A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges

Wenli Duo, MengChu Zhou, *Fellow, IEEE*, and Abdullah Abusorrah, *Senior Member, IEEE*

***Abstract*—A cyber physical system (CPS) is a complex system that integrates sensing, computation, control and networking into physical processes and objects over Internet. It plays a key role in modern industry since it connects physical and cyber worlds. In order to meet ever-changing industrial requirements, its structures and functions are constantly improved. Meanwhile, new security issues have arisen. A ubiquitous problem is the fact that cyber attacks can cause significant damage to industrial systems, and thus has gained increasing attention from researchers and practitioners. This paper presents a survey of state-of-the-art results of cyber attacks on cyber physical systems. First, as typical system models are employed to study these systems, time-driven and event-driven systems are reviewed. Then, recent advances on three types of attacks, i.e., those on availability, integrity, and confidentiality are discussed. In particular, the detailed studies on availability and integrity attacks are introduced from the perspective of attackers and defenders. Namely, both attack and defense strategies are discussed based on different system models. Some challenges and open issues are indicated to guide future research and inspire the further exploration of this increasingly important area.**

***Index Terms*—Attack detection, attack strategy, cyber attack, cyber physical system (CPS), secure control.**

I. Introduction

A cyber physical system (CPS) is a typical product of Industry 4.0, which plays an important role since a CPS is able to integrate the physical and virtual worlds by providing real-time data processing services [1]. More specifically, a CPS allows a physical system to be equipped with a virtual system as a monitor, enabling data collected from the physical world to be analyzed in the virtual world such that decisions can be made to affect the course of physical world. Therefore, a CPS enables integration, sharing and collaboration of information, as well as real-time monitoring and global optimization of systems [2]. There is a wide range of applications in modern industry based on CPSs, such as smart grids, healthcare, aircraft, digital manufacturing and robotics [3]−[6]. Literature shows that CPS includes, but is not limited to, networked control systems (NCSs), wireless sensor networks, and smart grids.

A CPS consists of a physical system and a cyber system. It results from an integration of physical processing, sensing, computation, communication and control [7]. Its general architecture is shown in Fig. 1. The physical system consists of physical processes, sensors and actuators. The cyber system includes communication networks, computing and control centers. Physical processes are usually considered as a plant that is controlled by a cyber system. As for other components, they have the following functions:

1) Sensors: They are used for real-time data acquisition.

2) Actuator: Control commands are executed by corresponding actuators to realize desired physical actions.

3) Computing and control center: It is responsible for receiving data measured by sensors. By analyzing the received data, corresponding control decisions are made by the control center to ensure that physical processes are performed correctly.

4) Communication network: It provides a communication platform for the control center and physical system. To be precise, measurements obtained by sensors are transmitted over the communication network to the control center. Control signals or decisions are transmitted from the control center to actuators by the communication network.

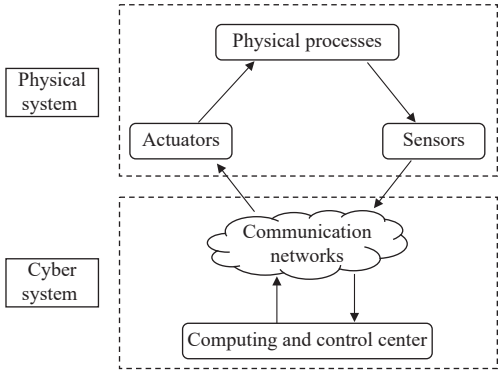

Fig. 1. An architecture of a CPS.

With the rapid development of modern industry, demands for CPS integration are growing to make up for shortcomings among networks, technologies, tools, and devices. The

Manuscript received December 20, 2021; accepted December 27, 2021. This work was supported by Institutional Fund Projects (IFPNC-001-135-2020). Therefore, authors gratefully acknowledge technical and financial support from the Ministry of Education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia. Recommended by Associate Editor Qing-Long Han. *(Corresponding author: MengChu Zhou.)*

Citation: W. L. Duo, M. C. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 5, pp. 784–800, May 2022.

W. L. Duo is with Macau Institute of Systems Engineering, Macau University of Science and Technology, Macau 999078, China (e-mail: duowenli@foxmail.com).

M. C. Zhou and A. Abusorrah are with the Department of Electrical and Computer Engineering K. A. CARE Energy Research and Innovation Center, and Center of Research Excellence in Renewable Energy and Power Systems, King Abdulaziz University, Jeddah 21481, Saudi Arabia. M. C. Zhou is also with Macao Institute of Systems Engineering, Macau University of Science and Technology, Macao 999078, China (e-mail: zhou@njit.edu; aabusorrah@kau.edu.sa).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2022.105548

integration of systems and technologies in CPS tends to be complex and diverse, making it a compatible and open system, which unfortunately provides a platform for adversaries to exploit CPS and results in numerous security issues. One of the most ubiquitous problems is cyber attacks, which can degrade system performance, or even cause catastrophic consequences. An example of a vicious event was the attack on Ukrainian power grids. The power grid is a typical CPS that consists of a power plant, transmission and distribution stations, consumers, control centers, and communication networks. Different components are monitored and connected by sensors and networks respectively, to guarantee a healthy system status. The Ukrainian power system contained a lot of open-source information in 2015, which provided an opportunity for attackers. First, a phishing email spread across networks to introduce a BlackEnergy malware. It allowed attackers to gain confidential data and critical system information. Such actions enabled access to control centers and shutdown of substations remotely. Then, another piece of malware was activated to destroy critical files and prevent the system from rebooting. Finally, a denial-of-service (DoS) attack was launched on call centers to deny consumers access to the latest information on blackout. Nearly 225 000 consumers suffered from this power outage for 1 to 6 hours. Another example is that many healthcare organizations were threatened by cyber attacks during the coronavirus disease 2019 (COVID-19), where attackers attempted to steal research data related to COVID-19 and cause chaos in the hospitals to gain revenue. For instance, a Czech hospital shut down its network due to a cyber attack in March 2020, which greatly impacted diagnosis of COVID-19 and patient care [8]. Important attack events are given in Table I, each of which has caused significant damage to global industry. Therefore, there is a growing interest in cyber attacks on CPSs.

TABLE I
TYPICAL CYBER ATTACK EVENTS FROM YEARS 2010 TO PRESENT

Year	Country/Institution	Details
2010	Iran	Stuxnet attack destroying core controllers of industries
2015	Ukraine	BlackEnergy attack on power grid, leading to massive power outage
2017	Russia, Ukraine, India, China	WannaCry attack aiming to encrypt data and demand ransom payments
2020	Brno University Hospital, Czech Republic	A cyber attack that shut down IT network of a Czech hospital
2020	US Dept. Health & Human Services	Unspecified attack on servers
2021	Colonial Pipeline, US	A ransomware attack on a US fuel pipeline, leading to shutdown of a critical fuel network

Security of CPSs is guaranteed by three features, i.e., availability, integrity, and confidentiality. Availability guarantees that the system is available whenever needed, i.e., every component of the system works correctly at all times. Integrity prevents data or signals in sensors, controllers and electronic devices from being altered by unauthorized parties. Confidentiality ensures security and personal privacy, i.e., key data and information can only be accessed by authorized parties [9]. Once one of these features is lost, the system is at risk of security problems. Hence, these three features are commonly used to determine if a system is secure. They form a security criterion, namely, any security deployment must ensure the availability, integrity and confidentiality of a system. On the other hand, they become targets of cyber criminals. Attackers often work to compromise them to degrade system security, especially availability and integrity.

On the basis of the intentions of attackers, cyber attacks on CPS can be divided into three classes, namely, availability, integrity and confidentiality ones. The availability attack is the most common cyber attack. Its objective is to block the communication network by making data and information unavailable. Typical availability attacks include DoS, distributed DoS and jamming ones. an integrity attack can occur on sensors, actuators, communication networks, and computing and control centers as data and control commands can be falsified under such an attack. There are many types of integrity attacks, e.g., false data injection attacks, middlemen, sparse and replay attacks. Confidentiality attacks may occur at any part of a system since any system information may be targeted by an attacker. Attack methods include eavesdropping, and the combination of DoS and integrity attacks.

Recently, many efforts have been made on dealing with cyber attacks in CPS based on system control theory, since a CPS can be considered as a physical system that is controlled by industrial control technologies. Based on system control theory, researchers study cyber attacks in two ways, i.e., attack and defense strategies. The former is to find the weaknesses of CPS and to propose possible attack strategies, while the latter is to design detection or control methods to defend attacks. Some surveys have outlined the recent work from the perspective of system control [10]−[19]. Table II shows their coverage in terms of: 1) attack types; 2) system models; 3) attack strategies; 4) defense strategies, and provides the main focus of them. It is clear that none of the existing surveys covers all the aspects indicated in the table, while they are important since they indicate attacks and methodologies in recent work. For the purpose of identifying current concerns, technologies, bottlenecks and future research, this paper provides a survey for cyber attacks on CPS that covers all the issues in Table II. More specifically, we review recent advances on availability, integrity and confidentiality attacks. In particular, attack and defense strategies for CPS availability and integrity are discussed based on time-driven and event-driven system models. Some challenges and open issues are summarized according to the survey.

Section II introduces some system models for CPS. Section III provides a review about availability attacks and defense strategies. Section IV focuses on recent studies on integrity attacks, and Section V gives a review of confidentiality attacks. Section VI concludes the paper and discusses some challenging topics to guide future work.

Notations: Let $\mathbb{N}$ be the set of natural numbers. $\mathbb{R}$ is the set of real numbers, where $\mathbb{R}^+$ denotes the set of non-negative real numbers. $\mathbb{R}^n$ is the set of n-dimensional Euclidean space.

TABLE II
RELATED SURVEYS ON CYBER ATTACK

(A: Availability attack; I: Integrity attack; C: Confidentiality attack; TD: Time-driven system; ED: Event-driven system; D: Detection; SC: Secure control; DES: Discrete event system)

Year	Reference	Attack types			Models		Attack strategies	Defense strategies		Main focus
		A	I	C	TD	ED		D	SC	
2018	Ding *et al*., [10]	√	√	×	√	×	√	√	√	Attack detection and secure control
	Giraldo *et al*., [11]	×	√	×	√	×	×	√	×	Detection mechanisms for integrity attack
2019	Mahmoud *et al*., [12]	√	√	×	√	×	×	√	√	Modeling, detection and control of attacks
	Rashidinejad *et al*., [13]	×	√	√	×	√	√	√	√	Attack defense based on DES
	Dibaji *et al*., [14]	√	√	√	√	×	√	√	√	Attack defense mechanisms
2020	Singh *et al*., [15]	√	√	√	√	×	×	√	√	Existing problems and challenges
	Cao *et al*., [16]	√	√	×	√	√	×	√	√	Attack defense based on DES
	Tan *et al*., [17]	√	√	×	√	×	×	√	√	Detection mechanisms
2021	Zhang *et al*., [18]	√	√	×	√	×	×	√	√	Attack defense for industrial CPS
	Ding *et al*., [19]	√	√	×	√	×	×	√	√	State estimation and secure control
	This study	√	√	√	√	√	√	√	√	All issues in this table

II. SYSTEM MODELS FOR CPS

A system model plays a fundamentally important role in realizing system control theory on CPS due to its ability to characterize the dynamic behavior of a CPS. Literature shows that a CPS under attack can be usually modeled as two types of systems, i.e., time-driven and event-driven ones.

Time-driven systems including continuous-time and discrete-time systems have caught much attention in CPS modeling [20]−[22]. We note that the linear time-invariant (LTI) system is the most commonly used model for both. Take a discrete-time LTI as an example. CPS is modeled as

$$\begin{aligned} x_{k+1} &= Ax_k + w_k \\ y_k &= Cx_k + v_k \end{aligned} \tag{1}$$

where $k \in \mathbb{N}$, x_k, $w_k \in \mathbb{R}^n$ and y_k, $v_k \in \mathbb{R}^m$, represent the system state, process noise, system measurement and measurement noise at time k, respectively. Moreover, w_k and v_k are uncorrelated zero-mean Gaussian noises with covariance Σ_w and Σ_v, respectively.

Based on such model, a variety of attack models are designed. A basic idea for describing availability attacks is provided in [23], [24]. Let S_a be the attack signal or power, and η_k be the decision of attackers at time k. An availability attack can be described as

$$\eta_k = \begin{cases} 1, & S_a \text{ is injected at time } k, \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

Integrity attacks target sensor measurements or control commands. Let a_k be an attack vector, the actual measurement under attacks is $y_k^a = y_k + a_k$, where $y_k^a \in \mathbb{R}^m$. A similar model can be constructed for attacks on control commands, i.e., $u_k^a = u_k + a_k$, where u_k and u_k^a are control inputs when attacks are absent and present, respectively [25].

In addition to conventional models, some stochastic models are proposed in the literature. A typical discrete-time stochastic model [26] is constructed as

$$\begin{aligned} x_{k+1} &= Ax_k + g_{(Z_{k+1})}Bu_k + v_{k+1} \\ y_k &= Cx_k + w_{k+1} \end{aligned} \tag{3}$$

where $\gamma_{(Z_k)} \in \{0, 1\}$ denotes an attack sequence that prevents the control signal from reaching the actuator and Z_k corresponds to the internal state of an attacker.

Interesting work has also appeared in event-driven systems recently, i.e., discrete event system (DES), which is accepted as a technical abstraction of CPS [27]. Two typical tools to model a CPS as a DES are finite state automata and Petri nets. The former can show system states clearly, while the latter can provide a compact model.

A finite state automaton G is a tuple $G = (X, \Sigma, f, x_0)$, where X is a finite set of system states, Σ is a finite set of events, f: $X \times \Sigma \to X$ is the partial transition function, and x_0 is the initial state. Given a physical system, a supervisor is computed based on supervisory control theory [28]. The supervisor can allow or forbid the occurrence of certain events according to observed events (sensor readings), so that behaviors of a system can be controlled. For example, Wakaiki *et al*. [29] present a simple model for cyber attacks on a computer system. Its automaton representation is shown in Fig. 2, where $X = \{Clean, s_1, s_2, \ldots, s_M, Denial\ of\ service, Illegal\ access\}$, $\Sigma = \{Exploit\ 1, Exploit\ 2, \ldots, Exploit\ M, Grant\ access, Deauthorize\}$, $x_0 = Clean$, states *Denial of service* and *Illegal access* are undesirable states. An attacker may gain access to the system via a series of exploits to make

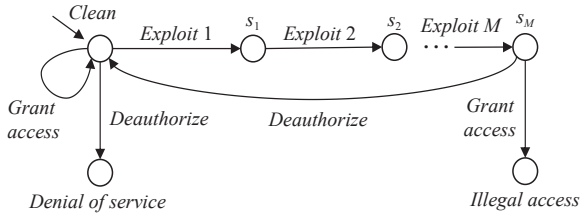

Fig. 2. An automaton G of a cyber attack on a computer system [29].

the system reach undesirable states. Thus, a supervisor is designed to control the occurrence of events *Grant access* and *Deauthorize*. However, such a supervisor can make wrong decisions since an integrity attacker may falsify event sequences sent to it. In [29], the attacker is assumed to be able to insert or remove event *Exploit i* in a sequence. Such an attack is characterized as a set

$$A = \{A_{\emptyset}, A_{Exploit\,1}, A_{Exploit\,2}, \ldots, A_{Exploit\,M}\}$$

where $A_{\emptyset}$ means that there is no attack and $A_{Exploit\,i}$ means the occurrence of *Exploit i* is altered by the attacker. Determining how to find a supervisor under such an attack set is the goal of the work [29].

A Petri net is another tool to model CPS. It is a 3-tuple $N = (P, T, F)$, where P and T are the set of places and transitions, respectively. $F \subseteq (P \times T) \cup (T \times P)$ is the set of flow relations that is represented by directed arcs. Modeling CPS and attacks as Petri nets is similar to the case with automata. Related models refer to [27].

Remark 1: The model in Fig. 2 is used to study an integrity attack, where " denial of service" is a state rather than an availability attack. Based on DES and control theory, most of the existing work is aimed at integrity attacks while almost none at availability ones. Compared with the former, availability attacks usually rely on external interference signals instead of system events. It means that the supervisor cannot handle an availability attack by controlling system events. In this sense, supervisory control of DES is not appropriate for handling availability attacks. Confidentiality attack models are usually diverse and complex. Their example can be found in [30], [31].

III. Availability Attack

The purpose of an availability attack is to make data, information and resources in the system unavailable. There are several ways for attackers to implement availability attacks, such as filling buffers in a user or the kernel domain, blocking or jamming the communication among key components, and altering a routing protocol. The most common availability attack is DoS one. In recent years, most studies about CPSs have concentrated on DoS. Researchers have extensively studied it based on time-driven systems, while rarely based on event-driven systems. Thus, we focus on the recent work about it in terms of time-driven systems.

A. DoS Attack Strategies Against CPS

As mentioned in Introduction, we need to study cyber attacks on CPS in terms of attack and defense strategies. The former means designing strategies to attack systems while the latter means protecting systems from being attacked. It is significant to have a sufficient understanding of attack strategies. In most cases, only knowing what kind of attack the system is subjected to, can we propose effective countermeasure. It is reasonable for researchers to study DoS attacks from an attacker's point of view.

Usually, DoS attacks block communication via a wireless network since its nodes' energy budget is limited [32]. Energy constraints become a tricky issue since they can impact the effectiveness of attacks. This problem is considered in recent attack strategies. They focus on allocating power and scheduling energy to gain more benefits for attackers. Consider a system modeled as (1), a DoS attack (2) is launched on the system. At time k, sensors can estimate the state x_k after obtaining y_k., i.e., generating a minimum mean squared error (MMSE) $\hat{x}_k^s = E[x_k|y_1, \ldots, y_k]$. Then, $\hat{x}_k^s$ is sent to a remote estimator through a wireless network under attacks, which can lead to data dropout. We use D_k to denote the set of data received at a remote estimator. The MMSE estimate $\hat{x}_k$ at the estimator and its error covariance P_k can be obtained as $\hat{x}_k = E[x_k|D_k]$ and $P_k = E[(x_k - \hat{x}_k)(x_k - \hat{x}_k)'|\, D_k]$. Let $\eta = (\eta_1, \eta_2, \ldots, \eta_T)$ be an attack schedule in a time horizon T. According to (2), $\eta_k = 1$ means that the attack power is injected at time k and $\eta_k = 0$, otherwise. Due to energy constraints, the attacker can launch at most n attacks during T, i.e., $\sum_{k=1}^{T} \eta_k \le n$, where $n < T$. In [33], *Average Error* is defined to evaluate system performance under a given attack schedule η, i.e.,

$$J_a(h) = \frac{1}{T} \sum_{k=1}^{T} E\left[P_k(\eta_k)\right]. \tag{4}$$

From the viewpoint of attackers, the work [33] tries to find an attack strategy that deteriorates the remote estimation by maximizing *Average Error*. It can be formalized as follows:

Problem 1:

$$\max_{\eta \in \Gamma} tr[J_a(\eta)] \tag{5}$$

$$\text{s.t.} \sum_{k=1}^{T} \eta_k = n \tag{6}$$

where $\Gamma = \{0, 1\}^T$ is the set of all possible attack schedules, and $tr[\cdot]$ is the trace of a matrix. Note that Γ is a Cartesian product set of multiplying $\{0, 1\}$ for T times, i.e.,

$$\Gamma = \overbrace{\{0,1\} \times \{0,1\} \times \cdots \{0,1\}}^{T \text{ times}}. \tag{7}$$

The solution to *Problem* 1 in [33] is any attack schedule that contains a sequence of n consecutive attacks.

Problem 1 is modified in [34] by replacing $J_a(\eta)$ in (5) with a Linear Quadratic Gaussian control cost function. Solution to the modified problem aims to maximize the attacking effect on a wireless NCS. It should be pointed out that strong assumptions are required in both studies [33], [34], i.e., the system is unaware of the existence of attacks, only a limited number of attacks can be launched during an active period, and no packets drop if the attack is absent.

An important situation is neglected in the above methods, i.e., it is unlikely for practical systems to work perfectly all the time. Hence, [35] focuses on a DoS attack under a scenario where packets may be lost even if no attack occurs. By solving Problem 1, an optimal scheduling method is proposed to maximize the expected estimation error. It greatly degrades the performance of a remote estimator, thus maximizing the attack effect on the system. In addition, the proposed method handles a problem of when to launch an attack to maximize damage to the system. However, the effect of attack power on system performance is ignored. Such issue is considered in [36], i.e., optimal DoS attack energy management is studied

while taking account of packet losses and the effect of attack power. As a result, two static attack power allocation policies and a dynamic one are proposed. The former aims to maximize expected terminal error and average error, while the latter considers two indexes based on a Markov decision process. They can work only if the packet transmitted from a sensor to an estimator is not lost at the initial time [35], [36].

Sensors are assumed to have computational capacity in the above attack strategies. Such strategies may lose effectiveness when facing un-computational sensors. This problem is discussed in [24], where such sensors are adopted in CPS under a round-robin protocol. A more general error cost function that contains terminal and average errors is proposed. Then, an optimal attack schedule is presented to maximize the error cost so that the performance of a state estimator can be degraded. However, sensors studied in the paper contain a single unit buffer only. Thus, the proposed method is not applicable to a multiple unit case.

B. Defense Strategies Against DoS Attack

Two strategies for defending against cyber attacks include attack detection and secure control. Advances on the former are mostly derived from computer science instead of system control theory. Many detection methods are designed based on artificial intelligence approaches, such as deep learning, reinforcement learning and neural network [37]−[40], which is beyond the scope of this paper. We only discuss secure control methods against DoS attacks in this section.

Once an availability attack is successfully launched, the closed-loop stability of CPS is destroyed since certain data packets are prevented from being transmitted over communication networks. Hence, most researchers pay their attention to resilient control for availability attacks since some degree of data loss can be tolerated with resilient control.

Event-triggered (ET) control has the advantage of saving network resources significantly while maintaining good closed-loop system performance. It is widely used to achieve resilient control for CPS, especially systems with limited network resources, such as NCSs and wireless networks. Usually, an ET scheme can be divided into ET sampling and ET transmission. The former embeds an event-generator into a sensor to select signals to be sampled, while the latter embeds it behind the sensor to determine whether the sampled signals should be released. A detailed analysis of this ET control framework is referred to [41].

In order to maintain desired control performance as well as reduce the number of transmitted packets, Peng *et al*. [42] model multi-area power system as an area control error-dependent time-delay model and presents a resilient ET transmission scheme for the system based on load frequency control. Based on the proposed model and scheme, DoS attacks can be defended with a priori knowledge of the maximum DoS attack duration.

Asynchronous DoS attacks are considered in [43], i.e., DoS attacks can occur on sensor-to-controller (S-C) channels and controller-to-actuator (C-A) channels. Two different ET mechanisms are designed for them, namely S-C ET and C-A ET. The former is embedded in a smart sensor system and the latter is introduced in a controller system. Under the proposed ET strategies, a closed-loop system is proved to be input-to-state stable.

Motivated by ET transmission schemes and periodic ET control schemes in [44] and [45], Hu *et al*. [46] propose an observer-based resilient ET transmission scheme for NCS, where a system suffers from periodic DoS jamming attacks. The DoS jamming signal is as follows:

$$S1_{\mathrm{DoS}}(t)=\begin{cases}0, & t\in[nT,nT+T_{\mathrm{off}}^{\min}]\\ 1, & t\in[nT+T_{\mathrm{off}}^{\min},(n+1)T]\end{cases}\tag{8}$$

where $n\in\mathbb{N}$ is the number of periods, $T>0$ is the action period of a jammer and $T_{\mathrm{off}}^{\min}$ is the sleeping period of a jammer in the nth period. The proposed method is effective to improve the efficiency of resource utilization and guarantee the stability of the system under the periodic DoS attack. Subsequently, Hu *et al*. [47] study a networked system under non-periodic DoS jamming attacks, where the attack signal is

$$S2_{\mathrm{DoS}}(t)=\begin{cases}0, & t\in[g_{n-1},g_{n-1}+b_{n-1})\\ 1, & t\in[g_{n-1}+b_{n-1},g_n)\end{cases}\tag{9}$$

where $\{g_n\}_{n\in\mathbb{N}}$ and $\{b_n\}_{n\in\mathbb{N}}$ are two sequences of real numbers such that $0\le g_0<g_0+b_0\le g_1<\cdots<g_{n-1}+b_{n-1}\le g_n<\cdots$ for $n\in\mathbb{N}$. The intervals $\cup_{n\in\mathbb{N}}[g_n,g_n+b_n)$ determine when the signal is off and the communication is allowed, and the intervals $\cup_{n\in\mathbb{N}}[g_n+b_{\mathrm{n}},g_{n+1})$ are the time intervals at which an attacker is active. By considering such an attack signal, an ET-based H_∞ filter is proposed to ensure the system stability.

It must be noted that internal and external environments are usually complex and uncertain in practice, leading to failure of the above methods since uncertainty of system parameters is not considered. Thus, some researchers treat CPS as a stochastic system. Chen *et al*. [48] consider resilient control for an uncertain NCS under quantization and pulse-width modulated (PWM) DoS jamming attacks [49]−[51]. An ET transmission scheme is proposed to solve the problem, based on which, a switched system model is obtained to preserve closed-loop stability, where parameter uncertainty is considered. Furthermore, an algorithm is designed to generate state-feedback controllers and communication strategies.

Different from [48], Zhao *et al*. [52] take into account a stochastic NCS under non-periodic DoS jamming attacks. They design an observer-based adaptive event generator to preserve control performance, while a secure controller is obtained to guarantee the system stability. Moreover, they provide a method for the joint design of observer gains, controller gains and ET parameters.

Similarly, ET control is employed in [53] to reduce the burden of communication for a stochastic NCS under DoS attacks. The event generator is embedded into a sensor, forming a new sensor node. The proposed scheme allows data packets to be dropped actively if they are transmitted successfully at the initial time. Different from the above methods, system performance in the presence and absence of DoS attacks is analyzed. An upper bound is provided to

describe system stability based on the bounded function.

An important issue we should take into account is that potential faults may occur in practical systems. They degrade the reliability of systems as well as the performance of aforementioned strategies. Sathishkumar and Liu [54] propose a resilient fault-tolerant control strategy for a nonlinear NCS to deal with periodic DoS jamming attacks, actuator saturation, randomly occurring nonlinearities and actuator faults. Specifically, an ET transmission scheme is designed to ensure the resilience of a system under DoS attacks.

In addition to an ET control framework, researchers also adopt other methodologies to realize secure control. For example, robust control for a NCS is studied in [55], where a dynamic observer-based control architecture is designed. It shows that the considered dynamic observer equipped with prediction and state resetting capabilities is applicable to a general class of DoS attacks. However, it works only if the process under control is observable. A Markov process is utilized in [56] to study the resilience and stability of a NCS under stochastic DoS attacks. The proposed method is effective for the case with full knowledge on DoS attacks but less effective for the case with partial knowledge only. In other words, its efficiency depends on how much knowledge about DoS attacks the system controller has. Yuan and Xia [57] consider DoS attacks between sensor and remote estimation. They present a multi-transmission strategy to reduce the probability of a system being attacked. In their work, two players are considered, i.e., a transmitter and an attacker. Their interaction is modeled as a stochastic game, based on which, a resilient control strategy is developed. Zhang *et al*. [58] consider DoS attacks that can be random or periodic but their duration time is limited. They propose some criteria to check whether a non-periodic sampled-data control system can preserve stability under such attacks. Based on the duration time of DoS attacks, they further present an algorithm to generate state-feedback controllers.

Apart from resilient control, stochastic control can be used to deal with DoS attacks. It often adopts a Markov process to model systems and DoS attacks to realize risk sensitive control [26], [59], [60]. After constructing a stochastic model (3), an exponential running cost is considered in [26], i.e.,

$$J(u)=\left(\frac{1}{\theta}\right)E\left[\exp\left\{\left(\frac{\theta}{2}\right)\left\{\sum_{k=0}^{N-1}\left(x_k^T X x_k + \gamma_{(Z_{k+1})}u_k^T Y u_k\right)+x_N^T X_N x_N\right\}\right\}\right] \tag{10}$$

where $\theta > 0$ is the risk-sensitive parameter. $u_k \in U_{0,N}$ is the admissible control signal at time k where $N \in \mathbb{N}$, $U_{0,N}=\{u_k\}_{k=0}^{N-1}$ is admissible control signals, and $E[\cdot]$ is the expectation with respect to a probability measure. X is a positive semidefinite matrix, and Y is a positive definite one.

Using a stochastic model, Befekadu *et al*. [26] design an optimal control policy for a discrete-time partially observed system. Their policy is based on a chain of measure transformation techniques and dynamic programming, such that a recursive optimal control policy and the considered information-state can be transformed into a fully observable stochastic control problem.

A real CPS usually consists of multiple subsystems, which are deployed in a distributed manner. It increases attack surfaces, making it more frangible in security [61]. For example, communication channels among subsystems can suffer from different DoS attacks. The whole system can be severely affected even if only one channel is attacked. Such a security problem cannot be handled well by a centralized method since attack modes are different on each channel. Hence, an urgent study is demanded in order to develop distributed defense approaches for cyber attacks. Determining how to achieve a consensus for a distributed CPS under DoS attacks is handled in many studies, e.g., [62]−[64]. By introducing a k-connected graph, [62] designs a distributed event-triggered controller for a CPS under mode-switching DoS attacks. Yet, some negative effects may be generated on the system since the method adopts a continuous Lyapunov function, which can generate mismatched terms. To mitigate this problem, the controller is further combined with an extended Laplacian matrix to ensure the system consensus. A practical case is investigated in [65] that answers how to address a distributed secure platoon control issue for connected vehicles under DoS attacks. Based on a switched time-delay system model, the work [65] captures the attack phenomena and designs a distributed state feedback controller to make the system achieve desired performance.

In order to give a clear review, Table III is provided to summarize the above work in terms of: reference, target system, model type, attack type, methodologies, advantages and disadvantages.

Remark 2: In Table III, the disadvantage of many methods is constraints on DoS frequency and duration, such as [52], [55], [66]. It is derived from two assumptions established in [67]. They specify the type of DoS attacks by limiting its frequency and duration, such that they can be considered as a special attack model. They are shown next.

Given a sequence of DoS off/on transitions as $\{h_n\}_{n\in\mathbb{N}}$ with $h_0 \geq 0$, the sequence means time instants at which DoS exhibits a transition from zero (communication is possible) to one (communication is interrupted). We have

$$H_n := \{h_n\} \cup [h_n, h_n+\tau_n] \tag{11}$$

to represent the nth DoS time-interval, of a length $\tau_n \in \mathbb{R}^+$, over which communication is not possible.

Given τ, $t \in \mathbb{R}^+$ with $t \geq \tau$, let $n(\tau, t)$ represent the number of DoS *off/on* transitions occurring during interval $[\tau, t]$. Let

$$\Xi(\tau,t) := \bigcup_{n\in\mathbb{N}_0} H_n \cap [\tau,t] \tag{12}$$

denote the time instants at which communication is denied.

Assumption 1 (DoS Frequency): There exist η and $\tau_D \in \mathbb{R}^+$ such that

$$n(\tau,t) \leq \eta + \frac{t-\tau}{\tau_D} \tag{13}$$

for all τ, $t \in \mathbb{R}^+$ all with $t \geq \tau$.

Assumption 2 (DoS Duration): There exist $k \in \mathbb{R}^+$ and $T \in$

TABLE III
SUMMARY OF RECENT DEFENSE WORK ON DOS ATTACK

(DT: Discrete-time system; CS: Continuous-time system)

Reference	Target	Model type	Attack type	Methodologies	Advantages	Disadvantages
[42]	Multi-area power system	CS	DoS	ET transmission,load frequency control	Improving the transaction efficiency	Limited attack duration time
[43]	CPS	CS	Asynchronous DoS	ET sampling and transmission	Handling system disturbance and measurement noise	Constraints on DoS frequency and duration
[46]	NCS	CS	Periodic DoS	Observer-based ET transmission	Preserving good control performance	A uniform lower bound for the attack sleeping period
[47]	Networked system	CS	Non-periodic DoS	ET transmission,H_∞ filtering	Achieving good filter performance and reducing unnecessary resource consumption	Known sleeping and active intervals of DoS attacks
[48]	Uncertain NCS	CS	PWM DoS	ET transmission	Handling system parameter uncertainties	Full state information
[52]	Stochastic NCS	CS	Non-periodic DoS	Observer-based ET framework	Preserving stability with a L_2-gain performance level	Constraints on DoS frequency and duration
[53]	Stochastic NCS	DT	Bernoulli distributed DoS	ET sampling	Handling active, consecutive packets dropout	Specified attack location
[54]	Nonlinear NCS	CS	Periodic DoS	ET transmission	Handling fault-prone systems	A uniform lower bound for the attack sleeping period
[55]	NCS	CS	DoS	Dynamic observer-based control	Handling general DoS attacks	Constraints on DoS frequency and duration
[56]	NCS	CS	Stochastic DoS	Markov process	Constructing stability and stabilization criterion	Sufficient knowledge on DoS attack
[57]	CPS	CS	DoS	Multi-transmission	Reducing the probability of being attacked	Full state information
[58]	NCS	CS	DoS	Sampled-data model	Handling random and periodic DoS attacks	Limited attack duration time
[26]	DT partially observed system	DT	Markov modulated DoS	Markov process	Optimal risk-sensitive control	Many assumptions
[62]	CPS	CS	Mode-switching DoS	k-connected graph, extended Laplacian matrix	A more general attack model	Negative effects on the system
[65]	Connected vehicles	CS	DoS	Graph theory, switched time-delay system	Establishing quantitative relations between platooning performance and attack parameters	A simple system structure
[66]	CPS	DT	DoS	Sliding mode control,zero-sum game	Preserving stability and reducing external disturbance	Constraints on DoS frequency and duration

$\mathbb{R}^+/[0, 1)$ such that

$$|\Xi(\tau,t)| \le k + \frac{t-\tau}{T} \tag{14}$$

for all τ, $t \in \mathbb{R}^+$ all with $t \ge \tau$.

IV. INTEGRITY ATTACK

Integrity attacks aim to destroy the data integrity of a CPS. They can be launched by altering or deleting sensor measurements and control decisions, or inserting incorrect data into them. In general, they are more subtle and difficult to be detected than availability attacks. The reason is that falsified data spreads through a sensor network in an epidemic way, leading to negative effects on systems [41]. Thus, more and more researchers pay attention to it. In this section, we discuss recent representative work on integrity attacks.

Note that integrity attacks are also known as deception attacks. To avoid any confusion, this work just uses integrity attacks.

A. Integrity Attack Strategies Against CPS

There are many results about integrity attack strategies. Some novel schemes are developed based on time-driven and event-driven system models.

1) Time-Driven System-Based Attack Strategies: Section II shows that a CPS is often modeled as an LTI system. For instance, Wu *et al*. [68] model a CPS as a continuous-time LTI system and design two optimal location switching strategies to implement false data injection attacks. However, their methods are limited by strong assumptions. For example, an attacker should have perfect knowledge about system parameters and state information, and the communication channel is perfect without any noise.

As most of the CPSs are equipped with an attack detector now, stealthiness of attacks should be considered [69], [70]. Usually, an attack is considered stealthy if it cannot be detected by an attack detector. The feasibility of implementing a replay attack on a control system with a bad-data detector is discussed in [71] and [72]. Hao *et al*. [73] study sparse false data injection attacks in smart grids, where sparse stealthy attacks are proposed for two typical scenarios, i.e., random and target attacks. The former can compromise arbitrary measurements while the latter only alters specific state variables. Both types of attacks in [73] are stealthy, but random attacks are subject to a strong assumption, namely, no

measurements are protected in the system.

Guo *et al*. [74] study a linear integrity attack on remote state estimation. They propose a new attack strategy as

$$c_k^a = T_k c_k + b_k \tag{15}$$

where c_k is an innovation sent to the estimator, T_k is an arbitrary matrix, b_k is an independent and identically distributed (i.i.d.) Gaussian random variable, and c_k^a is the modified innovation. They further give the corresponding constraints to ensure that false data can be injected to a system without being detected by a χ^2 -detector. However, such a strategy is restricted by the linear form and faces two problems. One is that a linear attack framework cannot cover the general form of possible attacks. Another is that a more general attack model exists and is able to cause a worse damage to the system. To solve them, Wu *et al*. [75] find a worst-case integrity attack. They extend the linear attack in [74] to a general form based on an innovation, i.e.,

$$c_k^a = f_k(c_k) \tag{16}$$

where $f_k(\cdot)$ is an arbitrary function. A criterion for judging whether an attack strategy can maximize estimation error is proposed to determine the strategy's optimality.

It should be noticed that the above stealthy attacks all focus on χ^2 -detectors, i.e., they are not detected by χ^2-detectors. However, detection techniques vary and are not limited to χ^2-detectors [11], [76]. An attack strategy applicable to χ^2-detectors may not be applicable to a CPS equipped with other detectors. Hence, stealthy attacks for other detectors are considered in [77]–[79]. A CPS equipped with a Kalman filter is considered in [80]. The Kullback-Leibler divergence is used to describe the stealthiness of attacks so that a necessary and sufficient condition for strict stealthy attack is proposed, i.e., a strict stealthy attack cannot result in an unbounded benefit. Both optimal and suboptimal attack strategies are studied in the paper. Finally, the authors provide a suboptimal strategy since the computational cost is usually too high to find an optimal one.

2) Event-Driven System-Based Attack Strategies: Attack issues in CPS have attracted the attention of researchers in the field of DES. A CPS can be characterized as a closed-loop supervisory control system as shown in Fig. 3 . Integrity attacks against a DES are divided into three classes, i.e., sensor, actuator, and general attacks. Sensor and actuator attacks are injected via sensor and actuator channels, respectively, while general ones are injected via both channels.

Now, we consider an automaton G in Fig. 2 . Assume that $M = 3$, thus $X = \{Clean, s_1, s_2, s_3, Denial\ of\ service, Illegal\ access\}$, $\Sigma = \{Exploit\ 1, Exploit\ 2, Exploit\ 3, Grant\ access, Deauthorize\}$. Since states *Denial of service* and *Illegal access* are undesirable, a supervisor is required to disable the occurrences of event *Grant access* at state s_3 and *Deauthorize* at state *Clean*. Suppose that an attacker A wants to induce the system into an undesirable state. For example, an event sequence $\{Grant\ access, Exploit\ 1, Exploit\ 2, Exploit\ 3\}$ is implemented and the system reaches state s_3. Such an event sequence is captured by sensors and sent to the supervisor. During this period, A intercepts it and removes event *Exploit* 3 from it, leading to a new sequence. As a result, the event sequence observed by the supervisor is $\{Grant\ access, Exploit\ 1, Exploit\ 2\}$. According to it, the supervisor believes that the system reaches state s_2 and does not disable event *Grant access*. Obviously, the system can reach a bad state *Illegal access* since it is actually at state s_3. Such an attack model A is common seen in the literature. The problem is determining how to get a well-defined attack model based on DES and under what conditions such a model exists. To solve the problem, Su [81] first introduces two concepts, i.e., attackability and attack under bounded sensor reading alterations. Then, a finite state automaton is employed to describe an attack model that can intercept and alter sensor measurements. It shows that such a model exists if the system and its supervisor can be described by finite state automata. In [82], a structure called insertion-deletion attack (IDA) is established by modeling game-like interactions between a supervisor and the environment. IDA embeds all possible cases that some sensor events are modified by attackers without being noticed by a supervisor, thus realizing a stealthy attack. It is worth noting that system models used in [82] and [81] are automata.

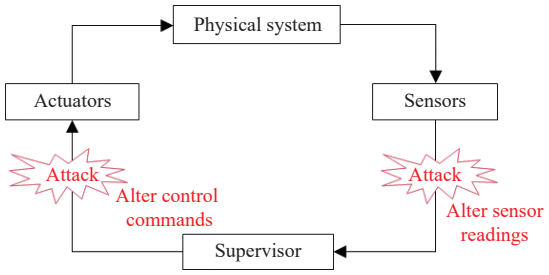

Fig. 3. A closed-loop supervisory control system under attacks.

Based on DES, another tool is also commonly used to study attacks, i.e., Petri nets. Li *et al*. [83] model a smart grid as a stochastic Petri net, where a smart grid is threatened by topology attacks and equipped with defense strategies. Topology attacks are coordinated attacks evolved from false data injection attacks. Li *et al*. [83] define two successful topology attacks and utilize Petri nets to capture behaviors of systems and such attacks.

B. Time-Driven System-Based Defense Strategies

There are many defense strategies to handle integrity attacks. They are divided into two parts: detection and secure control.

1) Attack Detection: Attack detection is an efficient way to protect CPS from serious damage. A detection method can identify occurrences of attacks such that warnings can be sent to an operator to take appropriate measures. Many methodologies are adopted to develop detection methods, such as state estimation, χ^2 -detector, fault detection, and watermarking-based methods.

State estimation is crucial to control systems and to defend from integrity attacks. Although many studies address integrity issues based on state estimation, most of them require such strong assumptions that their proposed methods

cannot be put into practical use, such as absolute protection for sensor measurements [84]−[86]. In order to break this limitation, Deng *et al*. [87] consider a more practical case, i.e., whether a measurement can be modified by an attacker depends on the defense budget on corresponding devices. They propose a least-budget defense strategy based on a measurement residual-based estimator to address false data injection attacks on a power system. However, their method is applicable to a specific known attack only. It becomes ineffective if an attack is unknown. Thus, Ge *et al*. [25] design distributed estimators based on Krein space to provide suitable residuals for attack detection. Then, a two-stage attack detection framework is developed to ensure that unknown attacks can be detected and identified by each estimator.

Equipping the system with filters to estimate states accurately is an effective way to deal with integrity attacks. Two classical filters often used in the literature are the Kalman filter [88]−[90] and H_∞ filter [91], [92]. For example, Mishra *et al*. [93] present an estimator based on a Kalman filter for a linear dynamic system under integrity attacks. Considering engineering reality, a distributed H_∞ filter is designed in [94] based on a round-robin protocol. H_∞ performance is ensured in this work such that security of a system is guaranteed under random integrity attacks.

It is worth noting that some assumptions are needed to apply Kalman and H_∞ filters. The former requires process and measurement noise to obey Gaussian distribution. The latter is only applicable to cases in which disturbances have bounded energy. Related methods cannot deal with practical cases that do not satisfy such assumptions. Hence, Ma *et al*. [95] study a variance-constrained distributed filtering problem, where both integrity attacks and disturbances are considered as unknown but bounded signals. A sufficient condition and an optimization problem are proposed to determine filter parameters to realize a desired state estimation under attacks. Song *et al*. [96] consider a stochastic nonlinear system with integrity attacks and non-Gaussian noises, i.e.,

$$\begin{aligned} x_{k+1} &= f(x_k) + g(x_k, a_k) + Bw_k \\ y_{i,k} &= h_i(x_k) + s_i(x_k, b_{ik}) + D_i v_{i,k} \end{aligned} \tag{17}$$

where $i \in N = \{1, 2, \ldots, n\}$, $y_{i,k} \in \mathbb{R}^m$ represents measurements of the ith sensor, $\alpha_k \in \mathbb{R}^\alpha$ and $\beta_{ik} \in \mathbb{R}^\beta$ are zero-mean arbitrary noise sequences. A distributed filter is designed in [96] to realize secure state estimation. The ith filter structure is constructed as follows:

$$\begin{cases} \hat{x}_{i,k}^- = f\left(\hat{x}_{i,k-1}^+\right) + \varepsilon \sum_{j \in N_i} a_{ij} (f(\hat{x}_{i,k-1}^+) - \hat{y}_{j,k}) \\ \hat{x}_{i,k}^+ = \hat{x}_{i,k}^- + K_{i,k}(y_{i,k} - h_i(\hat{x}_{i,k}^-)) \end{cases} \tag{18}$$

where $\hat{x}_{i,k}^-$ is a vector representing the one-step prediction of the i th sensor at time k, while $\hat{x}_{i,k}^+$ represents the one-step estimate. ε is a positive scalar describing the consensus gain, and matrix $K_{i,k}$ is a filter gain to be designed. As the filtering performance can be affected by attacks and noise, the work [96] adopts a weighted maximum correntropy criterion to replace the minimum covariance index. Compared with the traditional filters, the proposed one is effective under attacks and can be applied to many complicated cases.

Remark 3: Integrity attacks mentioned in [25], [94], and [95] are false data injection attacks. Reference [93] considers sensor attacks where an unknown subset of sensors can be corrupted by attackers.

χ^2-detectors are among the general tools to detect integrity attacks. They have the advantage of detecting bad or false data [17]. Mo *et al*. [97] define a replay attack model that cannot be identified by classical detection strategies. They further propose some measures to optimize detection probability. In particular, a noise control method is proposed to improve detection performance at the cost of control performance. Rawat and Bajracharya [98] study attack detection based on a χ^2-detector and cosine similarity matching in a smart grid communication system, where an attacker is assumed to have enough knowledge about system parameters. They reveal that the cosine similarity matching approach is more sensitive to false data injection attacks than a χ^2-detector. Miloševič *et al*. [99] analyze bias injection attacks in a stochastic linear dynamic system, where a χ^2 -detector is used as a detector. Based on their analysis results, they propose a method to select sensors to mitigate the negative impact caused by an attack.

Fault detection and isolation (FDI) focuses on determining whether the behavior of an underlying process is correct or not. Since attacks often incur erroneous system behaviors, an FDI technique is widely used and extended to confirm the occurrence of an integrity attack. In general, the design of an FDI-based method involves two steps, state estimation and threshold design. The first issue is often addressed by introducing observers, such as unknown input observers (UIOs) [100], [101]. Based on state estimation, a residual is generated to compare a measurement with its estimate. It is used to design detection thresholds. In [100] and [101], a false data injection attack can be identified if a component of a set of residuals exceeds a predefined threshold. It should be pointed out that [101] adopts an adaptive threshold to improve the detection performance. However, this method may miss attacks since it is too difficult to compute such a threshold in practice. Thus, Wang *et al*. [102] design a novel approach based on a nonlinear interval observer. Their approach mitigates the computation of this threshold. To be precise, interval residuals are adopted as a detection criterion rather than the traditional residual evaluation function and threshold.

An undesirable situation has emerged with the widespread application of the above methods. Attackers may have enough knowledge about these methods such that their vulnerabilities can be exploited to launch attack. For example, many attack strategies can bypass a χ^2-detector by utilizing its limitations, e.g., it fails to recognize attack signals that do not obey a Gaussian distribution [74], [103]. Moreover, the FDI technique needs to distinguish between attacks and faults to take appropriate countermeasures. It is possible for an attack to be disguised as a fault, preventing the system from detecting it and making correct decisions. Thus, it is a considerable issue to design new attack detection methods.

Combining watermarking techniques with existing detectors emerges to be a novel idea to identify integrity attacks. A

watermarking is useful to protect data transmitted through a communication network by encrypting and decrypting it. Each innovation sequence c_k is first processed at the sending side, i.e.,

$$g_k = ac_k + m_k \tag{19}$$

where $a \in \mathbb{R}$ is a constant, and $m_k \in \mathbb{R}^m$ is a watermarking that is a zero-mean i.i.d. Gaussian random variable with covariance Σ_m. Then, g_k is transmitted through a wireless network instead of the original innovation sequence. At the remote side, c_k can be recovered as follows:

$$g_k^r = \frac{\tilde{g}_k - m_k}{a} \tag{20}$$

where $\tilde{g}_k$ is the actual data received by the remote estimator, and g_k^r is the recovered data. Note that watermarking sequences on both sides are consistent such that the original data can be recovered on the remote side. Now, we consider a case that an attack (15) is launched on a system equipped with watermarking techniques. The attack can be rewritten as $c_k^a = T_k g_k + b_k$, and the recovered data is

$$g_k^r = T_k g_k + \frac{1}{a} b_k + \frac{1}{a}(T_k - I)m_k. \tag{21}$$

As a result, a new secure module is composed of (19) and (21). References [104] and [105] combine this module with the χ^2 -detector and Kullback-Leibler (K-L) divergence detector, respectively. Their methods can determine whether the data has been modified or not. Furthermore, the proposed method in [105] method can identify stealthy attacks in [74] and [103] by selecting proper watermarking parameters. A strategy to find appropriate watermarking is proposed in [106], based on which, Naha *et al*. develop the quickest detection method for a NCS under integrity attacks.

In addition to watermarking-based methods, new detection methods have been proposed. For instance, in [107], a finite-time memory fault detection filter is presented for randomly occurring integrity attacks in a nonlinear discrete system. Attack detection for a distributed CPS is considered in [108], where a new detector is proposed based on the latest updated data. The computational burden of this detector does not depend on the size of CPS. Thus, it has high scalability.

2) Secure Control: Usually, a detector just sends a warning to an operator once an attack is identified. The attack can still damage a system if the operator has no countermeasures or does not handle it in time. Secure control is required to guarantee the stability and safety of a system under attack.

The secure estimation and control problems for a discrete-time linear system are studied in [109]. Reference [109] designs an attack-resilient state observer and an observer-based controller to figure out integrity attacks on sensors and actuators. Motivated by [109], Xie and Yang [110] focus on false data injection attacks on communication channels from a controller to an actuator. They first design a switched attack-resilient observer and then present a supervisory switching strategy to guarantee attack-resilient performance. Such a method is effective to control a CPS under false data injection attacks. However, it may suffer from high computational complexity since it requires accurate state estimation.

In addition to false data injection attacks, a class of sparse attacks is studied in the work [111], [112]. Sparse sensor attack is able to tamper measurements of a subset of sensors in a feedback control loop. In [113], an event-triggered secure observer-based control scheme is proposed for a continuous-time CPS under actuator and sparse sensor attacks. It requires that the set of attacked channels remains unchanged. Hence, it may fail to handle cases that the set changes over time.

It is nontrivial to consider distributed secure control for a real industrial CPS, such as unmanned vehicle systems and power systems [114], [115]. For example, an attack-resilient cooperative control policy is developed in [116] for a power system to regulate the active power at a specific command. The policy contains an observation network to monitor all distributed generators and isolate the misbehaving one such that the rest can work properly. To enhance the resilience of an islanded microgrid to false data injection attacks, Bidram *et al*. [117] propose a control scheme based on a weighted mean subsequence reduced algorithm, which allows each distributed energy resource to neglect information altered by attackers. Such a mechanism is also employed in [118]. Different from [117], [118] considers a multi-microgrid system as a multi-agent one, which is modeled as a weighted directed graph. A distributed resilient control approach is presented in [119] for multiple energy storage systems in an islanded microgrid, which is inspired by the adaptive resilient control of multiagent systems in [120], [121]. By introducing the adaptive technique, negative effects caused by attacks and faults can be compensated. Additionally, distributed state estimation and control problems are discussed in [122] for an interconnected CPS with sensor attacks. The first issue is addressed by designing a distributed preselectors and an observer, while the second one is resolved based on secure state estimation and a virtual fractional dynamic surface.

C. Event-Driven System-Based Defense Strategies

Similar to time-driven system-based methods, defense strategies based on DES can be classified into two categories: attack detection and secure control.

1) Attack Detection: Attack detection in DES is an intrusion detection module. A detection module is connected with the supervisor. It can observe same events as the supervisor does. Once an attack is detected, the module sends information to the supervisor, such that the system can be prevented from entering an unsafe state before the attack causes damage.

The problem of intrusion detection and prevention is studied in [123] for supervisory control systems. After designing a mathematical model for a system under attacks, a defense method is proposed to detect actuator enablement attacks online. This work is further extended in [124], where both attacks on sensors and actuators are considered, including actuator enablement attacks, disablement ones, sensor erasure attacks and insertion ones. However, the methods in [123] and [124] disable all controllable events once an attack is detected, which may lead to unnecessary loss of resources. To deal with this problem, new detection methods are developed in [125]−[127], which disable all controllable events only when

their occurrence would allow an attack to damage a system. In particular, [125] proposes an automaton model and a supervisor for a close loop system under man-in-the-middle attacks. A property named NA-Safe controllability is introduced to describe safe controllability under attacks. This property provides a sufficient and necessary condition to determine whether an intrusion detection module exists. Lima *et al*. [127] extend this work. They demonstrate the correctness of NA-Safe controllability and show how to implement a security module against attacks in the communication channels of a CPS.

2) Secure Control: As attackers induce the system into an undesirable state, a general idea to implement secure control is to model a CPS as a DES first. Then, we design a control specification to disable all the undesirable states. Finally, a corresponding supervisor is obtained to prevent them from being reachable under attacks.

As mentioned before, Su [81] proposes an integrity attack model, called ABSRA. On the basis of the knowledge for ABSRA model, he further designs a synthesis algorithm to compute a robust supervisor that ensures any ABSRA is either detectable or inflicts no damage to a system. Note that the work [81] is motivated by that in [124]. The difference between them is that the former aims to detect attacks online, thereby requiring real-time fault diagnosis, while the latter does not require real-time detection but a prior knowledge of attack models.

Wakaiki *et al*. [29] study DES with multiple attacks. They address how to design a supervisor to enforce a specified language for unknown attacks and regardless of the attackers' action. To solve it, they propose a new concept, termed observability, which is a stronger version of the traditional one and shows the observability of a prefix-closed language under an attack. Based on it, an algorithm is designed to generate desired supervisors for a special attack, called output-symbol attack, which can alter output string symbols from a given set.

Meira-Góes *et al*. [128] model an underlying uncontrollable system as a discrete transition system, where sensor readings are represented as a set of finite observable events. An augmented model is then derived by adding an attacker to the original one, such that incorrect information can be sent to the system. The system may reach an undesirable state once receiving wrong information. Thus, control specification in [128] focuses on preventing certain bad states from being reachable. Thus, the problem of defending integrity attacks can be converted into a DES supervisory control problem.

A common limitation of above methods [29], [81], [128] is that only one robust supervisor can be provided each time for a specific attack. It affects their efficiency in handling real-life applications where multiple attacks appear. Hence, a framework is proposed in [129] to improve their efficiency, where robust supervisors are synthesized for general sensor attacks based on automaton and game theory. Given a system under attack, the proposed framework [129] embeds all robust supervisors for it, including supervisors obtained by methods in [29], [81], [128]. For different attacks, different supervisors can be extracted in the framework to defend them.

Note that the modeling tool utilized in the aforementioned methods [29], [81], [128], [129] is automata. Apart from automata, some approaches are developed based on Petri nets. For instance, You *et al*. [130] study sensor attacks based on Petri nets by considering a special property, i.e., liveness. Liveness is an important dynamic behavior of a system that is the basis for it to work properly. They first design a supervisor to enforce liveness for a bounded Petri net without attacks. Then, they propose a basic supervisor under sensor attacks. Such a basic supervisor ensures that states forbidden in the first step cannot be reached, thus liveness of the system can be guaranteed under attacks. The four types of attacks in [124], i.e., actuator enablement attacks, disablement ones, sensor erasure attacks and insertion ones, are studied in [27] based on labeled Petri nets. They design different supervisors for sensor and actuator attacks under different premises. For the former, given two feasible transition sequences with same observation, their one-step controllable extensions should violate or satisfy a specification. For the latter, attacks can be detected and controllable transitions can be disabled before reaching undesirable states.

DES-based methods have the advantage of intuitiveness, stability and robustness. However, most of them assume that an attack model is given or we have prior knowledge about it. In addition, most methods suffer from high computational complexity. For example, supervisor synthesis [81] is NP-hard and algorithms in [27], [29], [128] and [130] are of exponential complexity.

Table IV is provided to summarize recent advances on defense strategies in terms of references, target systems, model types, attack types, strategies, methodologies, pros and cons. It is worth noting that pros and cons of each method in Tables III and IV are derived from its unique feature or application scope rather than experimental results. In fact, it remains difficult and challenging to evaluate existing methods in a uniform framework due to different assumptions and configurations needed by them.

V. Confidentiality Attack

In this section, we introduce relevant work about confidentiality attacks on CPS, which relates to falsification and theft of secret information. However, little research has been performed to address this issue. A main reason is that confidentiality attacks are rather complicated and often involve availability and integrity attacks. For example, a secret key of confidential information can be inferred by a fault injection attack [131], [132]. Jiang *et al*. [30] focus on a distributed CPS under fault injection attacks and study fault detection design problem to meet the confidentiality-critical and real-time requirements. A secondary reason is that availability and integrity attacks belong to active attacks while confidentiality ones are more like passive attacks [13]. To be precise, availability and integrity attacks aim at damaging a system directly while confidentiality ones aim at stealing system information. The latter are more benign than the former.

A typical confidentiality attack is eavesdropping. Confidential information can be stolen by eavesdropping on

TABLE IV
SUMMARY OF RECENT DEFENSE WORK ON INTEGRITY ATTACK

(DT: Discrete-time system; CS: Continuous-time system; PF: Power flow model; DES: Discrete event system; CG: Communication graph)

Refe-rence	Target	Model type	Attack types	Strategy	Methodologies	Advantages	Disadvantages
[25]	Wireless sensor network	DT	False data injection	Detection	State estimation, Krein space	Handling unknown attacks	Unstable detection efficiency
[87]	Smart grid	PF	False data injection	Detection	State estimation, mixed integer nonlinear programming	Least budget	Many assumptions on attack model
[93]	Noisy linear dynamic system	CS	Sensor	Detection	State estimation	Optimal state estimation	Many assumptions
[98]	Smart grid	PF	False data injection, replay	Detection	χ^2 detector, cosine similarity matching	Good detection performance	Specific attack models
[99]	Stochastic linear dynamic system	DT	Bias injection	Detection	State estimation, χ^2 detector	Mitigating attack impacts	High computational expense for large-scale system
[100]	DC microgrid	CS	False data injection	Detection	Unknown Input Observer	Requiring limited system information	Specified attack models
[101]	Smart grid	CS	False data injection	Detection	Unknown Input Observer	Good detection performance	Difficulty to compute adaptive threshold
[102]	Smart grid	CS	False data injection	Detection	Nonlinear interval observer	Good detection performance	State estimation accuracy to be improved
[104]	CPS	DT	Middleman	Detection	Watermarking, state estimation	Improving χ^2 detector performance	Possibility to compromise data confidentiality
[105]	CPS	DT	Linear	Detection	Watermarking, K-L divergence	Mitigating attack impacts	Restricted to linear attacks
[107]	Nonlinear discrete system	DT	Integrity	Detection	Memory fault detection filter	Good detection performance	High computational complexity
[108]	Distributed CPS	DT	Integrity	Detection	State estimation, distributed filtering	Good scalability	Inapplicable to stealthy attacks
[110]	CPS	CS	False data injection	Secure control	Observer-based control	Good system resilience	High computational complexity
[113]	CPS	CS	Sparse sensor, actuator attack	Secure control	ET control, observer-based control	Good state estimation	Unchanged attack channels
[117]	Microgrids	CG	False data injection	Secure control	Weighted mean subsequence reduced technique	Allowing to discard attacked information	Possibility to affect system performance
[118]	Microgrids	CG	False data injection	Secure control	Weighted mean subsequence reduced technique	Recovering system while isolating attacks	Performance on asynchronous system to be improved
[122]	CPS	CS	Sensor	Secure control	Distributed observer, virtual fractional dynamic surface	Obtaining exact system state	Complicated parameter design
[125], [127]	Close-loop control system	DES	Middleman	Detection	Automaton, supervisory control theory	Taking proper actions under attacks	Unnecessary loss of resources
[124]	Close-loop control system	DES	Actuator, sensor	Detection	Automaton, supervisory control theory	Handling multiple integrity attacks	Unnecessary loss of resources
[81], [128]	Close-loop control system	DES	Sensor	Secure control	Automaton, supervisory control theory	Being robust to many attacks	Exponential computational complexity
[29]	Close-loop control system	DES	Sensor	Secure control	Supervisory control theory, game theory	Handling unknown attacks	Exponential computational complexity
[130]	Close-loop control system	DES	Sensor	Secure control	Petri nets, supervisory control theory	Compact model	Exponential computational complexity
[27]	Closed-loop control system	DES	Sensor, actuator	Secure control	Petri nets, supervisory control theory	Compact model	Known attack structures

communications between sensors and controllers. Many methodologies have been adopted to protect CPS under eavesdropping attacks, such as data encryption [133]−[135], transmission strategy [136], and observer-based method [137]−[139]. On the basis of system observability, Yang *et al*. [31] perform a security analysis for a CPS under eavesdropping attacks. It provides a condition under which an attacker can successfully eavesdrop on a networked system.

A concept, named opacity, has attracted researcher's attention recently [140]−[142]. Opacity is a cyber-security property related to the confidentiality and privacy of a CPS. A system is said to be opaque if attackers cannot infer the secret of a system based on their observations, where attackers are often assumed to have full information about the system

structure but just partial observability. Opacity can be used to verify the security of a CPS. For example, Yin and Li [143] consider confidentiality of a networked supervisory control system with insecure control channels, i.e., control decisions sent by supervisors can be eavesdropped by an attacker. They consider two transmission mechanisms, event-based transmission and decision-based transmission. The former means that a supervisor always sends the latest control decision once a new event is observed, while the latter sends a new decision when it is different from the previous one. Two types of opacities are developed in [143] for the two transmission mechanisms. They both require that for two strings that one reaches a secret state and another reaches a non-secret one, the supervisor can generate a same decision history for them. Therefore, secret states cannot be inferred by an attacker.

As the confidentiality of a system can be verified by using opacity, an interesting idea emerges to deal with confidentiality attacks. Assume that a CPS is vulnerable to a confidentiality attack, we can then make the confidential information opaque to attackers such that they are unable to destroy system confidentiality [144]. Defending confidentiality attacks with opacity has emerged in recent years and some issues remain to be addressed, such as high complexity [145].

VI. Conclusion and Future Research

The highly integrated feature allows CPS to be widely used in modern industry while exposes it to the threat of cyber attacks. It is a ubiquitous but crucial security problem that has gained increasing attention. This paper summarizes recent studies related to availability, integrity and confidentiality attacks. Especially for the first two attacks, we investigate attack and defense strategies based on different models and methodologies. Although various methodologies and techniques are adopted to deal with this problem, none of them is omnipotent. Furthermore, changing technologies and market requirements result in more challenges to their application. According to the survey of recent developments, we provide some open issues and challenges as follows.

1) Determining How to Defend Against Advanced Attacks: Cyber attacks are evolving rapidly with updating technologies. Attackers tend to launch advanced attacks to increase their success rate. For example, both DoS and integrity attacks can be launched on a CPS in a random way to enable stealthiness and avoid detection. Although some researchers have noticed this issue [146]−[148], the research results are relatively few. In addition, Table I shows some attack events in recent years, one of which we should pay attention to is ransomware attack. It is an attack that prevents or limits users from accessing their files and systems [149], [150]. Such attacks not only damage availability and confidentiality of a system, but also cause significant economic losses. Especially during COVID-19, many medical CPS and factories are attacked by ransomware, resulting in serious consequences. Therefore, effectively defending advanced attacks on CPS is a challenging but practical issue that deserves more attention.

2) Determining How to Defend Against Stealthy Attacks: In Section IV, we introduce the work on stealthy attacks since it is a current trend to study cyber attack. It is easy to find that these efforts focus on designing stealthy attacks rather than preventing them. They provide us with insight into possible attacks while also facilitate attackers. If a stealthy attack strategy is implemented on a system while we have no countermeasures, it can cause a worse consequence since it cannot be detected. Thus, it is worth considering how to defend against stealthy attacks effectively.

3) Determining How to Defend Against Confidentiality Attacks: Compared with availability and integrity attacks, fewer studies have been presented for confidentiality attacks on CPS. There remains much room to study this topic since privacy safety and protection have attracted much attention in recent years.

4) Determining How to Resolve a Partial Issue: "Partial issue", namely, partial information, knowledge or observability, has always been a challenging problem in this field. In most literature, attack strategies are developed on a premise that an attacker has full knowledge or observability about a system. The same is true for defense strategies, i.e., full information about system states or attack models is required. Such premises greatly limit their application since attacks are often unknown and the system may not always be fully observable in practice. It is essential to study attacks under this "partial issue" as it determines whether a method can be applied to real systems.

5) Determining How to Conduct Appropriate Parameter Design and Performance Evaluation: Performance of most methods is dependent on key parameters, such as detection thresholds and control parameters. However, a perfect parameter value does not exist in most cases. For a parameter, a value that maximizes one performance may degrade another. For example, [25] shows that a detection threshold with zero false alarm can result in low detection efficiency. An appropriate parameter design needs to be considered in existing studies. As different parameter designs lead to different performance, some methods try to find a trade-off between them, while others may sacrifice one performance to optimize another. It is difficult to evaluate all the methods in a uniform context. We lack a tool to indicate their strengths and weaknesses. Hence, providing an appropriate performance analysis for existing methods is a considerable issue.

6) Determining How to Realize Practical Applications: The applications of existing theory and model-based methods remain a challenging issue. To mitigate this, technical factors and barriers are discussed in several studies [117], while concrete engineering implementations are still missing. Moreover, studies on industrial CPSs are not sufficient. Although many methods are proposed for power systems and microgrids, most of them require too-strong assumptions, e.g., system dynamics should be simple and systems should work perfectly, which are unlikely for most real-world industrial CPSs. Only little work has been done for complex or fault-prone systems. It should be pointed out that there remains a deep gap between theoretical results and practical applications. To fill it, many researchers try to combine model-based methods with computer science, such as the work in [151]. It indicates a promising trend to realize highly desired practical applications. Yet, it is still an ongoing investigation.

REFERENCES

[1] Y. Lu, "Cyber physical system (CPS)-based industry 4.0: A survey," *J. Ind. Int. Manage.*, vol. 2, no. 3, p. 1750014, Sep. 2017. DOI: 10.1142/S2424862217500142.

[2] H. F. Fan, M. Ni, L. L. Zhao, and M. L. Li, "Review of cyber physical system and cyber attack modeling," in *Proc. 12th IEEE PES Asia-Pacific Power and Energy Eng. Conf.*, Nanjing, China, 2020, pp. 1 – 5.

[3] L. P. Chang, T. W. Kuo, C. Gill, and J. Nakazawa, "Introduction to the special issue on real-time, embedded and cyber-physical systems," *ACM Trans. Embed. Comput. Syst.*, vol. 13, no. 5S, p. 155, Nov. 2014.

[4] G. Franze, G. Fortino, X. H. Cao, G. M. L. Sarne, and Z. Song, "Resilient control in large-scale networked cyber-physical systems: Guest editorial," *IEEE/CAA J. Autom. Sinica* , vol. 7, no. 5, pp. 1201–1203, Sept. 2020.

[5] S. Karnouskos, "Cyber-physical systems in the SmartGrid," in *Proc. 9th IEEE Int. Conf. Industrial Informatics*, Lisbon, Portugal, 2011, pp. 20−23.

[6] Y. Zhang, M. K. Qiu, C. W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data," *IEEE Syst. J.*, vol. 11, no. 1, pp. 88–95, Mar. 2017.

[7] Y. Liu, Y. Peng, B. L. Wang, S. R. Yao, and Z. H. Liu, "Review on cyber-physical systems," *IEEE/CAA J. Autom. Sinica* , vol. 4, no. 1, pp. 27–40, Jan. 2017.

[8] M. Muthuppalaniappan and K. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health," *Int. J. Qual. Health Care*, vol. 33, no. 1, p. mzaa117, Feb. 2021. DOI: 10.1093/intqhc/mzaa117.

[9] A. Humayed, J. Q. Lin, F. J. Li, and B. Luo, "Cyber-physical systems security — A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[10] D. R. Ding, Q. L. Han, Y. Xiang, X. H. Ge, and X. M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.

[11] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–36, Jul. 2018.

[12] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges," *Neurocomputing* , vol. 338, pp. 101−115, Apr. 2019.

[13] A. Rashidinejad, B. Wetzels, M. Reniers, L. Y. Lin, Y. T. Zhu, and R. Su, "Supervisory control of discrete-event systems under attacks: An overview and outlook," in *Proc. 18th European Control Conf.*, Naples, Italy, 2019, pp. 1732−1739.

[14] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annu. Rev. Control*, vol. 47, pp. 394–411, Jan. 2019.

[15] S. Singh, N. Yadav, and P. K. Chuarasia, "A review on cyber physical system attacks: Issues and challenges," in *Proc. Int. Conf. Communication and Signal Processing*, Chennai, India, 2020, pp. 1133−1138.

[16] L. W. Cao, X. N. Jiang, Y. M. Zhao, S. G. Wang, D. You, and X. L. Xu, "A survey of network attacks on cyber-physical systems," *IEEE Access*, vol. 8, pp. 44219–44227, Mar. 2020.

[17] S. Tan, J. M. Guerrero, P. L. Xie, R. K. Han, and J. C. Vasquez, "Brief survey on attack detection methods for cyber-physical systems," *IEEE Syst. J.*, vol. 14, no. 4, pp. 5329–5339, Dec. 2020.

[18] D. Zhang, Q. G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber–physical systems," *ISA Trans.*, vol. 116, pp. 1–6, Oct. 2021.

[19] D. R. Ding, Q. L. Han, X. H. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 51, no. 1, pp. 176–190, Jan. 2021.

[20] H. Zhang, Y. F. Qi, and J. F. Wu, "Optimal jamming power allocation against remote state estimation," in *Proc. American Control Conf.*, Seattle, USA, 2017, pp. 1660−1665.

[21] Y. Zhao, Z. Chen, C. J. Zhou, Y. C. Tian, and Y. Q. Qin, "Passivity-based robust control against quantified false data injection attacks in cyber-physical systems," *IEEE/CAA J. Autom. Sinica* , vol. 8, no. 8, pp. 1440–1450, Aug. 2021.

[22] Y. Z. Li, D. E. Quevedo, S. Dey, and L. Shi, "SINR-based DoS attack on remote state estimation: A game-theoretic approach," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 3, pp. 632–642, Sep. 2017.

[23] H. Zhang, Y. F. Qi, J. F. Wu, L. K. Fu, and L. D. He, "DoS attack energy management against remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 383–394, Mar. 2018.

[24] J. H. Zhang, J. T. Sun, and H. Lin, "Optimal DoS attack schedules on remote state estimation under multi-sensor round-robin protocol," *Automatica*, vol. 127, p. 109517, May 2021. DOI: 10.1016/j.automatica.2021.109517.

[25] X. H. Ge, Q. L. Han, M. Y. Zhong, and X. M. Zhang, "Distributed Krein space-based attack detection over sensor networks under deception attacks," *Automatica*, vol. 109, p. 108557, Nov. 2019. DOI: 10.1016/j.automatica.2019.108557.

[26] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies," *IEEE Trans. Autom. Control*, vol. 60, no. 12, pp. 3299–3304, Dec. 2015.

[27] Y. Wang, Y. T. Li, Z. H. Yu, N. Q. Wu, and Z. W. Li, "Supervisory control of discrete-event systems under external attacks," *Inf. Sci.*, vol. 562, pp. 398–413, Jul. 2021.

[28] P. J. Ramadge and W. M. Wonham, "Supervisory control of a class of discrete event processes," *SIAM J. Control Optim.* , vol. 25, no. 1, pp. 206–230, Jan. 1987.

[29] M. Wakaiki, P. Tabuada, and J. P. Hespanha, "Supervisory control of discrete-event systems under attacks," *Dyn. Games Appl.*, vol. 9, no. 4, pp. 965–983, Dec. 2019.

[30] W. Jiang, L. Wen, J. Y. Zhan, and K. Jiang, "Design optimization of confidentiality-critical cyber physical systems with fault detection," *J. Syst. Archit.*, vol. 107, p. 101739, Aug. 2020. DOI: 10.1016/j.sysarc.2020.101739.

[31] W. Yang, Z. Q. Zheng, G. R. Chen, Y. Tang, and X. F. Wang, "Security analysis of a distributed networked system under eavesdropping attacks," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 67, no. 7, pp. 1254–1258, Jul. 2020.

[32] L. H. Peng, X. H. Cao, C. Y. Sun, Y. Cheng, and S. Jin, "Energy efficient jamming attack schedule against remote state estimation in wireless cyber-physical systems," *Neurocomputing* , vol. 272, pp. 571–583, Jan. 2018.

[33] H. Zhang, P. Cheng, L. Shi, and J. M. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.

[34] H. Zhang, P. Cheng, L. Shi, and J. M. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 3, pp. 843–852, May 2016.

[35] J. H. Qin, M. L. Li, L. Shi, and X. H. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1648–1663, Jun. 2018.

[36] J. H. Qin, M. L. Li, L. Shi, and Y. Kang, "Optimal denial-of-service attack energy management over an SINR-based network," arXiv: 1810.02558, 2018.

[37] B. B. Li, Y. H. Wu, J. R. Song, R. X. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber-physical systems," *IEEE Trans. Ind. Inf.*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021.

[38] L. Liu, O. De Vel, Q. L. Han, J. Zhang, and Y. Xiang, "Detecting and preventing cyber insider threats: A survey," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 2, pp. 1397–1417, Feb. 2018.

[39] F. O. Olowononi, D. B. Rawat, and C. M. Liu, "Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 1, pp. 524–552, Nov. 2021.

[40] S. Ramesh, C. Yaashuwanth, K. Prathibanandhi, A. R. Basha, and T. Jayasankar, "An optimized deep neural network based DoS attack detection in wireless video sensor network," *J. Ambient Intell. Hum. Comput.*, 2021, DOI: 10.1007/s12652-020-02763-9.

[41] X. M. Zhang, Q. L. Han, X. H. Ge, D. R. Ding, L. Ding, D. Yue, and

C. Peng, " Networked control systems: A survey of trends and techniques," *IEEE/CAA J. Autom. Sinic* , vol. 7, no. 1, pp. 1–17, Jan. 2020.

[42] C. Peng, J. C. Li, and M. R. Fei, "Resilient event-triggering H_∞ load frequency control for multi-area power systems with energy-limited DoS attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 4110–4118, Sep. 2017.

[43] Y. C. Sun and G. H. Yang, "Event-triggered resilient control for cyber-physical systems under asynchronous DoS attacks," *Inf. Sci.*, vol. 465, pp. 340–352, Oct. 2018.

[44] W. H. M. H. Heemels, M. C. F. Donkers, and A. R. Teel, "Periodic event-triggered control for linear systems," *IEEE Trans. Autom. Control*, vol. 58, no. 4, pp. 847–861, Apr. 2013.

[45] D. Yue, E. G. Tian, and Q. L. Han, " A delay system method for designing event-triggered controllers of networked control systems," *IEEE Trans. Autom. Control*, vol. 58, no. 2, pp. 475–481, Feb. 2013.

[46] S. L. Hu, D. Yue, Q. L. Han, X. P. Xie, X. L. Chen, and C. X. Dou, "Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks," *IEEE Trans. Cybern.* , vol. 50, no. 5, pp. 1952–1964, May 2020.

[47] S. L. Hu, D. Yue, X. L. Chen, Z. H. Cheng, and X. P. Xie, "Resilient H_∞ filtering for event-triggered networked systems under nonperiodic DoS jamming attacks," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 51, no. 3, pp. 1392–1403, Mar. 2021.

[48] X. L. Chen, Y. G. Wang, and S. L. Hu, " Event-based robust stabilization of uncertain networked control systems under quantization and denial-of-service attacks," *Inf. Sci.* , vol. 459, pp. 369–386, Aug. 2018.

[49] H. S. Foroush and S. Martínez, "On event-triggered control of linear systems under periodic denial-of-service jamming attacks," in *Proc. IEEE 51st IEEE Conf. Decision and Control*, Maui, USA, 2012, pp. 2551−2556.

[50] H. S. Foroush and S. Martinez, "On triggering control of single-input linear systems under pulse-width modulated DoS signals," *SIAM J. Control Optim.*, vol. 54, no. 6, pp. 3084–3105, Jan. 2016.

[51] D. J. Thuente and M. Acharya, " Intelligent jamming in wireless networks with applications to 802.11b and other networks," in *Proc. IEEE Conf. Military Communications*, Washington, USA: IEEE, 2006, pp. 1075−1081.

[52] N. Zhao, P. Shi, W. Xing, and J. Chambers, "Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks," *IEEE Trans. Control Netw. Syst.* , vol. 8, no. 1, pp. 158–167, Mar. 2021.

[53] L. Guo, H. Yu, and F. Hao, " Event-triggered control for stochastic networked control systems against Denial-of-Service attacks," *Inf. Sci.*, vol. 527, pp. 51–69, Jul. 2020.

[54] M. Sathishkumar and Y. C. Liu, " Resilient event-triggered fault-tolerant control for networked control systems with randomly occurring nonlinearities and DoS attacks," *Int. J. Syst. Sci.* , vol. 51, no. 14, pp. 2712–2732, Aug. 2020.

[55] S. Feng and P. Tesi, "Resilient control under denial-of-service: Robust design," *Automatica*, vol. 79, pp. 42–51, May 2017.

[56] H. T. Sun, C. Peng, T. C. Yang, H. Zhang, and W. L. He, "Resilient control of networked control systems with stochastic denial of service attacks," *Neurocomputing*, vol. 270, pp. 170–177, Dec. 2017.

[57] H. H. Yuan and Y. Q. Xia, " Resilient strategy design for cyber-physical system under DoS attack over a multi-channel framework," *Inf. Sci.*, vol. 454−455, pp. 312–327, Jul. 2018.

[58] X. M. Zhang, Q. L. Han, X. H. Ge, and L. Ding, "Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3616–3626, Aug. 2020.

[59] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under a class of denial-of-service attack models," in *Proc. American Control Conf.*, San Francisco, CA, USA, 2011, pp. 643−648.

[60] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under a Markov modulated denial-of-service attack model," in *Proc. 50th IEEE Conf. Decision and Control and European Control Conf.*, Orlando, FL, USA, 2011, pp. 5714−5719.

[61] W. Yang, Y. Zhang, G. R. Chen, C. Yang, and L. Shi, "Distributed filtering under false data injection attacks," *Automatica* , vol. 102, pp. 34–44, Apr. 2019.

[62] T. Y. Zhang and D. Ye, "Distributed secure control against denial-of-service attacks in cyber-physical systems based on K-connected communication topology," *IEEE Trans. Cybern.* , vol. 50, no. 7, pp. 3094–3103, Jul. 2020.

[63] A. Y. Lu and G. H. Yang, " Distributed consensus control for multi-agent systems under denial-of-service," *Inf. Sci.* , vol. 439-440, pp. 95–107, May 2018.

[64] Y. Xu, M. Fang, P. Shi, and Z. G. Wu, "Event-based secure consensus of mutiagent systems against DoS attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3468–3476, Aug. 2020.

[65] D. Zhang, Y. P. Shen, S. Q. Zhou, X. W. Dong, and L. Yu, "Distributed secure platoon control of connected vehicles subject to DoS attack: Theory and application," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 51, no. 11, pp. 7269–7278, Nov. 2021.

[66] C. W. Wu, L. G. Wu, J. X. Liu, and Z. X. Jiang, "Active defense-based resilient sliding mode control under denial-of-service attacks," *IEEE Trans. Inf. Foren. Sec.*, vol. 15, pp. 237–249, May 2020.

[67] C. De Persis and P. Tesi, " Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control* , vol. 60, no. 11, pp. 2930–2944, Nov. 2015.

[68] G. Y. Wu, J. Sun, and J. Chen, " Optimal data injection attacks in cyber-physical systems," *IEEE Trans. Cybern.* , vol. 48, no. 12, pp. 3302–3312, Dec. 2018.

[69] Y. Chen, S. Kar, and J. M. F. Moura, "Optimal attack strategies subject to detection constraints against cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 1157−1168, Sep. 2018.

[70] Y. L. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Trans. Autom. Control*, vol. 61, no. 9, pp. 2618–2624, Sep. 2016.

[71] Y. L. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Ann. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, USA, 2009, pp. 911−918.

[72] Y. L. Mo and B. Sinopoli, " Integrity attacks on cyber-physical systems," in *Proc. 1st Int. Conf. High Confidence Networked Systems*, Beijing, China, 2012, pp. 47−54.

[73] J. P. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Trans. Ind. Inf.*, vol. 11, no. 5, pp. 1–12, Oct. 2015.

[74] Z. Y. Guo, D. W. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 4–13, Mar. 2017.

[75] S. Wu, Z. Y. Guo, D. W. Shi, K. H. Johansson, and L. Shi, "Optimal innovation-based deception attack on remote state estimation," in *Proc. American Control Conf.*, Seattle, WA, USA, 2018, pp. 3017−3022.

[76] E. Mousavinejad, F. W. Yang, Q. L. Han, and L. Vlacic, " A novel cyber attack detection method in networked control systems," *IEEE Trans. Cybern.*, vol. 48, no. 11, pp. 3254–3264, Nov. 2018.

[77] C. Z. Bai, F. Pasqualetti, and V. Gupta, "Security in stochastic control systems: Fundamental limitations and performance bounds," in *Proc. American Control Conf.*, Chicago, IL, USA, 2015, pp. 195−200.

[78] C. Z. Bai, F. Pasqualetti, and V. Gupta, " Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs," *Automatica*, vol. 82, pp. 251–260, Aug. 2017.

[79] E. Kung, S. Dey, and L. Shi, "The performance and limitations of ϵ-stealthy attacks on higher order systems," *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 941–947, Feb. 2017.

[80] Q. R. Zhang, K. Liu, Y. Q. Xia, and A. Y. Ma, " Optimal stealthy deception attack against cyber-physical systems," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 3963–3972, Sep. 2020.

[81] R. Su, " Supervisor synthesis to thwart cyber attack with bounded sensor reading alterations," *Automatica*, vol. 94, pp. 35–44, Aug. 2018.

[82] R. Meira-Góes, E. Kang, R. H. Kwong, and S. Lafortune, "Synthesis of sensor deception attacks at the supervisory layer of cyber–physical systems," *Automatica* , vol. 121, p. 109172, Nov. 2020. DOI: 10.1016/j.automatica.2020.109172.

[83] B. B. Li, R. X. Lu, K. K. R. Choo, W. Wang, and S. Luo, "On reliability analysis of smart grids under topology attacks: A stochastic

petri net approach," *ACM Trans. Cyber-Phys. Syst.*, vol. 3, no. 1, pp. 1–25, Jan. 2018.

[84] O. Kosut, L. Y. Jia, R. J. Thomas, and L. Tong, " Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid* , vol. 2, no. 4, pp. 645–658, Dec. 2011.

[85] L. Y. Jia, R. J. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations," in *Proc. 45th Hawaii Int. Conf. System Sciences*, Maui, HI, USA, 2012, pp. 1907−1914.

[86] L. Xie, Y. L. Mo, and B. Sinopoli, " Integrity data attacks in power market operations," *IEEE Trans. Smart Grid* , vol. 2, no. 4, pp. 659–666, Dec. 2011.

[87] R. L. Deng, G. X. Xiao, and R. X. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Inf.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[88] H. Z. Fang, N. Tian, Y. B. Wang, M. C. Zhou, and M. A. Haile, "Nonlinear Bayesian estimation: From Kalman filtering to a broader horizon," *IEEE/CAA J. Autom. Sinica* , vol. 5, no. 2, pp. 401–417, Mar. 2018.

[89] C. Kwon, W. Y. Liu, and I. Hwang, " Security analysis for cyber-physical systems against stealthy deception attacks," in *Proc. American Control Conf.*, Washington, DC, USA, 2013, pp. 3344−3349.

[90] Y. Z. Li, L. Shi, and T. W. Chen, "Detection against linear deception attacks on multi-sensor remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 846–856, Sep. 2018.

[91] Q. Li, B. Shen, Y. R. Liu, and F. E. Alsaadi, "Event-triggered H_∞ state estimation for discrete-time stochastic genetic regulatory networks with Markovian jumping parameters and time-varying delays," *Neurocomputing*, vol. 174, pp. 912–920, Jan. 2016.

[92] V. Ugrinovskii, " Distributed robust estimation over randomly switching networks using H_∞ consensus," *Automatica* , vol. 49, no. 1, pp. 160–168, Jan. 2013.

[93] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada, " Secure state estimation against sensor attacks in the presence of noise," *IEEE Trans. Control Netw. Syst.* , vol. 4, no. 1, pp. 49–59, Mar. 2017.

[94] K. Liu, H. Guo, Q. R. Zhang, and Y. Q. Xia, " Distributed secure filtering for discrete-time systems under Round-Robin protocol and deception attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3571–3580, Aug. 2020.

[95] L. F. Ma, Z. D. Wang, Q. L. Han, and H. K. Lam, "Variance-constrained distributed filtering for time-varying systems with multiplicative noises and deception attacks over sensor networks," *IEEE Sens. J.*, vol. 17, no. 7, pp. 2279–2288, Apr. 2017.

[96] H. F. Song, D. R. Ding, H. L. Dong, and Q. L. Han, "Distributed maximum correntropy filtering for stochastic nonlinear systems under deception attacks," *IEEE Trans. Cybern.*, 2020, DOI: 10.1109/TCYB.2020.3016093.

[97] Y. L. Mo, R. Chabukswar, and B. Sinopoli, " Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, Jul. 2014.

[98] D. B. Rawat and C. Bajracharya, " Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[99] J. Miloševič, T. Tanaka, H. Sandberg, and K. H. Johansson, "Analysis and mitigation of bias injection attacks against a Kalman filter," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 8393–8398, Jul. 2017.

[100] A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, and G. Ferrari-Trecate, " Distributed cyber-attack detection in the secondary control of DC microgrids," in *Proc. European Control Conf.*, Limassol, Cyprus, 2018, pp. 344−349.

[101] X. Y. Luo, X. Y. Wang, X. Y. Pan, and X. P. Guan, "Detection and isolation of false data injection attack for smart grids via unknown input observers," *IET Gener. Transm. Distrib.* , vol. 13, no. 8, pp. 1277–1286, Apr. 2019.

[102] X. Y. Wang, X. Y. Luo, Y. Y. Zhang, and X. P. Guan, "Detection and isolation of false data injection attacks in smart grids via nonlinear interval observer," *IEEE Internet Things J.* , vol. 6, no. 4, pp. 6498–6512, Aug. 2019.

[103] Z. Y. Guo, D. W. Shi, K. H. Johansson, and L. Shi, "Worst-case stealthy innovation-based linear attack on remote state estimation," *Automatica*, vol. 89, pp. 117–124, 2018.

[104] J. H. Huang, D. W. C. Ho, F. F. Li, W. Yang, and Y. Tang, "Secure remote state estimation against linear man-in-the-middle attacks using watermarking," *Automatica* , vol. 121, p. 109182, Nov. 2020. DOI: 10.1016/j.automatica.2020.109182.

[105] D. Wang, J. H. Huang, Y. Tang, and F. F. Li, " A watermarking strategy against linear deception attacks on remote state estimation under K-L divergence," *IEEE Trans. Ind. Inf.* , vol. 17, no. 5, pp. 3273–3281, May 2021.

[106] A. Naha, A. Teixeira, A. Ahlen, and S. Dey, "Quickest detection of deception attacks in networked control systems with physical watermarking," arXiv: 2101.01466, 2021.

[107] W. L. Chen, J. Hu, Z. H. Wu, X. Y. Yu, and D. Y. Chen, "Finite-time memory fault detection filter design for nonlinear discrete systems with deception attacks," *Int. J. Syst. Sci.*, vol. 51, no. 8, pp. 1464–1481, May 2020.

[108] D. R. Ding, Q. L. Han, Z. D. Wang, and X. H. Ge, "Recursive filtering of distributed cyber-physical systems with attack detection," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 51, no. 10, pp. 6466–6476, Oct. 2021.

[109] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[110] C. H. Xie and G. H. Yang, "Observer-based attack-resilient control for linear systems against FDI attacks on communication links from controller to actuators," *Int. J. Robust Nonlinear Control*, vol. 28, no. 15, pp. 4382–4403, Oct. 2018.

[111] Y. Shoukry and P. Tabuada, " Event-triggered state observers for sparse sensor noise/attacks," *IEEE Trans. Autom. Control* , vol. 61, no. 8, pp. 2079–2091, Aug. 2016.

[112] M. Pajic, I. Lee, and G. J. Pappas, "Attack-resilient state estimation for noisy dynamical systems," *IEEE Trans. Control Netw. Syst.* , vol. 4, no. 1, pp. 82–92, Mar. 2017.

[113] A. Y. Lu and G. H. Yang, " Event-triggered secure observer-based control for cyber-physical systems under adversarial attacks," *Inf. Sci.*, vol. 420, pp. 96–109, Dec. 2017.

[114] D. R. Ding, Q. L. Han, Z. D. Wang, and X. H. Ge, " A survey on model-based distributed control and filtering for industrial cyber-physical systems," *IEEE Trans. Ind. Inf.*, vol. 15, no. 5, pp. 2483–2499, May 2019.

[115] M. H. Zhu and S. Martínez, " On distributed constrained formation control in operator—vehicle adversarial networks," *Automatica*, vol. 49, no. 12, pp. 3571–3582, Dec. 2013.

[116] Y. Liu, H. H. Xin, Z. H. Qu, and D. Q. Gan, " An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks," *IEEE Trans. Smart Grid* , vol. 7, no. 6, pp. 2923–2932, Nov. 2016.

[117] A. Bidram, B. Poudel, L. Damodaran, R. Fierro, and J. M. Guerrero, "Resilient and cybersecure distributed control of inverter-based islanded microgrids," *IEEE Trans. Ind. Inf.* , vol. 16, no. 6, pp. 3881–3894, Jun. 2020.

[118] N. Yassaie, M. Hallajiyan, I. Sharifi, and H. A. Talebi, "Resilient control of multi-microgrids against false data injection attack," *ISA Trans.*, vol. 110, pp. 238–246, Apr. 2021.

[119] C. Deng, Y. Wang, C. Y. Wen, Y. Xu, and P. F. Lin, "Distributed resilient control for energy storage systems in cyber-physical microgrids," *IEEE Trans. Ind. Inf.*, vol. 17, no. 2, pp. 1331–1341, Feb. 2020.

[120] C. Deng and G. H. Yang, "Distributed adaptive fault-tolerant control approach to cooperative output regulation for linear multi-agent systems," *Automatica*, vol. 103, pp. 62–68, May 2019.

[121] C. Deng, G. H. Yang, and M. J. Er, " Decentralized fault-tolerant MRAC for a class of large-scale systems with time-varying delays and actuator faults," *J. Process Control*, vol. 75, pp. 171–186, Mar. 2019.

[122] W. Ao, Y. D. Song, and C. Y. Wen, " Distributed secure state estimation and control for CPSs under sensor attacks," *IEEE Trans. Cybern.*, vol. 50, no. 1, pp. 259–269, Jan. 2020.

[123] L. K. Carvalho, Y. C. Wu, R. Kwong, and S. Lafortune, "Detection and prevention of actuator enablement attacks in supervisory control

systems," in *Proc. 13th Int. Workshop on Discrete Event Systems*, Xi'an, China, 2016, pp. 298−305.

[124] L. K. Carvalho, Y. C. Wu, R. Kwong, and S. Lafortune, "Detection and mitigation of classes of attacks in supervisory control systems," *Automatica*, vol. 97, pp. 121–133, Nov. 2018.

[125] P. M. Lima, M. V. S. Alves, L. K. Carvalho, and M. V. Moreira, "Security against network attacks in supervisory control systems," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 12333–12338, Jul. 2017.

[126] P. M. Lima, L. K. Carvalho, and M. V. Moreira, " Detectable and undetectable network attack security of cyber-physical systems," *IFAC-PapersOnLine*, vol. 51, no. 7, pp. 179–185, Jan. 2018.

[127] P. M. Lima, M. V. S. Alves, L. K. Carvalho, and M. V. Moreira, "Security against communication network attacks of cyber-physical systems," *J. Control. Autom. Electr. Syst.* , vol. 30, no. 1, pp. 125–135, Feb. 2019.

[128] R. Meira-Góes, H. Marchand, and S. Lafortune, " Towards resilient supervisors against sensor deception attacks," in *Proc. IEEE 58th Conf. Decision and Control*, Nice, France, 2019, pp. 5144−5149.

[129] R. Meira-Góes, S. Lafortune, and H. Marchand, " Synthesis of supervisors robust against sensor deception attacks," *IEEE Trans. Autom. Control*, vol. 66, no. 10, pp. 4990–4997, Oct. 2021.

[130] D. You, S. G. Wang, and C. Seatzu, "A Liveness-enforcing supervisor tolerant to sensor-reading modification attacks," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 52, no. 4, pp. 2398−2411, Apr. 2022.

[131] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "A parity code based fault detection for an implementation of the advanced encryption standard," in *Proc. 17th IEEE Int. Symp. on Defect and Fault Tolerance in VLSI Systems*, Vancouver, BC, Canada, 2002, pp. 51−59.

[132] J. Blömer and J. P. Seifert, "Fault based cryptanalysis of the advanced encryption standard (AES)," in *Porc. 7th Int. Conf. Financial Cryptography*, Guadeloupe, French West Indies, 2003, pp. 162−181.

[133] S. Bayat-Sarmadi, M. Mozaffari Kermani, R. Azarderakhsh, and C. Y. Lee, " Dual-basis superserial multipliers for secure applications and lightweight cryptographic architectures," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 61, no. 2, pp. 125–129, Feb. 2014.

[134] Y. J. Chen, L. C. Wang, and C. H. Liao, " Eavesdropping prevention for network coding encrypted cloud storage systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 8, pp. 2261–2273, Aug. 2016.

[135] K. Wang, H. Gao, X. L. Xu, J. F. Jiang, and D. Yue, " An energy-efficient reliable data transmission scheme for complex environmental monitoring in underwater acoustic sensor networks," *IEEE Sens. J.*, vol. 16, no. 11, pp. 4051–4062, Jun. 2016.

[136] L. Yuan, K. Wang, T. Miyazaki, S. Guo, and M. Wu, "Optimal transmission strategy for sensors to defend against eavesdropping and jamming attacks," in *Proc. IEEE Int. Conf. Communications*, Paris, France, 2017, pp. 1−6.

[137] A. Chapman, M. Nabi-Abdolyousefi, and M. Mesbahi, "Controllability and observability of network-of-networks via Cartesian products," *IEEE Trans. Autom. Control*, vol. 59, no. 10, pp. 2668–2679, Oct. 2014.

[138] B. B. Wang, L. Gao, Y. Gao, Y. Deng, and Y. Wang, "Controllability and observability analysis for vertex domination centrality in directed networks," *Sci. Rep.*, vol. 4, no. 1, pp. 1–10, Jun. 2014.

[139] T. Zhou, " On the controllability and observability of networked dynamic systems," *Automatica*, vol. 52, pp. 63–75, Feb. 2015.

[140] L. W. An and G. H. Yang, " Opacity enforcement for confidential robust control in linear cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 65, no. 3, pp. 1234–1241, Mar. 2020.

[141] S. Yang, J. Y. Hou, X. Yin, and S. Y. Li, " Opacity of networked supervisory control systems over insecure communication channels," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 2, pp. 884–896, Jun. 2021.

[142] X. Yin, Z. J. Li, W. L. Wang, and S. Y. Li, "Infinite-step opacity and K-step opacity of stochastic discrete-event systems," *Automatica*, vol. 99, pp. 266–274, Jan. 2019.

[143] X. Yin and S. Y. Li, "Verification of opacity in networked supervisory control systems with insecure control channels," in *Proc. IEEE Conf. Decision and Control*, Miami, FL, USA, 2018, pp. 4851−4856.

[144] Y. Tong, Z. W. Li, C. Seatzu, and A. Giua, " Current-state opacity enforcement in discrete event systems under incomparable observations," *Discrete Event Dyn. Syst.* , vol. 28, no. 2, pp. 161–182, Jun. 2018.

[145] R. Jacob, J. J. Lesage, and J. M. Faure, " Overview of discrete event systems opacity: Models, validation, and quantification," *Annu. Rev. Control*, vol. 41, pp. 135–146, Jun. 2016.

[146] J. L. Liu, Y. D. Wang, J. D. Cao, D. Yue, and X. P. Xie, "Secure adaptive-event-triggered filter design with input constraint and hybrid cyber attack," *IEEE Trans. Cybern.* , vol. 51, no. 8, pp. 4000–4010, Aug. 2021.

[147] C. Q. Yang, Z. G. Shi, H. Zhang, J. F. Wu, and X. F. Shi, "Multiple attacks detection in cyber-physical systems using random finite set theory," *IEEE Trans. Cybern.* , vol. 50, no. 9, pp. 4066–4075, Sep. 2020.

[148] X. Zhao, C. S. Liu, and E. G. Tian, "Finite-horizon tracking control for a class of stochastic systems subject to input constraints and hybrid cyber attacks," *ISA Trans.*, vol. 104, pp. 93–100, Sep. 2020.

[149] B. A. S. Al-Rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," *Comput. Secur.*, vol. 74, pp. 144–166, May 2018.

[150] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A survey on ransomware: Evolution, taxonomy, and defense solutions," arXiv: 2102.06249, 2021.

[151] S. Y. Xiao, X. H. Ge, Q. L. Han, and Y. J. Zhang, "Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks," *IEEE Trans. Cybern.*, 2021, DOI: 10.1109/TCYB.2021.3074318.

Wenli Duo received the B.S. degree and M.S. degree from the School of Information and Electronic Electronic Engineering, Zhejiang Gongshang University, in 2017 and 2020, respectively. She is currently pursuing the Ph.D. degree with the Institute of Systems Engineering, Macau University of Science and Technology, Macau, China. Her research interests include cyber attack, security of cyber physical system, and blockchain.

MengChu Zhou (Fellow, IEEE) received the B.S. degree from Nanjing University of Science and Technology in 1983, the M.S. degree from Beijing Institute of Technology in 1986, and the Ph.D. degree from Rensselaer Polytechnic Institute, Troy, USA in 1990. He then joined New Jersey Institute of Technology and is now a Distinguished Professor. His research interests include Petri nets, intelligent automation, Internet of Things, and big data analytics. He has over 900 publications including 12 books, 600+ journal papers (500+ in IEEE transactions), 30 patents and 29 book-chapters. He is Fellow of IFAC, AAAS, CAA and NAI.

Abdullah Abusorrah (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Nottingham in United Kingdom in 2007. His is a Professor in the Department of Electrical and Computer Engineering at King Abdulaziz University, and the Head of the Center of Research Excellence in Renewable Energy and Power Systems at King Abdulaziz University, Saudi Arabia. His research interests include energy systems, smart grid, and system analyses.