.R. Javed, S. Khan, G. Srivastava, Sustainable security for the internet of things using artificial intelligence architectures. ACM Trans. Int. Technol. (TOIT) **21**(3), 1–22 (2021)

A.N. Jahromi, H. Karimipour, A. Dehghantanha, R.M. Parizi, Deep representation learning for cyber-attack detection in industrial iot, in *AI-Enabled Threat Detection and Security Analysis for Industrial IoT* (Springer, 2021), pp. 139–162

A.N. Jahromi, J. Sakhnini, H. Karimpour, A. Dehghantanha, A deep unsupervised representation learning approach for effective cyber-physical attack detection and identification on highly imbalanced data, in *Proceedings of the 29th Annual International Conference on Computer Science and Software Engineering*, (2019), pp. 14–23

K.N. Junejo, J. Goh, Behaviour-based attack detection and classification in cyber physical systems using machine learning, in *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*, (2016), pp. 34–43

H. Karimipour, H. Leung, Relaxation-based anomaly detection in cyber-physical systems using ensemble Kalman filter. IET Cyber-Phys. Syst.: Theory Appl. **5**(1), 49–58 (2019)

M.T. Khan, D. Serpanos, H. Shrobe, M.M. Yousuf, Rigorous machine learning for secure and autonomous cyber physical systems, in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1 (IEEE, 2020), pp. 1815–1819

A. Khazraei, H. Kebriaei, F.R. Salmasi, A new watermarking approach for replay attack detection in LGG systems, in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)* (IEEE, 2017), pp. 5143–5148

A. Khazraei, H. Kebriaei, F.R. Salmasi, Replay attack detection in a multi agent system using stability analysis and loss effective watermarking, in *American Control Conference (ACC)* (IEEE, 2017), pp. 4778–4783

S. Kim, Y. Eun, K.-J. Park, Stealthy sensor attack detection and real-time performance recovery for resilient cps. IEEE Trans. Ind. Inf. **17**(11), 7412–7422 (2021)

H. Kitano, Biological robustness. Nat. Rev. Gen. **5**, 826–837 (2004)

R. Kozik, M. Choraś, M. Ficco, F. Palmieri, A scalable distributed machine learning approach for attack detection in edge computing environments. J. Parallel Distrib. Comput. **119**, 18–26 (2018)

S. Krishnamurthy, S. Sarkar, A. Tewari, Scalable anomaly detection and isolation in cyber-physical systems using bayesian networks, in *Dynamic Systems and Control Conference*, vol. 46193 (American Society of Mechanical Engineers, 2014), p. V002T26A006

D. Kumar, H. Nayyar, D. Pandey, A. Hussian Khan, Cyber physical security of the critical information infrastructure, in *ISUW 2019* (Springer, 2022), pp. 275–285

D. Lee, D. Kundur, Cyber attack detection in pmu measurements via the expectation-maximization algorithm, in *2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP)* (IEEE, 2014), pp. 223–227

P. Lee, A. Clark, L. Bushnell, R. Poovendran, A passivity framework for modeling and mitigating wormhole attacks on networked control systems. IEEE Trans. Autom. Control **59**(12), 3224–3237 (2014)

S.A. Levin, J. Lubchenco, Resilience, robustness, and marine ecosystem-based management. BioScience **58**(1), 27–32 (2008)

Q. Li, B. Bu, J. Zhao, A novel hierarchical situation awareness model for CBTC using SVD entropy and GRU with PRD algorithms. IEEE Access (2021a)

L. Li, W. Wang, Q. Ma, K. Pan, X. Liu, L. Lin, J. Li, Cyber attack estimation and detection for cyber-physical power systems. Appl. Math. Comput. **400** (2021b)

J. Li, Y. Liu, T. Chen, Z. Xiao, Z. Li, J. Wang, Adversarial attacks and defenses on cyber-physical systems: a survey. IEEE Int. Things J. **7**(6), 5103–5115 (2020)

I. Linkov, D. Eisenberg, M. E. Bates, D. Chang, M. Convertino, K. Plourde, J. Allen, T. Seager, *Measurable Resilience for Actionable Policy* (ACS Publications, 2013), pp. 25–29

I. Linkov, D. Eisenberg, K. Plourde, T. Seager, J. Allen, A. Kott, Resilience metrics for cyber systems. Environ. Syst. Decis. **33**(4), 471–476 (2013)

G.-P. Liu, Coordinated control of networked multiagent systems with communication constraints using a proportional integral predictive control strategy. IEEE Trans. Cybern. **50**(11), 4735–4743 (2019)

C. Liu, J. Wu, C. Long, Y. Wang, Dynamic state recovery for cyber-physical systems under switching location attacks. IEEE Trans. Control Netw. Syst. **4**(1), 14–22 (2016)

M. Long, C.-H. Wu, J.Y. Hung, Denial of service attacks on network-based control systems: impact and mitigation. IEEE Trans. Ind. Inf. **1**(2), 85–96 (2005)

G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, T. Vuong, A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. Ad Hoc Netw. **84**, 124–147 (2019)

A.-Y. Lu, G.-H. Yang, Observer-based control for cyber-physical systems under denial-of-service with a decentralized event-triggered scheme. IEEE Trans. Cybern. **50**(12), 4886–4895 (2019)

L. Ma, Z. Wang, Q.-L. Han, H.-K. Lam, Variance-constrained distributed filtering for time-varying systems with multiplicative noises and deception attacks over sensor networks. IEEE Sens. J. **17**(7), 2279–2288 (2017)

M. Massoumnia, G. Verghese, A. Willsky, Failure detection and identification. IEEE Trans. Autom. Control **34**(3), 316–321 (1989)
L.K. Mestha, O.M. Anubi, M. Abbaszadeh, Cyber-attack detection and accommodation algorithm for energy delivery systems, in *2017 IEEE Conference on Control Technology and Applications (CCTA)* (IEEE, 2017), pp. 1326–1331
S. Mishra, Y. Shoukry, N. Karamchandani, S.N. Diggavi, P. Tabuada, Secure state estimation against sensor attacks in the presence of noise. IEEE Trans. Control Netw. Syst. **4**(1), 49–59 (2016)
H. Modares, B. Kiumarsi, F.L. Lewis, F. Ferrese, A. Davoudi, Resilient and robust synchronization of multiagent systems under attacks on sensors and actuators. IEEE Trans. Cybern. **50**(3), 1240–1250 (2019)
R. Moghadam, H. Modares, Resilient autonomous control of distributed multiagent systems in contested environments. IEEE Trans. Cybern. **49**(11), 3957–3967 (2018)
A. Mosteiro-Sanchez, M. Barcelo, J. Astorga, A. Urbieta, Securing IIOT using defence-in-depth: towards an end-to-end secure industry 4.0. J. Manuf. Syst. **57**, 367–378 (2020)
A. Musleh, G. Chen, A. Dong, A survey on the detection algorithms for false data injection attacks in smart grids. IEEE Trans. Smart Grid **11**(3), 2218–2234 (2019)
Y. Nakahira, Y. Mo, Attack-resilient $\mathscr{H}_2/\mathscr{H}_\infty$ and ℓ_1 state estimator. IEEE Trans. Autom. Control **63**(12), 4353–4360 (2018)
S.K. Narayanan, S. Dhanasekaran, V. Vasudevan, Intelligent abnormality detection method in cyber physical systems using machine learning, in *Proceedings of International Conference on Machine Intelligence and Data Science Applications* (Springer, 2021), pp. 595–606
M. Noorizadeh, M. Shakerpour, N. Meskin, D. Unal, K. Khorasani, A cyber-security methodology for a cyber-physical industrial control system testbed. IEEE Access **9**, 16 239–16 253 (2021)
U.S.D. of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies* (Createspace Independent Pub, 2014), https://books.google.com/books?id=1OO8oQEACAAJ
F.O. Olowononi, D.B. Rawat, C. Liu, Resilient machine learning for networked cyber physical systems: a survey for machine learning security to securing machine learning for CPS. IEEE Commun. Surv. Tutor. **23**(1), 524–552 (2020)
E.F. Orumwense, K. Abo-Al-Ez, A systematic review to aligning research paths: energy cyber-physical systems. Cogen. Eng. **6**(1), 1700738 (2019)
S. Pan, T. Morris, U. Adhikari, Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. IEEE Trans. Ind. Inf. **11**(3), 650–662 (2015)
Z.-H. Pang, G.-P. Liu, Design and implementation of secure networked predictive control systems under deception attacks. IEEE Trans. Control Syst. Technol. **20**(5), 1334–1342 (2011)
Z.-H. Pang, G.-P. Liu, D. Zhou, F. Hou, D. Sun, Two-channel false data injection attacks against output tracking control of networked systems. IEEE Trans. Ind. Electron. **63**(5), 3242–3251 (2016)
C.M. Paredes, D. Martínez-Castro, V. Ibarra-Junquera, A. González-Potes, Detection and isolation of dos and integrity cyber attacks in cyber-physical systems with a neural network-based architecture. Electronics **10**(18), 2238 (2021)
J. Park, R. Ivanov, J. Weimer, M. Pajic, I. Lee, Sensor attack detection in the presence of transient faults, in *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems*, (2015), pp. 1–10
G. Park, C. Lee, H. Shim, Y. Eun, K.H. Johansson, Stealthy adversaries against uncertain cyber-physical systems: threat of robust zero-dynamics attack. IEEE Trans. Autom. Control **64**(12), 4907–4919 (2019)
F. Pasqualetti, F. Dörfler, F. Bullo, Attack detection and identification in cyber-physical systems. IEEE Trans. Autom. control **58**(11), 2715–2729 (2013)
C. Peng, J. Li, M. Fei, Resilient event-triggering $\mathscr{H}_\infty$ load frequency control for multi-area power systems with energy-limited dos attacks. IEEE Trans. Power Syst. **32**(5), 4110–4118 (2016)

C. Peng, H. Sun, M. Yang, Y. Wang, A survey on security communication and control for smart grids under malicious cyber attacks. IEEE Trans. Syst. Man Cybern.: Syst. **49**(8), 1554–1569 (2019)
P.S. Pessim, M.J. Lacerda, State-feedback control for cyber-physical LPV systems under dos attacks. IEEE Control Syst. Lett. **5**(3), 1043–1048 (2020)
M. Pirani, E. Nekouei, H. Sandberg, K.H. Johansson, A game-theoretic framework for the security-aware sensor placement problem in networked control systems. IEEE Trans. Autom. Control (2021)
M. Porter, P. Hespanhol, A. Aswani, M. Johnson-Roberson, R. Vasudevan, Detecting generalized replay attacks via time-varying dynamic watermarking. IEEE Trans. Autom. Control (2020)
J. Pöyhönen, J. Rajamäki, V. Nuojua, M. Lehto, Cyber situational awareness in critical infrastructure organizations. Digit. Transform. Cyber Secur. Resil. Mod. Soc. **84**, 161 (2021)
C.G. Rieger, D.I. Gertman, M.A. McQueen, Resilient control systems: next generation design research, in *2nd Conference on Human System Interactions*, (2009), pp. 632–636
C.G. Rieger, K.L. Moore, T.L. Baldwin, Resilient control systems: a multi-agent dynamic systems perspective, in *International Conference on Electro/Information Technology (EIT)* (2013)
T. Roy, S. Dey, Security of distributed parameter cyber-physical systems: cyber-attack detection in linear parabolic PDES (2021), arXiv:2107.14159
RTCA, DO-178/EUROCAE ED-12, *Software Considerations in Airborne Systems and Equipment Certification* (2011)
S. Sahoo, S. Mishra, J.C.-H. Peng, T. Dragičević, A stealth cyber-attack detection strategy for dc microgrids. IEEE Trans. Power Electron. **34**(8), 8162–8174 (2018)
B. Satchidanandan, P.R. Kumar, Dynamic watermarking: active defense of networked cyber-physical systems. Proc. IEEE **105**(2), 219–240 (2016)
B. Satchidanandan, P. Kumar, On the design of security-guaranteeing dynamic watermarks. IEEE Control Syst. Lett. **4**(2), 307–312 (2019)
P. Semwal, A multi-stage machine learning model for security analysis in industrial control system, in *AI-Enabled Threat Detection and Security Analysis for Industrial IoT* (Springer, 2021), pp. 213–236
J. Shin, Y. Baek, Y. Eun, S.H. Son, Intelligent sensor attack detection and identification for automotive cyber-physical systems. IEEE Symp. Ser. Comput. Intell. (SSCI) **2017**, 1–8 (2017)
Y. Shoukry, P. Tabuada, Event-triggered state observers for sparse sensor noise/attacks. IEEE Trans. Autom. Control **61**(8), 2079–2091 (2015)
Y. Shoukry, P. Nuzzo, A. Puggelli, A.L. Sangiovanni-Vincentelli, S.A. Seshia, P. Tabuada, Secure state estimation for cyber-physical systems under sensor attacks: a satisfiability modulo theory approach. IEEE Trans. Autom. Control **62**(10), 4917–4932 (2017)
J. Slay, M. Miller, Lessons learned from the maroochy water breach, in *International Conference on Critical Infrastructure Protection* (Springer, 2007), pp. 73–82
S. Sridhar, M. Govindarasu, Model-based attack detection and mitigation for automatic generation control. IEEE Trans. Smart Grid **5**(2), 580–591 (2014)
Q. Su, Z. Fan, Y. Long, J. Li, Attack detection and secure state estimation for cyber-physical systems with finite-frequency observers. J. Franklin Inst. **357**(17), 12 724–12 741 (2020)
Y. Sun, D. Ding, H. Dong, H. Liu, Event-based resilient filtering for stochastic nonlinear systems via innovation constraints. Inf. Sci. **546**, 512–525 (2021)
M. Taheri, K. Khorasani, I. Shames, N. Meskin, Cyber attack and machine induced fault detection and isolation methodologies for cyber-physical systems (2020), arXiv:2009.06196
S. Tan, J.M. Guerrero, P. Xie, R. Han, J.C. Vasquez, Brief survey on attack detection methods for cyber-physical systems. IEEE Syst. J. **14**(4), 5329–5339 (2020)
R. Taormina, S. Galelli, N.O. Tippenhauer, A. Ostfeld, E. Salomons, Assessing the effect of cyber-physical attacks on water distribution systems. World Environ. Water Res. Cong. **2016**, 436–442 (2016)
A. Teixeira, F. Kupzog, H. Sandberg, K.H. Johansson, Cyber-secure and resilient architectures for industrial control systems, in *Smart Grid Security* (Elsevier, 2015), pp. 149–183

J. Tian, B. Wang, T. Li, F. Shang, K. Cao, R. Guo, Total: Optimal protection strategy against perfect and imperfect false data injection attacks on power grid cyber-physical systems. IEEE Int. Things J. **8**(2), 1001–1015 (2020)
K. Tierney, M. Bruneau, Conceptualizing and measuring resilience: a key to disaster loss reduction. TR News **250**(1), 14–17 (2007)
D.D. Tiwari, S. Naskar, A.S. Sai, V.R. Palleti, Attack detection using unsupervised learning algorithms in cyber-physical systems. Comput. Aided Chem. Eng. Elsevier **50**, 1259–1264 (2021)
L. Tsiami, C. Makropoulos, Cyber-physical attack detection in water distribution systems with temporal graph convolutional neural networks. Water **13**(9), 1247 (2021)
C.M.P. Valencia, R.E. Alzate, D.M. Castro, A.F. Bayona, D.R. García, Detection and isolation of dos and integrity attacks in cyber-physical microgrid system, in *2019 IEEE 4th Colombian Conference on Automatic Control (CCAC)* (IEEE, 2019), pp. 1–6
X. Wang, S. Li, M. Liu, Y. Wang, A.K. Roy-Chowdhury, Multi-expert adversarial attack detection in person re-identification using context inconsistency (2021a), arXiv:2108.09891
H. Wang, X. Wen, S. Huang, B. Zhou, Q. Wu, N. Liu, Generalized attack separation scheme in cyber physical smart grid based on robust interval state estimation. Int. J. Electr. Power Energy Syst. **129** (2021b)
H. Wang, X. Wen, Y. Xu, B. Zhou, J.-C. Peng, W. Liu, *Operating state reconstruction in cyber physical smart grid for automatic attack filtering*. IEEE Trans. Ind. Inf. (2020)
M. Wolf, D. Serpanos, Safety and security in cyber-physical systems and internet-of-things systems. Proc. IEEE **106**(1), 9–20 (2017)
C. Wu, W. Yao, W. Pan, G. Sun, J. Liu, L. Wu, Secure control for cyber-physical systems under malicious attacks. IEEE Trans. Control Netw. Syst. (2021)
C.-H. Xie, G.-H. Yang, Secure estimation for cyber-physical systems with adversarial attacks and unknown inputs: an l 2-gain method. Int. J. Robust Nonlinear Control **28**(6), 2131–2143 (2018)
J. Xiong, J. Wu, Construction of approximate reasoning model for dynamic CPS network and system parameter identification. Comput. Commun. **154**, 180–187 (2020)
W. Xu, G. Hu, D.W. Ho, Z. Feng, Distributed secure cooperative control under denial-of-service attacks from multiple adversaries. IEEE Trans. Cybern. **50**(8), 3458–3467 (2019)
Y. Xuan, M. Naghnaeian, Detection and identification of cps attacks with application in vehicle platooning: a generalized luenberger approach, in *American Control Conference (ACC)* (IEEE, 2021), pp. 4013–4020
W. Yan, L. Mestha, J. John, D. Holzhauer, M. Abbaszadeh, M. McKinley, Cyberattack detection for cyber physical systems security–a preliminary study, in *Proceedings of the Annual Conference of the PHM Society*, vol. 10 (2018)
W. Yan, L.K. Mestha, M. Abbaszadeh, Attack detection for securing cyber physical systems. IEEE Int. Things J. **6**(5), 8471–8481 (2019)
W. Yang, Y. Zhang, G. Chen, C. Yang, L. Shi, Distributed filtering under false data injection attacks. Automatica **102**, 34–44 (2019)
L. Ye, F. Zhu, J. Zhang, Sensor attack detection and isolation based on sliding mode observer for cyber-physical systems. Int. J. Adapt. Control Signal Process. **34**(4), 469–483 (2020)
K. Zhang, C. Keliris, T. Parisini, M.M. Polycarpou, Identification of sensor replay attacks and physical faults for cyber-physical systems. IEEE Control Syst. Lett. (2021a)
K. Zhang, C. Keliris, M.M. Polycarpou, T. Parisini, Discrimination between replay attacks and sensor faults for cyber-physical systems via event-triggered communication. Eur. J. Control (2021b)
J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, Y. Xiang, Deep learning based attack detection for cyber-physical system cybersecurity: a survey. IEEE/CAA J. Automatica Sinica (2021c)
D. Zhang, Q.-G. Wang, G. Feng, Y. Shi, A. V. Vasilakos, A survey on attack detection, estimation and control of industrial cyber–physical systems. ISA Trans. (2021d)
T. Zhang, Y. Wang, X. Liang, Z. Zhuang, W. Xu, Cyber attacks in cyber-physical power systems: a case study with gprs-based scada systems, in *29th Chinese control and decision conference (CCDC)* (IEEE, 2017), pp. 6847–6852

X. Zhang, F. Zhu, Observer-based sensor attack diagnosis for cyber-physical systems via zonotope theory. Asian J. Control (2020)
H. Zhang, Y. Shu, P. Cheng, J. Chen, Privacy and performance trade-off in cyber-physical systems. IEEE Netw. **30**(2), 62–66 (2016)
D. Zhao, Z. Wang, D.W. Ho, G. Wei, Observer-based PID security control for discrete time-delay systems under cyber-attacks, in *IEEE Transactions on Systems, Man, and Cybernetics: Systems* (2019)
K. Zhou, J. Doyle, *Diagnosis and Fault-Tolerant Control* (Prentice-Hall, 1998)
Q. Zhu, T. Basar, Robust and resilient control design for cyber-physical systems with an application to power systems, in *50th IEEE Conference on Decision and Control* (IEEE, 2011)
M. Zhu, K. Ye, C.-Z. Xu, Network anomaly detection and identification based on deep learning methods, in *International Conference on Cloud Computing* (Springer, 2018), pp. 219–234
M. Zhu, S. Martinez, On the performance analysis of resilient networked control systems under replay attacks. IEEE Trans. Autom. Control **59**(3), 804–808 (2013)
Y. Zhu, W.X. Zheng, Observer-based control for cyber-physical systems with periodic dos attacks via a cyclic switching strategy. IEEE Trans. Autom. Control **65**(8), 3714–3721 (2019)