A Review on Cybersecurity Analysis, Attack Detection, and Attack Defense Methods in Cyber-physical Power Systems

Dajun Du, Minggao Zhu, Xue Li, Minrui Fei, Siqi Bu, *Senior Member*, *IEEE*, Lei Wu, *Fellow*, *IEEE*, Kang Li, *Senior Member*, *IEEE*

***Abstract*—Potential malicious cyber-attacks to power systems which are connected to a wide range of stakeholders from the top to tail will impose significant societal risks and challenges. The timely detection and defense are of crucial importance for safe and reliable operation of cyber-physical power systems (CPPSs). This paper presents a comprehensive review of some of the latest attack detection and defense strategies. Firstly, the vulnerabilities brought by some new information and communication technologies (ICTs) are analyzed, and their impacts on the security of CPPSs are discussed. Various malicious cyber-attacks on cyber and physical layers are then analyzed within CPPSs framework, and their features and negative impacts are discussed. Secondly, two current mainstream attack detection methods including state estimation based and machine learning based methods are analyzed, and their benefits and drawbacks are discussed. Moreover, two current mainstream attack defense methods including active defense and passive defense methods are comprehensively discussed. Finally, the trends and challenges in attack detection and defense strategies in CPPSs are provided.**

***Index Terms*—Cyber-physical power systems, security threat, attack detection, attack defense, state estimation, machine learning.**

I. Introduction

With the accelerated development of information and communication technologies (ICTs), a critical mass of instruments and devices with communication functions have been widely deployed in power systems to enhance the state observability, control responsiveness, and operation flexibility in the face of increased penetration of renewable generations at all voltage levels and mass roll-out of electrification plans across many end user sectors. This trend is transforming power systems to cyber-physical power systems (CPPSs), allowing seamless integration and interaction between power system assets covering physical infrastructure, information sensing and mining as well as system operation and control in cyber space [1]. This will promote optimal power flow calculation [2], [3] and optimal integration of distributed renewable energy [4], [5], and support decarbonization of other sectors such as the transportation [6], [7]. Eventually, CPPSs can intelligently integrate the behaviors of all stakeholders in the energy supply chain, thereby providing economic and safe power supply, and promoting the sustainable development of the environment and economy [8], [9].

It is evident that CPPSs would profoundly change the operation method of conventional power systems, yet the integration of communication and computation technologies will also bring new cybersecurity challenges to CPPSs. Firstly, the control equipment in conventional power systems is often designed without considering cybersecurity issues since conventional power systems have been working in an isolated physical environment for a long period of time in the history. Secondly, when communication and computation devices are coupled with conventional control systems of power system infrastructure, the existing security technologies cannot be directly extended to almost defenseless control devices, leading to inherent cybersecurity vulnerabilities. Further, due to multi-point, multi-type, and multi-layer features of CPPSs, the attackers may easily identify these cybersecurity vulnerabilities and hence launch malicious cyber-attacks. As a consequence, new cybersecurity issues may emerge from time to time as a price of the increasing digitalization of power systems and continual development of CPPSs.

As illustrated in Fig. 1, cyber-attack events have exhibited the features of increasing the frequency and impact in the last decades. In 2000, 150 sewage pumping stations of Malucci sewage treatment plant in Australia were hijacked by the attackers. As a result, over one million liters of sew-

Manuscript received: September 2, 2021; revised: December 23, 2021; accepted: May 28, 2022. Date of CrossCheck: May 28, 2022. Date of online publication: July 22, 2022.

The work of D. Du, M. Zhu, X. Li, and M. Fei was supported in part by the National Science Foundation of China (No. 92067106) and 111 Project (No. D18003).

D. Du (corresponding author), M. Zhu, X. Li, and M. Fei are with Shanghai Key Laboratory of Power Station Automation Technology, School of Mechatronics Engineering and Automation, Shanghai University, Shanghai, China (e-mail: ddj@i.shu.edu.cn; minggaozhu@shu.edu.cn; lixue@shu.edu.cn; mrfei@staff.shu.edu.cn).

S. Bu is with the Department of Electrical Engineering, The Hong Kong Polytechnic University, Hong Kong, China (e-mail: siqi.bu@polyu.edu.hk).

L. Wu is with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ 07030, USA (e-mail: lei.wu@stevens.edu).

K. Li is with the School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, UK (e-mail: k.li1@leeds.ac.uk).

DOI: 10.35833/MPCE.2021.000604

age were directly discharged from the storm drain into the natural water system without the treatment, causing serious damages to the local environment. The stuxnet virus attacked Iran's nuclear power plant in 2010, and over 1000 centrifuges have been scrapped [10]. In 2015, the hackers intruded into supervisory control and data acquisition (SCADA) system and caused a wide blackout in Kiev and west Ukraine [11]. Another cyber-attack was launched in 2016 again to part of Kiev Ukrainian capital. The attack led to the shut-down of 200 MW power generation [12]. Recently, the 765 trunk line of Venezuela's national grid was attacked in 2020, causing blackouts in all eleven states except the capital Caracas. According to a Clark school study at the University of Maryland [13], hacker attacks every 39 s on average. Furthermore, it is found that cybercrime will cost companies world wide from 3 trillion USD in 2015 to an estimated 10.5 trillion USD annually by 2025 [14]. These attack events have shown that although CPPSs can bring significant and societal benefits, new cybersecurity threats to these critical infrastructure need to be cautiously dealt with.

Fig. 1. Timeline of major attack events.

Cybersecurity methods of CPPSs have been intensively studied in the past decade, and review papers on these methods are summarized in Table I. While most of these review papers [15]-[26] focus on one aspect of attack analysis, attack detection, and attack defense. Considering that attack detection is the premise of defense, it is necessary to include these aspects. However, these are still not analyzed in depth by considering the characters of CPPSs.

TABLE I
REVIEW OF PUBLISHED LITERATURE RELATED TO ATTACK DETECTION AND ATTACK DEFENSE

Topic	Reference	Content
Attack detection	[15]	Analysis of false data injection attack and corresponding detection methods
	[16]	Analysis of physics-based anomaly detection
	[17]	Analysis of attack detection methods
	[18]	Analysis of centralized and distributed attack detection methods
	[19]	Analysis of attack detection, estimation, and control for industrial CPPSs
	[20]	Analysis of attack detection based on deep learning
Attack defense	[21]	Analysis of prominent attack methods
	[22]	Analysis of power systems against malicious attacks
	[23]	Security threats for smart metering infrastructure
	[24]	Security issues of advanced metering infrastructure
	[25]	Analysis of security requirements and attack defense methods
	[26]	Analysis of secure control for CPPSs

This paper presents an overview of attack analysis, attack detection, and attack defense methods for CPPSs, and their challenges are elaborated in detail. The research framework of cyber-attacks on CPPSs is illustrated in Fig. 2.

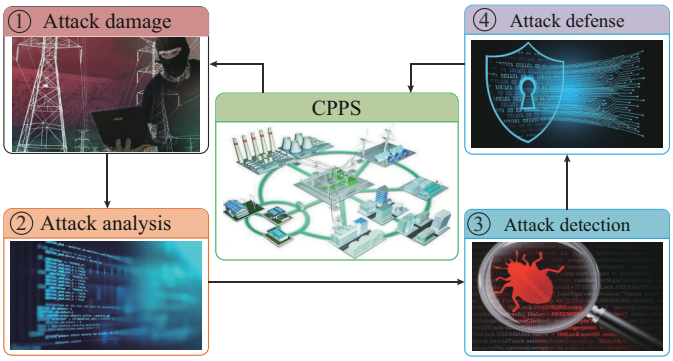

Fig. 2. Research framework of cyber-attacks on CPPSs.

The main ideas are as follows. When a system suffers from cyber-attacks, the impacts of cyber-attacks on CPPSs are firstly discussed. The characteristics of cyber-attacks are then analyzed, and the attack detection is implemented to diagnose and identify cyber-attacks. After the detection, different defense methods are proposed to guarantee safe operation of CPPSs. Different from the existing review papers, this paper focuses on the attack detection and cybersecurity defense of CPPSs.

Specifically, the rest of this paper is organized as follows. Section II presents the development and security risks of CPPSs. Section III presents the characteristics and impacts of cyber-attacks on CPPSs. The cyber-attack detection is presented in Section IV. For cyber-attack defense, a survey is conducted on the popular methods including active defense

and passive defense methods in Section V. The conclusion and challenging issues are given in Section VI.

II. Development and Security Risks of CPPSs

This section firstly analyzes the key factors that drive the rapid development of CPPSs, and compares CPPSs with conventional power systems. The evolution of CPPSs involves the deployment of new technologies, which also brings a number of security vulnerabilities.

A. Emergence of CPPSs

There exist many factors that drive the rapid development of CPPSs, while the most influential ones include the rapid deployment of renewable generation technologies, the growing number of prosumers, and the mass roll-out of demand-side management technologies.

First of all, the biggest challenge facing sustainable development is climate change which is the most important drive for the transformational change of conventional energy structure to a low-carbon energy structure [27], [28]. To facilitate the transition, many new technologies, including energy-saving technologies and other low-carbon technologies, have been widely utilized [29], [30]. For example, wind and solar energy are two most popular renewable energy sources [31], while connecting these renewable power generations to the existing power system leads to both technical and economic challenges. One trend to modernize the distribution system is to develop a number of microgrids and effectively interconnect them through point of common coupling (PCC). The growing number of microgrids to integrate renewable energies at medium- and low-voltage levels advances the development of CPPSs [32].

Further, considering the consumers' expectations of increased power supply while meeting more strict legislations on both pollutant and carbon emissions. Utility grids are moving progressively to connect renewable generations as much as possible, so as to reduce the carbon footprint of power generation while meeting the growing public demands for both generation sustainability and more generation capacity. However, traditional solutions are difficult to cope with the increased complexities of the utility grid under the transition to a low-carbon system, the concept of CPPSs have then been proposed to offer a potential better framework to operate and control such a complex system. As the aggregation of advanced monitoring systems, home area networks, two-way communication, and remote control technology, CPPSs can enable the intelligent demand-side management (DSM) and offer a seemly integrated platform for the consumers to actively participate in the ancillary services of power systems through two-way interaction [33], resulting in an intelligent distribution grid, which benefits both power system operation and the consumers.

B. Comparison Between Conventional Power System and CPPSs

The emergence of CPPSs is to meet the needs for power system digitalization as well as more sustainable low-carbon power supply. In fact, CPPSs are power systems that can intelligently integrate the behavior of all stakeholders in the energy supply chain, so as to provide satisfactory power supply to the consumers [34]. Hence, with the increasing integration of modern technologies into the existing power systems, CPPSs transform the current power systems to be more interactive, responsive, and organic.

Conventionally, power system is an one-way centralized system delivering the power from the generator set to the end users [35]. Power flow in conventional power systems is in one direction—from power supply system to the customer point of interconnection. However, bi-directional power flow in CPPSs is in two opposite directions like tide. When power sources like photovoltaic (PV) and electric vehicle (EV) are connected to power supply system at the utility customer's site, power has the potential to flow in the opposite direction—from the customer to power supply system, i. e., this reverses original direction of power flow [36], [37]. Therefore, the current energy management requires a smarter grid, and CPPSs are the solution that enables digital intelligence in power systems. As shown in Fig. 3, CPPSs are composed of both a physical layer and a cyber layer (the control functionality is a part of cyber layer). Physical layer refers to specific physical infrastructure and assets such as generation substation, transmission substation, distribution substation, and smart meter, etc., while the cyber layer refers to the information exchanges across the whole energy chain from generation units to the end users or service providers through wired or wireless networks. Moreover, it also integrates analytical tools to support the monitoring and controlling of the energy flow from the generators to the end users. In Fig. 3, ops is short for operator; EMS is short for energy management system; BSM is short for bulk storage management; ISO is short for independent system operator; RTO is short for regional transmission organization; LFC is short for load frequency control; ED is short for economic dispatch; AMI is short for advanced metering infrastructure; CIS is short for customer information system; WAN is short for wide area network; FAN is short for field area network; LAN is short for local area network; NAN is short for neighborhood area network; HAN is short for home area network; IED is short for intelligent electronic device; PMU is short for phasor measurement unit; RTU is short for remote terminal unit; PLC is short for programmable logical controller; DG is short for distribution generation; and ES is short for energy storage.

In general, CPPSs can maximize the reliability, availability, and efficiency of grid operation, bringing tangible benefits to the economy and the society as a while. A comprehensive comparison of two systems is presented in [34], and a summary of the differences is given in Table II.

C. New Features of CPPSs

CPPSs are expected to bring a number of benefits to the operation and control of power systems with significant penetration of renewable generations at different voltage levels and to support the decarbonization of different sectors.

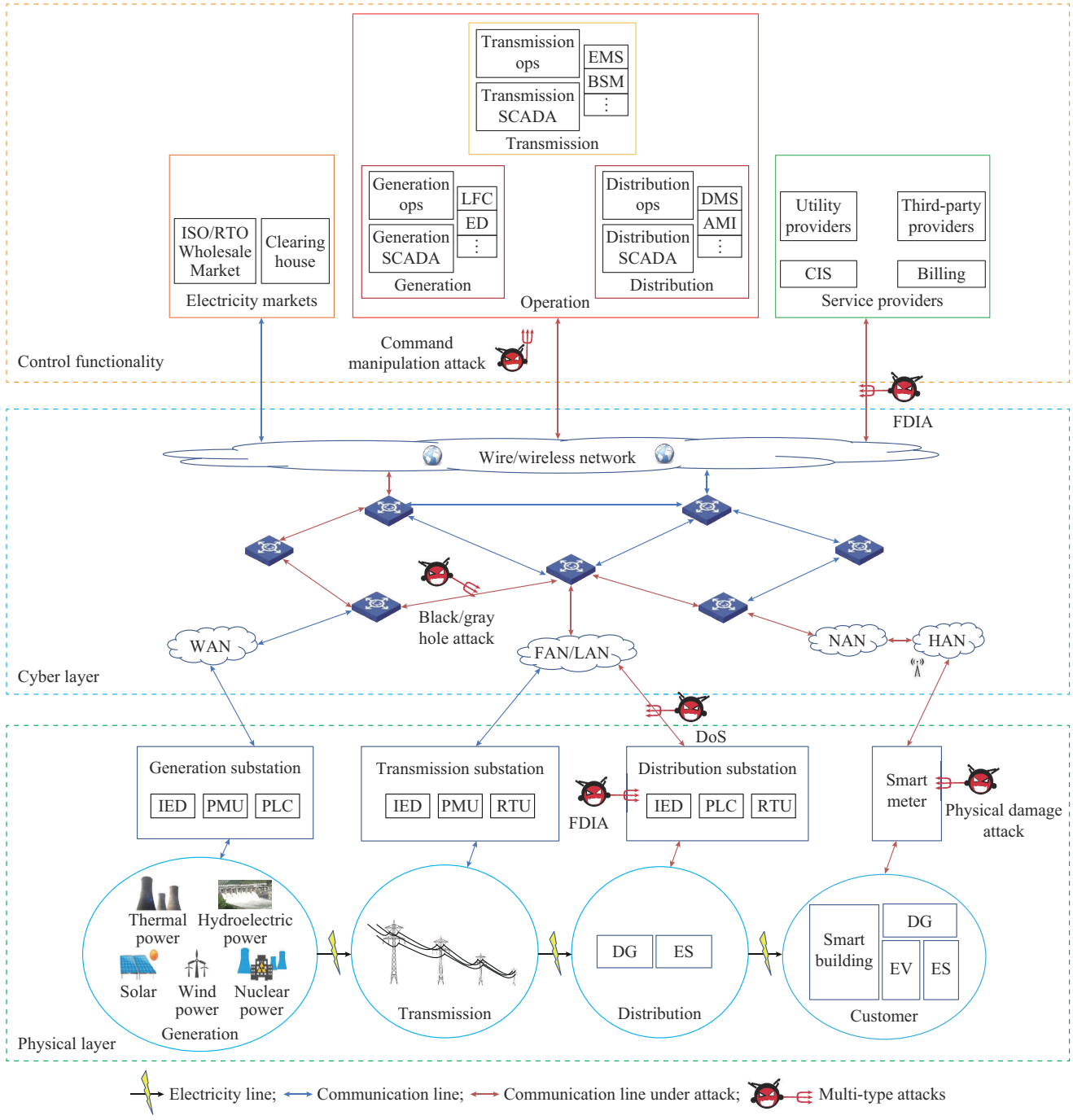

Fig. 3. Framework of CPPSs under multi-type attacks.

TABLE II
COMPARISON BETWEEN CONVENTIONAL POWER SYSTEMS AND CPPSS

Character-istic	Conventional power system	CPPS
Measure-ment	Electromagnetic meters	More two-way communication smart meters
Communi-cation	One-way communication between power systems and users	Two-way communication between power systems and users
Power flow mode	Unidirectional power flow	Bi-directional power flow
Control	Centralized control	Centralized and distributed control

Many technical challenges, which are related not only to control and communication but also to real-time monitoring and management, need to be tackled such as real-time monitoring of demand-side power consumption changes, microgrid management, charging support of electric vehicles [38], and the utilization of renewable energy [39] and battery storage systems [40]. To address these challenges, a range of new technologies have been developed.

1) New CPPS technologies: in recent years, some new CPPS technologies [41], [42] have been developed for the construction of smart grids. Specifically, these technologies cover power generation, transmission, distribution, and de-

mand side.

To achieve efficient grid management, it is necessary to apply advanced smart meters and control technologies in smart grids at all levels. DSM is one of the efficient grid management technologies, which aims to lower the power demand by taking effective incentive and inducement measures and appropriate operation mode. It in turn avoids the cost of building new generators and transmission lines, saves customers' money, and lowers the pollution from electric generators [43]-[45]. Demand response (DR) is one key program in DSM. According to Federal Energy Regulatory Commission [46], DR is defined as "changes in electric usage by end-use customers from their normal consumption patterns in response to changes in the price of electricity over time, or to incentive payments designed to induce lower electricity use at times of high wholesale market prices or when system reliability is jeopardized". According to different response modes of the users, DR in electricity market is roughly classified into two categories: price-based DR strategy and incentive-based DR strategy [47]. The former refers to that the users change and adjust power load in term of electricity price and respond to power supply. The latter refers to that the contracted users receive direct compensation or other preferential tariffs and the suppliers are allowed to reduce their power loads [43]. Specially, when the system reliability is threatened, the power supplier can directly control and manage part of the user's power load through direct load control (DLC) [48]. Some other technologies can be employed to reduce the electrical losses such as superconductive power transmission or control with appropriate utilization of dispatchable resources (distributed generation, load, and storage) [49], [50].

Furthermore, distributed energy resources (DERs) can be flexibly connected to smart grids, so that the power suppliers and the users can effectively manage energy utilization. For example, a current-controlled voltage-mode control method for dispatchable electronically coupled DER units is proposed, which can quickly stabilize the terminal voltage and frequency [51]. To regulate the voltage, a model-free optimal strategy is proposed by the output power of inverter-interfaced DERs [52]. A fast frequency control framework of distributed DERs is proposed, which optimizes the inertia coefficients of each DER [53]. Considering the aggregation and disaggregation processes of massive DERs of small capacity, a model predictive control (MPC) strategy is proposed for real-time secondary frequency regulation in an islanded microgrid [54]. An architecture for controlling hybrid energy storage system integrated with PV DERs is proposed to achieve frequency regulation [55]. More distributed control strategies for DERs are summarized in [56].

2) New features of CPPSs: the incorporation of these technologies into CPPSs brings many new features. As summarized in Fig. 4, these features [57] can be summarized as follows: compatibility implies that CPPSs are compatible with different types of power generation solutions and needs; flexibility refers to the ability of CPPSs to flexibly apply power resources and involve users; efficiency refers to the utilization of advanced information technologies to dynamically optimize power system resources and thus improve the operation efficiency. Moreover, some new technologies are utilized to reduce power losses: applicability refers to the ability of CPPSs to support new products, services, and markets such as integrated smart home appliances and consumer devices, ensuring the necessary power quality for a variety of needs; and security means that CPPSs shall have self-healing ability, and be resilient to the attacks and natural disasters.

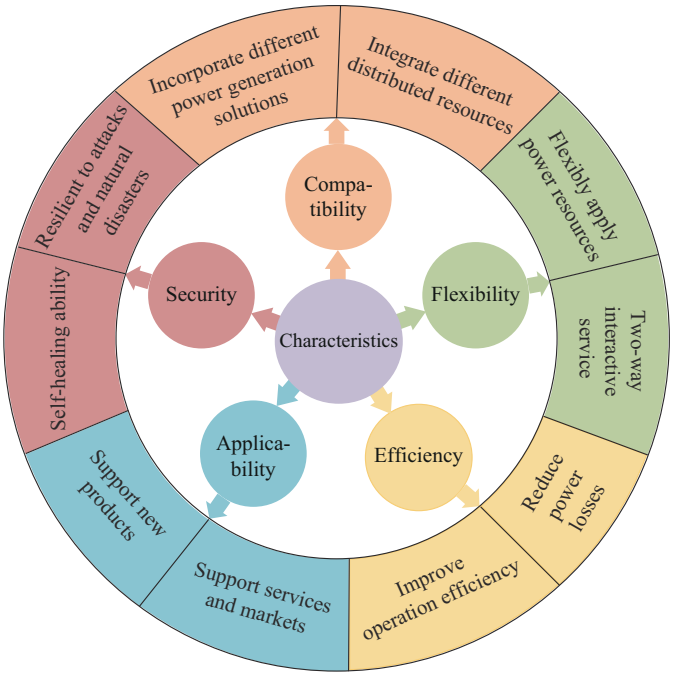

Fig. 4. New features of CPPSs.

The first three are the basic features of CPPSs, "applicability" is the purpose of CPPSs, and "security" is the key step to ensure the reliable operation of CPPSs. These new features are vital for interacting with power consumers, meeting power quality requirements, and supporting modern electricity markets.

D. Security Risks of CPPSs

The large-scale structure and complex networked environment of CPPSs increase their complexities and vulnerabilities, giving the attackers new opportunities to launch malicious cyber-attacks. Therefore, security assessment can enable the defenders to better identify security vulnerabilities of CPPSs, thereby improving defense strategies.

Firstly, there are loopholes in CPPSs. For example, [58] considers the vulnerabilities at different layers of microgrid as well as various factors relating to power system resilience, and proposes a cyber-physical security assessment metric (CP-SAM). By investigating the relevance of electricity and meteorological data, a data-driven model is developed to predict and detect security vulnerabilities of power systems [59]. A dynamic security assessment method is proposed to evaluate the safety performance of wind power generation system based on deep learning [60]. From the perspective of complex network theory, a vulnerability analysis

method is presented based on power system topologies [61]. This method examines the influence of the entire grid structure on fault propagation, and can be used to study the cascading fault propagation mechanism in large power systems. Moreover, a smart grid standard on cybersecurity assessments is proposed [62].

Secondly, the vulnerabilities of CPPSs will be greatly aggravated under malicious cyber-attacks. Therefore, the security assessment of CPPSs under cyber-attacks is also extremely important. An intrusion and defense model based on markov decision process (MDP) is proposed to evaluate the security of substations in the harsh network environment [63]. A dynamic security assessment method is proposed [64], which can quickly achieve dynamic security classification. A security index for vulnerability assessment is proposed to assess the risk of data attacks on power system state estimation [65]. Finally, cyber resilient communication network for CPPSs is proposed to quantify the security risk of denial-of-service (DoS) attacks on intelligent devices and networks [66].

III. Characteristics and Impacts of Cyber-attacks on CPPSs

As cyber-attacks could pose a huge threat to CPPSs, it is essential to analyze these attacks in much more details. In this section, we firstly discuss the structure of CPPSs, and comprehensively analyze possible cyber-attacks to each network layer and extract their features. Then, we further analyze the specific impacts of different cyber-attacks on CPPSs.

A. Analysis of Cyber-attack Features

According to propagation methods of cyber-attacks [17], these attacks can be classified into communication-based, cyber-based, physical-based, and network-based cyber-attacks. As illustrated in Figs. 3 and 5, cyber-attack features are first extracted and analyzed below.

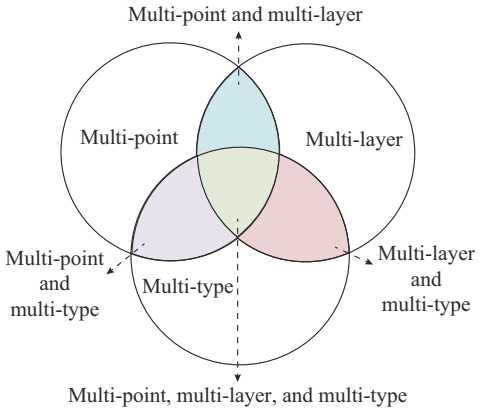

Fig. 5. Analysis of cyber-attack features.

Due to physical isolation of CPPSs from the external environment, the attackers need to break through the physical isolation and enter into the internal network firstly, before they can launch any cyber-attacks. At this stage, a popular method taken by the attackers is to use phishing emails to plant a back door in the system and breaks through physical isolation with an unintentional click by the operator. Another method is to search for vulnerabilities of physical isolation technology such as firewall security vulnerabilities, to break the protection barrier between the internal and external networks by using password cracking. Once having gained an access to the internal network, the attackers can attack physical devices and communication devices connected with the internal network in the smart grid. Then, the key features of cyber-attacks are summarized below.

1) Multi-point: multi-point means that the attacker can launch cyber-attacks by weakly protected/unprotected devices or nodes in power generation, transmission, distribution and consumption. For example, PMU is usually deployed in the 330 kV and above backbone network, and important power plants and substations. RTU is installed in power plant or substation, and IED is necessary for substation automation system. These smart measuring meters and devices with communication are connected to each other [67]. However, under open network environment, CPPSs can be exposed to the attacks, which provides the opportunity to invade the weak nodes. Regarding Ukrainian blackout in 2015, the attackers firstly launched phishing emails to implant BlackEnergy malware, and several key hosts were captured in the monitoring and device area to obtain the control ability of SCADA system, causing a wide blackout. Therefore, cyber-attacks can be launched against weakly protected/unprotected devices, as shown in Fig. 3, indicating that the feature of cyber-attacks can be multi-point.

2) Multi-layer: multi-layer means that cyber-attacks can spread across different layers due to the high coupling among physical, cyber, and control layers. The above smart measuring meters and devices in physical layer are interconnected through wired/wireless networks, e.g., Ethernet [68], profibus [69], NB-IoT [70], a hybrid wired/wireless combining time triggered Ethernet and 5G [71], etc, in cyber layer, supporting the running of control center in control layer [72]. When the information are exchanged among these three layers, they are easily attacked. For example, the attackers launched DoS against the renewable energy power company in Utah by exploiting known vulnerabilities in Cisco firewall [73]. Therefore, as shown in Fig. 3, multi-layer is another feature of cyber-attacks.

3) Multi-type: multi-type means that the types of attacks against different devices are also heterogeneous. In the physical layer, the attackers can launch different cyber-attacks aiming at destructing physical devices such as measuring meters, protection devices, and so on [15], [74], and different potential cyber-attacks against physical devices are also summarized [75]. In the cyber layer, the attackers often launch some typical attacks such as DoS [76], black hole and gray hole attacks [77], false data injection attack (FDIA) [78], etc, which will destroy the stable operation of CPPSs. In the control layer, the attackers can launch command manipulation attacks by injecting false command, causing the operator to perform wrong operations [79]. In summary, as shown in Fig. 3, another feature of cyber-attacks is multi-type.

4) Cross: it should be noted that the above three features are coupled with each other in Fig. 5. For example, multi-layer and multi-point mean that the attackers can invade dif-

ferent vulnerable nodes not only in the same layer but also in different layers. Multi-layer and multi-type mean that the attackers can launch different types of attacks for vulnerable nodes in different layers to achieve different purposes. Multi-point and multi-type mean that the attackers can launch different types of attacks against different vulnerable nodes. Finally, multi-layer, multi-point, and multi-type are the comprehensiveness of the above three cases. It is clear from the above analysis that the diversity and complexity of the three features of cyber-attacks coupled to each other make them difficult to detect and defend, which bring huge challenges for CPPSs.

Therefore, extensive research works on the security of CPPSs have been conducted to hedge against attacks by analyzing the vulnerabilities and exploring reliable solutions, which are reviewed in Sections IV and V.

B. Analysis of Popular Attack Models

To better illustrate the characters of multi-type of cyber-attacks, we list several popular attack models such as FDIAs, replay attacks (RAs), and DoS.

The following linear discrete model of CPPSs [80] is considered as:

$$\begin{cases} \boldsymbol{x}_{k+1} = \boldsymbol{A}\boldsymbol{x}_k + \boldsymbol{\omega}_k \\ \boldsymbol{z}_k = \boldsymbol{H}\boldsymbol{x}_k + \boldsymbol{v}_k \end{cases} \tag{1}$$

where $\boldsymbol{x}_k$ and $\boldsymbol{z}_k$ are the system state and measurement output vectors at the sampling instant, respectively; $\boldsymbol{A}$ is the state transition matrix; $\boldsymbol{H}$ is the Jacobian matrix; and $\boldsymbol{\omega}_k$ and $\boldsymbol{v}_k$ are the independent process and measurement noise, respectively. For system model in (1), three cyber-attacks are analyzed as follows.

1) FDIAs [15]: FDIA means that the attackers can tamper with system measurement $\boldsymbol{z}_k$. This type of attacks transmits incorrect values to the control center, resulting in wrong control commands. When the attackers are able to hack part of all measuring meters to achieve FDIA [81], the corresponding model is usually described as:

$$\boldsymbol{z}_k^a = \boldsymbol{z}_k + \boldsymbol{\Gamma}\boldsymbol{a}_k = \boldsymbol{H}\boldsymbol{x}_k + \boldsymbol{v}_k + \boldsymbol{\Gamma}\boldsymbol{a}_k \tag{2}$$

where $\boldsymbol{\Gamma} = \mathrm{diag}(\gamma_1, \gamma_2, \ldots, \gamma_n)$, $\gamma_i = 1$ represents the i^{th} measuring meter is attacked, otherwise, $\gamma_i = 0$; and $\boldsymbol{a}_k$ is the attack vector designed by the attackers.

2) RAs [82]: RAs are done by stealing the already transmitted information, which is used to forge and ultimately achieve the attacker's purpose. The attackers will implement the following attack steps.

Sept 1: the attackers record the measured output $\boldsymbol{z}_k$ for enough time without giving the system desired attacked control commands $\boldsymbol{u}_k^a$.

Sept 2: the attackers inject the desired attacked control commands $\boldsymbol{u}_k^a$ into the system while replaying previously recorded data $\boldsymbol{z}_k$ to eliminate the effects of the attack, which makes it difficult to detect.

The attack model is described as:

$$\begin{cases} \boldsymbol{x}_{k+1} = \boldsymbol{A}\boldsymbol{x}_k + \boldsymbol{\omega}_k + \boldsymbol{u}_k^a \\ \boldsymbol{z}_k^a = \boldsymbol{z}_{k-\alpha} \end{cases} \tag{3}$$

where the subscript α denote a large enough replaying period.

3) DoS: DoS means that the attackers continuously send forged packets on communication network channel, which makes the communication unavailable and the information cannot be exchanged normally. In this case, once the attackers successfully block the communication channel, $\boldsymbol{z}_k$ will be lost. The corresponding model is usually described as:

$$\boldsymbol{z}_k^a = \boldsymbol{\lambda}_k \boldsymbol{z}_k \tag{4}$$

where $\boldsymbol{\lambda}_k = \mathrm{diag}(\lambda_k(1), \lambda_k(2), \ldots, \lambda_k(n))$ is a diagonal matrix with elements 0 or 1, i.e., $\lambda_k(i) = 1$ represents that the corresponding measurements are successfully transmitted, otherwise, $\lambda_k(i) = 0$.

The above three attack models are popular, and some literatures had done detailed research on these attack models, attack scenario, and specific detection methods, e. g., FDIA [15], [17], DoS [19], and RA [20], [25].

In summary, the diversity of attack methods is due to different vulnerabilities of CPPSs considered by the attackers. However, the essence of the attack method is the malicious manipulation of data on different devices with security vulnerabilities in CPPSs, including data tampering, e. g., FDIA and RA, and interruption of transmission, e.g., DoS.

C. Impacts of Cyber-attacks on CPPSs

As mentioned above, cyber-attacks pose a huge security threat to CPPSs. Recent research on cyber-attacks clearly indicates that the impact of cyber-attacks on CPPSs is increasing. Generally, the impacts of cyber-attacks include systems stability, i.e., the destructive behavior induced by the attackers can affect system stability such as cascading failure, and the economy, i.e., the profit-making of the attackers.

1) Cascading Failure Caused by Cyber-attacks

Cyber and physical layers of CPPSs are highly coupled, i.e., the control of power systems depends on communication networks, and the power supply of communication networks also relies on power systems, which brings unprecedented improvement and functionalities to power systems. However, such interdependent systems are also vulnerable to the failures, natural disasters, and especially cyber-attacks with the above features. When an attack occurs in an interdependent system, a failure caused by cyber-attacks in one network may cascade down to a dependent node in another network [83], eventually leading to the collapse of the entire system [84] and ultimately to a blackout. For example, a blackout occurred in Italy in 2003, some communication nodes were initially lost as the result of the shut-down of the corresponding power station, and the loss of this communication information led to a wider power outage [85]. Therefore, the cascading failures caused by cyber-attacks would be the most direct result.

2) Impacts on Stable Operation

The cascading failures caused by cyber-attacks can affect the stable operation of power systems. The impacts on stable operation are related to misleading data and information after cyber-attacks successfully hack into CPPSs. For example, the attackers may implement unnecessary generation operation and load shedding by injecting false data [86]. The operation and control of CPPSs may conduct improper response or no response, eventually leading to unstable conditions.

The fake measurements from cyber-attacks will lead to the secondary voltage controller to take wrong setting values, which compromises the overall system stability [87]. The impacts of cyber-attacks on the frequency control of CPPSs are extensively studied [88], and it also shows how a frequency-based cyber-attacks can lead to a wide-area blackout.

3) Impacts on Economy

The cascading failures caused by cyber-attacks can lead to wide-area blackouts, hence affecting the economy, which is also a major concern. Most of the attackers pursue some economic goals such as seeking for personal interests or being employed by hostile countries to influence the economic development of other countries. The economic impact of cyber-attacks can be summarized as follows.

Firstly, energy theft is a major target for many attackers. The attackers can modify the data in CPPSs or modify their own smart meter readings directly to pursue economic benefits. Both situations will bring illegal profits to the attackers [89], [90]. On this basis, a new locational marginal price (LMP) attack model is proposed [91]. With this model, cyber-attacks have a significant impact on the energy market even without the need for a complete knowledge of power systems.

Secondly, cyber-attacks may change grid topology and even generation plans, which eventually have a significant impact on grid operational cost. For example, the failures caused by cyber-attacks may cascade down interdependent systems, leading to large-scale outage [92]. Moreover, the load redistribution attack is utilized to trip off a critical lines or breakers by misleading the control center to make improper dispatch actions [93]. It should be pointed out that the stability impact and the economy impact often coexist. To mitigate the challenges and negative impacts of cyber-attacks, many attack detection methods have been proposed.

IV. Cyber-attack Detection

In response to potential threats induced by cyber-attacks, many methods have been proposed for cyber-attack detection, and these can be categorized into two groups, e. g., model-based and machine learning based detection methods. Model-based detection method aims to quantify the changes of the internal state of the system under cyber-attacks, so as to achieve the purpose of attack detection. For the latter, machine learning based detection method is utilized to train the classifier for attack detection.

A. Model-based Detection Methods

Model-based state estimation of power systems uses measurement sets and system models to estimate internal states, and they can be categorized as static and dynamic state estimation models. Traditional state estimation of power systems usually adopts static estimation methods [17]. However, as real CPPSs constantly change in real time, dynamic state estimation is becoming more important [94]. Hence, attack detection methods can also be based both on static and dynamic state estimation.

State estimation based detection methods often have two steps: ① estimating or predicting the internal states of the system; and ② processing the measured state information, and comparing the differences based on various similarity tests.

1) Static State Estimation

Weighted least square (WLS) estimation is perhaps the most popular static state estimation method. It has been widely used in attack detection. For FDIA detection, WLS-based detection method is utilized to detect FDIA [95], [96]. Some other static estimation methods include the median filter (MF) [97] and the maximal likelihood (ML) estimation [98], which are used to achieve the detection for FDIA. These estimation methods have advantages of simplicity and versatility, but their performances will be seriously degraded when there exist uncertainties in the system parameters.

2) Dynamic State Estimation

Compared with traditional static state estimation methods, dynamic state estimation methods are gaining more popularity in power systems. Kalman filter (KF) and its variants such as extended Kalman filter (EKF) and unscented Kalman filter (UKF) are among the most popular methods. The specific process of KF can be described as:

$$\begin{cases} \hat{\boldsymbol{x}}_k^- = \boldsymbol{A}\hat{\boldsymbol{x}}_{k-1} \\ \boldsymbol{P}_k^- = \boldsymbol{A}\boldsymbol{P}_{k-1}\boldsymbol{A}^{\mathrm{T}} + \boldsymbol{Q} \end{cases} \tag{5}$$

$$\begin{cases} \boldsymbol{K}_k = \boldsymbol{P}_k^- \boldsymbol{H}^{\mathrm{T}} (\boldsymbol{H}\boldsymbol{P}_k^- \boldsymbol{H}^{\mathrm{T}} + \boldsymbol{R})^{-1} \\ \boldsymbol{P}_k = \boldsymbol{P}_k^- - \boldsymbol{K}_k \boldsymbol{H}\boldsymbol{P}_k^- \\ \hat{\boldsymbol{x}}_k = \hat{\boldsymbol{x}}_k^- + \boldsymbol{K}_k (\boldsymbol{z}_k - \boldsymbol{H}\hat{x}_k^-) \end{cases} \tag{6}$$

where the prior estimation state vector $\hat{\boldsymbol{x}}_k^-$ is the estimation at time instant k by using the measurements up to time instant $k-1$; the posterior estimation state vector $\hat{\boldsymbol{x}}_k$ is the estimation at time instant k by using measurements up to time instant k; $\boldsymbol{P}_k^-$ and $\boldsymbol{P}_k$ are the prior and posterior covariances of the estimation error, respectively; $\boldsymbol{Q}$ is the process noise covariance matrix; $\boldsymbol{R}$ is the measurement noise covariance matrix; and $\boldsymbol{K}_k$ is the Kalman gain.

The operation of KF includes the following two steps: ① a state prediction is built upon time update; and ② the updated measurement is used to modify the state prediction.

A number of extend detection methods have been proposed based on KF. For FDIA detection, a FDIA detection method is proposed by using KF [99], and an online detection method based on KF is used to detect FDIA [100]. A model prediction method based on KF is proposed to detect electromechanical abnormal oscillations caused by FDIA [101]. An online CUSUM attack detection method based on KF is proposed for hybrid FDIA or jamming attacks [102].

Next, considering the error caused by the linearization of CPPS model, EKF and UKF are also proposed to achieve attack detection. For FDIA detection, according to successive batch-mode regression representation of EKF, a statistical outlier method based on S-estimator is implemented to detect FDIA [103]. An anomaly detection including Luenberger observer and EKF is proposed, which improves the ability to detect FDIA [104]. A novel dynamic watermarking (DW) based EKF detection method is proposed to detect FDIA [105], and an adaptive UKF method is proposed to detect FDIA [106]. A method based on UKF and WLS is proposed to estimate system state and identify FDIA according to the difference of estimation results [107].

To reduce the communication burden and computational complexity, a distributed Kalman filter (DKF) is proposed to achieve global accurate estimation. It has been widely used in attack detection. For FDIA detection, DKF is combined with blockchain technology to protect network databases and network communication channels from FDIA [108]. For RA detection, a DKF with trust-based dynamic combination strategy is proposed to detect RA [109], [110]. For DoS detection, a distributed dynamic state estimator is proposed, where the generalized cumulative sum method is used to detect DoS [111].

For FDIA detection, interval state estimation (ISE) is employed to carry out attack detection. An ISE combined with deep learning method is proposed to improve the detection accuracy for FDIA [112], [113]. A generalized ISE method based on UKF is proposed to quantify the normal fluctuation of all states, which is then used to detect FDIA [114]. An ISE forecasting method is proposed to approximate the possible largest variation bounds of each state variable to achieve FDIA detection [115].

Moreover, KF selects the minimum linear variance gain as Kalman gain, while the optimal gain of unknown input observer (UIO) is obtained by pole configuration. In addition, UIO can take attack signals as unknown inputs and detect it by estimating attack signal [116]. For FDIA detection, a UIO-based attack detection method is proposed to detect FDIA, where the adaptive threshold is set to improve the detection accuracy [117]. Some UIO-based attack detection methods are proposed to detect FDIA or RA [118]-[122]. Interval observer (IO) can also be used for FDIA detection. For example, an IO-based detection method against FDIA is proposed, where the traditional residual evaluation functions are replaced by interval residuals [123]. A method based on stochastic UI estimator is proposed to detect FDIA for automatic generation control (AGC) system [124]. Furthermore, some IO-based detection methods are proposed to estimate the interval state and to detect FDIA [125], [126].

3) Detection Tests

Detection test is to detect cyber-attacks by processing the estimated state and comparing its similarity against actual measured value. The popular detection schemes can be grouped into the following categories [17].

Euclidean distance (L_2 norm) detection test [97], [118] is:

$$f_{L_2}(\boldsymbol{z}_k)=\begin{cases}1 & \left\|\boldsymbol{z}_k-\boldsymbol{H}\hat{\boldsymbol{x}}_k\right\|_2>\bar{f}_1\\ 0 & \text{otherwise}\end{cases} \tag{7}$$

where $f_{L_2}(\boldsymbol{z}_k)$ is the Euclidean distance detector, and 1 means that the attacks are detected, 0 otherwise; $\boldsymbol{H}\hat{\boldsymbol{x}}_k$ is the estimated value; $\left\|\boldsymbol{z}_k-\boldsymbol{H}\hat{\boldsymbol{x}}_k\right\|_2$ is the L_2 norm of the difference; and $\bar{f}_1$ is a prior threshold value, which is generally given by the experienced operators according to practical situations.

The largest normalized residual (LNR) detection test [127] is:

$$f_{LNR}(\boldsymbol{z}_k)=\begin{cases}1 & \left\|\dfrac{\boldsymbol{z}_k-\boldsymbol{H}\hat{\boldsymbol{x}}_k}{\boldsymbol{N}_k}\right\|_\infty\geq\bar{f}_2\\ 0 & \text{otherwise}\end{cases} \tag{8}$$

where $\boldsymbol{N}_k$ is covariance matrix of residual $\boldsymbol{r}_k$.

χ^2-detection test [96] is:

$$f_{\chi^2}(\boldsymbol{z}_k)=\begin{cases}1 & J(\hat{\boldsymbol{x}}_k)\geq\bar{f}_3\\ 0 & \text{otherwise}\end{cases} \tag{9}$$

where $f_{\chi^2}(\boldsymbol{z}_k)$ is the χ^2-detector; and $J(\hat{\boldsymbol{x}}_k)$ is the objective function.

Cumulative sum (CUSUM) detection test [103] is:

$$f_{CUSUM}(\boldsymbol{z}_k)=\begin{cases}1 & \boldsymbol{S}_t=\boldsymbol{S}_{t-1}+(\boldsymbol{z}_k-\boldsymbol{H}\hat{\boldsymbol{x}}_k)\geq\bar{f}_4\\ 0 & \text{otherwise}\end{cases} \tag{10}$$

where $\boldsymbol{S}_t$ is the collected measurement at time instant k. This method is usually used to monitor the variations in the collected measurements.

Kullback-Leibler distance (KLD) detection test [99] is:

$$f_{KLD}(\boldsymbol{z}_k)=\begin{cases}1 & \sum\limits_{\boldsymbol{z}_k}p(\boldsymbol{x}_k)\ln\dfrac{p(\boldsymbol{x}_k)}{Q(\boldsymbol{x}_k)}\geq\bar{f}_5\\ 0 & \text{otherwise}\end{cases} \tag{11}$$

where $p(\boldsymbol{x}_k)$ is the probability distribution of historical state changes; and $Q(\boldsymbol{x}_k)$ is the probability distribution of the state changes at previous moment and current moment. This method uses probability distribution functions to detect cyber-attacks.

Cosine similarity detection test [128] is:

$$f_{sim}(\boldsymbol{z}_k,\hat{\boldsymbol{z}}_k)=\begin{cases}1 & 1-\dfrac{\boldsymbol{z}_k\cdot\hat{\boldsymbol{z}}_k}{\left\|\boldsymbol{z}_k\right\|\left\|\hat{\boldsymbol{z}}_k\right\|}\geq\bar{f}_6\\ 0 & \text{otherwise}\end{cases} \tag{12}$$

where the numerator in (12) is dot product of vectors $\boldsymbol{z}_k$ and $\hat{\boldsymbol{z}}_k$; and the denominator denotes the product of their euclidean lengths. When there are no cyber-attacks, $\boldsymbol{z}_k\cdot\hat{\boldsymbol{z}}_k\Big/\left(\left\|\boldsymbol{z}_k\right\|\left\|\hat{\boldsymbol{z}}_k\right\|\right)$ is equal to 1; and the prior thresholds $\bar{f}_i$ ($i=1,2,\ldots,6$) is discussed in [129]. It is worth noting that the setting of threshold will affect the detection rate of cyber-attacks. If too high threshold is set, the detection rate will be decrease; otherwise, it can lead to a higher false alarm rate.

B. Machine Learning Based Detection Methods

Different from the aforementioned state estimation based detection method, machine learning based detection method does not need mathematical model of physical system, and it completely depends on historical data of the system under test. Machine learning is an interdisciplinary field of statistics, artificial intelligence, and computer science, which can be used to extract the knowledge from data. Machine learning methods can be utilized for classification and regression. The essence of regression is to realize numerical prediction, which has been widely applied to power system load forecasting. The classification is to divide the predicted values into specific categories, and cyber-attack detection is a typical classification task. For example, we can use historical data to train a machine learning based classifier, which is then utilized to detect abnormal changes in the data for identifying potential cyber-attacks in CPPSs. In general, machine learning based detection methods include the following three categories: supervised, unsupervised, and semi-supervised learning methods.

1) Supervised Learning

Generally, the users provide paired input and expected output, i.e., $\{\boldsymbol{u}_i, \boldsymbol{z}_i\}$, to train the method, so that the method will give the expected output according to the given input. For attack detection, the expected output describes whether there is an attack or not. For FDIA detection, linear regression (LR) is employed to detect FDIA by comparing the difference between the measurement vector and model predictions based on historical data [130]. Support vector machine (SVM) is also used to detect FDIA [131], and K-nearest neighbour (KNN) is also used to detect FDIA [132]. Decision tree (DT) is used to detect electricity stealing caused by FDIA [133], [134], and naive bayes classifier (NBC) is used to detect FDIA [135]. For DoS detection, a big data framework using SVM, NBC, and DT is proposed to detect traffic anomalies caused by DoS [136].

In addition to the aforementioned methods, as an extremely popular tool, artificial neural network (ANN) has also been widely used for classification and prediction. The ANN model could be a simple feedforward neural network (FNN) or a deep neural network (DNN). Their model can be obtained by the optimization problem, which can be solved by different local and global methods such as gradient based search techniques [137], genetic method [138]. The ANN has also been widely used in attack detection. For FDIA detection, FNN is employed to detect FDIAs [139], and recurrent neural network (RNN) can be used to achieve FDIA detection [140], [141]. DNN is used to detect FDIA [136], where the hidden layers determine the accuracy of attack detection. Convolutional neural network (CNN) has been used to detect FDIA by extracting different features from the samples [142]. For DoS detection, FNN is used to detect FDIA [143], and RNN is employed to detect DoS [144]. For RA detection, CNN is proposed to detect RA [145].

2) Unsupervised Learning (UL)

UL refers to learning some useful patterns from unlabeled data, i.e., learning valuable information such as effective features, categories, and structures directly from the original data without any manual guidance such as tags or feedback. For cyber-attacks, the classes of abnormal data are different from normal data. For FDIA detection, K-means clustering (KMC) is employed to achieve FDIA detection [146]. Considering large-scale data sets, isolation forest (IF) is used to isolate anomalies caused by FDIA by analyzing the data difference between various IF [147]. Other classic UL methods such as autoencoder (AE) have also been used for FDIA detection [148], [149]. For DoS detection, deep belief network (DBN) is employed to detect abnormal network traffic caused by DoS [150]. Some existing attack detection methods based on DBN have been reviewed in [151].

3) Semi-supervised Learning (SSL)

SSL is also an important branch of machine learning. It falls between supervised learning and UL and uses both labeled and unlabeled data to fit the model. This method is also widely utilized in attack detection. For FDIA detection, a semi-supervised adversarial autoencoder (SSAA) based method is proposed to detect FDIA [152]. The generative-adversarial based semi-supervised (GBSS) learning framework is proposed to detect FDIA [153]. A semi-supervised deep learning method for intrusion detection (SS-deep-ID) is proposed to improve detection efficiency for FDIA [154]. A robust semi-supervised prototypical network (RSSPN) classifier is proposed to detect FDIA [155].

Finally, state estimation based detection method versus machine learning based detection method is shown in Fig. 6. The specific implementation process of the two detection methods based on state estimation and machine learning are shown in Tables III and IV, and their advantages and disadvantages are analyzed. Especially, dynamic state estimation is divided into centralized and distributed state estimations, and their advantages and disadvantages are discussed, respectively. Moreover, the computational complexity and detection rate of these methods have also been summarized [17].

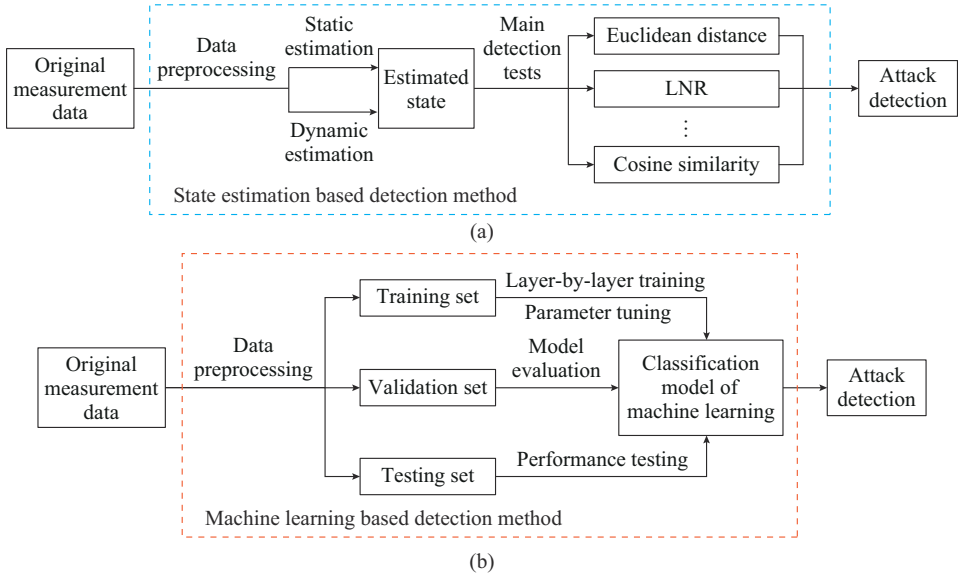

Fig. 6. State estimation based detection method versus machine learning based detection method. (a) State estimation based detection method. (b) Machine learning based detection method.

TABLE III
STATE ESTIMATION BASED ATTACK DETECTION

Category	Method	Advantage	Disadvantage
Static	WLS [95], [96], MF [97], ML [98]	① Low time complexity ② High implementation	① Low estimation accuracy ② Low suitability for large system
Dynamic	Centralized: KF [99]-[102], EKF [103]-[105], UKF [106], [107]	① High estimation accuracy ② High applicability to nonlinear models ③ High detection rate	① High time complexity ② Easy divergence
	Distributed: DKF [108]-[111], ISE [112]-[115], UIO [116]-[122], IO [123]-[126]	① High estimation accuracy ② High suitability for large systems ③ High detection rate	① High time complexity ② Easy local optimization

TABLE IV
MACHINE LEARNING BASED ATTACK DETECTION

Category	Method	Advantage	Disadvantage
Supervised	LR [130], SVM [131], [136], KNN [132], DT [133], [134], NBC [135], ANN [139], [144]	① System models are not required ② Known attack detection is fast	① Data set with label is required ② New attack detection is not applicable
Unsupervised	KMC [135], FC [146], IF [147], AE [148], [149], DBN [150]	① System models are not required ② New attack detection is applicable	Large number of training is required
Semi-supervised	SSAA [152], GBSS [153], SS-deep-ID [154], RSSPN [155]	① System models are not required ② Known attack detection is fast ③ New attack detection is applicable	Unlabeled data are extensively trained

V. CYBER-ATTACK DEFENSE

To further improve the security of CPPSs and reduce the threat of cyber-attacks, many corresponding defense strategies have been developed based on the aforementioned attack detection methods. Similar to the aforementioned detection methods, the defense methods can be grouped into two categories: ① active defense methods, aiming at eliminating the possibility of any successful cyber-attacks; and ② passive defense methods, quickly locating and isolating the attacked locations and taking appropriate measures to ensure the normal operation of CPPSs when cyber-attacks are successfully launched.

A. Active Defense Methods

From the previous analysis of cyber-attacks, it is evident that three features of cyber-attacks, including multi-point, multi-type, and multi-layer, bring challenges to attack defense. Moreover, due to the limited defense resources, the common active defense strategies often select a limited number of specific facilities for protection to achieve the best defense effect.

For FDIA defense, a hidden moving target defense (HMTD) method is proposed to maintain power flow, which prevents FDIA intrusion by changing the susceptance of transmission lines [156]. The defender actively learns different attack scenarios, which can tolerate some attacks [157]. Moreover, game theory (GT) is also employed to defense FDIA [158]-[160]. To avoid the key services in CPPSs suffering from FDIA, a polymorphic heterogeneous security architecture (PHSA) is proposed to improve its security [161]. For DoS defense, when the attacker resources are uncertain, a multiple-attack-scenario (MAS) defender-attacker-defender (DAD) model is proposed to protect the transmission system from DoS [162].

B. Passive Defense Methods

Different from active defense methods, the primary goal of passive defense methods is to locate and isolate the attacked nodes as quickly as possible, and to take the corresponding attack-tolerant measures for reducing the damage caused by cyber-attacks.

1) Isolation of Attacks

In general, attack detection can be performed simultaneously with isolation. For FDIA defense, a prediction-based attack isolation method is proposed [163] to achieve FDIA detection and isolation. For distributed CPPSs, an FDIA detection and isolation method based on UIO is proposed [164]. An FDIA detection and isolation method based on unknown input IO interval observer and logical judgment matrix is proposed [165]. Furthermore, a topology-based power system subregion division method is proposed to reduce the difficulty in FDIA detection and isolation [166], and a supervised FDIA isolation method combining statistical metrics and ensemble tree model (ETM) is proposed [167]. A deep learning based locational detection architecture (DLLD) is proposed to detect the exact locations of FDIA [168], which combines bad data detector (BDD) with CNN.

2) Attack Tolerance

Based on the above cyber-attack location and isolation methods, certain attack tolerant technologies also need to be utilized to ensure the stable operation of CPPSs. Attack tolerant technologies are quite similar to the fault tolerant control. In general, the fault tolerant control adopts the corresponding control measures for different fault sources to ensure normal operation of the equipment before or after the equipment failure, or the equipment can still perform basic functions within the specified time at the cost of sacrificing the performance loss. Similar to the fault tolerant control described above, attack tolerance technologies also have the

similar features. However, this research work is still at its infancy, and only a very limited results have been reported so far, hence deserving further exploration.

For FDIA defense, a parametric feedback linearization (PFL) control is proposed to achieve the stability of power systems under FDIA [169]. A controlled switching unit is proposed to ensure the frequency stability under FDIA [170]. A recovery strategy based on deep reinforcement learning (DRL) framework is proposed to reclose the tripped transmission lines caused by FDIA, which has the adaptability and real-time decision ability for uncertain cyber-attack scenarios [171]. To eliminate the influence of FDIA, a state reconstruction method is proposed to filter out FDIA [172]. A method based on synchronous input and state estimation is proposed to detect FDIA, and the estimated value is used to reduce the effect of the attack [173]. For FDIA defense and DoS, considering hybrid cyber-attacks from FDIA and DoS, a distributed estimation method based on the alternating direction method of multipliers (ADMM) is proposed to improve the security of CPPSs [174]. For FDIA defense and RA, an optimal two-stage Kalman filter (OTS-KF) is proposed to achieve the defense against FDIA and RA in AGC systems [175].

Finally, Table V is a summary of the aforementioned cyber-attack defense methods, including their advantages and disadvantages.

TABLE V
SUMMARY OF CYBER-ATTACK DEFENSE METHODS

Category	Reference	Advantage	Disadvantage
Active defense	HMDT [156], MFD-based [157], GT-based [158], [160], DAD model-based [162]	① Low utilization of defense resources ② Simple operation for defender	① Inconsistency between attacked and protected objects ② Imbalance between attack resources and defense resources on the same target
Passive defense	VAR [163], UIO [164]-[166], ETM [167], DLLD [168], PFL [169], DRL [171], ADMM [174], OTS-KF [175]	① Fast location of attacked nodes ② Normal operation of system under attack	① Easy to incorrectly isolate safe nodes ② Prone to attack-tolerance delay ③ Easy to exacerbate the instability of system

VI. CONCLUSION AND CHALLENGING ISSUES

Due to the landscape change of power systems and the increased utilization of new ICTs, attack detection and defense for CPPSs have become a research hotspot in the recent years. This paper presents a comprehensive literature review in regards to cybersecurity of CPPSs and three key methods, including attack analysis, attack detection, and attack defense, are discussed in detail. The attack defense has gained substantial attention in the academic community, and a range of detection and defense methods have been proposed. However, there still exist several unsolved open problems in this area, which are summarized as follows.

1) Holistic design of CPPSs: with the support of modern communication resources and technology, CPPSs integrate various physically dispersed computing and control resources to provide system support for core tasks, resulting in significantly improved capacity to solve more complex problems than ever before. Compared with the conventional power systems, CPPSs promote the goals such as intelligent resource allocation and energy management through the integration of communication, computation, and control. Based on this, ICTs can quickly and effectively provide supports for control tasks at a global scale, guaranteeing the feasibility and effectiveness of the global optimization and regulation of CPPSs. However, it also brings more challenges and difficulties to its security control and defense. Therefore, the design and planning of CPPSs should not only consider the development of resource strategic plans, the characteristics of consumers, and the dynamic operation characteristics of power systems, but also the holistic design of security defense mechanism to further strengthen the distributed, interactive, and dynamic features of CPPSs.

2) The gaming between attackers and defenders: the relationship between the attackers and defenders is also worth exploring. For the defenders, it is necessary to ensure the security of CPPSs as much as possible by analyzing and evaluating the vulnerability of CPPSs and configuring the limited defense resources. For the attackers, identifying the weakest point in power systems is the main target. From the perspective of GT, the above behaviors of the attackers and defenders can be modeled by a static zero-sum game. However, in actual situations, the attackers may not know the defense strategies partially or fully, and the defenders may also know nothing about the attack strategies. Therefore, in the case of information asymmetry, investigating the interactions of the attackers and defenders is an interesting topic. Moreover, multiple defenders and multiple attackers may be involved. Thus, it is necessary to investigate dynamic gaming such as Markov games, to describe the process of dynamic interactions between the attackers and defenders.

3) Analysis of new attacks mechanism: with the significantly increasing intelligence of CPPSs, more security vulnerabilities are also identified, offering new opportunities for attackers. Meanwhile, with the continuous update of cyber-attacks means, novel cyber-attacks against CPPSs emerge endlessly. By analyzing the vulnerability of system detection mechanisms, the attackers can build covert attacks to bypass common detection mechanism such as the popular FDIA. Moreover, due to the high coupling between cyber layer and physical layer of CPPSs, any small fault caused by the attacks may propagate rapidly due to the strong coupling of dual networks and may result in more frequent large-scale blackouts, seriously endangering the security, stability, and economic operation of CPPSs. Therefore, the analysis of the attack mechanism and cascading failure is one of the research trends that deserve further investigation.

4) Detection and defense based on physical mechanism: the current attack detection methods are still limited. The state estimation based detection methods can only detect specific cyber-attacks, and their generalization is poor. In practical applications, it is desirable to develop the detection methods independent of system models and parameters. The machine learning based detection methods can only detect the existing cyber-attacks, but they have difficulties in meeting the needs against the endless novel cyber-attacks. However, multi-type cyber-attacks designed by the attackers always directly or indirectly affect physical properties of power systems. Therefore, it is necessary to analyze physical properties based on physical mechanism of the systems, and to develop the detection methods that can be easily scaled up. Further, most research works only focus on attack detection, while there are limited preventive measures. In general, whether an attacker can compromise a device in reality depends on the level of protection that the defender has deployed on the device. Therefore, it is worth considering which devices shall be protected and how many layers of protection shall be deployed so that no state variables can be altered by the attackers. Besides, a limited number of research works have studied attack location and isolation, which is very important for the defenders to take the corresponding attack-tolerance methods for ensuring the normal operation of the system under cyber-attacks. CPPSs are required to have fault-tolerance and attack-tolerance, which can ensure that it can still operate normally in extreme cases. Therefore, it is important for the defenders to utilize the fault-tolerant control to enhance the robustness of CPPSs.

5) Verification and application of attack/defense strategies: most of the existing literatures primarily focus on theoretical investigation. However, the practical applications are limited. To investigate the practicality of these methods, microgrid has attracted much attention. Through the PCC, microgrid is connected with the distribution system as a complementary controllable subsystem to the main grid. Microgrids therefore can enhance the overall control performance of the system during grid-connected mode, achieving the coordinated operation of microgrid and the main grid. When microgrid is in islanded operation mode, it can also meet the power quality requirements of local users, ensure the reliable operation of loads, avoid the negative impact of distributed generation on power systems, and thus play an important role in supporting the distribution network.

REFERENCES

[1] R. He, H. Xie, J. Deng *et al.*, "Reliability modeling and assessment of cyber space in cyber-physical power systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3763-3773, Sept. 2020.

[2] A. Nawaz and H. Wang, "Risk-aware distributed optimal power flow in coordinated transmission and distribution system," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 3, pp. 502-515, Jan. 2021.

[3] Y. Lin, X. Zhang, J. Wang *et al.*, "Voltage stability constrained optimal power flow for unbalanced distribution system based on semidefinite programming," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 6, pp. 1614-1624, Apr. 2022.

[4] S. Wang, D. Yu, J. Yu *et al.*, "Optimal generation scheduling of interconnected wind-coal intensive power systems," *IET Generation, Transmission and Distribution*, vol. 10, no. 13, pp. 3276-3287, Oct. 2016.

[5] S. Wang, D. Yu, and J. Yu, "A coordinated dispatching strategy for wind power rapid ramp events in power systems with high wind power penetration," *Journal of Power Sources*, vol. 478, pp. 1-16, Jan. 2020.

[6] Y. Hua, S. Zhou, Y. Huang *et al.*, "Sustainable value chain of retired lithium-ion batteries for electric vehicles," *Electrical Power and Energy Systems*, vol. 64, pp. 986-995, Dec. 2015.

[7] A. Burnham, E. Dufek, T. Stephens *et al.*, "Enabling fast charging-infrastructure and economic considerations," *Journal of Power Sources*, vol. 367, pp. 237-249, Nov. 2017.

[8] X. Yu and Y. Xue, "Smart grids: a cyber-physical systems perspective," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1058-1070, May 2016.

[9] L. Das, S. Munikoti, B. Natarajan *et al.*, "Measuring smart grid resilience: methods, challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 130, pp. 1-16, Sept. 2021.

[10] M. Chung, W. Ahn, B. Min *et al.*, "An analytical method for developing appropriate protection profiles of instrumentation and control system for nuclear power plants," *Journal of Supercomputing*, vol. 74, no. 3, pp. 1378-1393, Mar. 2018.

[11] L. M. Robert, A. J. Michael, and C. Tim. (2016, Dec.). Analysis of the cyber attack on the ukrainian power grid. [Online]. Available: https:// media. kasperskycontenthub. com/wp-content/uploads/sites/58/2016/12/ 21181126/E-ISAC_SANS_Ukraine_DUC_5.pdf

[12] J. Condliffe. (2016, Dec.). Ukraines power grid gets hacked again, a worrying sign for infrastructure attacks. [Online]. Available: https:// www. technologyreview. com/2016/12/22/5969/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/

[13] M. Cukier. (2021, Jan.). Study: hackers attack every 39 seconds. [Online]. Available: https://eng. umd. edu/news/story/study-hackers-attack-every-39-seconds

[14] M. Miller. (2021, Jan.). 2021 must-know cyber attack statistics and trends. [Online]. Available: https://www. embroker. com/blog/cyber-attack-statistics

[15] G. Liang, J. Zhao, F. Luo *et al.*, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630-1638, Jul. 2017.

[16] J. Giraldo, D. Urbina, A. Cardensa *et al.*, "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Survey*, vol. 51, no. 4, pp. 1-36, Sept. 2018.

[17] A. Musleh, G. Chen, and Z. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *Journal of Hardware and Systems Security*, vol. 11, no. 3, pp. 2218-2234, May 2020.

[18] S. Tan, J. Guerrero, P. Xie *et al.*, "Brief survey on attack detection methods for cyber-physical systems," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5329-5339, Dec. 2020.

[19] D. Zhang, Q. Wang, G. Feng *et al.*, "A survey on attack detection, estimation and control of industrial cyber physical systems," *ISA Transactions*, vol. 116, pp. 1-16, Oct. 2021.

[20] J. Zhang, L. Pan, Q. Han *et al.*, "Deep learning based attack detection for cyber-physical system cybersecurity: a survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 377-391, Mar. 2022.

[21] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13-27, Dec. 2016.

[22] S. Mehrdad, S. Mousavian, G. Madraki *et al.*, "Cyber-physical resilience of electrical power systems against malicious attacks: a review," *Current Sustainable/Renewable Energy Reports*, vol. 5, pp. 14-22, Mar. 2018.

[23] P. Kumar, Y. Lin, G. Bai *et al.*, "Smart grid metering networks: a survey on security, privacy and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886-2927, Feb. 2019.

[24] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: a survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2831-2848, Mar. 2019.

[25] Z. Muhammed and D. Resul, "Cyber-security on smart grid: threats and potential solutions," *Computer Networks*, vol. 169, no. 14, pp. 1-14, Mar. 2020.

[26] D. Ding, Q. Han, X. Ge *et al.*, "Secure state estimation and control of cyber-physical systems: a survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 176-190, Jan. 2021.

[27] L. Zhang, X. Hu, Z. Wang *et al.*, "Hybrid electrochemical energy storage systems: an overview for smart grid and electrified vehicle applications," *Renewable and Sustainable Energy Reviews*, vol. 139, pp. 1-10, Apr. 2021.

[28] S. Silva, M. Hejazi, G. Iyer *et al.*, "Power sector investment implications of climate impacts on renewable resources in Latin America and

the Caribbean," *Nature Communications*, vol. 12, no. 1, pp. 1-12, Feb. 2021.
[29] M. Daneshvar, I. Mohammadi, K. Zare *et al.*, "Transactive energy management for optimal scheduling of interconnected microgrids with hydrogen energy storage," *International Journal of Hydrogen Energy*, vol. 46, pp. 16267-16278, Apr. 2021.
[30] Y. Chang, I. Kocar, J. Hu *et al.*, "Coordinated control of DFIG converters to comply with reactive current requirements in emerging grid codes," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 2, pp. 502-514, Oct. 2022.
[31] D. Geleta and M. Manshahia, "Gravitational search algorithm-based optimization of hybrid wind and solar renewable energy system," *Computational Intelligence*. doi:10.1111/coin.12336
[32] L. Zhang, F. Wang, Y. Xu *et al.*, "Evaluating and selecting renewable energy sources for a microgrid: a bi-capacity-based multicriteria decision making approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 921-931, Mar. 2021.
[33] P. Kong, "Optimal configuration of interdependence between communication network and power grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4054-4065, Jul. 2019.
[34] M. Tuballa and M. Abundo, "A review of the development of smart grid technologies," *Renewable and Sustainable Energy Reviews*, vol. 59, pp. 710-725, Jun. 2016.
[35] X. Fang, S. Misra, G. Xue *et al.*, "Smart grid–the new and improved power grid: a survey," *IEEE Communications Surveys and Tutorials*, vol. 14, pp. 944-980, Dec. 2012.
[36] C. Tang, P. Chen, and J. He, "Bidirectional power flow control and hybrid charging strategies for three-phase PV power and energy storage systems," *IEEE Transactions on Power Electronics*, vol. 36, no. 11, pp. 12710-12720, Nov. 2021.
[37] A. Mohamed and O. Mohammed, "Bilayer predictive power flow controller for bidirectional operation of wirelessly connected electric vehicles," *IEEE Transactions on Industry Applications*, vol. 55, no. 4, pp. 4258-4267, Aug. 2019.
[38] Q. Hu, S. Bu, and V. Terzija, "A distributed P and Q provision based voltage regulation scheme by incentivized EV fleet charging for resistive distribution networks," *IEEE Transactions on Transportation Electrification*, vol. 7, no. 4, pp. 2376-2389, Dec. 2021.
[39] T. Wu, S. Bu, X. Wei *et al.*, "Multitasking multi-objective operation optimization of integrated energy system considering biogas-solar-wind renewables," *Energy Conversion and Management*, vol. 229, pp. 1-15, Feb. 2021.
[40] R. Anderson, A. Boulanger, W. Powell *et al.*, "Adaptive stochastic control for the smart grid," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 1098-1115, Jun. 2011.
[41] K. Di-Santo, E. Kanashiro, S. Di-Santo *et al.*, "A review on smart grids and experiences in Brazil," *Renewable and Sustainable Energy Reviews*, vol. 52, pp. 1072-1082, Aug. 2015.
[42] S. Zahurul, N. Mariun, I. Grozescu *et al.*, "Future strategic plan analysis for integrating distributed renewable generation to smart grid through wireless sensor network: Malaysia prospect," *Renewable and Sustainable Energy Reviews*, vol. 53, pp. 978-992, Jan. 2016.
[43] T. Samad, E. Koch, and P. Stluka, "Automated demand response for smart buildings and microgrids: the state of the practice and research challenges," *Proceedings of the IEEE*, vol. 104, no. 4, pp. 726-744, Apr. 2016.
[44] N. Guo, Y. Wang, and G. Yan, "A double-sided non-cooperative game in electricity market with demand response and parameterization of supply functions," *International Journal of Electrical Power and Energy Systems*, vol. 126, pp. 1-11, Mar. 2021.
[45] K. Andras, "On the computational complexity of tariff optimization for demand response management," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 3204-3206, May 2018.
[46] V. S. K. Balijepalli, V. Pradhan, S. A. Khaparde *et al.*, "Review of demand response under smart grid paradigm," in *Proceedings of 2011 IEEE PES Innovative Smart Grid Technologies*, Kollam, India, Dec. 2011, pp. 1-8.
[47] M. Alizadeh, X. Li, Z. Wang *et al.*, "Demand-side management in the smart grid: information processing for the power switch," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 55-67, Sept. 2012.
[48] S. Yilmaz, X. Xu, D. Cabrera *et al.*, "Analysis of demand-side response preferences regarding electricity tariffs and direct load control: key findings from a swiss survey," *Energy*, vol. 212, pp. 1-12, Dec. 2020.
[49] J. Ma, S. Zhang, L. Wu *et al.*, "Probabilistic evaluations on marginal price and capacity adequacy of power systems with price-elastic demand," *Electric Power Systems Research*, vol. 194, pp. 1-9, May 2021.
[50] S. Koloushani, M. Nasri, and M. Rezaei, "Strategic management of stochastic power losses in smart transmission grids," *International Transactions on Electrical Energy Systems*, vol. 29, no. 8, pp. 1-18, Aug. 2019.
[51] M. Delghavi and A. Yazdani, "Sliding-mode control of AC voltages and currents of dispatchable distributed energy resources in master-slave-organized inverter-based microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 980-991, Jan. 2019.
[52] H. Nazaripouya, H. Pota, C. Chu *et al.*, "Real-time model-free coordination of active and reactive powers of distributed energy resources to improve voltage regulation in distribution systems," *IEEE Transactions on Sustainable Energy*, vol. 11, no. 3, pp. 1483-1494, Jul. 2020.
[53] L. Subramanian, V. Debusschere, H. Gooi *et al.*, "A distributed model predictive control framework for grid-friendly distributed energy resources," *IEEE Transactions on Sustainable Energy*, vol. 12, no. 1, pp. 727-738, Jan. 2020.
[54] Z. Yi, Y. Xu, W. Gu *et al.*, "Distributed model predictive control based secondary frequency regulation for a microgrid with massive distributed resources," *IEEE Transactions on Sustainable Energy*, vol. 12, no. 2, pp. 1078-1089, Apr. 2021.
[55] A. Joshi, A. Suresh, and S. Kamalasadan, "Grid frequency regulation based on point of common coupling angle deviation control of distributed energy resources with fully active hybrid energy storage system," *IEEE Transactions on Industry Applications*, vol. 57, no. 5, pp. 4473-4485, Sept. 2021.
[56] X. Han, H. Heussen, O. Gehrke *et al.*, "Taxonomy for evaluation of distributed control strategies for distributed energy resources," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 5185-5195, Sept. 2018.
[57] Y. Zhang, W. Chen, and W. Gao, "A survey on the development status and challenges of smart grids in main driver countries," *Renewable and Sustainable Energy Reviews*, vol. 79, pp. 137-147, Nov. 2017.
[58] V. Venkataramanan, A. Hahn, and A. Srivastava, "CP-SAM: cyber-physical security assessment metric for monitoring microgrid resiliency," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1055-1065, Mar. 2020.
[59] T. Huang, Q. Guo, H. Sun *et al.*, "A deep spatial-temporal data-driven approach considering microclimates for power system security assessment," *Applied Energy*, vol. 237, pp. 36-48, Mar. 2019.
[60] R. Hassan, C. Li, and Y. Liu, "Online dynamic security assessment of wind integrated power system using SDAE with SVM ensemble boosting learner," *Electrical Power and Energy Systems*, vol. 135, pp. 1-9, Feb. 2021.
[61] X. Wei, S. Gao, T. Huang *et al.*, "Complex network-based cascading faults graph for the analysis of transmission network vulnerability," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1265-1276, Mar. 2019.
[62] R. Leszczyna, "Standards on cyber security assessment of smart grid," *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 70-89, Sept. 2018.
[63] Y. Chen, J. Hong, and C. Liu, "Modeling of intrusion and defense for assessment of cyber security at power substations," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2541-2552, Jul. 2018.
[64] Q. Ai-Gburi and M. Ariff, "Dynamic security assessment for power system under cyber-attack," *Journal of Electrical Engineering & Technology*, vol. 14, pp. 549-559, Mar. 2019.
[65] K. Pan, A. Pan, M. Cvetkovic *et al.*, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3044-3056, May 2019.
[66] H. Maziku, S. Shetty, and D. Nicol, "Security risk assessment for SDN-enabled smart grids," *Computer Communications*, vol. 133, pp. 1-11, Jan. 2019.
[67] C. Sun, A. Hahn, and C. Liu, "Cyber security of a power grid: state-of-the-art," *Computer Communications*, vol. 5, no. 3, pp. 45-56, Jul. 2018.
[68] E. Padilla, K. Agbossou, and A. Cardenas, "Towards smart integration of distributed energy resources using distributed network protocol over ethernet," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1686-1695, Jul. 2014.
[69] M. Urbina, A. Astarloa, J. Lazaro *et al.*, "CPPS gateway: implementation of modbus and profibus on a programmable SoC platform," *IEEE Latin America Transactions*, vol. 16, no. 2, pp. 335-341, Feb. 2018.
[70] S. Khan, M. Alam, Y. Moullec *et al.*, "An empirical modeling for the baseline energy consumption of an NB-IoT radio transceiver," *IEEE Internet of Things Journal*, vol. 8, no. 19, pp. 14756-14772, Oct. 2021.
[71] B. Hu and H. Gharavi, "A hybrid wired/wireless deterministic network for smart grid," *IEEE Wireless Communications*, vol. 28, no. 3, pp. 138-143, Jun. 2021.

[72] W. Li and X. Zhang, "Simulation of the smart grid communications: challenges, techniques, and future trends," *Computers and Electrical Engineering*, vol. 40, no. 1, pp. 270-288, Jan. 2014.
[73] S. Lyngaas. (2020, Jun.). Utah renewables company was hit by rare cyberattack in March. CyberScoop. [Online]. Available: https://www.cyberscoop.com/spower-power-grid-cyberattack-foia/
[74] Y. Song, X. Liu, Z. Li *et al.*, "Intelligent data attacks against power systems using incomplete network information: a review," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 4, pp. 630-641, Jul. 2018.
[75] C. Konstantinou and M. Maniatakos, "Hardware-layer intelligence collection for smart grid embedded systems," *Journal of Hardware and Systems Security*, vol. 3, pp. 132-146, Jan. 2019.
[76] A. Huseinovic, S. Mrdovic, and K. Bicakci, "A taxonomy of the emerging denial-of-service attacks in the smart grid and countermeasures," in *Proceeding of 2018 26th Telecommunications Forum*, Belgrade, Serbia, Nov. 2018, pp. 285-288.
[77] C. Ge, L. Zhou, G. Hancke *et al.*, "A provenance-aware distributed trust model for resilient unmanned aerial vehicle networks," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12481-12489, Aug. 2021.
[78] L. Song, A. Striegel, and A. Mohammed, "Sniffing only control packets: a lightweight client-side WiFi traffic characterization solution," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6536-6548, Apr. 2021.
[79] R. Khan, K. McLaughlin, J. Hastings *et al.*, "Demonstrating cyber-physical attacks and defense for synchrophasor technology in smart grid," in *Proceeding of 2018 16th Annual Conference on Privacy, Security and Trust*, Belfast, Ireland, Aug. 2018, pp. 257-266.
[80] L. Hu, Z. Wang, Q. Han *et al.*, "State estimation under false data injection attacks: security analysis and system protection," *Automatica*, vol. 87, pp. 176-183, Jan. 2018.
[81] L. An and G. Yang, "Distributed secure state estimation for cyber-physical systems under sensor attacks," *Automatica*, vol. 107, pp. 526-538, Jan. 2019.
[82] F. Miao, M. Pajic, and G. Pappas, "Stochastic game approach for replay attack detection," in *Proceeding of 52nd IEEE Conference on Decision and Control*, Firenze, Italy, Dec. 2013, pp. 1854-1859.
[83] X. Li, C. Jiang, D. Du *et al.*, "Optimization and control of cyber-physical power systems under dual-network interactive cascading failure," *Control Engineering Practice*, vol. 111, p. 104789, Jun. 2021.
[84] Y. Zhang and O. Yagan, "Robustness of interdependent cyber-physical systems against cascading failures," *IEEE Transactions on Automatic Control*, vol. 65, no. 2, pp. 711-726, Feb. 2020.
[85] Y. Cai, Y. Cao, Y. Li *et al.*, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 530-538, Jan. 2016.
[86] J. Chen, G. Liang, Z. Cai *et al.*, "Impact analysis of false data injection attacks on power system static security assessment," *Journal of Modern Power Systems and Clean Energy*, vol. 4, no. 3, pp. 496-505, Jul. 2016.
[87] X. Shangguan, Y. He, C. Zhang *et al.*, "Switching system-based load frequency control for multi-area power system resilient to denial-of-service attacks," *Control Engineering Practice*, vol. 107, p. 104678, Feb. 2021.
[88] M. Rahman, M. Rana, and H. Pota, "Mitigation of frequency and voltage disruptions in smart grid during cyber-attack," *Journal of Control, Automation and Electrical Systems*, vol. 31, no. 2, pp. 412-421, Apr. 2020.
[89] Y. Liu, T. Liu, H. Sun *et al.*, "Hidden electricity theft by exploiting multiple-pricing scheme in smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2453-2468, Jan. 2020.
[90] A. Takiddin, M. Ismail, U. Zafar *et al.*, "Robust electricity theft detection against data poisoning attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2675-2684, May 2020.
[91] A. Tajer, "False data injection attacks in electricity markets by limited adversaries: stochastic robustness," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 128-138, Jan. 2019.
[92] J. Wu, B. Fang, J. Fang *et al.*, "Sequential topology recovery of complex power systems based on reinforcement learning," *Physica A: Statistical Mechanics and its Applications*, vol. 535, pp. 1-13, Dec. 2019.
[93] L. Lee and P. Hu, "Vulnerability analysis of cascading dynamics in smart grids under load redistribution attacks," *Electrical Power and Energy Systems*, vol. 111, pp. 182-190, Oct. 2019.
[94] A. Rouhani and A. Abur, "Linear phasor estimator assisted dynamic state estimation," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 211-219, Jan. 2018.
[95] J. Duan, W. Zeng, and M. Y. Chow, "Resilient distributed DC optimal power flow against data integrity attack," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3543-3552, Jul. 2018.
[96] L. Sun, T. Chen, X. Chen *et al.*, "Optimum placement of phasor measurement units in power systems," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 2, pp. 421-429, Feb. 2019.
[97] I. Lukicheva, D. Pozo, and A. Kulikov, "Cyberattack detection in intelligent grids using non-linear filtering," in *proceeding of 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe*, Sarajevo, Bosnia and Herzegovina, Oct. 2018, pp. 257-262.
[98] Y. Chen, F. Huang, F. Liu *et al.*, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2158-2169, Mar. 2019.
[99] R. Moslemi, A. Mesbahi, and J. Velni, "A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4930-49419, Sept. 2018.
[100] R. Chen, X. Li, H. Zhong *et al.*, "A novel online detection method of data injection attack against dynamic state estimation in smart grid," *Neurocomputing*, vol. 344, pp. 73-81, Jun. 2019.
[101] H. Khalid and J. Peng, "Immunity toward data-injection attacks using multisensor track fusion-based model prediction," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 697-707, Mar. 2017.
[102] M. Kurt, Y. Yilmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 498-513, Feb. 2019.
[103] Y. Chakhchoukh, H. Lei, and B. Johnson, "Diagnosis of outliers and cyber attacks in dynamic PMU-based power state estimation," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1188-1197, Mar. 2020.
[104] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad *et al.*, "Resilient control design for load frequency control system under false data injection attacks," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 9, pp. 7951-7962, Sept. 2020.
[105] X. Li, Z. Wang, C. Zhang *et al.*, "A novel dynamic watermarking-based EKF detection method for FDIAs in smart grid," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, pp. 1-4, Mar. 2022.
[106] K. Miao, W. Zhang, and X. Qiu, "An adaptive unscented Kalman filter approach to secure state estimation for wireless sensor networks," *Asian Journal of Control*. doi:10.1002/asjc.2783
[107] N. Zivkovic and A. Saric, "Detection of false data injection attacks using unscented Kalman filter," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 847-859, Sept. 2018.
[108] M. Kurt, Y. Yilmaz, and X. Wang, "Secure distributed dynamic state estimation in wide-area smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 800-815, Jul. 2020.
[109] C. Liang, F. Wen, and Z. Wang, "Trust-based distributed Kalman filtering for target tracking under malicious cyber attacks," *Information Fusion*, vol. 46, pp. 44-50, Mar. 2019.
[110] F. Wen and Z. Wang, "Distributed Kalman filtering for robust state estimation over wireless sensor networks under malicious cyber attacks," *Digital Signal Processing*, vol. 78, pp. 92-97, Jul. 2018.
[111] M. Kurt, Y. Yilmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2015-2030, Aug. 2018.
[112] H. Wang, G. Ruan, G. Wang *et al.*, "Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4766-4778, Nov. 2018.
[113] H. Wang, J. Ruan, Z. Ma *et al.*, "Deep learning aided interval state prediction for improving cyber security in energy internet," *Energy*, vol. 174, pp. 1292-1304, May 2019.
[114] H. Wang, A. Meng, Y. Liu *et al.*, "Unscented Kalman filter based interval state estimation of cyber physical energy system for detection of dynamic attack," *Energy*, vol. 188, pp. 1-15, Dec. 2019.
[115] H. Wang, J. Ruan, B. Zhou *et al.*, "Dynamic data injection attack detection of cyber physical power systems with uncertainties," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 10, pp. 5505-5518, Oct. 2019.
[116] T. Yang, C. Murguia, M. Kuijper *et al.*, "An unknown input multiobserver approach for estimation and control under adversarial attacks," *IEEE Transactions on Control of Network System*, vol. 8, no. 1, pp. 475-486, Mar. 2021.
[117] Y. Li, J. Li, X. Luo *et al.*, "Cyber attack detection and isolation for smart grids via unknown input observer," in *Proceedings of 2018 37th Chinese Control Conference*, Wuhan, China, Jul. 2018, pp. 6207-6212.
[118] A. Ameli, A. Hooshyar, F. El-Saadany *et al.*, "Attack detection and

identification for automatic generation control systems," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 4760-4774, Sept. 2018.
[119] X. Wang, X. Luo, M. Zhang *et al.*, "Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers," *International Journal of Electrical Power and Energy Systems*, vol. 110, pp. 208-222, Sept. 2019.
[120] Z. Wang, Y. Zhao, K. Yang *et al.*, "UIO-based cyber attack detection and mitagation scheme for load frequency control system," in *Proceedings of 2019 3rd International Conference on Electronic Information Technology and Computer Engineering*, Xiamen, China, Oct. 2019, pp. 1257-1262.
[121] Z. Kazemi, A. Safavi, F. Naseri *et al.*, "A secure hybrid dynamic-state estimation approach for power systems under false data injection attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7275-7286, Dec. 2020.
[122] A. Gallo, M. Turan, F. Boem *et al.*, "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3800-3815, Sept. 2020.
[123] X. Wang, X. Luo, M. Zhang *et al.*, "Detection of false data injection attack in smart grids via interval observer," in *Proceedings of 2019 Chinese Control and Decision Conference*, Nanchang, China, Jun. 2019, pp. 3238-3243.
[124] A. Ameli, A. Hooshyar, A. Yazdavar *et al.*, "Attack detection for load frequency control systems using stochastic unknown input estimators," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2575-2590, Oct. 2018.
[125] X. Luo, X. Wang, M. Zhang *et al.*, "Distributed detection and isolation of bias injection attack in smart energy grid via interval observer," *Applied Energy*, vol. 256, pp. 1-19, Dec. 2019.
[126] X. Wang, X. Luo, M. Zhang *et al.*, "Detection and localization of biased load attacks in smart grids via interval observer," *Information Sciences*, vol. 552, pp. 291-309, Apr. 2021.
[127] M. Rahman and M. Alam, "Imperfect nonlinear false data injection attack against largest normalized residual test," in *Proceedings of 2019 IEEE PES General Meeting*, Atlanta, USA, Aug. 2019, pp. 1-5.
[128] B. Danda and B. Chandra, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652-1656, Oct. 2015.
[129] H. Poor, *An Introduction to Signal Detection and Estimation.* New York: Springer-Verlag, 1994.
[130] J. Zhang and X. Wang, "Low-complexity quickest change detection in linear systems with unknown time-varying pre- and post-change distributions," *IEEE Transactions on Information Theory*, vol. 67, no. 3, pp. 1804-1824, Mar. 2021.
[131] R. Nawaz, R. Akhtar, M. Shahid *et al.*, "Machine learning based false data injection in smart grid," *International Journal of Electrical Power and Energy Systems*, vol. 130, pp. 1-12, Sept. 2021.
[132] D. Wang, X. Wang, Y. Zhang *et al.*, "Detection of power grid disturbances and cyber-attacks based on machine learning," *Journal of Information Security and Applications*, vol. 46, pp. 42-52, Jun. 2019.
[133] R. Punmiya and S. Choe, "Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 2326-2329, Mar. 2019.
[134] R. Razavi, A. Gharipour, M. Fleury *et al.*, "A practical feature-engineering framework for electricity theft detection in smart grids," *Applied Energy*, vol. 238, pp. 481-494, Mar. 2019.
[135] M. Cui, J. Wang and M. Yue, "Machine learning-based anomaly detection for load forecasting under cyber attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5724-5734, Nov. 2019.
[136] K. Vimalkumar and N. Radhika, "A big data framework for intrusion detection in smart grids using apache spark," in *Proceedings of 2017 International Conference on Advances in Computing, Communications and Informatics*, Udupi, India, Sept. 2017, pp. 198-204.
[137] J. Han, C. Moraga, and S. Sinne, "Optimization of feedforward neural networks," *Engineering Applications of Artificial Intelligence*, vol. 9, no. 2, pp. 109-119, Apr. 1996.
[138] S. Wang, M. Roger, J. Sarrazin *et al.*, "Hyperparameter optimization of two-hidden-layer neural networks for power amplifiers behavioral modeling using genetic algorithms," *IEEE Microwave and Wireless Components Letters*, vol. 29, no. 12, pp. 802-805, Dec. 2019.
[139] M. Albahar and M. Binsawad, "Deep autoencoders and feedforward networks based on a new regularization for anomaly detection," *Security and Communication Networks*, vol. 2020, pp. 1-9, Jul. 2020.
[140] Y. Wang, W. Shi, Q. Jin *et al.*, "An accurate false data detection in smart grid based on residual recurrent neural network and adaptive threshold," in *Proceedings of 2019 IEEE International Conference on Energy Internet*, Nanjing, China, May 2019, pp. 1-6.
[141] A. Ayad, H. Farag, A. Youssef *et al.*, "Detection of false data injection attacks in smart grids using recurrent neural networks," in *Proceedings of 2018 IEEE PES Innovative Smart Grid Technologies Conference*, Washington DC, USA, Feb. 2018, pp. 1-5.
[142] M. Ismail, M. Shaaban, M. Naidu *et al.*, "Deep learning detection of electricity theft cyber-attacks in renewable distributed generation," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3428-3437, Jul. 2020.
[143] J. Gao, L. Gan, F. Buschendorf *et al.*, "Omni SCADA intrusion detection using deep learning algorithms," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 951-961, Jan. 2021.
[144] R. SaiSindhuTheja and G. Shyam, "An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment," *Applied Soft Computing Journal*, vol. 100, pp. 1-11, Mar. 2021.
[145] S. Yoon and H. Yu, "Multiple points input for convolutional neural networks in replay attack detection," in *Proceedings of 2020 IEEE International Conference on Acoustics, Speech and Signal Processing*, Barcelona, Spain, May 2020, pp. 6444-6448.
[146] M. Zanetti, E. Jamhour, M. Pellenz *et al.*, "A tunable fraud detection system for advanced metering infrastructure using short-lived patterns," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 830-840, Jan. 2019.
[147] S. Ahmed, Y. Lee, S. Hyun *et al.*, "Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2765-2777, Oct. 2019.
[148] J. Wang, D. Shi, Y. Li *et al.*, "Distributed framework for detecting PMU data manipulation attacks with deep autoencoders," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4401-4410, Jul. 2019.
[149] M. Aboelwafa, K. Seddik, M. Eldefrawy *et al.*, "A machine-learning-based technique for false data injection attacks detection in industrial IoT," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8462-8471, Sept. 2020.
[150] K. Lu, G. Zeng, X. Luo *et al.*, "Evolutionary deep belief network for cyber-attack detection in industrial automation and control system," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7618-7627, Nov. 2021.
[151] I. Sohn, "Deep belief network based intrusion detection techniques: a survey," *Expert Systems with Applications*, vol. 167, pp. 1-9, Apr. 2021.
[152] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: a semi-supervised deep learning approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623-634, Jan. 2021.
[153] M. Farajzadeh-Zanjani, E. Hallaji, R. Razavi-Far *et al.*, "Adversarial semi-supervised learning for diagnosing faults and attacks in power grids," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3468-3478, Jul. 2021.
[154] M. Abdel-Basset, H. Hawash, R. Chakrabortty *et al.*, "Semi-supervised spatiotemporal deep learning for intrusions detection in IoT networks," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12251-12265, Aug. 2021.
[155] T. Zheng, Y. Liu, Y. Yan *et al.*, "RSSPN: robust semi-supervised prototypical network for fault root cause classification in power distribution systems," *IEEE Transactions on Power Delivery.* doi: 10.1109/TPWRD.2021.3125704.
[156] J. Tian, R. Tan, X. Guan *et al.*, "Enhanced hidden moving target defense in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2208-2223, Mar. 2019.
[157] C. Chen, M. Cui, X. Fang *et al.*, "Load altering attack-tolerant defense strategy for load frequency control system," *Applied Energy*, vol. 280, pp. 1-14, Dec. 2020.
[158] A. Abusorrah, A. Alabdulwahab, Z. Li *et al.*, "Minimax-regret robust defensive strategy against false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2068-2079, Mar. 2019.
[159] S. Hasan, A. Dubey, G. Dubey *et al.*, "A game-theoretic approach for power systems defense against dynamic cyber-attacks," *International Journal of Electrical Power and Energy Systems*, vol. 115, pp. 1-13, Feb. 2020.
[160] A. Ferdowsi, W. Saad, and N. Mandayam, "Colonel blotto game for sensor protection in interdependent critical infrastructure," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2857-2874, Feb. 2021.
[161] Z. Wang, D. Jiang, F. Wang *et al.*, "A polymorphic heterogeneous security architecture for edge-enabled smart grids," *Sustainable Cities and Society*, vol. 67, pp. 1-16, Apr. 2021.
[162] Y. Xiang and L. Xiang, "An improved defender-attacker-defender model for transmission line defense considering offensive resource uncer-

tainties," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2534-2546, May 2019.
[163] W. Shi, Y. Wang, Q. Jin *et al.*, "PDL: an efficient prediction-based false data injection attack detection and location in smart grid," in *Proceedings of 2018 IEEE 42nd Annual Computer Software and Applications Conference*, Tokyo, Japan, Jul. 2018, pp. 676-681.
[164] X. Luo, X. Wang, X. Pan *et al.*, "Detection and isolation of false data injection attack for smart grids via unknown input observers," *IET Generation Transmission and Distribution*, vol. 13, no. 8, pp. 1277-1286, Apr. 2019.
[165] X. Wang, X. Luo, M. Zhang *et al.*, "Detection and isolation of false data injection attacks in smart grid via unknown input interval observer," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3214-3229, Apr. 2020.
[166] X. Wang, X. Luo, M. Zhang *et al.*, "Detection and isolation of false data injection attacks in smart grid via nonlinear interval observer," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6498-6512, Aug. 2019.
[167] J. Jiang, J. Wu, C. Long *et al.*, "Location of false data injection attacks in power system," in *Proceedings of 2019 Chinese Control Conference*, Guangzhou, China, Jul. 2019, pp. 7473-7478.
[168] H. Wang, X. Wen, S. Huang *et al.*, "Generalized attack separation scheme in cyber physical smart grid based on robust interval state estimation," in *Proceedings of International Journal of Electrical Power and Energy Systems*, vol. 129, pp. 1-11, Jul. 2021.
[169] A. Farraj, E. Hammad, and D. Kundur, "A distributed control paradigm for smart grid to address attacks on data integrity and availability," *IEEE Transactions on Signal and Information Processing over Network*, vol. 4, no. 1, pp. 70-81, Mar. 2018.
[170] M. Rahman, M. Rana, and H. Pota, "Mitigation of frequency and voltage disruptions in smart grid during cyber-attack," *Journal of Control, Automation and Electrical Systems*, vol. 31, pp. 412-421, Apr. 2020.
[171] F. Wei, Z. Wang, and H. He, "Cyber-attack recovery strategy for smart grid based on deep reinforcement learning," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2476-2486, May 2020.
[172] H. Wang, X. Wen, Y. Xu *et al.*, "Operating state reconstruction in cyber physical smart grid for automatic attack filtering," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 2909-2922, May 2022.
[173] M. Khalaf, A. Youssef, and E. El-Saadany, "Joint detection and mitigation of false data injection attacks in AGC systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 4985-4995, Sept. 2019.
[174] D. Du, X. Li, W. Li *et al.*, "ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1698-1711, Aug. 2019.
[175] A. Tummala and R. Inapakurthi, "A two-stage Kalman filter for cyber-attack detection in automatic generation control system," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 1, pp. 50-59, Jan. 2022.

Dajun Du received the B.Sc. degree in electrical technology, the M.Sc. degree in control theory and control engineering from Zhengzhou University, Zhengzhou, China, in 2002 and 2005, respectively, and the Ph.D. degree in control theory and control engineering from Shanghai University, Shanghai, China, in 2010. From September 2008 to September 2009, he was a Visiting Ph.D. Student at Queen's University Belfast, Belfast, UK. From April 2011 to August 2012, he was a Research Fellow at Queen's University Belfast. He is currently a Professor in Shanghai University. His main research interests include system modelling and identification and networked control systems.

Minggao Zhu received the B.Sc. degree in industrial automation from Nanjing University of Science and Technology Taizhou College, Taizhou, China, in 2016, and the M.Sc. degrees in control theory and control engineering from Yanshan University, Hebei, China, in 2019. He is currently pursuing the Ph.D. degree in control theory and control engineering in Shanghai University. His main research interests include cyber security of cyber-physical power systems and state estimation.

Xue Li received the B.Sc. degree in electrical technology, the M.Sc. degree in power system and automation from Zhengzhou University, Zhengzhou, China, in 2002 and 2006, respectively, and the Ph.D. degree in control theory and control engineering from Shanghai University, Shanghai, China, in 2009. She is currently a Professor in Shanghai University. Her main research interests include security control and performance assessment of smart grids.

Minrui Fei received the B.S. and M.S. degrees in industrial automation from the Shanghai University of Technology, Shanghai, China, in 1984 and 1992, respectively, and the Ph.D. degree in control theory and control engineering from Shanghai University, Shanghai, China, in 1997. Since 1998, he has been a full Professor at Shanghai University. He is Chairman of Embedded Instrument and System Sub-society, and Standing Director of China Instrument & Control Society, Chairman of Life System Modeling and Simulation Sub-society, Vice-chairman of Intelligent Control and Intelligent Management Sub-society, and Director of Chinese Artificial Intelligence Association. His research interests include networked control systems, intelligent control, complex system modeling, hybrid network systems, and field control systems.

Siqi Bu received the Ph.D. degree from the electric power and energy research cluster, The Queen's University of Belfast, Belfast, UK, where he continued his postdoctoral research work before entering industry. Then he was with National Grid UK as an experienced UK National Transmission System Planner and Operator. He is an Associate Professor with The Hong Kong Polytechnic University, Hong Kong, China, and also a Chartered Engineer with UK Engineering Council, London, UK. His research interests include power system stability analysis and operation control, considering renewable energy integration and smart grid application.

Lei Wu received the B.Sc. degree in electrical engineering, the M.Sc. degree in systems engineering from Xi'an Jiaotong University, Xi'an, China, in 2001 and 2004, respectively, and the Ph.D. degree in electrical engineering from Illinois Institute of Technology (IIT), Chicago, USA, in 2008. From 2008 to 2010, he was a Senior Research Associate with the Robert W. Galvin Center for Electricity Innovation, IIT. He was a summer Visiting Faculty at New York Independent System Operator in 2012. He was a Professor with the Electrical and Computer Engineering Department, Clarkson University, Potsdam, USA, till 2018. He is currently a Professor with the Electrical and Computer Engineering Department, Stevens Institute of Technology, Hoboken, USA. His research interests include power system operation and planning, energy economics, and community resilience microgrid.

Kang Li received the B.Sc. degree in industrial automation from Xiangtan University, Xiangtan, China, in 1989, the M.Sc. degree in control theory and applications from the Harbin Institute of Technology, Harbin, China, in 1992, and the Ph.D. degree in control theory and applications from Shanghai Jiao Tong University, Shanghai, China, in 1995. Between 1995 and 2012, he was with Shanghai Jiao Tong University, Delft University of Technology, Delft, the Netherlands, and Queen's University Belfast, Belfast, UK, as a Research Fellow. In 2002, he joined Queen's University Belfast, as a Lecturer, and became a Senior Lecturer in 2007 and a Reader in 2009 with the School of Electronics, Electrical Engineering and Computer Science, and he has been a Professor since 2011. He is currently a Full Professor with Leeds University in 2019. He is the author or co-author of more than 200 articles, and edited or coedited more than 10 conference proceedings. His research interests include nonlinear system modeling, identification, and control, and bio-inspired computational intelligence, with applications to energy and power systems, smart grids, electric vehicles, and polymer processing, with focus on the development of advanced control technologies for decarbonizing the whole energy systems from head to tail, including a new generation of low-cost minimal-invasive monitoring system and intelligent control platform for energy intensive industries.