Bibliographical review on cyber attacks from a control oriented perspective

Helem S. Sánchez[a,b], Damiano Rotondo[a,c], Teresa Escobet[a,d], Vicenç Puig[a,b,c], Joseba Quevedo[a,b]

[a] *Research Center for Supervision, Safety and Automatic Control (CS2AC) of the Universitat Politècnica de Catalunya (UPC)*
[b] *Automatic Control Department, UPC-ESAII, Rambla de Sant Nebridi, 11, 08222 Terrassa, Spain*
[c] *Institut de Robotica i Informatica Industrial (IRI), UPC-CSIC Carrer de Llorens i Artigas, 4-6, 08028 Barcelona, Spain*
[d] *Department of Mining, Industrial and ICT Engineering, UPC, Av. de les Bases de Manresa, 61-73, 08242 Manresa, Spain*

Abstract

This paper presents a bibliographical review of definitions, classifications and applications concerning cyber attacks in networked control systems (NCSs) and cyber-physical systems (CPSs). This review tackles the topic from a control-oriented perspective, which is complementary to information or communication ones. After motivating the importance of developing new methods for attack detection and secure control, this review presents security objectives, attack modeling, and a characterization of considered attacks and threats presenting the detection mechanisms and remedial actions. In order to show the properties of each attack, as well as to provide some deeper insight into possible defense mechanisms, examples available in the literature are discussed. Finally, open research issues and paths are presented.

Keywords: Cyber-physical systems, networked control systems, cyber attacks, attack detection, secure control.

1. Introduction

With the advent of networks, the use of feedback control loops closed via communication networks has replaced traditional point-to-point control systems, giving birth to the concept of networked control systems (NCSs) [1]. An NCS connects the cyber space to the physical space, so that the

execution of several tasks is allowed remotely [2]. Compared with traditional control systems, NCSs have several advantages, such as low installation and maintenance costs, high reliability, increased system flexibility, and decreased wiring [3].

Strictly connected with NCSs, cyber-physical systems (CPSs) have attracted the attention of the research community, due to the need for a better integration of computation and physical processes. The term *cyber-physical* was first used by Helen Gill at the National Science Foundation in the USA [4] in order to indicate the presence of discrete processing and communication of information (*cyber*) together with the engineered system (*physical*). Although the related terminology is quite new, the emergence of this class of systems can be seen as the continuation of the technological evolution that began in the 18th century, when the first notions of feedback control (e.g., the steam engine governor) were applied during the Industrial Revolution [5]. Its first vision dates back to 1926, when Nikola Tesla described the *teleautomation concept*[1] [6], which is becoming true nowadays thanks to the widespread availability of smart-phones and similar devices. The same term *cyber-physical* systems comes from the root of the word *cybernetics*, which was coined by Norbert Wiener to define the interdisciplinarity of automatic control when applied to engineering, systems control, computer science, biology, neuroscience, philosophy and the organization of society.

In the same way as the frequency domain approach [7–9] and the state-space approach [10–12] can be seen as the theoretical foundations for the first and second generation of control systems, the development of CPSs can be seen as the arising of a third generation of control systems. Given the distributed nature of CPSs, it is natural to study them using techniques from the domain of NCSs [13]. Actually, both concepts are so closely related that it is hard to identify a clear frontier between them. The main difference comes especially from the different emphasis given to control in the case of

[1] *When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole. We shall be able to communicate with one another instantly, irrespective of distance. Not only this, but through television and telephony we shall see and hear one another as perfectly as though we were face to face, despite intervening distances of thousands of miles; and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket.* - Nikola Tesla

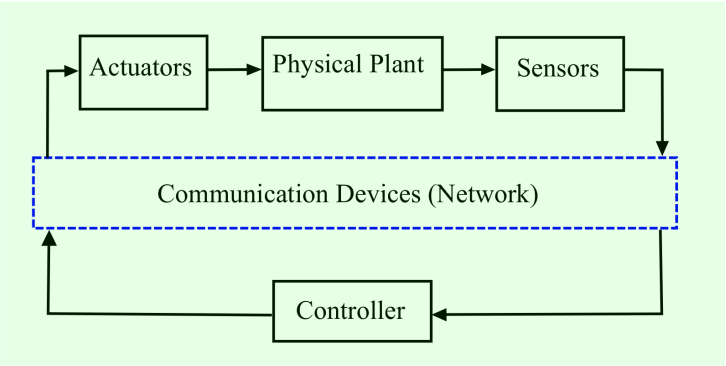

Figure 1: General architecture of a cyber physical system.

NCSs and to the component interconnection in the case of CPSs.

Modern NCSs and CPSs have revolutionized several areas, and have been used with success in many sectors, as resumed in Table 1. In its simplest form, a CPS consists of actuators, physical plant, sensors and controllers, interconnected by a communication network (see Fig. 1). Several architectures have been proposed to describe the data flow, and to adapt to the issues that arise depending on the field of application [14]. The most common architecture for CPSs is divided into seven layers : i) physical; ii) data link; iii) network; iv) transport; v) session; vi) presentation; and vii) application. However, alternative architectures have been proposed in the literature or in different drafts by standardization organizations, such as: service-based [15], event-oriented [16], information-centric [17], and machine-to-machine (M2M) [18], just to name a few.

The integration between cyber and physical components increases the efficiency of NCSs and CPSs but, at the same time, introduces the risk of cyber attacks, i.e., actions that exploit the system's vulnerabilities and result in some kind of damage. Cyber attacks can be malicious (trojan horses, computer worms, sabotage attacks) or unintentional (incorrect software updates, erroneous protocols, or unwanted network connections), and may occur in the cyber space, the physical world, or in both. The motivation for malicious attacks may arise from terrorism, geopolitics, criminality, or social issue driven organizations.

Over the past decade, many concerns have been raised about the vulnerabilities of control systems to both random cyber failures and security attacks.

Application Field	Description
Healthcare and medical system	Due to recent advances in medical sensors [19, 20], CPSs are potential candidates for healthcare applications [21] in which the patient's conditions can be observed remotely, and appropriate actions can be taken regardless of his or her location [22, 23]. Notable examples of healthcare applications are: electrical medical records (EMR) [24], LiveNet [25], HipGuard [26], MobiHealth [27], CodeBlue [28] and Health-CPS [29], just to name a few.
Energy systems	The systematic embedding of cyber technologies in order to adapt to new challenges and exhibit adaptive performance such as flexibility, efficiency, sustainability, reliability and security, has changed significantly energy systems, converting them into cyber-physical energy systems [30, 31]. Examples of energy applications are: zero-net energy buildings [32], smart grids [33] and next-generation wind energy conversion systems [34].
Smart transportation	In this case, the application of CPSs is motivated by the wish to achieve efficient and safe transportation. Since people are a key element in smart transportation problems [35], appropriate behavior information need to be integrated with the physical information. Smart transportation applications based on CPSs are: traffic control systems [35], car merging assistants [36], traffic flow control [37], traffic delay estimation [38], traffic flow dynamics [39] and vehicle tracking systems [40].
Automotive	Autonomous driving is an appealing emerging CPS technology, in which motion planning, sensor fusion, computer vision and other artificial intelligence algorithms are run in real-time inside a car [41]. Examples and challenges of the application of CPSs in the automotive domain can be found in [42–44].
Industrial process control	CPSs provide broad control capacity over complex industrial processes by exploiting the available network architecture of sensors, actuators and processors [45]. Many production control systems are made by several autonomous control systems, denoted as *stages*, and CPSs help in avoiding that the failure of a stage brings down the entire production line. Notably, CPSs are one of the key pieces of the Industry 4.0 paradigm [46], which refers to the deep integration of next generation information technologies into industrial scenarios, solutions and procedures [14].
Air transportation	By injecting cyber-physical interaction, e.g. by means of satellite-based aircraft navigation, trajectory-based flight operations, or sharing of aircraft position monitoring data, flights can be performed in an optimal and highly precise time [47], future aircraft maintenance processes can be improved, and the overall emissions for greener performances [48].
Water infrastructures	The breakthrough represented by CPSs has affected several water-based infrastructures, such as reservoirs [49], water and wastewater treatment plants [50] and water distribution systems [51]. These CPSs exploit the interaction between the physical water assets and the networked devices which were designed to monitor, operate and supervise the physical processes, such as sensor networks [52–54], mobile sensors [55] and smart meters [56, 57].
Other applications	CPSs have found applications in many other fields, among which: smart buildings [58], social networks and gaming [59, 60], cloud computing [61], surveillance [62], search engines [63], civil engineering [64], and robotics [65].

Table 1: Existing applications of CPSs.

As remarked by [66], the consequences of a successful attack on control networks can be more damaging than attacks on other networks, because control systems are at the core of many critical infrastructures. Attacks against medical CPSs can harm or kill patients by reprogramming the devices [67] (e.g., an attacker might program an infusion pump to administer a larger than necessary dose of medicine [22]), or prevent them from performing their tasks [68]. Recent history provides several examples of cyber attacks on electric infrastructures, which illustrate the threat that they represent, and show the necesity to investigate about prevention and protection from them [69]. In 2007, the Department of Defense of the United States conducted an experiment where a replica of a power plant control system was hacked, causing a generator to self-destroy [70]. In 2008, Ira Winkler (a penetration-testing consultant) and a team of other experts took a day to launch an attack on a power company's desktops, taking over several machines and obtaining the ability to hack into the control network, thus overseeing power production and distribution [71]. At the same time, a study of the Government Accountability Office of the United States showed that the Tennessee Valley Authority (TVA) was vulnerable to cyber attacks that could sabotage critical systems that provide electricity to more than 8.7 million people, due to several weak configurations, such as bad configured firewalls, lack of effective virus protection and weak passwords [72]. Moreover, in March 2008, a unit of the Hatch power plant (Georgia, United States) was forced into an emergency shutdown for 48 hours after a software update was installed on a single computer. When the computer rebooted, the lack of data in the system was interpreted as a drop in the reactor's cooling water, which was treated by the plant as a severe failure [73].

It is relevant to recall that the Tennessee Eastman process (a continuous, nonlinear two-phase reactor [74]) has been used to analyse the effects of attacks in the process control domain, with some experimental work conducted by [75] and [76]. In [77], *process diagnostic* for the Tennessee Eastman plant, i.e. testing and evaluating its performance and reaction to new or unknown conditions, was performed in such a way that the resilience against cyber-physical assaults could be tested. In particular, various integrity, denial of service (DoS) and situational awareness attacks were considered. A remarkable attack to a water distribution facility happened in 2000 at Maroochy Water Services (Queensland, Australia), affecting the SCADA of a sewage system, which caused the release of almost 1 million liters of wastewater into waterways and parks [78]. Other relevant incidents are the Pennsylvania Wa-

ter Company hack in 2006, as well as the Florida's Key Largo Wastewater Treatment District hack, and the computer malfunction blamed for major sewage spill into the Tijuana River in 2012 [79]. These events have motivated a lot of recent research on cyber security in water systems, see e.g. the works about automated canal networks [80, 81], the synergic security for water networks [82], water distribution networks [83], and the creation of a water distribution testbed for motivating research in the design of secure cyber-physical systems [84].

Further examples of cyber attacks affecting critical infrastructures are listed in Table 2. NCSs and CPSs are likely to be affected by cyber attacks and failures on their physical infrastructure and on their data management or communication layer [93]. Their complexity and the heterogeneity of their components have introduced significant difficulties to secure and protect them [94]. At the same time, it is also difficult to trace, classify or identify the threat, which may move or spread, and target multiple components of the system. For this reason, research on cyber attacks and secure control has found increasing interest since the end of the last century. As a matter of fact, Fig. 2 shows the results provided by the database Scopus, where the total number of papers in which several words related to cyber attacks[2] were searched among title, abstract and keywords. It can be seen clearly that this research topic is currently in a phase of exponential growth.

Owing to this, we consider important to realize a bibliographic review on the literature related to definitions, classifications and applications concerning cyber attacks, with the purpose of shedding some lights on the origins, challenges and advances in this topic, and helping the research community to develop new strategies that can increase resilience to possible threats. In particular, this review will tackle the topic from a control-oriented perspective and, as such, the topic of security from the informatics or communication point of view will not be explored. The reader interested in these other perspectives is referred to available surveys in the literature, such as [95–97]. This review is structured as depicted in Fig. 3.

[2] *Cyber attacks*, *denial of service*, *replay attacks*, *false data injection attacks*, *zero dynamics attacks*, *covert attacks* and *secure control*.

Table 2: Cyber attacks affecting critical infrastructures.

Attack	Description
Siberian Pipeline Explosion (1982)	The first known cyber security incident involving a critical infrastructure. The attacker inserted a trojan horse into the SCADA system; the result was the most monumental non-nuclear explosion and fire ever seen from space [85, 86].
Chevron Emergency Alert System (1992)	A fired employee managed to disable emergency alert protocols in 22 states in the United State of America and six unspecified areas of Canada were on risk. The attacker hacked into the computer in New York and San José, California, and reconfigured them so that they would crash [87].
Worcester, MA Airport (1997)	A hacker entered and disabled a telephone computer that served the Worcester Airport in Massachusetts. As a result, many services such as the aviation control tower, the fire department, security, and various private airfreight companies, were disabled for six hours [87].
Gazprom (1999)	A hacker penetrated into Gazprom, a gas company in Russia; the hackers used a trojan horse to gain control of the central switchboard, which controls gas flows in pipelines [87].
CSX Corporation (2003)	A computer virus named Sobig shut down train signalling systems in Florida, U.S. It shut down the signalling, dispatching and other systems at CSX Corporation. There were no major incidents caused by this event, but trains were delayed [88].
Stuxnet (2010)	This worm infected industrial computer systems, compromised PLC, and tried to destroy centrifuges by frequently switching the speed, which ultimately led to their failure and to the disruption of the Iranian nuclear facility at Natanz. [89].
Night Dragon (2011)	Five global energy and oil firms were targeted by a combination of attacks including social engineering, trojans and Windows-based exploits. These attacks, which have been ongoing for over two years, although did not affect directly any SCADA system, allowed the attackers to exfiltrate data such as operational blueprints [88].
Flame (2012)	A piece of malware operating in Iran, Lebanon, Syria, Sudan, the West Bank and other places in the Middle East and North Africa for at least two years was used to extract documents and open a backdoor to infected systems, that allowed the attackers to tweak the toolkit and add new functionality [90].
Havex (2014)	This malware was earlier reported to have specific interest in the energy sector and, during the spring of 2014, in industrial control systems. The group behind it used an innovative trojan horse approach to compromise victims. A trojanized software installer dropped and executed this file as a part of the normal installation. The user was left with a working system, but the attacker had a backdoor to access and control the computer [91].
Ukrainian power companies (2015)	Power plants experienced unscheduled power outages impacting a large number of customers. There were also reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors. Public reports indicate that the Black Energy malware was discovered on the companies computer networks [92].

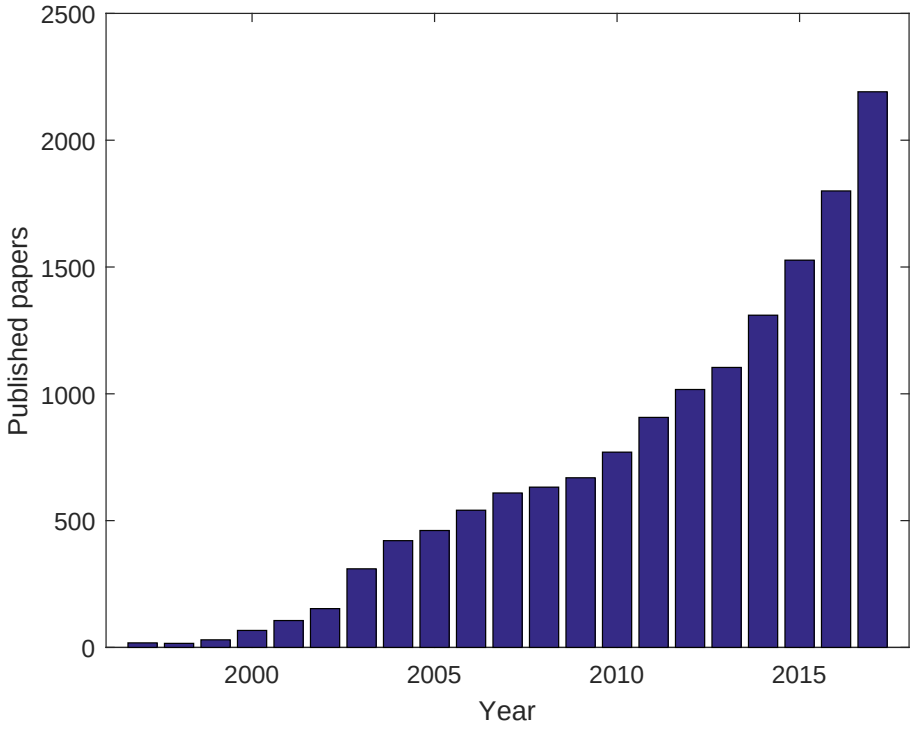

Figure 2: Searched results in Scopus.

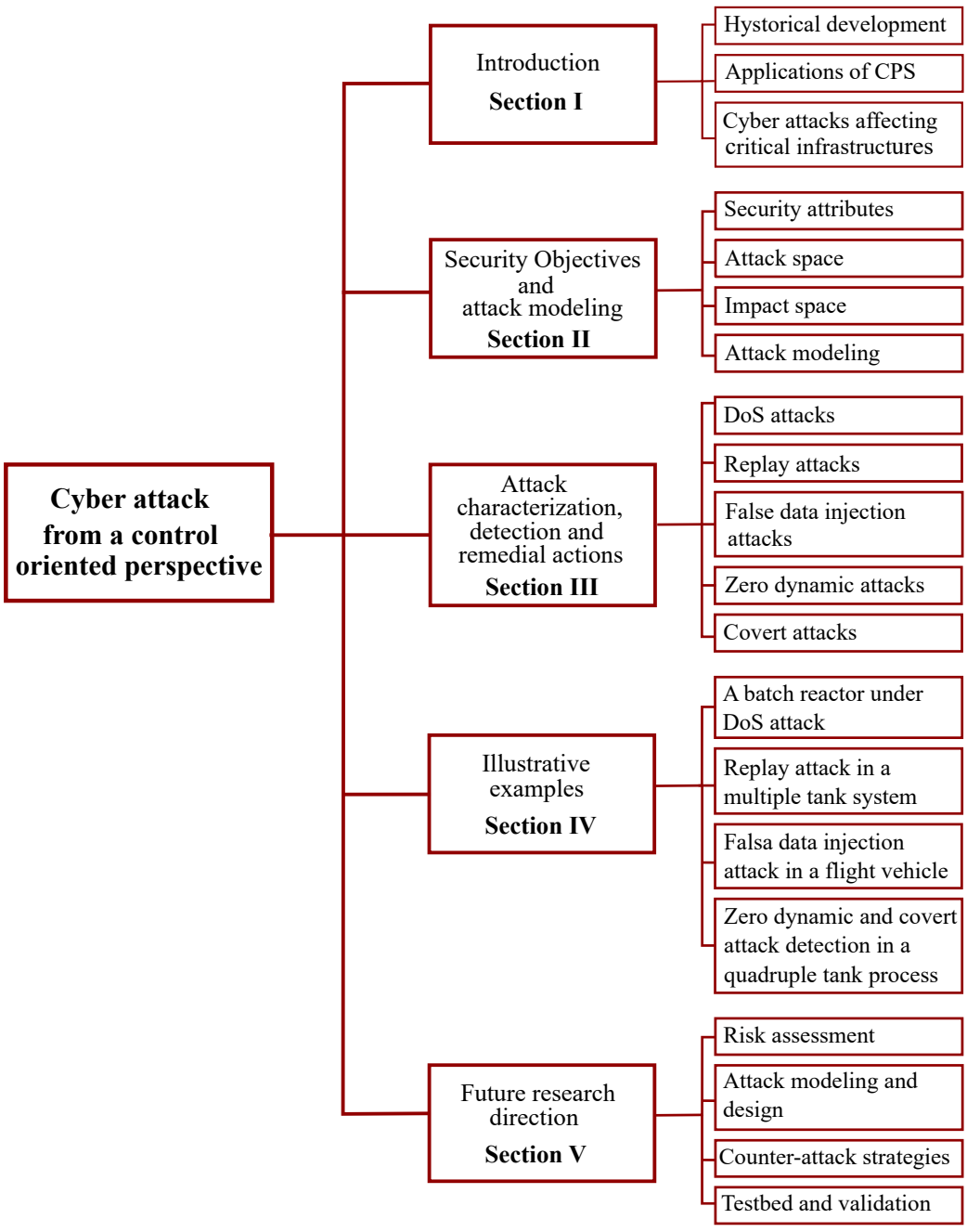

Figure 3: Structure of the review.

2. Security objectives and attack modeling

Recent studies have shown that there is a growing interest in security for CPSs [98–107] in order to detect, respond and recover an NCS or a CPS after a cyber attack has happened. Such an interest has materialized in a number of applications from different fields, such as medical devices [67], smart grids [102], industrial control systems [108] and transportation systems [109], and has lead to the development of new CPS architectures with enhanced security and robustness [110].

The concept of security was first introduced in the book [111] as a property which characterizes control systems affected by intentional malicious faults, i.e., cyber attacks. Since then, a lot of research on security has been performed that, according to [112], can be divided into two big categories: *information security* which, by focusing on encryption and data security, provides methods that are effective on software layers of NCSs and CPSs, without using any physical model [113]; and *secure control theory*, which studies how cyber attacks affect the control system's physical dynamics [114]. As stated by [112], the safety tools provided by information security need to be complemented by secure control theory which, being based on attack models and a description of the interaction between the physical world and the control system, allows a better understanding of the consequences of the attacks, and the development of new detection methods, algorithms and architectures, that make the control systems more resilient to possible attacks and failures.

The main target related to security is to design estimation and control algorithms that protect operational goals such as closed-loop stability, safety, reliability, or the optimization of some performance function, but also non-operational goals such as the date information from an attacker who wishes to disrupt the system. There are several definitions of security properties, with slight variations [115]. However, the most established definition of security is as the combination of three primary attributes, known by the acronym CIA (confidentiality, integrity and availability) [116]:

- **Confidentiality**: it refers to the ability to keep the information hidden from unauthorized users. A lack of confidentiality results in a disclosure of information, which is a circumstance or event whereby an entity gains access to information for which it is not authorized [117]. Achieving confidentiality in a control system would prevent an adversary from inferring the state of the physical system by eavesdropping

on the communication channels between the sensors and the controller, and between the controller and the actuators [118];

- **Integrity**: it refers to the capability of achieving operational goals by preventing, detecting, or blocking attacks on the information sent and received by the sensors, the actuators or the controllers [119]. In the context of control systems, integrity refers to the trustworthiness of sensor and control data packets. A lack of integrity results in deception, i.e., in a component receiving false data (such as incorrect measurements, incorrect time stamps, or incorrect sender identity) and believing it to be true [66];

- **Availability**: it is the property of the system or the system's components (sensors, controllers and actuators) to be accessible, usable or operational by an authorized system entity upon demand [66].

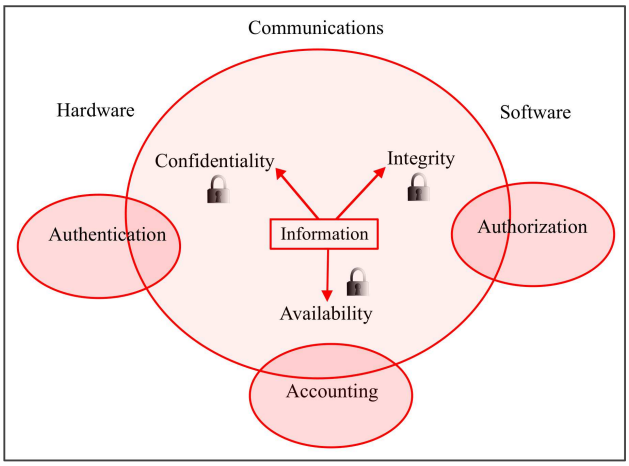

Figure 4: Security goals of CPSs.

Note that these three properties are necessary for achieving security in NCSs and CPSs, but they are not sufficient. In fact, according to [120], another set of properties, known by the acronym AAA, is needed in order to achieve security:

- **Authentication**: it is needed to ensure that the data, transactions, and the communications are original. Furthermore, it is important to

validate that all the implicated sides are who they claim to be [118] and not, e.g., impostors. According to [119], authentication in CPSs must be obtained in all the related processes, such as sensing, communication and actuation;

- **Authorization**: it provides the permission or approval to specific technology resources (e.g., access to the control unit, server, etc.), once the authentication has been performed;

- **Accounting**: it provides tracking of events, allowing to check the record of the possible activities carried out in the system (e.g., see at what time, location and who has performed an activity).

These properties are the main goals to achieve security, as shown in Fig. 4. Research challenges about security in control systems have been highlighted in [114], while [121] and [122] have provided surveys concerning topics related to security, presenting some trends and current efforts in securing the next generation of systems.

Cyber attacks consist in computer actions in remote or local connection (as e.g. program executions) which aim at compromising the security of the system by affecting one or more security attributes [123]. Notably, when it comes to the development of secure control theory, only the three primary attributes CIA have been considered, such that the attention on the secondary attributes AAA has been restricted so far to information security. Distinguishing features of cyber attacks, which differentiate them from faults, are that they appear in the system without any signs or hints of a failure, they are performed in an intelligent manner, with a purpose (such as sabotage or theft), and they have the ability of spreading within seconds. According to [124], the attackers usually wish to disrupt the measurements or the physical states in the control system, while avoiding being detected by the monitoring systems, which is usually achieved by maximizing the time between the beginning of the attack and its detection. The impact of cyber attacks has been investigated in [125–128], where some insight into the impact of cyber security have been presented, while an asset-based dynamic impact assessment has been developed in [129].

The literature on cyber attacks is fairly new, and many classifications have been proposed, see e.g. the ones provided by [66, 129, 130]. A successful classification is the one proposed by [131, 132], who introduced the *attack space* as a three dimensional graphical characterization of the attacks. The three

dimensions correspond to the attacker's a priori knowledge of the system's model, the disruption resources and the disclosure resources. The knowledge of the system's model allows the attacker to develop sophisticated attacks, which have more severe consequences and are harder to detect. The disclosure resources let the attacker obtain sensitive informations, but cannot be used to disrupt the system operation in order to cause damage. Conversely, the disruption resources can be used to affect the system operation.

Finally, in order to describe comprehensively the attacks, two elements are needed: a mathematical model of the control system and a description of the attack policy. Following [124], a CPS can be described as a descriptor system [133][3]:

$$E\dot{x}(t) = Ax(t) + Bu(t) + Fw(t) \tag{1}$$
$$y(t) = Cx(t) + Dw(t) \tag{2}$$

where x is the state, u is the control input (actuator signals), y is the output (sensor data), A, B, C, D, E, F are matrices of appropriate dimensions (with E possibly singular), and $w(t)$ is a signal which is used to describe the effect of cyber attacks on the control system.

On the other hand, the attack policy [131] describes the adversary model, and is defined as:

$$a(t) = [\tilde{u}(t), \tilde{y}(t)] = h\left(S, u(t), y(t)\right) \tag{3}$$

where $a(t)$ is the attack vector at time t, S represents the system knowledge including the physical plant, the controller and the detector, while $\tilde{u}(t)$ and $\tilde{y}(t)$ are the corrupted sensor and actuator, which is used in the equations (1)-(2) instead of $u(t)$ and $y(t)$, respectively.

In this review, along with the classification proposed by [131, 132] in terms of the *attack space*, we propose an additional classification based on the model (1)-(2) and the attack policy (3). This classification considers whether the attack corrupts $u(t)$ and $y(t)$ into $\tilde{u}(t)$ and $\tilde{y}(t)$, or if the attacker interacts with the system by means of the signal $w(t)$. In this way, another three dimensional graphical characterization of the attacks can be obtained, which will be referred to in the following as *impact space*.

[3]Note that a discrete-time setting can also be considered, see e.g. [131].

3. Attack characterization, detection and remedial actions

This section provides a description of the possible attacks and threats, as well as a detailed discussion about the results developed in the literature in order to characterize them, analyze their impact and suggest defense mechanisms that allow detecting or counteracting them. Since this paper aims at providing a review on cyber attacks from a control oriented perspective, the description of attacks concerning information security (such as man-in-the-middle attacks [134], compromised key attacks [135] and routing attacks [136]) will be omitted. Hence, five attacks will be described: i) denial of service (DoS) attacks, ii) replay attacks, iii) false data injection attacks (FDIAs), iv) zero dynamics attacks (ZDAs), and v) covert attacks, for which Fig. 5, inspired by the work of [132], provides their positioning in terms of the attack space while Fig. 6 provides their positioning with respect to the impact space described in the previous section. Moreover, Table 3 provides a classification of papers according to the application field. It is worth remarking that real events concerning cyber attacks are performed usually as a combination of the simpler (and more ideal) cases described in the academic literature[4].

Table 3: Application fields

Application field	**References**
Batch reactor system	[138]
Electricity market	[100, 139–149]
Power systems	[150–166]
Servo system	[167]
Smart grids	[168–201]
Unmanned vehicles	[202]
Water systems	[203–214]

3.1. DoS attacks

DoS attacks, also referred to as *jamming attacks* [215], prevent the actuator and sensor data from reaching their respective destinations [66], resulting in a loss of availability. In order to generate a DoS attack, once the attacker

[4]As a matter of example, the synchronized and coordinated cyber attack that caused the 2015 Ukraine blackout used a combination of credential theft via phishing, DoS attack and firmware attack in order to enable the primary attack, which used SCADA hijack with malicious operation to open breakers and cause a power outage [137].

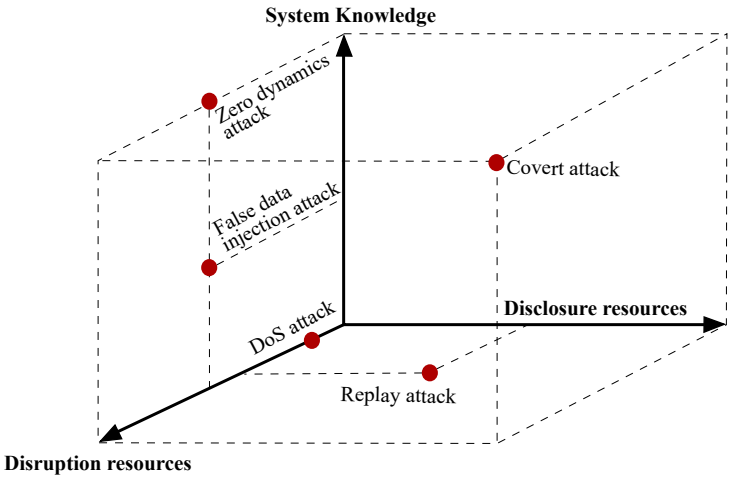

Figure 5: Positioning of the five attacks in the *attack space*.

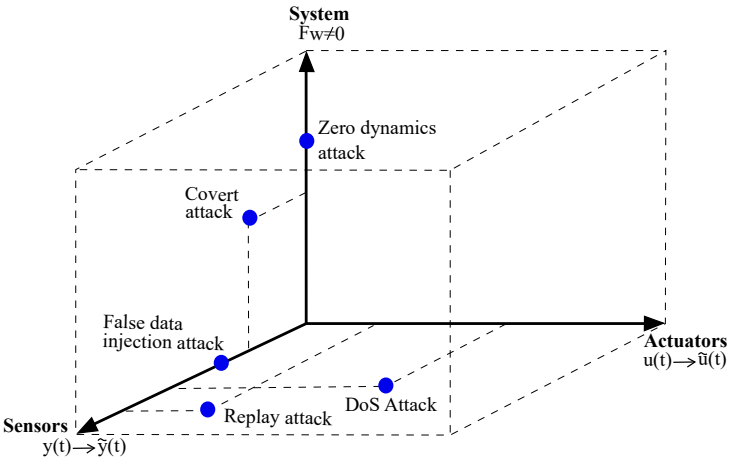

Figure 6: Positioning of the five attacks in the *impact space*.

has gained access to the communication network, he/she can jam the communication channels, compromise devices and prevent them from sending data, attack the routing protocols, flood with network traffic some devices, etc. [66]. DoS attacks have been listed as one of the most financially expensive security threats [216] and, according to a database on cyber incidents affecting the industry [217], they are the most likely threat to control systems.

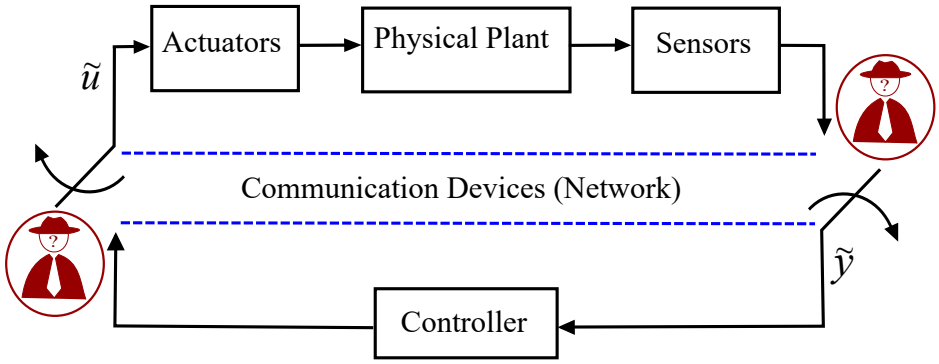

Figure 7: Example of DoS attack scenario.

For this reason, several case studies have been considered to analyze their effects (see Table 4 for a resume of relevant works found in the literature). As mentioned by [104], a DoS attack does not require any model knowledge ($S = \emptyset$ according to the attack policy (3)) and does not causes disclosure of the resources.

In Fig. 7, an example of DoS attack is presented, in which the attacker prevents the plant from communicating with the controller. Note that DoS attacks can result in either a complete lack of data or in the replacement of the absent data with the last received/transmitted data. The first case, referred to as *zero-input strategy*, has been considered by [221, 222] and, following [223, 224], can be expressed by particularizing the attack policy (3) as $\tilde{y}(t) = 0$ or $\tilde{u}(t) = 0$ for DoS attacks affecting the sensors or the actuators, respectively. On the other hand, the second case (*hold-input strategy*), has been considered by [225, 226], and can be modeled as [132] $\tilde{y}(t) = y_{\tau_y}$ or $\tilde{u}(t) = u_{\tau_u}$, where y_{τ_y} and u_{τ_u} are the last available sensor and actuator data, respectively. Notably, [227] has studied the LQ performance of networked control systems in both cases, and has showed that none of the two could be claimed to be superior to the other, since one can find many scenarios where one strategy performs better than the other, while there are scenarios where the converse occurs. Since DoS attacks corrupt both $u(t)$ and $y(t)$, they are placed on the sensors-actuators plane of the impact space depicted in Fig. 5.

In order to model the loss of information caused by DoS attacks, several mathematical models have been proposed. The first steps towards understanding DoS attacks were rooted in networked control formulations of

Table 4: DoS attacks - Case studies

Case study	Description
Uninterrupted power systems (UPSs) [150]	The resilient voltage regulation of a UPS is performed by means of a hybrid-theoretical framework, in which the controller switches in accordance with the competing result of the cyber attacker and the defender. The output voltage is shown to be maintained at a desired setting under DoS attack.
Automotive CAN networks [218]	This work summarizes the results of four selected tests performed on automotive systems based on CAN bus technology, among which two DoS scenarios: the unauthorized blocking of a window system, and the suppression of the warning light system.
Chemical plants [75]	This paper evaluates the physical and economic consequences of the attacks on a chemical reactor system, revealing two important points: i) a DoS attack does not have a significant effect when the reactor is in the steady state; however, combining the DoS attack with an innocuous integrity attack, causes the reactor to move to an unsafe state; ii) increasing the operational cost of the reactor involves a completely different strategy than an attack on the plant safety.
Nuclear plants [219]	In January 2003, the Slammer worm struck the monitoring system of the Davis-Besse nuclear power plant in the US, causing congestion that slowed down the plant's network, eventually crashing the safety-parameter display system, which monitors the most important safety indicators.
Connected vehicle systems [220]	Vehicle-to-vehicle and vehicle-to-infrastructure communication make connected vehicles vulnerable to cyber attacks. This paper, by proposing a real-time scheme that can detect the occurrence of attacks, and estimate their effect on the connected vehicle system, can be considered a first step towards obtaining an attack-resilient control system.

packet drops caused by random events [228, 229], using relatively simple models, such as the Bernoulli one, in which the attacker randomly jams a measurement or control packet according to independent trials with given success probability [66, 222, 230]. In fact, this simpler model was deemed to be a good starting point for developing methodologies to perform risk sensitive control under DoS attacks [231]. However, real DoS attacks change their targets and strategies in response to the protective measures taken against them, such that more advanced models were needed and later developed. These models take into account the existence of limitations on the resources of the attacker, which limits the number of times a transmission can be blocked, as well as the attack duration. The reader can find a list of the most significant DoS models, together with related works, in Table 5.

Table 5: DoS attacks - Mathematical models

Model type	References	Model type	References
Bernoulli models	[66, 167, 222, 230, 231]	Periodic or PWM signals	[232, 233]
Markov models	[150, 234, 235]	Unstructured signals	[138, 236–240]
Queuing models	[241]	Time delay	[151, 242]

Several works have considered the problem of making a control system resilient against DoS attacks, which could be achieved either by designing control laws that are robust against the attacker's actions [66] or, in case sensor measurements are compromised, by means of secure state estimation [152]. From a mathematical point of view, the problem can be characterized as the one of finding an optimal control policy γ^* among all the possible control policies $\gamma \in \Gamma$ such that for some cost function of interest $J(\gamma, \mu)$, where $\mu \in \mathcal{M}$ denotes the possible attack policies:

$$J(\gamma^*, \mu) \leq J(\gamma, \mu) \qquad \forall \gamma \in \Gamma, \forall \mu \in \mathcal{M} \tag{4}$$

A list of strategies that have proven to be successful for achieving this goal, and the related references, are provided in Table 6.

Table 6: DoS attacks - Resilient control strategies

Strategy	**References**	**Strategy**	**References**
LQG control	[66, 222, 243]	Robust control	[150, 151, 153, 235]
Risk sensitive control	[231, 234]	Event-triggered control	[232, 233, 236–240, 244]

Conversely, the opposite problem is to consider the DoS attack from the attacker point of view, meaning that optimal strategies for making the attack efficient and hard to detect have been studied [230, 244–248] which, similarly to the above, can be characterized as finding $\mu^* \in \mathcal{M}$ such that:

$$J(\gamma, \mu) \leq J(\gamma, \mu^*) \qquad \forall \gamma \in \Gamma, \forall \mu \in \mathcal{M} \tag{5}$$

Note that in this case, the assumption that the attacker does not have any physical knowledge about the plant can be relaxed to some extent, in order to allow for some knowledge concerning the plant itself or the existing implementation of secure control/anomaly detection techniques.

When the defender and the attacker are not studied independently, but considered together, a race between the two entities arises (where the controller is the minimizer and the attacker is the maximizer), which has an equilibrium corresponding to some pair $(\gamma^*, \mu^*) \in \Gamma \times \mathcal{M}$ such that [243]:

$$J(\gamma^*, \mu) \leq J(\gamma, \mu) \leq J(\gamma, \mu^*) \qquad \forall \gamma \in \Gamma, \forall \mu \in \mathcal{M} \tag{6}$$

which can be found using elements from the game theory [153, 243, 249–252].

An alternative mechanism to increase the defense properties of a system against DoS attacks is attack detection. Attack detection schemes expose the

attacks after they happen by monitoring unexpected changes in the measured variables [253]. The existing approaches can be classified mainly into two categories: pattern-based and anomaly-based. Pattern-based approaches (using, e.g., on state transition analysis [254] or Petri nets [255]) compare real-time data with available records of data corresponding to attack situations, hence they are effective only in the case of known attacks, because new or slightly modified old attacks would not have related data stored for comparison. On the other hand, anomaly-based detection approaches detect deviations from normal or expected behavior of the system, without any prior knowledge of the attack. A list of techniques proposed for performing anomaly-based DoS attack detection is given in Table 7.

Table 7: DoS attacks - Anomaly-based detection techniques

Strategy	**References**	**Strategy**	**References**
Statistical methods	[256–259]	Data mining	[260–263]
Artificial intelligence	[264–270]	Information theoretic	[271]

For a comprehensive review on this attack and a discussion of the potential research directions on this topic, the reader is referred to [272, 273]. It is also worth recalling that a lot of recent literature on DoS attacks has focused on a specific kind referred to as *distributed DoS* (DDoS) attacks. DDoS attacks follow the same pattern as DoS attacks, but they are coordinated across many hijacked systems (*zombies*) by a single attacker (*master*), thanks to the use of botnets[5] [274]. As remarked by [216], techniques that detect DoS attacks also apply to DDoS attacks. The interested readers can find extensive surveys on DDoS attacks in [253, 273, 275–277], and the references therein.

3.2. Replay attacks

Replay attacks are a type of deception attacks in which the adversary replaces the real-time measurements coming from the sensors, or the control actions sent to the actuators, with previously recorded data. This attack is often depicted in movies, in which security videos are recorded and later replayed to hide thefts or sabotages. Other examples are the interception of smart grids' usage patterns by hijacking smart meters in order

[5] A botnet is a wide chain of hundreds or thousands of remotely controlled compromised hosts (zombies or bots or slave agents) under the control of one or more intruders to attack a particular victim [120, 253].

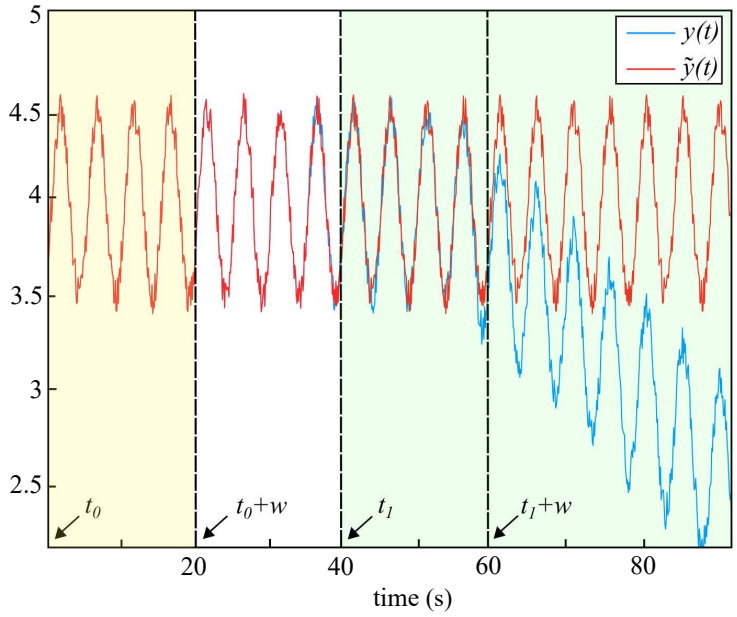

Figure 8: Example of a replay attack.

to produce inaccurate predictions of energy consumption [168, 169] and the famous Stuxnet case, in which a worm recorded the sensor values in the attacked uranium enrichment facility for twenty-one seconds, and replayed those twenty-one seconds in a constant loop during the attack, in order to keep it undetected by alarm routines and officials in the control room [278].

This type of attack is carried out in two stages (see Fig. 8):

1. In the first stage, the attacker collects the data without disturbing the system, such that $\tilde{u}(t) = u(t)$ and $\tilde{y}(t) = y(t)$. Note that this stage has been often referred to in the literature as *eavesdropping attack* [279];
2. In the second stage, the attacker begins to replay the collected data such that the attack policy (3) becomes $\tilde{u}(t) = u(t + t_0 - t_1 - (N_f - 1)w)$ or $\tilde{y}(t) = y(t + t_0 - t_1 - (N_f - 1)w)$ for attacks in the input and in the output, respectively, where t_0 is the time at which the recording of the data started, w is the size of the attack window, t_1 is the time at which the attacker begins to replay the collected data, and N_f indicates the number of repetitions of the recorded sequence.

Additionally, the attacker could have access to a set of external actuators,

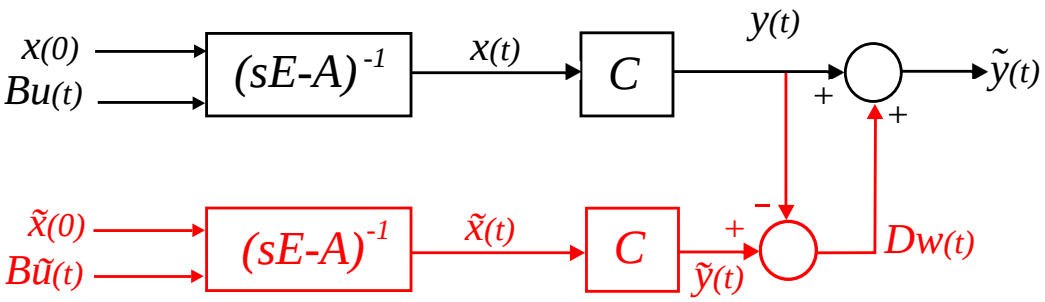

Figure 9: Block diagram representing a replay attack.

with some corresponding input matrix B_a, which can be used to inject an external input $u_a(t)$ and achieve some malicious objective, for instance, to cause physical damage to the attacked plant [280]. As stated by [281], the attacker does not need knowledge about the attacked system, except for being aware of the fact that the system itself will be in steady-state during the attack ($S = \emptyset$). However, in case the external input $u_a(t)$ could be injected, some knowledge of the system model (for example, $S = \{T_{ya}(s)\}$, where $T_{ya}(s)$ denotes the transfer function from the input $u_a(t)$ to the output $y(t)$) would allow a smart design of the input signal $u_a(t)$, which better achieves the malicious objective [280]. Since replay attacks can corrupt both $u(t)$ and $y(t)$, they are placed on the sensors-actuators plane of the impact space. In particular, the position of replay attacks w.r.t. DoS attacks in Fig. 6 aims at highlighting that most of the works found in the literature consider the case of replay attacks affecting the sensors rather than the actuators.

According to [282], there are three ways to perform a replay attack: i) in *open-loop*, if after disconnecting the actuator/sensor signal, the attacker sends all the recorded signal; ii) through *bias injection*, if the actuator/sensor is kept in the loop, but the attacker injects the difference between the real signal and the recorded signal; and iii) using an *internal model*, if the attacker inserts an internal model block which generates the repeated signal. Fig. 9 shows an example of block diagram for a replay attack performed through an internal model. In this case, the internal model generates fake measurements $\tilde{y}(t)$ using a pre-registered initial condition $\tilde{x}(0)$ and previously recorded control inputs $\tilde{u}(t)$. Then, the difference between the real measurements $y(t)$ and the generated ones $\tilde{y}(t)$, denoted as $Dw(t)$ following the notation introduced in (1)-(2), is injected into the sensors.

From the defender point of view, the actions to perform to face a replay attack vary depending on whether the attack is affecting the actuators or the sensors. While in the first case, it is possible to design control strategies which achieve resilience against the attack, see e.g. [202, 283], in the second case resilience is based on secure distributed fusion estimation, as detailed in [170]. In all these works, an assumption about the existence of energy constraints, which limit the maximum number of consecutive repetitions of the recorded sequence, was stated. Since in many scenarios, this assumption does not hold, much of the available literature has focused on replay attack detection, with the goal of shutting down the controlled plant as soon as a malicious behavior has been detected. The approaches available in the literature can be classified roughly into two categories (see Table 8).

Table 8: Replay attack detection - Existing approaches

Approach	**References**	**Approach**	**References**
Watermarking-based	[203, 280, 281, 284–286]	Alternative methods	[287, 288]

In the watermarking-based approaches, an authentication signal is added to the signal sent to the actuators (at the cost of sacrificing the control performance), and the received sensor measurements are analyzed to check whether there is or there is not the effect of the authentication signal on the physical system. If the attacker is unaware of the watermark or if he/she does not have enough knowledge about the plant's model, he/she is unable to provide a consistent output to be replayed. In [281], the authentication signal was drawn from an independent and identically distributed (IID) Gaussian distribution. [280] investigated further the problem of designing the optimal watermark signal in the class of stationary Gaussian processes, i.e. a generalization of the IID distribution, while satisfying constraints on the control performance. [284] considered a more advanced adversary, who could use knowledge of the system as well as access to a subset of the control inputs and sensor outputs to construct stealthy replayed outputs. In this case, it was shown that a Neyman-Pearson detector was optimal, in the sense of maximizing the probability of determining whether an attack has occurred for a given probability of false alarm. With the aim of reducing the negative effect on the closed-loop performance, while guaranteeing the detection performance, [203] proposed to employ a periodic watermarking strategy. The watermark considered by [285] aims at destabilizing the difference between the estimated and measured output of the system (residual), while preserving

the stability of the main system. On the other hand, the authentication signature used by [289, 290] is a sinusoidal signal with a time-varying frequency. Finally, a multi-agent extension of this concept was provided by [286], under the assumption that the watermarking signals could be shared among the agents through the network, which gives more degrees of freedom to detect the replay attack, thus resulting in better detection performance.

On the other hand, the alternative methods try to detect replay attacks without injecting signals in the control input. [287] assumed that the actuation and sensing signals were transmitted over an additive white Gaussian noise channel, and showed that the information distortion induced by the channel could play a similar role to the injected watermark. Such distortion could be studied by means of spectral estimation techniques, thus providing a viable detector for replay attacks. On the other hand, the approach developed by [288] inserted a nonlinear element in the control loop and exploited the theory of the describing function to design robust harmonic oscillations, which could be used for achieving the replay attack detection.

3.3. False data injection attacks (FDIAs)

The concept of FDIAs, in which the attacker injects malicious measurements to mislead the state estimation process [171], was first developed by [172]. This type of attack can be formulated against systems with unstable modes, in order to make them unobservable by means of an appropriate modification of the system measurements [291]. An exemplification of FDIA suggested by [292] is shown in Fig. 10, where the attacker corrupts the measurements in order to make the mode corresponding to the eigenvalue λ unobservable from the measurements. Obviously, if λ has positive real part, hiding this mode can lead to catastrophic consequences, since the controller would not be able anymore to stabilize the plant.

In its most basic form, an FDIA can be described by particularizing the attack policy (3) as $\tilde{u}(t) = u(t)$ and $\tilde{y}(t) = y(t) + y_a(t)$, where $y_a(t)$ is the malicious data added to the original measurements, thus constraining its position in the impact space to lie on the sensors axis. By denoting as $\tilde{x}(t)$ and $\hat{x}(t)$ the state estimates obtained using $\tilde{y}(t)$ and $y(t)$, respectively, the attacker can use knowledge about the relationship between state variables and sensor measurements ($S = \{C\}$) in order to construct $y_a(t)$ such that $\tilde{x}(t) = \hat{x}(t) + k(t)$, where $k(t)$ reflects the estimation error injected by the attacker. In particular, [172] showed that, by using $y_a(t) = Ck(t)$, the following

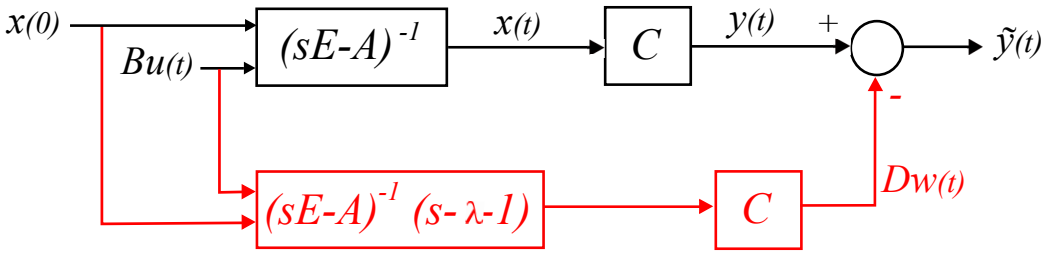

Figure 10: Block diagram representing an FDIA.

holds:

$$\|\tilde{y}(t) - C\tilde{x}(t)\| = \|y(t) - C\hat{x}(t)\| \tag{7}$$

such that the attacker can bypass existing bad measurement detection techniques.

Note that several works have relaxed the assumption that $S = \{C\}$, in order to take into account uncertainties in the system information gathered by the hacker, see e.g. [173–175]. Moreover, commonly analyzed scenarios involve cases where the attacker has limited access to sensors or limited resources to compromise them [172].

The research on FDIAs has focused on three main aspects [293]: theoretical research on constructing a valid FDIA, application research on the impacts of FDIAs, and defensive research, in which the key point is proposing defense strategies from the viewpoint of the system operator (see Table 9 for an overview).

3.3.1. Theoretical research on constructing FDIAs

Theoretical research on constructing FDIAs starts from relaxing the assumption that the attacker has gathered perfect knowledge about the system's output matrix C and he/she has access to all the measurements for manipulation. For this reason, several works have focused on designing FDIAs taking into account the existence of constraints and the availability of partial and imperfect information about the system. Early works have considered the case in which the attacker has full knowledge about the system, but has the ability to hack only a limited number of sensors [171, 172, 176]. In this situation, a relevant research problem is the one of constructing a valid FDIA by minimizing the number of attacked sensors, which has been solved using mixed-integer linear programming (MILP) [178], matching pursuit [172] or

Table 9: Overview of FDIA research.

Research	Description	References
Theoretical research on constructing FDIAs	The attacker has full knowledge about the system, but he/she can hack only a limited number of sensors.	[171, 172, 176–178]
	The attacker has incomplete information about the system	[139, 140, 154, 179, 180]
	The attacker can manipulate the topology of the system	[181]
	The attacker has to deal with a nonlinear system	[173, 182, 183]
	Analysis of security indexes to quantify the effort required to launch an FDIA	[184]
Application research on the impact of FDIAs	Economic attacks in electricity markets	[100, 141–149]
	Load redistribution attacks in power systems	[155, 156]
	Energy deceiving attacks in energy routing processes	[185]
Protection-based defense strategies	Locate and protect a set of basic measurements	[157, 158, 171, 186]
	Apply phasor measurement units (PMUs)	[159, 160, 187–189]
Detection-based defense strategies	Design-centric (DeC) approaches	[196, 197, 204, 205, 294, 295]
	Data-centric (DaC) approaches	[192, 193, 198, 205–210, 296]
	Other approaches	[162, 163, 190, 191, 194, 199–201, 297–301]

least absolute shrinkage and selection operator (LASSO) [177]. Later research has established that it is possible for an attacker to launch valid FDIAs even with incomplete information about the system. For example, [179] have shown that such information can be estimated using a combination of off-line data collection, during which the attacker collects the system information manually, and online data collection performed using hacked sensors. In the context of energy price regulation, [139] showed that the system topology could be recovered based solely on publicly available market data, upon observing successive outcomes of the linear programs usually employed to calculate real-time energy prices. On the other hand, [140] proposed an independent component analysis (ICA) algorithm that could extract topology information from the correlations among different measurements. Moreover, [180] showed that an FDIA can be launched on a subsystem without needing to know any network information about other subsystems in the network. [154] has considered an FDIA performed by a malicious software based on local information and measurements from its host substation, showing that artificial intelligence in the form of reinforcement learning can be used to learn how to conduct the attack. Very recently, the case in which the topology is being falsified, i.e. not only continuous data but also discrete data can be manipulated by the attacker (e.g. the on-off status of switching devices), has been considered, see e.g. [181]. Further topics of theoretical research on FDIAs are the nonlinear case, usually exemplified through AC power flow models [173, 182, 183], and the analysis of security indexes to quantify the least effort required to launch FDIAs without triggering bad-bata detection alarms [184].

3.3.2. Application research on the impact of FDIAs

Application research on the impacts of FDIAs has been conducted to study how these attacks affect the electricity market, power system operation, and distributed energy routing [293].

In order to integrate renewable sources and promote economic energy efficiency in smart grids, real-time electrical market mechanisms have been adopted with the goal to balance supply and load, clear market prices and maintain grid stability [302]. Through these mechanisms, the electricity price is updated periodically based on real-time power generation and consumption status, thus reducing over-provisioning and increasing the efficiency [303]. However, the deregulated energy market is vulnerable to FDIAs, by means of which the attacker can introduce errors and affect its operation. This type

of FDIA, which has been referred to as *economic attack* has been addressed by several works. [141, 142] were the first works to investigate the impact of FDIAs on power market. The evaluation of the generated market revenues and their maximization were studied by [100, 143]. Control theory was used by [144] with the goal of analyzing the effect of economic attacks on pricing stability. The relations between attackers and defenders within electricity prizing were modeled as a zero-sum game by [145]. Recently, the assumption that the attacker has full knowledge about the targeted power system has been relaxed by a few works, see e.g. [146–148]. A scenario based on the Australian electricity market trading mechanism has been analyzed by [149], showing that economic attacks pose no security threats to power systems, but mislead the customers to pay higher electricity bills. The power system operation can be affected by load redistribution attacks [155, 156], which aim at disrupting the security-constrained economic dispatch (SCED) in such a way that the system is driven to an uneconomic operating state. On the other hand, the energy deceiving attack is a type of FDIA that affects the energy routing process, potentially creating an imbalance between the demand and the supply, which can increase the cost of the energy distribution and disrupt its effectiveness [185].

3.3.3. Defensive research on FDIAs

The defensive research can be classified broadly into two categories [304], i.e. protection-based approaches [157, 171, 305] and detection-based approaches [190–194, 196, 197, 204, 294, 295]. In the first case, the system is protected from FDIAs by identifying critical sensors and ensuring their security by encryption. These methods suffer from two drawbacks [161]: i) the decrease of redundancy, because only the protected measurements are trusted and used; and ii) the protection might not be secure all of the time, since the attackers could penetrate the protection and manipulate the measurements. In particular, the works [172, 176] have demonstrated that it is necessary and sufficient to protect a set of basic measurements in order to be able to defend against FDIAs. Hence, some works have focused on researching how to locate and protect a set of basic measurements [157, 171, 186]. Other works have focused on applying phasor measurement units (PMUs), which are devices equipped with GPS technology for precise timing [187, 188]. Measurements obtained with PMUs are harder to be compromised by an attacker, although due to their high capital cost, they cannot be deployed on a large scale. Hence, it is important to find the best locations to place PMUs so

that their number can be minimized [159, 189]. The work [158] has focused on designing the least-budget defense strategy to achieve protection against FDIAs, investigating which sensors to be protected and how much defense budget to be deployed on each of them. Notably, some recent research has applied game theory to the case of FDIAs. For instance, [195] considered multiple adversaries and a single defender, showing that by defending a very small set of measurements, and taking into account that multiple attackers play a destructive role towards each other by carrying out attacks that cancel each other out, an equilibrium in which the attacks have no effect on the system can be achieved. On the other hand, [160] presented a two-layer attack-defense model for an FDIA against PMUs, in which the upper layer simulates the vulnerability of state estimation to the FDIA, and in the lower layer a two-player zero-sum game is used to determine the dynamic optimal strategy to protect and attack the PMUs.

Conversely, detection-based approaches aim at recognizing maliciously altered measurements, e.g. analyzing the raw measurements and detecting the ones that do not fit the distribution of historical data. Many detection-based approaches rely on state-based invariants to identify deviations of the plant from its normal behavior. Since this deviation is an *anomaly*, such approaches are referred to as *anomaly-based*, and can be divided roughly into two categories: design-centric (DeC) and data-centric (DaC) [205]. In DeC approaches, plant design and component specifications are input to an invariant generator, which uses fundamental laws of physics to generate invariants. Subsequently, statistical quality control techniques such as the cumulative sum control chart (CUSUM) [196, 197, 204, 294, 295] are used for monitoring changes such that attacks can be detected. On the other hand, in DaC approaches the invariants are generated via machine learning from plant state data describing the normal behavior of the plant [192, 193, 198, 206–210, 296]. It is worth mentioning that some recent research [205] has demonstrated the advantage of using a mix of DeC and DaC approaches, since this leads to a richer set of invariants and thus a higher accuracy of attack detection than when either approach is used without the other. Further approaches that fall in the detection-based category are the ones based on the Kullback-Leibler distance (KLD) [297], Markov graphs [191], Kalman filters [199], sparse optimization [190], generalized likelihood ratio [194], state forecasting [200], distributed observers [201, 298], sliding mode observers [299], principal component analysis [300], topology perturbation [301] wavelet transforms and deep neural networks [162]. Some recent work has focused also on enhancing

the detectability and identifiability of FDIAs without introducing significant operational cost, such as power losses on transmission lines [163]. The reader is referred to [306] for a detailed review of FDIA detection-based approaches with a qualitative comparison based on their properties.

3.4. Zero dynamics attacks (ZDAs)

ZDAs exploit the linearity of the plant as well as the existence of invariant zeros in order to be undetectable. In particular, [124] proved that an attack is undetectable if and only if it excites uniquely the zero dynamics of the input-output relationship, and [164] gave necessary and sufficient graph-theoretic conditions for the absence of zero dynamics, and hence for the absence of undetectable attacks. A scheme of ZDA is given in Fig. 11, where the attacker excites the zero dynamics of the plant by choosing appropriately the signal $Fw(t)$ such that it induces a state response $x_A(t)$ without producing a change in the output signal ($y_A(t) = 0$). Note that in this case $S = \{T_{yw}(s)\}$ since, in order to perform successfully the ZDA, the attacker needs to know how the available signal $w(t)$ affects the output $y(t)$, while $\tilde{u}(t) = u(t)$ and $\tilde{y}(t) = y(t)$, due to the fact that the attacker does not modify directly either signals. As a consequence, ZDAs are placed on the system axis of the impact space.

ZDAs are particularly critical when the attacked plant has some nonminimum phase zeros, since if the attacker knows the system model, then unstable modes can be introduced in the state response without being noticed by any type of detector. Worse yet, [165] has shown that even if the system model is known only up to some uncertainty, the attacker can still employ robust control techniques to construct a disturbance observer which generates an auxiliary zero dynamics, thus replacing the role of the real zero dynamics. Moreover, minimum phase plants are not completely safe from ZDAs: since most CPSs consist of an integration between the continuous-time physical plant and the discrete-time digital controller, they are sampled data systems. In the sampled data domain, unstable sampling zeros may be created when the continuous-time plant has relative degree greater than two and the sampling period is small, which happens in several critical infrastructures such as nuclear power plants and smart grids [307].

Since ZDAs cannot be detected from the output signal, classical fault detection strategies are useless to reveal these stealthy attacks, and alternative remedies must be seeked. One possible method is to modify the plant's

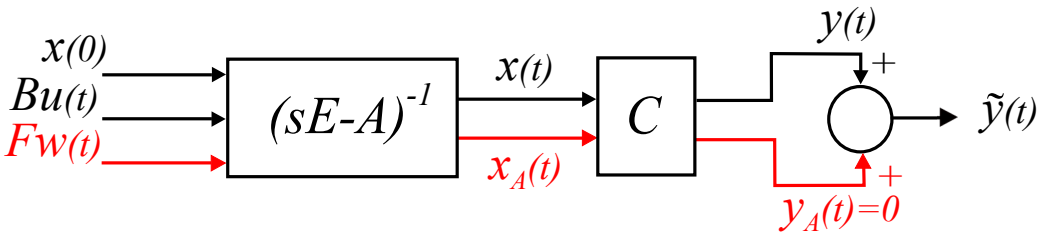

Figure 11: Block diagram representing a ZDA.

structure by changing actuators and sensors, as suggested by [308], who characterized classes of changes that reveal attacks, as well as those that do not. [309] noticed that multivariable zeros are linked to the input direction, which can be influenced by adding a modulation block in front of the control input, making harder to excite the zero dynamics of the system. The solution proposed by [166] is based on the multi-rate operation of the sampler, showing that if the sampler measures the system output more frequently than the attacker expects, the ZDA may become detectable in the extended measurements. In the case of sampled data systems, [307] proposed to make the outcome of the ZDA less effective by making the plant be of minimum phase through the use of a piecewise constant generalized hold.

Notably, some recent research has extended the notion of ZDA to stochastic systems, for which zero dynamics, as defined mathematically in systems theory, may not exist [310]. In this case, an attacker is defined to be stealthy if there exists no detector that can perform better than a detector that makes a decision by ignoring all the measurements and making a random guess to decide whether an attack is in progress or not. In particular, the work [310] characterizes some properties of such attacks, and quantifies the performance degradation that an attacker that seeks to be undetected can introduce.

3.5. Covert attacks

The term *covert agent* was introduced by [211] to denote a malicious agent who does not want to reveal to the controller that the CPS is being compromised. In this reference, it was shown that, under the assumption that the covert agent can modify the sensing and actuation signals, if the plant is linear, time-invariant and known to the covert agent, then the agent can use a parameterized feedback based structure to gain control of the plant in a manner that cannot be detected by the controller. A definition of covert

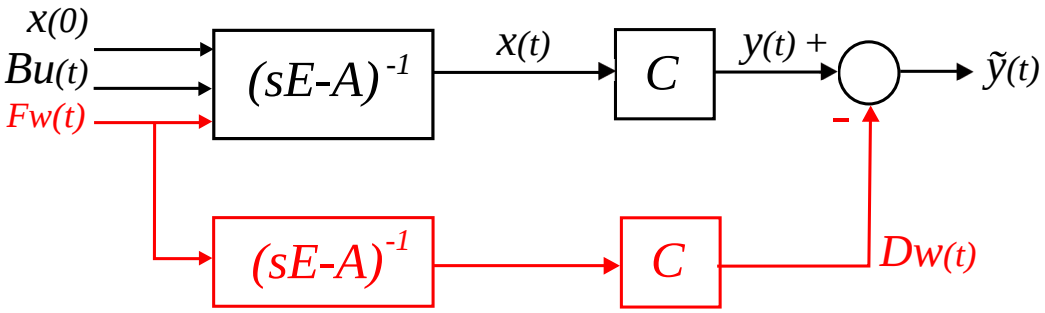

Figure 12: Block diagram representing a covert attack.

attacks was provided by Pasqualetti et al. within their theoretical framework as *closed-loop attacks in which the output is chosen to cancel out the effect on measurements of the state attack* [124]. A block diagram related to this definition is shown in Fig. 12: the attacker uses the signal $Fw(t)$ to affect the CPS while, at the same time, generating a signal $Dw(t)$ in such a way that the effect of $Fw(t)$ on the measurements is erased. In this case, the attack policy (3) can be particularized as: $\tilde{u}(t) = u(t)$, $\tilde{y}(t) = y(t) + Dw(t)$ and $S = \{T_{yw}(s)\}$, such that covert attacks are located on the system-sensors plane of the impact space. A classification of covert attacks into two categories was proposed by [311]: *cybernetically covert attacks*, which have low probability to be detected by algorithms that monitor the softwares, communications and data of the CPS; and *physically covert attacks*, which cause physical effects that cannot be easily noticed or identified by a human observer.

The design of successful covert attacks against output tracking control of CPSs was considered by [312] in which, based on whether the covert agent has perfect model knowledge or no model knowledge, sufficient conditions under which the output tracking control can be compromised successfully are proposed. On the other hand, [212, 213] have proposed a two-loop structure consisting of a covert loop and an attack loop. In particular, the covert loop covers up the effect of the real attack on the physical plant by closely imitating the expected behavior of the physical plant over a finite time window. As exploratory attempts to establish the feasibility of machine learning-based covert attacks, these works construct the attacks by applying least squares support vector machine (LSSVM). Comprehensive examples of covert attacks were provided in [313], namely an irrigation canal modeled by two partial differential (Saint-Venant) equations [314] and a nonlinear DC motor. It was

shown that the covert actions within the frequency range where the nominal control system has low sensitivity will be hard to detect and that the better the covert agent's model of the plant, the easier it is for the covert agent to remain undetected.

One approach to detect covert attacks is for the defender to gain more knowledge of the system than the attacker. [315] proposed to perform the detection by altering the system dynamics through the extension of the plant with time-variant external states. As mentioned in Section 3.4, [309] constructed a time-varying modulation matrix to change the system inputs, which allows detecting not only ZDAs, but covert attacks as well. The idea of the detection scheme proposed by [214] is to obtain this superior knowledge by extending the original plant with an auxiliary system. The auxiliary system is a switched system which changes its dynamics at random time instants, based on which a detection system which uses a switched Luenberger observer is presented.

An alternative approach to mitigate issues related to covert attacks has been suggested by [316]. Since covert attacks are designed based on an accurate model of the attacked system, it is possible to use a randomly switching controller to hinder the identification of the controller, so that the model obtained by the attacker is imprecise or ambiguous. When deciding for using this countermeasure, the existence of a tradeoff between mitigating the effect of the attack and increasing the settling time of the system, which is not necessarily a drawback, must be considered.

4. Illustrative examples

This section provides some examples taken from the literature concerning the listed cyber attacks, which are used to show some of their relevant properties and provide some deeper insight into possible defense mechanisms. We would like to point out that this section is not meant to be exhaustive from a descriptive viewpoint (several technical details are omitted, and the interested reader is referred to the provided references). Moreover, due to the review style of the paper, a comparison of different techniques is not included.

4.1. Resilient control of a batch reactor under DoS using a robust design

The paper [138] has studied NCSs in the presence of DoS attacks that prevent transmission over the communication network, and has characterized

a critical threshold for the duration and frequency of DoS attacks under which stability could be lost irrespective of the adopted controller.

The authors model the NCS as in (1)-(2), with $E = I, D = F = 0$, and assume that transmission attempts are carried out periodically with some constant period Δ. Due to DoS attacks, some transmission attempts may fail, according to a general DoS model that constrains the attacker action in time by posing limitations on the frequency of DoS attacks, i.e. an average time interval between attacks τ_D, and a bound $1/T$ on the average fraction of time over which communication is interrupted.

The control objective considered by [138] is to design the transmission period Δ and a controller K, possibly dynamic, in such a way that the maximum value of $1/T + \Delta/\tau_D$ for which closed-loop stability is preserved (resilient control) is as large as possible, in the sense of boundedness of the signals when noise and disturbances are considered. The main contribution is to show that when the process under control is observable, the closed-loop stability can be preserved for all the DoS signals which satisfy:

$$\frac{1}{T} + \frac{\Delta}{\tau_D} < 1 - (\mu - 1)\frac{\Delta}{\tau_D} \tag{8}$$

where μ is the observability index of $(C, e^{A\Delta})$.

The simulation results reported hereafter show the time response of a state of an open-loop unstable process (a batch reactor system [138]) under two DoS scenarios, where DoS signal equal to 1 corresponds to the attackless situation. In the first scenario, the condition (8) is satisfied, such that the overall closed-loop stability is kept. On the other hand, in the second scenario, the condition (8) is not satisfied, and the system under DoS attacks becomes unstable.

4.2. Replay attack detection in a multiple tank system

The paper [290] has presented a method for the detection of cyber attacks based on a watermarking approach. The overall scheme that achieves detection consists of: i) a decoupler, designed using a dynamical decoupling technique named *vector fitting*, which guarantees that a sinusoidal signal introduced in an input channel will affect only one output channel; ii) a bank of band-pass filters, each one extracting from the output the signal content at a possible frequency of the sinusoidal signature; and iii) a detection logic, which makes a decision about whether an output channel is being affected by a replay attack based on the energies of the band-pass filters' outputs.

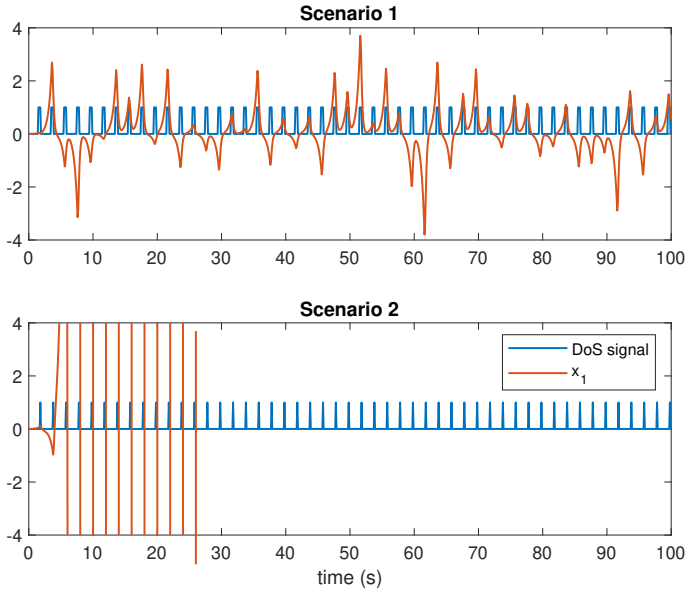

Figure 13: Time response of the state x_1 under DoS attacks (batch reactor).

Hereafter, we show the results obtained with the linearized model of a multiple tank system, in a scenario where the first output (level measurement of a tank) is affected by a replay attack starting from time 200 s. Fig. 14 shows the outputs of the band-pass filters (blue and yellow lines for $z_{low}(t)$ and $z_{high}(t)$, respectively) and the frequency profile of the time-varying sinusoidal signature (black line). Under no replay attack occurrence, the output of the band-pass filter with the biggest energy is the one corresponding to the instantaneous frequency $\omega_\sigma(t)$ of the signature (z_{low} if ω_σ has the low frequency value, z_{high} otherwise). On the other hand, under replay attack, this does not occur anymore, which allows deciding about the presence of a replay attack in the i-th output channel when $\sigma_i(t) \neq \hat{\sigma}_i(t)$, where $\hat{\sigma}_i(t)$ is the estimation of $\sigma_i(t)$ based on signals z_{low} and z_{high} (see Fig. 15). The reader is referred to [290] for technical details.

4.3. Security analysis and protection against FDIAs in a flight vehicle

The paper [318] has considered the problem of finding the conditions under which a state estimator is not protected against FDIAs, in the sense

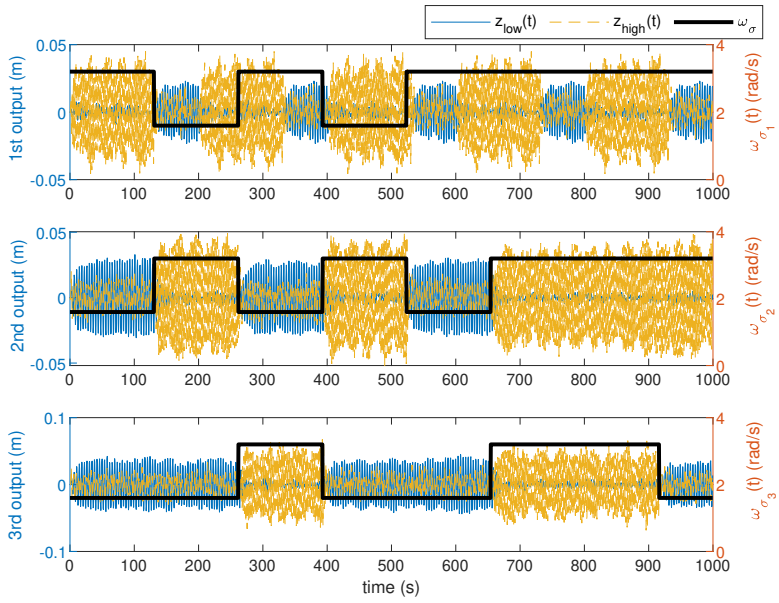

Figure 14: Outputs of the band-pass filters and signature frequency (multiple tank system) [289].

that there exist malicious attacks that can bypass χ^2-based anomaly detectors but still lead to unbounded estimation errors.

In particular, for an estimator (state observer) with estimation residual $z(k)$ and state estimate $\hat{x}(t)$, the system is insecure if the following two conditions are satisfied simultaneously: i) for the difference $\Delta\hat{x}(k)$ between the attackless state estimate $x^o(k)$ and the attacked state estimate $x^a(k)$:

$$\lim_{k\to\infty} \|\Delta\hat{x}(k)\| = \lim_{k\to\infty} \|x^a(k) - x^o(k)\| \to \infty \tag{9}$$

and ii) for the estimation residual difference $\Delta z(k) = z^o(k) - z^a(k)$ with $z^o(k)$, $z^a(k)$ denoting the attackless and attacked estimation residual, respectively, $\|\Delta z(k)\| \leq M$, where M represents the tolerant level of the χ^2 detector. [318] prove that, under the assumption that the attacker has perfect knowledge about the system model and the ability to inject false data over all the communication channels, the system is insecure if and only if $\rho(A) \geq 1$, where $\rho(A)$ denotes the spectral radius of A. [318] also provide an algorithm to construct the attack signal $a(k)$ to add to the sensors' measurements in order to deviate the state estimation without affecting the residual reference.

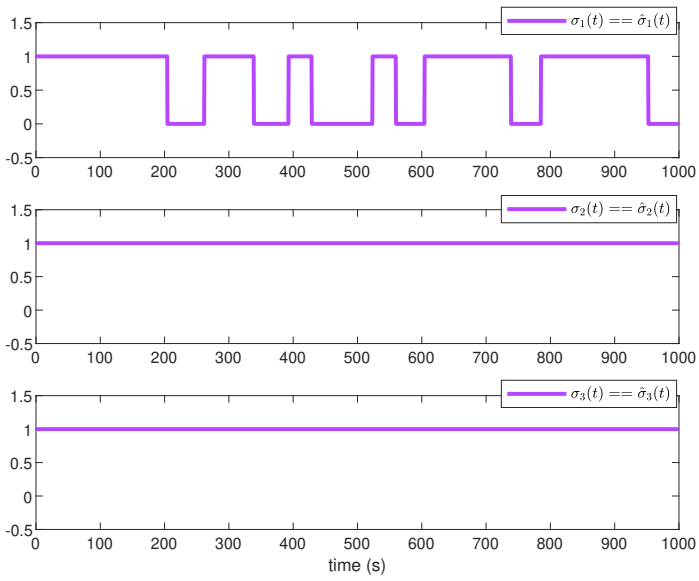

Figure 15: Comparison between the real signature frequencies $\sigma_i(t)$ and the estimated ones $\hat{\sigma}_i(t)$ (multiple tank system).

For instance, for a moving vehicle with three sensors measuring the three state variables (pitch angle, pitch rate and normal velocity) and one remote estimator, it is shown that one of the eigenvalues of the state matrix lies in 1, which makes the vehicle insecure. For instance, Fig. 16 shows the attack signal generated by Algorithm 1 in [318] which, exploiting the knowledge about the system, injects the attack above all in the direction corresponding to the marginally stable eigenvalue, although one should note that the values of $a_2(k)$ and $a_3(k)$ do not equal zero, which shows that false data are injected into all three communication channels.

Fig. 17 shows the state estimate difference $\Delta\hat{x}(k)$ and the residual difference $\Delta z(k)$. As predicted from the theory, the sequence $\{\Delta\hat{x}(k)\}$ diverges to ∞, whereas the sequence $\{|\Delta z(k)|\}$ is always less than the prescribed scalar M. Hence, under attack the estimated trajectory of the vehicle deviates significantly from the attackless scenario, albeit without triggering an alarm by the χ^2 detector.

Moreover, in case the assumption about the ability of the attacker to inject false data over all the communication channels is relaxed, [318] provide

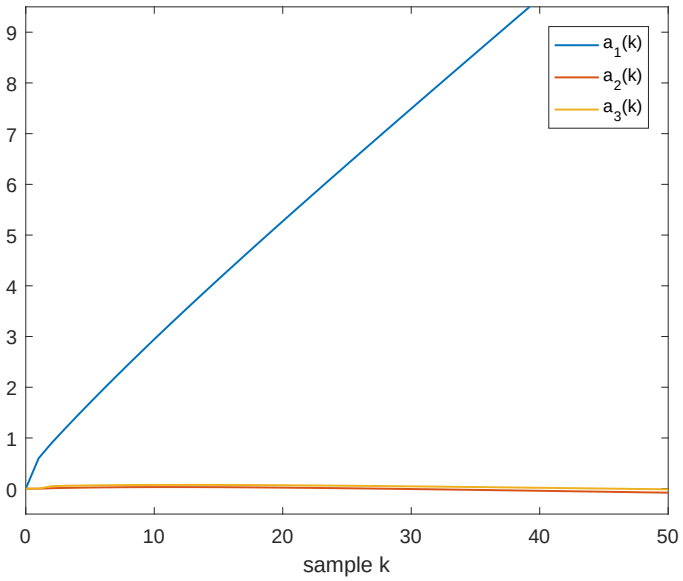

Figure 16: Attack sequences (FDIA in a flight vehicle).

another theoretical results (involving checking the rank of an appropriate matrix) that states under which conditions the estimator is secure. By applying this result, it can be proven that the state estimate system of the flight vehicle is secure if the communication channel between the pitch angle sensor and the estimator is protected.

4.4. ZDA and covert attack detection in a quadruple-tank process

The paper [308] has characterized the output-nulling property of a discrete-time system with structure similar to (1)-(2), with $E = I$, $D = 0$ and $F = B$. More specifically, they have demonstrated that any attack $w(k) = Hz(k)$ with $z(k+1) = (A+BH)z(k)$ and $(A+BF)\mathcal{V} \subseteq \mathcal{V} \subseteq \text{Ker}(C)$, where $\mathcal{V}$ is a controlled invariant subspace for the system, is such that if $z(0) = x(0) \in \mathcal{V}$, then $y(k) = 0\,\forall k \geq 0$. Indeed, Fig. 18 shows the simulated response under a ZDA attack of the linearized model of the quadruple-tank process described in [308], which is a system with two outputs and an unstable zero.

[308] have shown that in order to reveal a ZDA attack, appropriate modification should be introduced in the system's matrices so that the attack signal is no longer an output-nulling input. For instance, one might add an

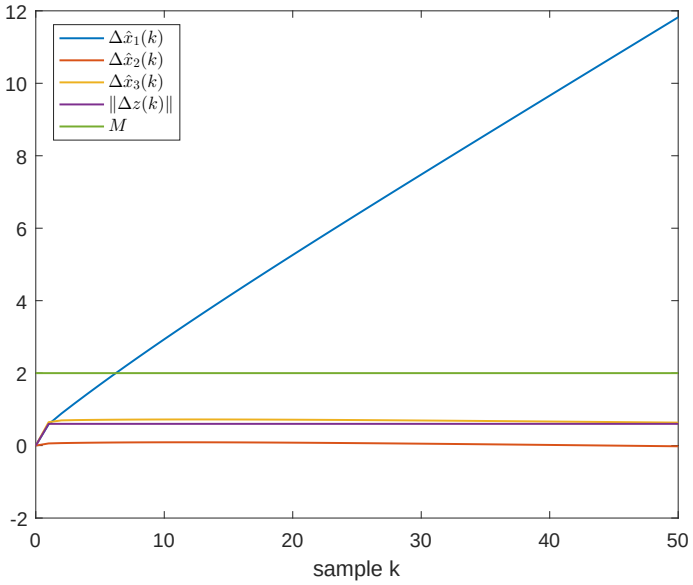

Figure 17: Estimation/residual differences (FDIA in a flight vehicle).

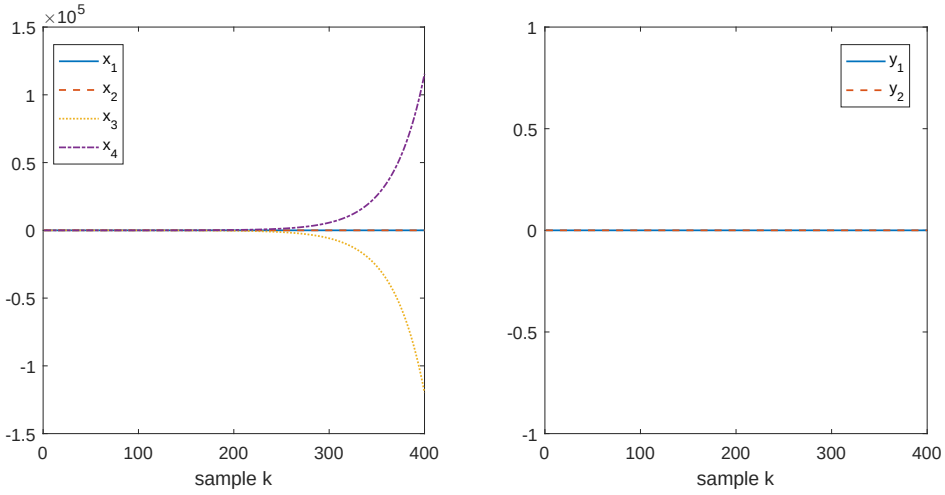

Figure 18: ZDA attack in the linearized model of the quadruple-tank process.

extra connection between tanks, which corresponds to a perturbation in the system's state matrix A. Alternatively, one can consider modification in the input matrix B, e.g., by changing the actuator gains as $\tilde{B} = BW$, where W is a diagonal matrix unknown to the attacker, which can be interpreted as a coding or encryption scheme performed by the actuator and the controller, with W as the shared private key. For instance, Fig. 19 shows the output responses obtained under the same conditions as the ones in Fig. 19, but assuming that a small perturbation in the matrix B is introduced ($W = 0.987I$) at sample $k = 200\,s$. It can be seen that thanks to this action, the attack becomes visible in the outputs, which allows the successful detection.

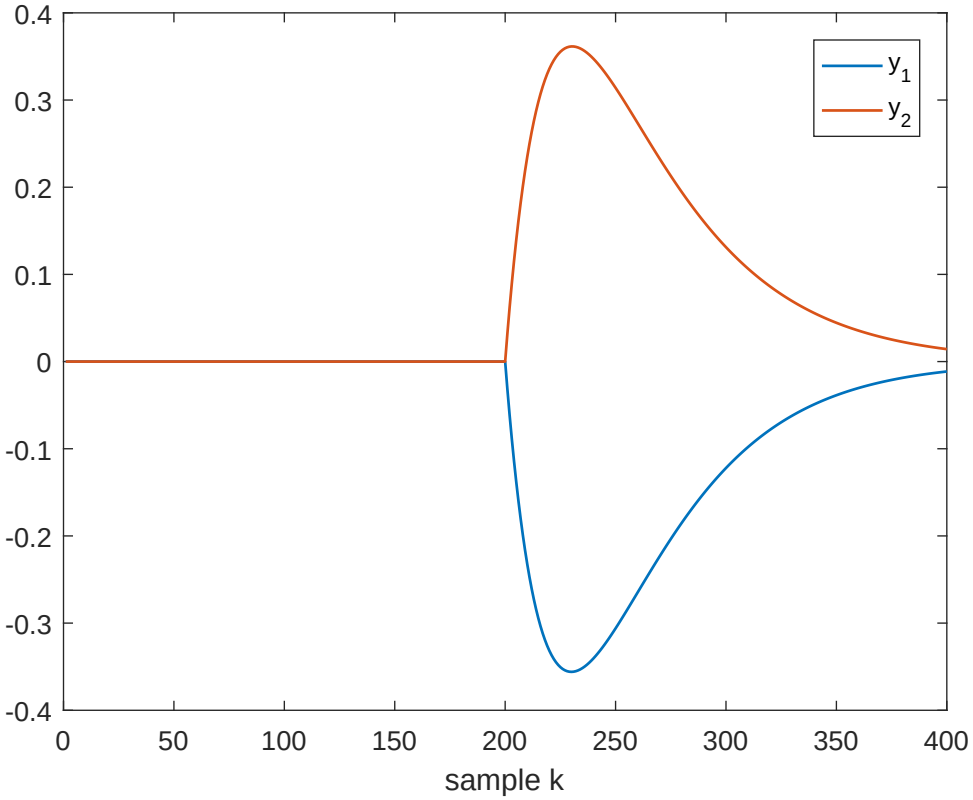

Figure 19: ZDA in the linearized model of the quadruple-tank process (perturbation in the matrix B).

Notably, the same strategy is effective to detect covert attacks. For instance, let us consider the case in which an attacker introduces sinusoidal signals $w(k)$ into the system, exploits its knowledge about the model to predict the component of the state response $x_w(k)$ which corresponds to the introduced attack signal, and modifies the output signals to remove $y_w(k) = Cx_w(k)$ from $y(k) = Cx(k)$ in order to hide the physical sinusoidal attack. For the sake of illustration, we will consider the attack to start from sample $k = 100$, and the above described strategy to reveal attacks (perturbation in the matrix B) to be implemented starting from sample $k = 200$. The overall state and output responses are depicted in Fig. 20, and show that the covert attack remains undetected until the perturbation in the matrix B is introduced.

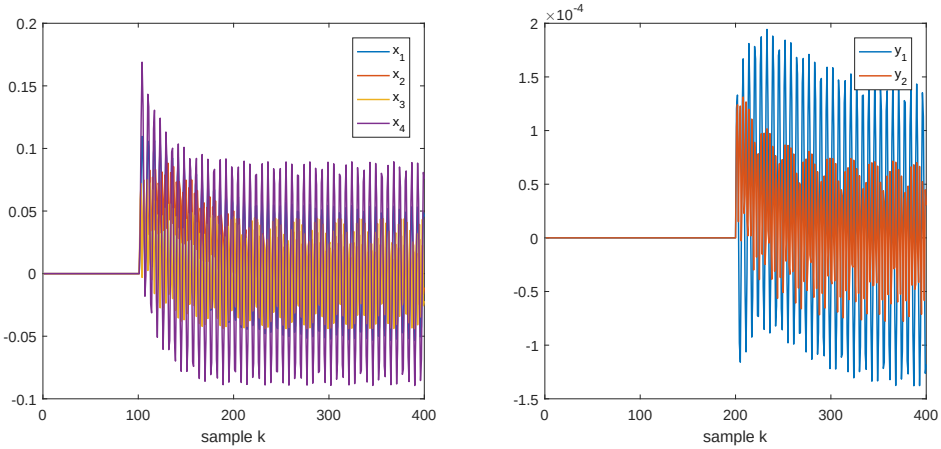

Figure 20: Covert attack in the linearized model of the quadruple-tank process (perturbation in the matrix B).

5. Future research directions

As systems and devices become more connected and the hardware and software involved in modern applications grow more powerful and productive, the risk due to malicious agents that use new technologies and techniques to penetrate networks and systems to steal data, violate the privacy and take remote control of assets, continues to increase. For this reason, there is a

never-ending quest for developing new solutions for addressing the cybersecurity challenges. Based on the existing research on cybersecurity, some works have discussed open issues and future directions for further research in the field.

As a consequence of the Executive Order 13636 *Improving Critical Infrastructure Cybersecurity*, issued by Former President of the USA Barack Obama in 2013, the National Institute of Standards and Technology (NIST) created the NIST Cybersecurity Framework, developed in collaboration with the industry, to provide guidance to organizations to better manage and reduce cybersecurity risks. In 2017, NIST produced a Roadmap [319], which provides a description of anticipated future activities related to this framework, focusing on 12 high-priority areas for research and development, listed below:

1. **Confidence Mechanisms** that, based on conformity assessment, provide means for determining the sufficiency and efficacy of organizational cybersecurity risk management, considering product, service, and systems conformity;
2. **Cyber-Attack Lifecycle**, which involves a sequence of events that a malicious agent undertakes to penetrate successfully a network for non-authorized purposes. It is important to approach cybersecurity from this perspective by identifying threat sources, threat events, and vulnerabilities that predispose an environment to be attacked. For this reason, it is important that cyber threat information is available in the form of threat and vulnerability metrics that support decision-making;
3. **Cybersecurity Workforce**, which is required to meet the unique cybersecurity needs of critical infrastructure. As threats, vulnerabilities, and technology evolve, the cybersecurity workforce should continuously adapt to design, develop, implement, maintain and improve the necessary cybersecurity procedures and mechanisms within critical infrastructure environments;
4. **Cyber Supply Chain Risk Management**, which is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of technology product and service supply chains;
5. **Federal Agency Cybersecurity Alignment**, which allows establishing cybersecurity recommendations and requirements for critical infrastructures at national level;

6. **Governance and Enterprise Risk Management**, that aligns the efforts of public and private sectors in terms of cybersecurity;
7. **Identity Management**, that faces current risk challenges, due to the using and adoption of new identity technologies as, e.g., biometric technology;
8. **International Aspects**, which relate to the lack of a common language or taxonomy among international entities relative to cybersecurity. Since many countries are developing their own standards, interoperability at international level is a challenging process. International collaboration and alignment, together with the development of globally accepted standards, guidelines and practices regarding cybersecurity, would lead to a more effective and efficient utilization of resources;
9. **Measuring Cybersecurity**, by developing reliable ways to measure risk and effectiveness of cybersecurity mechanisms;
10. **Privacy Engineering**, that deals with how to design information technologies and systems that protect individuals' privacy in an increasingly connected world;
11. **Referencing Techniques**, which has been added to the Roadmap to address the relationship of one set of cybersecurity requirements, controls, or outcomes, to another;
12. **Small Business Awareness and Resources**, due to the fact that a vulnerability common to many small businesses could pose a threat to a bigger economic base.

Notably, addressing present challenges in the field of cybersecurity is highly prioritized not only by the USA, but also by other entities, such as the European Union through H2020 research projects, e.g., Hermeneut[6]. As a matter of fact, the EU Commission has launched calls to support the creation of a cybersecurity competence network, with the goal of developing and implementing a common cybersecurity research and innovation roadmap[7].

As mentioned by [113], four points require major attention when research on cybersecurity is tackled from a control-oriented perspective:

1. **Risk assessment:** assessing how a risk impacts cybersecurity will provide a guide for designing mitigation methods. As such, qualitative

[6]https://www.hermeneut.eu/

[7]https://era.gv.at/object/news/3815

and quantitative approaches to vulnerability assessment are found to be in urgent need. For example, in order to assess and decrease the risk of threats, [104] proposed a risk management cycle which contains risk analysis, treatment, and monitoring.

2. **Attack modeling and design:** assumptions in existing works about the presence of noise and uncertainty, and about the knowledge of the system trajectory, should be reconsidered. The attackers' intentions and behaviors can be further studied in order to design effective defense mechanisms. According to [292], some aspects regarding the attacker with limited capabilities and specific goal requires future investigation. Generally, the attackers have limited capabilities, and they have access only to approximate models of some subsystems, and it is not clear if and how undetectable attacks can be cast [124].
3. **Counter-attack strategies:** how to design effective counter measures and detection algorithms for all known attacks, in order to degrade their impacts and minimize the damage to the system, is an open issue. In addition, how to reduce the economic cost of security mitigation and coordinate different security measures still need further study. The defense mechanisms have been classified in three different aspects [132]: prevention, detection and mitigation. Moreover, isolation can also be added, see for example [100, 124, 320].
4. **Testbed and validation:** with the development of new approaches to cybersecurity, testbeds are needed in order to evaluate the emerging theories, methods and techniques. These testbeds should provide a practical environment to conduct some attack-defense experimentations. In this sense, [321] has presented a benchmark for the detection and isolation of cyber attacks, based on a two tank system, in which a malicious attacker wants to remain hidden while stealing water, by altering the signals coming from the sensors. Moreover, [322] has introduced an open source Matlab toolbox called epanetCPA for modelling the hydraulic response of water distribution system for physical attacks. Similarly, the SWaT testbed [323] is based on a water treatment plant, and has been used to understand the impact of cyber & physical attacks. On the other hand, the Matpower Polish system, which is an open source Matlab-based power system simulation package, is so far the most used tool for assessing security in smart grids [324].

Furthermore, [224] has discussed about the limitations of existing ap-

proaches and proposed several challenging issues that deserve further research, some of which are resumed hereafter: the need for taking into account time-varying or nonlinear behaviors; how to make effective secure control schemes that satisfy hard constraints on security; to take into account that a system could be affected by multiple attacks; to fuse attack detection and resilient control in a uniform framework, which would lead to significant improvements in the security performance; to co-design the system parameters by considering both the security requirements and the resource constraints (communication bandwidth, limited energy, etc.).

6. Conclusions

The need for enhancing the security of networked control systems and cyber-physical systems has brought more and more attention to the topic of cyber attacks. This paper has presented a bibliographical review from the control-oriented perspective, which discusses some references found in the literature, thus providing an overall picture of historical, current, and future developments in this area. First, the security objectives and attack models are introduced. Then, a set of attacks considered in the literature are characterized introducing the proposed detection mechanisms and remedial actions. Later, some examples have been provided in order to show some features and characteristics of the described attacks and detection mechanisms. Finally, some future research directions in the cyberacttack field are described from a general and control-oriented perspective. In particular, the high-priority areas for research and development contained in the Roadmap for Improving Critical Infrastructure Cybersecurity of the USA National Institute of Standards and Technology have been described. Moreover, four points that require major attention when cybersecurity is tackled from a control-oriented perspective have been discussed (risk assessment, attack modeling and design, counter-attack strategies and testbed/validation), and the limitations of existing approaches and challenging issues that require further research have been mentioned.

Due to the huge amount of published papers (more than 2000 if we considered only the year 2017), the review is in no way meant to be exhaustive. We feel that we have done our best to provide to the readers a list of useful references, and whenever specific reviews about some topic were available, a suggestion to look at those reviews, and the references therein, has been

provided. However, in spite of our best effort, many publications could not be included, and we would like to apologize in advance for any omission.

7. Acknowledgments

This work has been partially funded by the Spanish State Research Agency (AEI) and the European Regional Development Fund (ERFD) through the projects SCAV (ref. MINECO DPI2017-88403-R) and DEOCS (ref. MINECO DPI2016-76493), and also by AGAUR ACCIO RIS3CAT UTILITIES 4.0 P7 SECUTIL. This work has been also supported by the AEI through the Maria de Maeztu Seal of Excellence to IRI (MDM-2016-0656) and the grant Juan de la Cierva-Formacion (FJCI-2016-29019)

References

[1] X. Ge, F. Yang, Q.-L. Han, Distributed networked control systems: A brief overview, Information Sciences 380 (2017) 117–131.

[2] X.-M. Zhang, Q.-L. Han, X. Yu, Survey on recent advances in networked control systems, IEEE Transactions on Industrial Informatics 12 (2016) 1740–1752.

[3] L. Zhang, H. Gao, O. Kaynak, Network-induced constraints in networked control systems: a survey, IEEE transactions on industrial informatics 9 (2013) 403–416.

[4] S. Jeschke, C. Brecher, T. Meisen, D. Özdemir, T. Eschert, Industrial internet of things and cyber manufacturing systems, in: Industrial Internet of Things, Springer, 2017, pp. 3–19.

[5] K.-D. Kim, P. R. Kumar, Cyber–physical systems: A perspective at the centennial, Proceedings of the IEEE 100 (2012) 1287–1308.

[6] J. B. Kennedy, When woman is boss: an interview with Nikola Tesla, Colliers (1926).

[7] H. Nyquist, Regeneration theory, Bell Labs Technical Journal 11 (1932) 126–147.

[8] W. R. Evans, Control system synthesis by root locus method, AIEE Transactions 69 (1950) 66–69.

[9] J. G. Ziegler, N. B. Nichols, Optimum settings for automatic controllers, Transactions of the ASME 64 (1942).

[10] R. Bellman, Dynamic programming, Science 153 (1966) 34–37.

[11] L. S. Pontryagin, Mathematical theory of optimal processes, CRC Press, 1987.

[12] R. E. Kalman, Mathematical description of linear dynamical systems, Journal of the Society for Industrial and Applied Mathematics, Series A: Control 1 (1963) 152–192.

[13] A. Annaswamy, S. Chakraborty, D. Soudbakhsh, D. Goswami, H. Voit, The arbitrated networked control systems approach to designing cyber-physical systems, IFAC Proceedings Volumes 45 (2012) 174–179.

[14] B. B. Sánchez, R. Alcarria, D. S. de Rivera, A. Sánchez-Picot, Enhancing process control in industry 4.0 scenarios using cyber-physical systems., JoWUA 7 (2016) 41–64.

[15] H. J. La, S. D. Kim, A service-based approach to designing cyber physical systems, in: Computer and Information Science (ICIS), 2010 IEEE/ACIS 9th International Conference on, IEEE, Yamagata, Japan, pp. 895–900.

[16] Y. Tan, S. Goddard, L. C. Perez, A prototype architecture for cyber-physical systems, ACM Sigbed Review 5 (2008) 26.

[17] K. D. Kang, S. H. Son, Real-time data services for cyber physical systems, in: Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on, IEEE, Beijing, China, pp. 483–488.

[18] J. Wan, M. Chen, F. Xia, L. Di, K. Zhou, From machine-to-machine communications towards cyber-physical systems, Computer Science and Information Systems 10 (2013) 1105–1128.

[19] A. Pantelopoulos, N. G. Bourbakis, A survey on wearable sensor-based systems for health monitoring and prognosis, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 40 (2010) 1–12.

[20] H. Alemdar, C. Ersoy, Wireless sensor networks for healthcare: A survey, Computer Networks 54 (2010) 2688–2710.

[21] A. Milenković, C. Otto, E. Jovanov, Wireless sensor networks for personal health monitoring: Issues and an implementation, Computer communications 29 (2006) 2521–2533.

[22] I. Lee, O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. Kim, A. King, M. Mullen-Fortino, S. Park, A. Roederer, K. K. Venkatasubramanian, Challenges and research directions in medical cyber–physical systems, Proceedings of the IEEE 100 (2012) 75–90.

[23] S. A. Haque, S. M. Aziz, M. Rahman, Review of cyber-physical system in healthcare, International Journal of Distributed Sensor Networks 10 (2014) 1–20.

[24] E. O. Méndez, S. Ren, Design of cyber-physical interface for automated vital signs reading in electronic medical records systems, in: Electro/Information Technology (EIT), 2012 IEEE International Conference on, IEEE, Indianapolis, IN, USA, pp. 1–10.

[25] M. Sung, C. Marci, A. Pentland, Wearable feedback systems for rehabilitation, Journal of neuroengineering and rehabilitation 2 (2005) 17.

[26] P. Iso-Ketola, T. Karinsalo, J. Vanhala, Hipguard: A wearable measurement system for patients recovering from a hip operation, in: Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on, IEEE, Tampere, Finland, pp. 196–199.

[27] D. Konstantas, R. Herzog, Continuous monitoring of vital constants for mobile users: the MobiHealth approach, in: Engineering in Medicine and Biology Society, 2003. Proceedings of the 25th Annual International Conference of the IEEE, volume 4, IEEE, Cancún, México, pp. 3728–3731.

[28] V. Shnayder, B.-R. Chen, K. Lorincz, T. R. Jones, M. Welsh, Sensor networks for medical care, Technical Report, Harvard Computer Science Group Technical Report TR-08-05, 2005.

[29] Y. Zhang, M. Qiu, C. W. Tsai, M. M. Hassan, A. Alamri, Health-CPS: Healthcare cyber-physical system assisted by cloud and big data, IEEE Systems Journal 11 (2017) 88–95.

[30] H. Farhangi, The path of the smart grid, IEEE power and energy magazine 8 (2010).

[31] M. D. Ilic, L. Xie, U. A. Khan, J. M. Moura, Modeling of future cyber–physical energy systems for distributed sensing and control, IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans 40 (2010) 825–838.

[32] J. Kleissl, Y. Agarwal, Cyber-physical energy systems: Focus on smart buildings, in: Proceedings of the 47th Design Automation Conference, ACM, Anaheim, CA, USA, pp. 749–754.

[33] C. A. Macana, N. Quijano, E. Mojica-Nava, A survey on cyber physical energy systems and their applications on smart grids, in: Innovative Smart Grid Technologies (ISGT Latin America), 2011 IEEE PES Conference on, IEEE, Medellín, Colombia, pp. 1–7.

[34] M. Moness, A. M. Moustafa, A survey of cyber-physical advances and challenges of wind energy conversion systems: prospects for internet of energy, IEEE Internet of Things Journal 3 (2016) 134–145.

[35] S. Jianjun, W. Xu, G. Jizhen, C. Yangzhou, The analysis of traffic control cyber-physical systems, Procedia-Social and Behavioral Sciences 96 (2013) 2487–2496.

[36] M. Bell, L. Muirhead, F. Hu, Cyber-physical system for transportation applications, Cyber-Physical Systems: Integrated Computing and Engineering Design (2013) 239.

[37] D. P. Möller, A. X. Fidencio, E. Cota, I. A. Jehle, H. Vakilzadian, Cyber-physical smart traffic light system, in: Electro/Information Technology (EIT), 2015 IEEE International Conference on, IEEE, Dekalb, IL, USA, pp. 546–551.

[38] V. Astarita, V. P. Giofrè, G. Guido, D. C. Festa, Traffic delays estimation in two-lane highway reconstruction, Procedia Computer Science 32 (2014) 331–338.

[39] M. Treiber, A. Kestling, Traffic flow dynamics, Springer Publ. (2014).

[40] D. P. Möller, T. Deriyenko, H. Vakilzadian, Cyber-physical vehicle tracking system: Requirements for using a radio frequency identification technique, in: Electro/Information Technology (EIT), 2015 IEEE International Conference on, IEEE, Dekalb, IL, USA, pp. 552–557.

[41] J. Kim, H. Kim, K. Lakshmanan, R. R. Rajkumar, Parallel scheduling for cyber-physical systems: Analysis and case study on a self-driving car, in: Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems, ACM, Philadelphia, PA, USA, pp. 31–40.

[42] D. Goswami, R. Schneider, A. Masrur, M. Lukasiewycz, S. Chakraborty, H. Voit, A. Annaswamy, Challenges in automotive cyber-physical systems design, in: Embedded Computer Systems (SAMOS), 2012 International Conference on, IEEE, Samos, Greece, pp. 346–354.

[43] S. Osswald, S. Matz, M. Lienkamp, Prototyping automotive cyber-physical systems, in: Adjunct Proceedings of the 6th International Conference on Automotive User Interfaces and Interactive Vehicular Applications, ACM, Seattle, WA, USA, pp. 1–6.

[44] J. Petit, S. E. Shladover, Potential cyberattacks on automated vehicles, IEEE Transactions on Intelligent Transportation Systems 16 (2015) 546–556.

[45] Y. Wang, M. C. Vuran, S. Goddard, Cyber-physical systems in industrial process control, ACM Sigbed Review 5 (2008) 12.

[46] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, M. Hoffmann, Industry 4.0, Business & Information Systems Engineering 6 (2014) 239–242.

[47] K. Sampigethaya, R. Poovendran, Aviation cyber–physical systems: Foundations for future aircraft and air transport, Proceedings of the IEEE 101 (2013) 1834–1855.

[48] M. Andreacchio, A. Bekrar, R. Benmansour, D. Trentesaux, Balancing preventive and corrective maintenance of aircraft assets: A cyber-physical systems approach, in: Industrial Informatics (INDIN), 2016

IEEE 14th International Conference on, IEEE, Poitiers, France, pp. 500–503.

[49] A. Bobat, T. Gezgin, H. Aslan, The SCADA system applications in management of Yuvacik Dam and Reservoir, Desalination and Water Treatment 54 (2015) 2108–2119.

[50] F. R. Spellman, Handbook of water and wastewater treatment plant operations, CRC Press, 2013.

[51] A. Rasekh, A. Hassanzadeh, S. Mulchandani, S. Modi, M. K. Banks, Smart water networks and cyber security, Journal of Water Resources Planning and Management 142 (2016) 1–3.

[52] R. Sarrate, V. Puig, T. Escobet, A. Rosich, Optimal sensor placement for model-based fault detection and isolation, in: Decision and Control, 2007 46th IEEE Conference on, IEEE, New Orleans, LA, USA, pp. 2584–2589.

[53] R. Pérez, V. Puig, J. Pascual, A. Peralta, E. Landeros, L. Jordanas, Pressure sensor distribution for leak detection in barcelona water distribution network, Water science and technology: water supply 9 (2009) 715–721.

[54] R. Pérez, V. Puig, J. Pascual, J. Quevedo, E. Landeros, A. Peralta, Methodology for leakage isolation using pressure sensitivity analysis in water distribution networks, Control Engineering Practice 19 (2011) 1157–1167.

[55] W. Gong, M. A. Suresh, L. Smith, A. Ostfeld, R. Stoleru, A. Rasekh, M. K. Banks, Mobile sensor networks for optimal leak and backflow detection and localization in municipal water networks, Environmental Modelling & Software 80 (2016) 306–321.

[56] D. García, D. Gonzalez, J. Quevedo, V. Puig, J. Saludes, Water demand estimation and outlier detection from smart meter data using classification and big data methods, in: Proceedings of 2nd IWA New Developments in IT and Water Conference, Rotterdam (Netherlands), pp. 1–8.

[57] V. Puig, C. Ocampo-Martínez, R. Pérez, G. Cembrano, J. Quevedo, T. Escobet, Real-time monitoring and operational control of drinking-water systems, 2017.

[58] A. Savvides, I. Paschalidis, M. Caramanis, Cyber-physical systems for next generation intelligent buildings, ACM SIGBED Review 8 (2011) 35–38.

[59] C.-H. Wu, Y.-T. Chang, Y.-C. Tseng, Multi-screen cyber-physical video game: An integration with body-area inertial sensor networks, in: PerCom Workshops, Mannheim, Germany, pp. 832–834.

[60] X. Yu, A. Pan, L.-A. Tang, Z. Li, J. Han, Geo-friends recommendation in GPS-based cyber-physical social network, in: Advances in Social Networks Analysis and Mining (ASONAM), 2011 International Conference on, IEEE, Kaohsiung, Taiwan, pp. 361–368.

[61] L. Parolini, B. Sinopoli, B. H. Krogh, Z. Wang, A cyber–physical systems approach to data center modeling and control for energy efficiency, Proceedings of the IEEE 100 (2012) 254–268.

[62] J. Chen, R. Tan, G. Xing, X. Wang, X. Fu, Fidelity-aware utilization control for cyber-physical surveillance systems, IEEE Transactions on Parallel and Distributed Systems 23 (2012) 1739–1751.

[63] L. Shou, K. Chen, G. Chen, C. Zhang, Y. Ma, X. Zhang, What-you-retrieve-is-what-you-see: a preliminary cyber-physical search engine, in: Proceedings of the 34th international ACM SIGIR conference on Research and development in Information Retrieval, ACM, Beijing, China, pp. 1273–1274.

[64] G. Hackmann, W. Guo, G. Yan, Z. Sun, C. Lu, S. Dyke, Cyber-physical codesign of distributed structural health monitoring with wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems 25 (2014) 63–72.

[65] J. O. Ringert, B. Rumpe, A. Wortmann, A requirements modeling language for the component behavior of cyber physical robotics systems, arXiv preprint arXiv:1409.0394 (2014).

[66] S. Amin, A. A. Cárdenas, S. Sastry, Safe and secure networked control systems under denial-of-service attacks, in: HSCC, volume 5469, Springer, San Francisco, CA, USA, pp. 31–45.

[67] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, W. H. Maisel, Security and privacy for implantable medical devices, IEEE pervasive computing 7 (2008) 30–39.

[68] T. Denning, K. Fu, T. Kohno, Absence makes the heart grow fonder: new directions for implantable medical device security, in: Proceedings of the 3rd conference on Hot topics in security (2008), USENIX Association, San José, CA, USA, pp. 1–7.

[69] M. Negrete-Pincetic, F. Yoshida, G. Gross, Towards quantifying the impacts of cyber attacks in the competitive electricity market environment, in: IEEE PowerTech Conference, IEEE, Bucharest, Romania, pp. 1–8.

[70] M. Jeanne, CNN, Sources: Staged cyber attack reveals vulnerability in power grid, 2007. [Available at `http://www.cnn.com/2007/US/09/26/power.at.risk/index.html`].

[71] T. Greene, Experts hack power grid in no time, 2008. [Available at `https://www.networkworld.com/article/2277908/lan-wan/experts-hack-power-grid-in-no-time.html`].

[72] B. Krebs, TVA power plants vulnerable to cyber attacks, GAO finds, 2008. [Available at `http://www.washingtonpost.com/wp-dyn/content/article/2008/05/20/AR2008052002354.html`].

[73] B. Krebs, Cyber incident blamed for nuclear power plant shutdown, 2008. [Available at `http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html`].

[74] N. L. Ricker, Model predictive control of a continuous, nonlinear, two-phase reactor, Journal of Process Control 3 (1993) 109–123.

[75] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, S. Sastry, Understanding the physical and economic consequences of attacks on control systems, International Journal of Critical Infrastructure Protection 2 (2009) 73–83.

[76] R. Chabukswar, B. Sinópoli, G. Karsai, A. Giani, H. Neema, A. Davis, Simulation of network attacks on SCADA systems, in: First Workshop on Secure Control Systems, Cyber Physical Systems Week, Stockholm, Sweden, pp. 1–8.

[77] M. Krotofil, A. A. Cárdenas, Resilience of process control systems to cyber-physical attacks, in: Nordic Conference on Secure IT Systems, Springer, Berlin, Heidelberg, pp. 166–182.

[78] J. Slay, M. Miller, Lessons learned from the Maroochy Water breach, International Conference on Critical infrastructure protection (2007) 73–82.

[79] Repository of Industrial Security Incidents (RISI), 2015. [Available at `http://www.risidata.com/Database/`].

[80] 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 Transactions on Control Systems Technology 21 (2013) 1963–1970.

[81] S. Amin, X. Litrico, S. Sastry, A. M. Bayen, Cyber security of water SCADA systems–Part II: Attack detection using enhanced hydrodynamic models, IEEE Transactions on Control Systems Technology 21 (2013) 1679–1693.

[82] A. Laszka, W. Abbas, Y. Vorobeychik, X. Koutsoukos, Synergic security for smart water networks: redundancy, diversity, and hardening, in: Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks, ACM, Pittsburgh, PA, USA, pp. 21–24.

[83] R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons, A. Ostfeld, Characterizing cyber-physical attacks on water distribution systems, Journal of Water Resources Planning and Management 143 (2017) 1–12.

[84] C. M. Ahmed, V. R. Palleti, A. P. Mathur, WADI: a water distribution testbed for research in the design of secure cyber physical systems, in: Proceedings of the 3rd International Workshop on Cyber-Physical

Systems for Smart Water Networks, ACM, Pittsburgh, PA, USA, pp. 25–28.

[85] D. Tudorica, Communication security in SCADA pipeline monitoring systems, in: Roedunet International Conference (RoEduNet), 2011 10th, IEEE, Iasi, Romania, pp. 1–5.

[86] J. Markoff, Old trick threatens the newest weapons, 2009. [Available at http://www.nytimes.com/2009/10/27/science/27trojan.html].

[87] D. E. Denning, Cyberterrorism: the logic bomb versus the truck bomb, Global Dialogue 2 (2000) 1–7.

[88] A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke, SCADA security in the light of cyber-warfare, Computers & Security 31 (2012) 418–436.

[89] J. P. Farwell, R. Rohozinski, Stuxnet and the future of cyber war, Survival 53 (2011) 23–40.

[90] K. Zetter, 'Flame' spyware infiltrating Iranian computers, 2012. [Available at http://edition.cnn.com/2012/05/29/tech/web/iran-spyware-flame/index.html].

[91] D. Hentunen, A. Tikkanen, Havex hunts for ics-scada systems, 2014. [Available at https://www.f-secure.com/weblog/archives/00002718.html].

[92] ICS-CERT, Cyber-attack against Ukrainian critical infrastructure, 2016. [Available at https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01l].

[93] A. R. Metke, R. L. Ekl, Security technology for smart grid networks, IEEE Transactions on Smart Grid 1 (2010) 99–107.

[94] A. Humayed, J. Lin, F. Li, B. Luo, Cyber-physical systems security–a survey, IEEE Internet of Things Journal (2017).

[95] S. Ali, T. Al Balushi, Z. Nadir, O. K. Hussain, Cyber Security for Cyber Physical Systems, volume 768, Springer, 2018.

[96] R. Alguliyev, Y. Imamverdiyev, L. Sukhostat, Cyber-physical systems and their security issues, Computers in Industry 100 (2018) 212–223.

[97] A. Burg, A. Chattopadhyay, K.-Y. Lam, Wireless communication and security issues for cyber–physical systems and the internet-of-things, Proceedings of the IEEE 106 (2018) 38–60.

[98] R. J. Turk, Cyber incidents involving control systems, Technical Report, Technical Report, Idaho National Laboratory (INL), 2005.

[99] A. A. Cárdenas, S. Amin, S. Sastry, Research challenges for the security of control systems, in: Proceedings of the 3rd conference on Hot topics in security, San Jose, CA, USA, pp. 1–6.

[100] O. Kosut, L. Jia, R. J. Thomas, L. Tong, Malicious data attacks on the smart grid, IEEE Transactions on Smart Grid 2 (2011) 645–658.

[101] S. Sundaram, M. Pajic, C. N. Hadjicostis, R. Mangharam, G. J. Pappas, The wireless control network: Monitoring for malicious behavior, in: Decision and Control (CDC), 2010 49th IEEE Conference on, IEEE, Atlanta, GA, USA, pp. 5979–5984.

[102] Y. Mo, T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli, Cyber–physical security of a smart grid infrastructure, Proceedings of the IEEE 100 (2012) 195–209.

[103] S. Amin, G. A. Schwartz, A. Hussain, In quest of benchmarking security risks to cyber-physical systems, IEEE Network 27 (2013) 19–24.

[104] A. Teixeira, K. C. Sou, H. Sandberg, K. H. Johansson, Secure control systems: A quantitative risk management approach, IEEE Control Systems 35 (2015) 24–45.

[105] C. C. Neuman, Challenges in security for cyber-physical systems, in: DHS Workshop on Future Directions in Cyber-Physical Systems Security, ewark, New Jersey, USA, pp. 22–24.

[106] V. Reppa, M. M. Polycarpou, C. G. Panayiotou, Distributed sensor fault diagnosis for a network of interconnected cyberphysical systems, IEEE Transactions on Control of Network Systems 2 (2015) 11–23.

[107] E. Kyriakides, M. Polycarpou, Intelligent monitoring, control, and security of critical infrastructure systems, volume 565, Springer, 2014.

[108] M. Cheminod, L. Durante, A. Valenzano, Review of security issues in industrial networks, IEEE Transactions on Industrial Informatics 9 (2013) 277–293.

[109] B. Hoh, M. Gruteser, H. Xiong, A. Alrabady, Enhancing security and privacy in traffic-monitoring systems, IEEE Pervasive Computing 5 (2006) 38–46.

[110] S. Mohan, S. Bak, E. Betti, H. Yun, L. Sha, M. Caccamo, S3a: Secure system simplex architecture for enhanced security and robustness of cyber-physical systems, in: Proceedings of the 2nd ACM international conference on High confidence networked systems, ACM, pp. 65–74.

[111] J.-C. Laprie, Dependability: Basic concepts and terminology, in: Dependability: Basic Concepts and Terminology, Springer, 1992, pp. 3–245.

[112] C. Kwon, W. Liu, I. Hwang, Security analysis for cyber-physical systems against stealthy deception attacks, in: American Control Conference (ACC), 2013, IEEE, Washington, DC, USA, pp. 3344–3349.

[113] G. Wu, J. Sun, J. Chen, A survey on the security of cyber-physical systems, Control Theory Technol 14 (2016) 2–10.

[114] A. A. Cardenas, S. Amin, S. Sastry, Secure control: Towards survivable cyber-physical systems, in: Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on, IEEE, Beijing, China, pp. 495–500.

[115] R. J. Anderson, Security engineering: a guide to building dependable distributed systems, John Wiley & Sons, 2010.

[116] A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, Basic concepts and taxonomy of dependable and secure computing, IEEE transactions on dependable and secure computing 1 (2004) 11–33.

[117] R. Shirey, Internet security glossary, version 2 (2007) 1–365.

[118] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, K. P. Chow, Security issues and challenges for cyber physical system, in: Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing, IEEE Computer Society, Hangzhou, China, pp. 733–738.

[119] E. K. Wang, C. W. Lin, T. Y. Wu, C. M. Chen, Y. Ye, Privacy protection framework in social networked cars, in: International Conference on Multidisciplinary Social Networks Research, Springer, Matsuyama, Japan, pp. 553–561.

[120] M. Ciampa, Security+ guide to network security fundamentals, Cengage Learning, 2012.

[121] J. Giraldo, E. Sarkar, A. Cardenas, M. Maniatakos, M. Kantarcioglu, Security and privacy in cyber-physical systems: A survey of surveys, IEEE Design & Test (2017).

[122] S. R. Chhetri, S. Faezi, N. Rashid, M. A. Al Faruque, Manufacturing supply chain and product lifecycle security in the era of industry 4.0, Journal of Hardware and Systems Security (2017) 1–18.

[123] S. Chi, J. Park, K. Jung, J. Lee, Network security modeling and cyber attack simulation methodology, in: Australasian Conference on Information Security and Privacy, Springer, Sydney, Australia, pp. 320–333.

[124] F. Pasqualetti, F. Dörfler, F. Bullo, Attack detection and identification in cyber-physical systems, IEEE Transactions on Automatic Control 58 (2013) 2715–2729.

[125] D. Kundur, X. Feng, S. Liu, T. Zourntos, K. L. Butler-Purry, Towards a framework for cyber attack impact analysis of the electric smart grid, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, IEEE, Gaithersburg, MD, USA, pp. 244–249.

[126] B. Genge, I. Kiss, P. Haller, A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures, International Journal of Critical Infrastructure Protection 10 (2015) 3–17.

[127] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, A. K. Srivastava, Analyzing the cyber-physical impact of cyber events on the power grid, IEEE Transactions on Smart Grid 6 (2015) 2444–2453.

[128] H. Orojloo, M. A. Azgomi, A method for evaluating the consequence propagation of security attacks in cyber–physical systems, Future Generation Computer Systems 67 (2017) 57–71.

[129] X. Li, C. Zhou, Y. C. Tian, N. Xiong, Y. Qin, Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems, IEEE Transactions on Industrial Informatics (2017).

[130] Y. L. Huang, A. A. Cárdenas, S. Amin, Z. S. Lin, H. Y. Tsai, S. Sastry, Understanding the physical and economic consequences of attacks on control systems, International Journal of Critical Infrastructure Protection 2 (2009) 73–83.

[131] A. Teixeira, D. Pérez, H. Sandberg, K. H. Johansson, Attack models and scenarios for networked control systems, in: Proceedings of the 1st international conference on High Confidence Networked Systems, ACM, Beijing, China, pp. 55–64.

[132] A. Teixeira, I. Shames, H. Sandberg, K. H. Johansson, A secure control framework for resource-limited adversaries, Automatica 51 (2015) 135–148.

[133] G.-R. Duan, Analysis and design of descriptor linear systems, volume 23, Springer Science & Business Media, 2010.

[134] M. Conti, N. Dragoni, V. Lesyk, A survey of man in the middle attacks, IEEE Communications Surveys & Tutorials 18 (2016) 2027–2051.

[135] A. D. Yein, C. Y. Chen, T. C. Hsu, W. S. Hsieh, J. A. Lin, Attack wireless sensor network using compromised key redistribution, in: Applied Mechanics and Materials, volume 263, Trans Tech Publ, pp. 920–925.

[136] H. Deng, W. Li, D. P. Agrawal, Routing security in wireless ad hoc networks, IEEE Communications magazine 40 (2002) 70–75.

[137] G. Liang, S. R. Weller, J. Zhao, F. Luo, Z. Y. Dong, The 2015 ukraine blackout: Implications for false data injection attacks, IEEE Transactions on Power Systems 32 (2017) 3317–3318.

[138] S. Feng, P. Tesi, Resilient control under denial-of-service: Robust design, Automatica 79 (2017) 42–51.

[139] V. Kekatos, G. B. Giannakis, R. Baldick, Online energy price matrix factorization for power grid topology tracking, IEEE Transactions on Smart Grid 7 (2016) 1239–1248.

[140] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, Z. Han, A stealthy attack against electricity market using independent component analysis, IEEE Systems Journal 12 (2018) 297 – 307.

[141] L. Xie, Y. Mo, B. Sinopoli, False data injection attacks in electricity markets, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, IEEE, Gaithersburg, MD, USA, pp. 226–231.

[142] L. Xie, Y. Mo, B. Sinopoli, Integrity data attacks in power market operations, IEEE Transactions on Smart Grid 2 (2011) 659–666.

[143] L. Jia, R. J. Thomas, L. Tong, Malicious data attack on real-time electricity market, in: Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on, IEEE, pp. 5952–5955.

[144] R. Tan, V. Badrinath Krishna, D. K. Yau, Z. Kalbarczyk, Impact of integrity attacks on real-time pricing in smart grids, in: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, ACM, pp. 439–450.

[145] M. Esmalifalak, G. Shi, Z. Han, L. Song, Bad data injection attack and defense in electricity market using game theory study, IEEE Transactions on Smart Grid 4 (2013) 160–169.

[146] M. Mengis, A. Tajer, Data injection attacks on electricity markets by limited adversaries: Worst-case robustness, IEEE Transactions on Smart Grid (2017).

[147] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, Z. Han, A stealthy attack against electricity market using independent component analysis, IEEE Systems Journal 12 (2018) 297–307.

[148] S. Tan, W.-Z. Song, M. Stewart, J. Yang, L. Tong, Online data integrity attacks against real-time electrical market in smart grid, IEEE Transactions on Smart Grid 9 (2018) 313–322.

[149] G. Liang, S. R. Weller, F. Luo, J. Zhao, Z. Y. Dong, Generalized fdia-based cyber topology attack with application to the australian electricity market trading mechanism, IEEE Transactions on Smart Grid 9 (2018) 3820–3829.

[150] Y. Yuan, F. Sun, Q. Zhu, Resilient control in the presence of DoS attack: Switched system approach, International Journal of Control, Automation and Systems 13 (2015) 1423–1435.

[151] C. Peng, J. Li, M. Fei, Resilient event-triggering h_∞ load frequency control for multi-area power systems with energy-limited dos attacks, IEEE Transactions on Power Systems 32 (2017) 4110–4118.

[152] L. An, G.-H. Yang, Secure state estimation against sparse sensor attacks with adaptive switching mechanism, IEEE Transactions on Automatic Control (2017).

[153] Q. Zhu, T. Başar, Robust and resilient control design for cyber-physical systems with an application to power systems, in: Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on, IEEE, Orlando, FL, USA, pp. 4066–4071.

[154] Y. Chen, S. Huang, F. Liu, Z. Wang, X. Sun, Evaluation of reinforcement learning based false data injection attack to automatic voltage control, IEEE Transactions on Smart Grid (2018).

[155] Y. Yuan, Z. Li, K. Ren, Modeling load redistribution attacks in power systems, IEEE Transactions on Smart Grid 2 (2011) 382–390.

[156] Y. Yuan, Z. Li, K. Ren, Quantitative analysis of load redistribution attacks in power systems, IEEE Transactions on Parallel and Distributed Systems 23 (2012) 1731–1738.

[157] S. Bi, Y. J. Zhang, Graphical methods for defense against false-data injection attacks on power system state estimation, IEEE Transactions on Smart Grid 5 (2014) 1216–1227.

[158] R. Deng, G. Xiao, R. Lu, Defending against false data injection attacks on power system state estimation, IEEE Transactions on Industrial Informatics 13 (2017) 198–207.

[159] J. Chen, A. Abur, Placement of PMUs to enable bad data detection in state estimation, IEEE Transactions on Power Systems 21 (2006) 1608–1615.

[160] Q. Wang, W. Tai, Y. Tang, M. Ni, S. You, A two-layer game theoretical attack-defense model for a false data injection attack against power systems, International Journal of Electrical Power & Energy Systems 104 (2019) 169–177.

[161] G. Chaojun, P. Jirutitijaroen, M. Motani, Detecting false data injection attacks in AC state estimation, IEEE Transactions on Smart Grid 6 (2015) 2476–2483.

[162] J. James, Y. Hou, V. O. Li, Online false data injection attack detection with wavelet transform and deep neural networks, IEEE Transactions on Industrial Informatics (2018).

[163] C. Liu, J. Wu, C. Long, D. Kundur, Reactance perturbation for detecting and identifying fdi attacks in power system state estimation, IEEE Journal of Selected Topics in Signal Processing 12 (2018) 763–776.

[164] F. Pasqualetti, A. Bicchi, F. Bullo, A graph-theoretical characterization of power network vulnerabilities, in: American Control Conference (ACC), 2011, IEEE, San Francisco, CA, USA, pp. 3918–3923.

[165] G. Park, H. Shim, C. Lee, Y. Eun, K. H. Johansson, When adversary encounters uncertain cyber-physical systems: Robust zero-dynamics attack with disclosure resources, in: Decision and Control (CDC), 2016 IEEE 55th Conference on, IEEE, Las Vegas, NV, USA, pp. 5085–5090.

[166] M. Naghnaeian, N. Hirzallah, P. G. Voulgaris, Dual rate control for security in cyber-physical systems, in: Decision and Control (CDC), 2015 IEEE 54th Annual Conference on, IEEE, Osaka, Japan, pp. 1415–1420.

[167] D. Ding, Z. Wang, G. Wei, F. E. Alsaadi, Event-based security control for discrete-time stochastic systems, IET Control Theory & Applications 10 (2016) 1808–1815.

[168] T.-T. Tran, O.-S. Shin, J.-H. Lee, Detection of replay attacks in smart grid systems, in: Computing, Management and Telecommunications (ComManTel), 2013 International Conference on, IEEE, Ho Chi Minh City, Vietnam, pp. 298–302.

[169] T. Irita, T. Namerikawa, Detection of replay attack on smart grid with code signal and bargaining game, in: American Control Conference (ACC), 2017, IEEE, Seattle, WA, USA, pp. 2112–2117.

[170] B. Chen, D. W. Ho, G. Hu, L. Yu, Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks, IEEE transactions on cybernetics (2017).

[171] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, W. Zhao, On false data-injection attacks against power system state estimation: Modeling and countermeasures, IEEE Transactions on Parallel and Distributed Systems 25 (2014) 717–729.

[172] Y. Liu, P. Ning, M. K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Transactions on Information and System Security (TISSEC) 14 (2011) 13.

[173] M. A. Rahman, H. Mohsenian-Rad, False data injection attacks against nonlinear state estimation in smart power grids, in: Power and Energy Society General Meeting (PES), 2013 IEEE, IEEE, Vancouver, BC, Canada, pp. 1–5.

[174] J. Zhao, G. Zhang, Z. Y. Dong, K. P. Wong, Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation, IEEE Transactions on Smart Grid 7 (2016) 6–8.

[175] X. Liu, Z. Li, False data attacks against ac state estimation with incomplete network information, IEEE Transactions on Smart Grid 8 (2017) 2239–2248.

[176] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, T. J. Overbye, Detecting false data injection attacks on DC state

estimation, in: First Workshop on Secure Control Systems (SCS), Stockholm, Sweden, pp. 1–9.

[177] K. C. Sou, H. Sandberg, K. H. Johansson, Electric power network security analysis via minimum cut relaxation, in: Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on, IEEE, Orlando, FL, USA, pp. 4054–4059.

[178] K. C. Sou, H. Sandberg, K. H. Johansson, Computing critical k-tuples in power networks, IEEE Transactions on Power Systems 27 (2012) 1511–1520.

[179] M. A. Rahman, H. Mohsenian-Rad, False data injection attacks with incomplete information against smart power grids, in: Global Communications Conference (GLOBECOM), 2012 IEEE, IEEE, Anaheim, California, USA, pp. 3153–3158.

[180] X. Liu, Z. Bao, D. Lu, Z. Li, Modeling of local false data injection attacks with reduced network information, IEEE Transactions on Smart Grid 6 (2015) 1686–1696.

[181] J. Kim, L. Tong, On topology attack of a smart grid: Undetectable attacks and countermeasures, IEEE Journal on Selected Areas in Communications 31 (2013) 1294–1305.

[182] G. Hug, J. A. Giampapa, Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks, IEEE Transactions on Smart Grid 3 (2012) 1362–1370.

[183] W.-L. Chin, C.-H. Lee, T. Jiang, Blind false data attacks against ac state estimation based on geometric approach in smart grid communications, IEEE Transactions on Smart Grid 9 (2018) 6298–6306.

[184] H. Sandberg, A. Teixeira, K. H. Johansson, On security indices for state estimators in power networks, in: First Workshop on Secure Control Systems (SCS), Stockholm, 2010, Stockholm, Sweden, p. 6.

[185] J. Lin, W. Yu, X. Yang, G. Xu, W. Zhao, On false data injection attacks against distributed energy routing in smart grid, in: Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, IEEE Computer Society, Beijing, China, pp. 183–192.

[186] A. Anwar, A. N. Mahmood, Z. Tari, Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid, Information Systems 53 (2015) 201–212.

[187] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, K. Poolla, Smart grid data integrity attacks: characterizations and countermeasures π, in: Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on, IEEE, Brussels, Belgium, pp. 232–237.

[188] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, A. Tajer, Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions, IEEE Signal Processing Magazine 29 (2012) 106–115.

[189] T. T. Kim, H. V. Poor, Strategic protection against data injection attacks on power grids, IEEE Transactions on Smart Grid 2 (2011) 326–333.

[190] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, Z. Han, Detecting false data injection attacks on power grid by sparse optimization, IEEE Transactions on Smart Grid 5 (2014) 612–621.

[191] H. Sedghi, E. Jonckheere, Statistical structure learning to ensure data integrity in smart grid, IEEE Transactions on Smart Grid 6 (2015) 1924–1933.

[192] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, H. V. Poor, Machine learning methods for attack detection in the smart grid, IEEE transactions on neural networks and learning systems 27 (2016) 1773–1786.

[193] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, Z. Han, Detecting stealthy false data injection using machine learning in smart grid, IEEE Systems Journal 11 (2017) 1644–1652.

[194] S. Li, Y. Yılmaz, X. Wang, Quickest detection of false data injection attack in wide-area smart grids, IEEE Transactions on Smart Grid 6 (2015) 2725–2735.

[195] A. Sanjab, W. Saad, Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective, IEEE Transactions on Smart Grid 7 (2016) 2038–2049.

[196] Y. Huang, H. Li, K. A. Campbell, Z. Han, Defending false data injection attack on smart grid network using adaptive cusum test, in: Information Sciences and Systems (CISS), 2011 45th Annual Conference on, IEEE, pp. 1–6.

[197] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, Z. Han, Real-time detection of false data injection in smart grid networks: an adaptive cusum method and analysis, IEEE Systems Journal 10 (2016) 532–543.

[198] S. Pan, T. Morris, U. Adhikari, Developing a hybrid intrusion detection system using data mining for power systems, IEEE Transactions on Smart Grid 6 (2015) 3104–3113.

[199] K. Manandhar, X. Cao, F. Hu, Y. Liu, Detection of faults and attacks including false data injection attack in smart grid using Kalman filter, IEEE transactions on control of network systems 1 (2014) 370–379.

[200] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, J. Wang, Short-term state forecasting-aided method for detection of smart grid general false data injection attacks, IEEE Transactions on Smart Grid 8 (2017) 1580–1590.

[201] A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, G. Ferrari-Trecate, Distributed cyber-attack detection in the secondary control of DC microgrids, in: European Control Conference, Limassol, Cyprus, pp. 1–6.

[202] M. Zhu, S. Martínez, On distributed constrained formation control in operator–vehicle adversarial networks, Automatica 49 (2013) 3571–3582.

[203] C. Fang, Y. Qi, P. Cheng, W. X. Zheng, Cost-effective watermark based detector for replay attacks on cyber-physical systems, in: Control Conference (ASCC), 2017 11th Asian, IEEE, Gold Coast, QLD, Australia, pp. 940–945.

[204] D. I. Urbina, J. A. Giraldo, A. A. Cardenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, H. Sandberg, Limiting the impact of stealthy attacks on industrial control systems, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, pp. 1092–1105.

[205] M. A. Umer, A. Mathur, K. N. Junejo, S. Adepu, Integrating design and data centric approaches to generate invariants for distributed attack detection, in: Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, ACM, pp. 131–136.

[206] K. Junejo, D. Yau, Data driven physical modelling for intrusion detection in cyber physical systems, in: Singapore Cyber Security R&D Conference, pp. 43 – 57.

[207] P. Nader, P. Honeine, P. Beauseroy, Detection of cyberattacks in a water distribution system using machine learning techniques, in: Digital Information Processing and Communications (ICDIPC), 2016 Sixth International Conference on, IEEE, pp. 25–30.

[208] J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt, J. Sun, Anomaly detection for a water treatment system using unsupervised machine learning, in: Data Mining Workshops (ICDMW), 2017 IEEE International Conference on, IEEE, pp. 1058–1065.

[209] K. Pal, S. Adepu, J. Goh, Effectiveness of association rules mining for invariants generation in cyber-physical systems, in: High Assurance Systems Engineering (HASE), 2017 IEEE 18th International Symposium on, IEEE, pp. 124–127.

[210] R. Taormina, S. Galelli, Deep-learning approach to the detection and localization of cyber-physical attacks on water distribution systems, Journal of Water Resources Planning and Management 144 (2018) 04018065.

[211] R. S. Smith, A decoupled feedback structure for covertly appropriating networked control systems, IFAC Proceedings Volumes 44 (2011) 90–95.

[212] W. Li, L. Xie, Z. Wang, A novel covert agent for stealthy attacks on industrial control systems using least squares support vector regression, Journal of Electrical and Computer Engineering 2018 (2018).

[213] W. Li, L. Xie, Z. Wang, Two-loop covert attacks against constant-value control of industrial control systems, IEEE Transactions on Industrial Informatics (2018).

[214] C. Schellenberger, P. Zhang, Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system, in: Decision and Control (CDC), 2017 IEEE 56th Annual Conference on, IEEE, Melbourne, VIC, Australia, pp. 1374–1379.

[215] K. Pelechrinis, M. Iliofotou, S. V. Krishnamurthy, Denial of service attacks in wireless networks: The case of jammers, IEEE Communications surveys & tutorials 13 (2011) 245–257.

[216] G. Carl, G. Kesidis, R. R. Brooks, S. Rai, Denial-of-service attack-detection techniques, IEEE Internet computing 10 (2006) 82–89.

[217] E. Byres, The myths and facts behind cyber security risks for industrial control systems, in: Proceedings of the VDE Kongress, volume 116, Citeseer, pp. 213–218.

[218] T. Hoppe, S. Kiltz, J. Dittmann, Security threats to automotive CAN networks–Practical examples and selected short-term countermeasures, Reliability Engineering & System Safety (2011) 11–25.

[219] D. Geer, Security of critical control systems sparks concern, Computer 39 (2006) 20–23.

[220] Z. A. Biron, S. Dey, P. Pisu, Real-time detection and estimation of denial of service attack in connected vehicle systems, IEEE Transactions on Intelligent Transportation Systems (2018) 1–10.

[221] O. C. Imer, S. Yüksel, T. Başar, Optimal control of LTI systems over unreliable communication links, Automatica 42 (2006) 1429–1439.

[222] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, S. S. Sastry, Foundations of control and estimation over lossy networks, Proceedings of the IEEE 95 (2007) 163–187.

[223] D. Wang, Z. Wang, B. Shen, F. E. Alsaadi, T. Hayat, Recent advances on filtering and control for cyber-physical systems under security and resource constraints, Journal of the Franklin Institute 353 (2016) 2451–2466.

[224] 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 (2018) 1674–1683.

[225] W. Zhang, M. S. Branicky, S. M. Phillips, Stability of networked control systems, IEEE Control Systems 21 (2001) 84–99.

[226] Q. Ling, M. D. Lemmon, Robust performance of soft real-time networked control systems with data dropouts, in: Decision and Control, 2002, Proceedings of the 41st IEEE Conference on, volume 2, IEEE, Las Vegas, NV, USA, USA, pp. 1225–1230.

[227] L. Schenato, To zero or to hold control inputs with lossy links?, IEEE Transactions on Automatic Control 54 (2009) 1093–1099.

[228] V. Gupta, N. C. Martins, On stability in the presence of analog erasure channel between the controller and the actuator, IEEE Transactions on Automatic Control 55 (2010) 175–179.

[229] H. Gao, Y. Zhao, T. Chen, H_∞ fuzzy control of nonlinear systems under unreliable communication links, IEEE Transactions on Fuzzy systems 17 (2008) 265–278.

[230] H. Zhang, P. Cheng, L. Shi, J. Chen, Optimal denial-of-service attack scheduling with energy constraint, IEEE Transactions on Automatic Control 60 (2015) 3023–3028.

[231] G. K. Befekadu, V. Gupta, P. J. Antsaklis, Risk-sensitive control under a class of denial-of-service attack models, in: American Control Conference (ACC), 2011, IEEE, San Francisco, CA, USA, pp. 643–648.

[232] H. S. Foroush, S. Martínez, On event-triggered control of linear systems under periodic denial-of-service jamming attacks, in: Decision and Control (CDC), 2012 IEEE 51st Annual Conference on, IEEE, pp. 2551–2556.

[233] H. Shisheh Foroush, S. Martínez, On triggering control of single-input linear systems under pulse-width modulated DoS signals, SIAM Journal on Control and Optimization 54 (2016) 3084–3105.

[234] G. K. Befekadu, V. Gupta, P. J. Antsaklis, Risk-sensitive control under markov modulated denial-of-service (DoS) attack strategies, IEEE Transactions on Automatic Control 60 (2015) 3299–3304.

[235] H. Sun, C. Peng, T. Yang, H. Zhang, W. He, Resilient control of networked control systems with stochastic denial of service attacks, Neurocomputing 270 (2017) 170–177.

[236] C. De Persis, P. Tesi, Input-to-state stabilizing control under denial-of-service, IEEE Transactions on Automatic Control 60 (2015) 2930–2944.

[237] A. Cetinkaya, H. Ishii, T. Hayakawa, Event-triggered output feedback control resilient against jamming attacks and random packet losses, IFAC-PapersOnLine 48 (2015) 270–275.

[238] C. De Persis, P. Tesi, Networked control of nonlinear systems under denial-of-service, Systems & Control Letters 96 (2016) 124–131.

[239] D. Senejohnny, P. Tesi, C. De Persis, A jamming-resilient algorithm for self-triggered network coordination, IEEE Transactions on Control of Network Systems (2017).

[240] V. Dolk, P. Tesi, C. De Persis, W. Heemels, Event-triggered control systems under denial-of-service attacks, IEEE Transactions on Control of Network Systems 4 (2017) 93–105.

[241] M. Long, C.-H. Wu, J. Y. Hung, Denial of service attacks on network-based control systems: impact and mitigation, IEEE Transactions on Industrial Informatics 1 (2005) 85–96.

[242] R. Cao, J. Wu, C. Long, S. Li, Stability analysis for networked control systems under denial-of-service attacks, in: Decision and Control (CDC), 2015 IEEE 54th Annual Conference on, IEEE, pp. 7476–7481.

[243] A. Gupta, C. Langbort, T. Başar, Optimal control in the presence of an intelligent jammer with limited actions, in: Decision and Control (CDC), 2010 49th IEEE Conference on, IEEE, Atlanta, GA, USA, pp. 1096–1101.

[244] H. Zhang, Y. Qi, J. Wu, L. Fu, L. He, Dos attack energy management against remote state estimation, IEEE Transactions on Control of Network Systems 5 (2018) 383–394.

[245] C. Yang, X. Ren, W. Yang, H. Shi, L. Shi, Jamming attack in centralized state estimation, in: Control Conference (CCC), 2015 34th Chinese, IEEE, Hangzhou, China, pp. 6530–6535.

[246] H. Zhang, P. Cheng, L. Shi, J. Chen, Optimal DoS attack scheduling in wireless networked control system, IEEE Transactions on Control Systems Technology 24 (2016) 843–852.

[247] L. Peng, L. Shi, X. Cao, C. Sun, Optimal attack energy allocation against remote state estimation, IEEE Transactions on Automatic Control (2017).

[248] L. Peng, X. Cao, C. Sun, Y. Cheng, S. Jin, Energy efficient jamming attack schedule against remote state estimation in wireless cyber-physical systems, Neurocomputing 272 (2018) 571–583.

[249] M. Zhu, S. Martinez, Stackelberg-game analysis of correlated attacks in cyber-physical systems, in: American Control Conference (ACC), 2011, IEEE, San Francisco, CA, USA, pp. 4063–4068.

[250] Y. Li, L. Shi, P. Cheng, J. Chen, D. E. Quevedo, Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach, IEEE Transactions on Automatic Control 60 (2015) 2831–2836.

[251] Q. Zhu, T. Basar, Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems, IEEE control systems 35 (2015) 46–65.

[252] K. Ding, Y. Li, D. E. Quevedo, S. Dey, L. Shi, A multi-channel transmission schedule for remote state estimation under DoS attacks, Automatica 78 (2017) 194–201.

[253] P. Kaur, M. Kumar, A. Bhandari, A review of detection approaches for distributed denial of service attacks, Systems Science & Control Engineering 5 (2017) 301–320.

[254] J. Branch, A. Bivens, C. Y. Chan, T. K. Lee, B. K. Szymanski, Denial of service intrusion detection using time dependent deterministic finite automata, in: Proc. Graduate Research Conference, pp. 45–51.

[255] A. Dolgikh, T. Nykodym, V. Skormin, J. Antonakos, M. Baimukhamedov, Colored petri nets as the enabling technology in intrusion detection systems, in: Military Communications Conference, 2011-MILCOM 2011, IEEE, pp. 1297–1301.

[256] C. Manikopoulos, S. Papavassiliou, Network intrusion and fault detection: a statistical anomaly approach, IEEE Communications Magazine 40 (2002) 76–82.

[257] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu, A system for denial-of-service attack detection based on multivariate correlation analysis, IEEE transactions on parallel and distributed systems 25 (2014) 447–456.

[258] J. Li, C. Manikopoulos, Early statistical anomaly intrusion detection of dos attacks using mib traffic parameters, in: Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, IEEE, pp. 53–59.

[259] R. Nagadevi, P. N. Rao, R. Anand, A new way of identifying dos attack using multivariate correlation analysis, International Journal of Computational Engineering Research (IJCER) 4 (2014).

[260] P. Dokas, L. Ertoz, V. Kumar, A. Lazarevic, J. Srivastava, P.-N. Tan, Data mining for network intrusion detection.

[261] M. Ektefa, S. Memar, F. Sidi, L. S. Affendey, Intrusion detection using data mining techniques, in: Information Retrieval & Knowledge Management,(CAMP), 2010 International Conference on, IEEE, pp. 200–203.

[262] K. Labib, V. R. Vemuri, NSOM: A tool to detect denial of service attacks using self-organizing maps, in: Technical Report.

[263] M.-Y. Su, Real-time anomaly detection systems for denial-of-service attacks by weighted k-nearest-neighbor classifiers, Expert Systems with Applications 38 (2011) 3492–3498.

[264] G. Wang, J. Hao, J. Ma, L. Huang, A new approach to intrusion detection using artificial neural networks and fuzzy clustering, Expert systems with applications 37 (2010) 6225–6232.

[265] A. A. Alfantookh, Dos attacks intelligent detection using neural networks, Journal of King Saud University-Computer and Information Sciences 18 (2006) 31–51.

[266] G. Oke, G. Loukas, A denial of service detector based on bayesian classifiers and the random neural network, in: IEEE International Fuzzy Systems Conference.

[267] R. K. Idowu, Z. A. OTHMAN, et al., Denial of service attack detection using trapeizodal fuzzy reasoning spiking neural p system, Journal of Theoretical & Applied Information Technology 75 (2015).

[268] S. F. Tabatabaei, M. Salleh, M. R. Abbasy, M. R. N. Torkaman, Denial of service (dos) attack detection by using fuzzy logic over network flows, in: Proceedings of the International Conference on Security and Management (SAM), The Steering Committee of The World Congress in Computer Science, Computer . . . , p. 1.

[269] S. Mukkamala, A. H. Sung, Detecting denial of service attacks using support vector machines, in: Fuzzy Systems, 2003. FUZZ'03. The 12th IEEE International Conference on, volume 2, IEEE, pp. 1231–1236.

[270] A. P. Chan, W. W. Ng, D. S. Yeung, C. Tsang, Refinement of rule-based intrusion detection system for denial of service attacks by support vector machine, in: Machine Learning and Cybernetics, 2004. Proceedings of 2004 International Conference on, volume 7, IEEE, pp. 4252–4256.

[271] G. Gu, P. Fogla, D. Dagon, W. Lee, B. Skorić, Measuring intrusion detection capability: an information-theoretic approach, in: Proceedings of the 2006 ACM Symposium on Information, computer and communications security, ACM, pp. 90–101.

[272] Y. Dong, P. Zhou, Jamming attacks against control systems: A survey, in: Intelligent Computing, Networked Control, and Their Engineering Applications, Springer, 2017, pp. 566–574.

[273] K. M. Prasad, A. R. M. Reddy, K. V. Rao, DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey, Global Journal of Computer Science and Technology (2014).

[274] C. Douligeris, A. Mitrokotsa, DDoS attacks and defense mechanisms: classification and state-of-the-art, Computer Networks 44 (2004) 643–666.

[275] S. T. Zargar, J. Joshi, D. Tipper, A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks, IEEE communications surveys & tutorials 15 (2013) 2046–2069.

[276] S. S. Sahu, M. Pandey, Distributed denial of service attacks: a review, International Journal of Modern Education and Computer Science 6 (2014) 65.

[277] K. N. Mallikarjunan, K. Muthupriya, S. M. Shalinie, A survey of distributed denial of service attack, in: Intelligent Systems and Control (ISCO), 2016 10th International Conference on, Ieee, Coimbatore, India, pp. 1–6.

[278] R. Langner, Stuxnet: Dissecting a cyberwarfare weapon, IEEE Security & Privacy 9 (2011) 49–51.

[279] M. Burmester, E. Magkos, V. Chrissikopoulos, Modeling security in cyber–physical systems, International journal of critical infrastructure protection 5 (2012) 118–126.

[280] Y. Mo, S. Weerakkody, B. Sinopoli, Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs, IEEE Control Systems 35 (2015) 93–109.

[281] Y. Mo, B. Sinopoli, Secure control against replay attacks, in: 47th Annual Allerton Conference on Communication, Control, and Computing, IEEE, Monticello, IL, USA, pp. 911–918.

[282] K. Murakami, H. Suemitsu, T. Matsuo, Classification of repeated replay-attacks and its detection monitor, in: Consumer Electronics (GCCE), 2017 IEEE 6th Global Conference on, IEEE, Nagoya, Japan, pp. 1–2.

[283] M. Zhu, S. Martínez, On the performance analysis of resilient networked control systems under replay attacks, IEEE Transactions on Automatic Control 59 (2014) 804–808.

[284] S. Weerakkody, Y. Mo, B. Sinopoli, Detecting integrity attacks on control systems using robust physical watermarking, in: Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on, IEEE, Los Angeles, CA, USA, pp. 3757–3764.

[285] A. Khazraei, H. Kebriaei, F. R. Salmasi, A new watermarking approach for replay attack detection in LQG systems, in: Decision and Control (CDC), 2017 IEEE 56th Annual Conference on, IEEE, Melbourne, VIC, Australia, pp. 5143–5148.

[286] 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), 2017, IEEE, Seattle, WA, USA, pp. 4778–4783.

[287] B. Tang, L. D. Alvergue, G. Gu, Secure networked control systems against replay attacks without injecting authentication noise, in: American Control Conference (ACC), 2015, IEEE, Chicago, IL, USA, pp. 6028–6033.

[288] A. Hoehn, P. Zhang, Detection of replay attacks in cyber-physical systems, in: American Control Conference (ACC), 2016, IEEE, Boston, MA, USA, pp. 290–295.

[289] H. Sánchez, D. Rotondo, T. Escobet, V. Puig, J. Quevedo, Frequency-based detection of replay attacks: Application to a multiple tank system, in: 10th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS), Warsaw, Poland, pp. 1–6.

[290] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, J. Saludes, J. Quevedo, Detection of replay attacks in cyber-physical systems using a frequency-based signature, Journal of the Franklin Institute 356 (2019) 2798–2824.

[291] Y. Mo, E. Garone, A. Casavola, B. Sinopoli, False data injection attacks against state estimation in wireless sensor networks, in: Decision

and Control (CDC), 2010 49th IEEE Conference on, IEEE, pp. 5967–5972.

[292] F. Pasqualetti, F. Dorfler, F. Bullo, Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems, IEEE Control Systems 35 (2015) 110–127.

[293] G. Liang, J. Zhao, F. Luo, S. R. Weller, Z. Y. Dong, A review of false data injection attacks against modern power systems, IEEE Transactions on Smart Grid 8 (2017) 1630–1638.

[294] C. Murguia, J. Ruths, Cusum and chi-squared attack detection of compromised sensors, in: Control Applications (CCA), 2016 IEEE Conference on, IEEE, pp. 474–480.

[295] C. Murguia, J. Ruths, Characterization of a cusum model-based sensor attack detector, in: Decision and Control (CDC), 2016 IEEE 55th Conference on, IEEE, pp. 1303–1309.

[296] S. S. Roy, A. Mallik, R. Gulati, M. S. Obaidat, P. Krishna, A deep learning based artificial neural network approach for intrusion detection, in: International Conference on Mathematics and Computing, Springer, pp. 44–53.

[297] S. K. Singh, K. Khanna, R. Bose, B. K. Panigrahi, A. Joshi, Joint-transformation-based detection of false data injection attacks in smart grid, IEEE Transactions on Industrial Informatics 14 (2018) 89–97.

[298] F. Boem, A. J. Gallo, G. Ferrari-Trecate, T. Parisini, A distributed attack detection method for multi-agent systems governed by consensus-based control, in: Decision and Control (CDC), 2017 IEEE 56th Annual Conference on, IEEE, Melbourne, VIC, Australia, pp. 5961–5966.

[299] M. L. Corradini, A. Cristofaro, Robust detection and reconstruction of state and sensor attacks for cyber-physical systems using sliding modes, IET Control Theory & Applications 11 (2017) 1756–1766.

[300] V. B. Krishna, G. A. Weaver, W. H. Sanders, Pca-based method for detecting integrity attacks on advanced metering infrastructure, in: International Conference on Quantitative Evaluation of Systems, Springer, pp. 70–85.

[301] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, T. J. Overbye, Topology perturbation for detecting malicious data injection, in: System Science (HICSS), 2012 45th Hawaii International Conference on, IEEE, pp. 2104–2113.

[302] A. L. Ott, Experience with pjm market operation, system design, and implementation, IEEE Transactions on Power Systems 18 (2003) 528–534.

[303] G. Wang, A. Kowli, M. Negrete-Pincetic, E. Shafieepoorfard, S. Meyn, A control theorist's perspective on dynamic competitive equilibria in electricity markets, IFAC Proceedings Volumes 44 (2011) 4933–4938.

[304] M. Mohammadpourfard, A. Sami, Y. Weng, Identification of false data injection attacks with considering the impact of wind generation and topology reconfigurations, IEEE Transactions on Sustainable Energy 9 (2018).

[305] O. Vukovic, K. C. Sou, G. Dan, H. Sandberg, Network-aware mitigation of data integrity attacks on power system state estimation, IEEE Journal on Selected Areas in Communications 30 (2012) 1108–1118.

[306] M. Mohammadpourfard, A. Sami, A. R. Seifi, A statistical unsupervised method against false data injection attacks: A visualization-based approach, Expert Systems with Applications 84 (2017) 242–261.

[307] J. Back, J. Kim, C. Lee, G. Park, H. Shim, Enhancement of security against zero dynamics attack via generalized hold, in: Decision and Control (CDC), 2017 IEEE 56th Annual Conference on, IEEE, Melbourne, VIC, Australia, pp. 1350–1355.

[308] A. Teixeira, I. Shames, H. Sandberg, K. H. Johansson, Revealing stealthy attacks in control systems, in: Communication, Control, and Computing (Allerton), 50th Annual Allerton Conference on, IEEE, Monticello, IL, USA, pp. 1806–1813.

[309] A. Hoehn, P. Zhang, Detection of covert attacks and zero dynamics attacks in cyber-physical systems, in: American Control Conference (ACC), 2016, IEEE, Boston, MA, USA, pp. 302–307.

[310] C.-Z. Bai, F. Pasqualetti, V. Gupta, Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs, Automatica 82 (2017) 251–260.

[311] A. O. de Sá, L. F. R. da Costa Carmo, R. C. Machado, Covert attacks in cyber-physical control systems, IEEE Transactions on Industrial Informatics 13 (2017) 1641–1651.

[312] F. Hou, J. Sun, Covert attacks against output tracking control of cyber-physical systems, in: Industrial Electronics Society, IECON 2017-43rd Annual Conference of the IEEE, IEEE, Beijing, China, pp. 5743–5748.

[313] R. S. Smith, Covert misappropriation of networked control systems: Presenting a feedback structure, IEEE Control Systems 35 (2015) 82–92.

[314] R. S. Sánchez-Pena, Y. Bolea, V. Puig, Mimo smith predictor: Global and structured robust performance analysis, Journal of Process Control 19 (2009) 163–177.

[315] S. Weerakkody, B. Sinopoli, Detecting integrity attacks on control systems using a moving target approach, in: Decision and Control (CDC), 2015 IEEE 54th Annual Conference on, IEEE, Osaka, Japan, pp. 5820–5826.

[316] A. O. de Sá, L. F. da Costa Carmo, R. C. Machado, A controller design for mitigation of passive system identification attacks in networked control systems, Journal of Internet Services and Applications 9 (2018) 2.

[317] J. P. Hespanha, A. S. Morse, Stability of switched systems with average dwell-time, in: Proceedings of the 38th IEEE conference on decision and control, volume 3, IEEE, pp. 2655–2660.

[318] L. Hu, Z. Wang, Q.-L. Han, X. Liu, State estimation under false data injection attacks: Security analysis and system protection, Automatica 87 (2018) 176–183.

[319] Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, 2017. [Available at `https://www.nist.gov/sites/`

default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf].

[320] H. S. Foroush, S. Martínez, On multi-input controllable linear systems under unknown periodic dos jamming attacks, in: 2013 Proceedings of the Conference on Control and its Applications, SIAM, pp. 222–229.

[321] J. Quevedo, H. Sánchez, D. Rotondo, T. Escobet, V. Puig, A two-tank benchmark for detection and isolation of cyber attacks, in: 10th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS), Warsaw, Poland, pp. 1–6.

[322] R. Taormina, S. Galelli, H. Douglas, N. Tippenhauer, E. Salomons, A. Ostfeld, A toolbox for assessing the impacts of cyber-physical attacks on water distribution systems, Environmental Modelling & Software 112 (2019) 46–51.

[323] A. P. Mathur, N. O. Tippenhauer, SWaT:A water treatment testbed for research and training on ics security, in: Cyber-physical Systems for Smart Water Networks (CySWater), 2016 International Workshop on, IEEE, pp. 31–36.

[324] R. D. Zimmerman, C. E. Murillo-Sánchez, R. J. Thomas, et al., MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education, IEEE Transactions on power systems 26 (2011) 12–19.