IEEE Access
The journal for rapid open access publishing

IEEE Xplore
Digital Library
http://ieeexplore.ieee.org/Xplore

Smart Grid Cyber-Physical Attack and Defense: A Review

HANG ZHANG[1], *Student Member, IEEE*, BO LIU[1], *Student Member, IEEE*, HONGYU WU[1],*SENIOR MEMBER, IEEE*

Abstract*—ecent advances in the cyber-physical smart grid (CPSG) have enabled a broad range of new devices based on the information and communication technology (ICT). However, these ICT-enabled devices are susceptible to a growing threat of cyber-physical attacks. This paper performs a thorough review of the state-of-the-art cyber-physical security of the smart grid. By focusing on the physical layer of the CPSG, this paper provides an abstracted and unified state-space model, in which cyber-physical attack and defense models can be effectively generalized. The existing cyber-physical attacks are categorized in terms of their target components. We then discuss several operational and informational defense approaches that present the current state-of-the-art in the field, including moving target defense, watermarking, and data-driven approaches. Finally, we discuss challenges and future opportunities associated with the smart grid cyber-physical security.*ecent advances in the cyber-physical smart grid (CPSG) have enabled a broad range of new devices based on the information and communication technology (ICT). However, these ICT-enabled devices are susceptible to a growing threat of cyber-physical attacks. This paper performs a thorough review of the state-of-the-art cyber-physical security of the smart grid. By focusing on the physical layer of the CPSG, this paper provides an abstracted and unified state-space model, in which cyber-physical attack and defense models can be effectively generalized. The existing cyber-physical attacks are categorized in terms of their target components. We then discuss several operational and informational defense approaches that present the current state-of-the-art in the field, including moving target defense, watermarking, and data-driven approaches. Finally, we discuss challenges and future opportunities associated with the smart grid cyber-physical security.R**

***Index Terms*—Cyber-physical power system, cyber-physical security, false data injection, dynamic watermarking, moving target defense.**

I. Introduction

CYBER-PHYSICAL systems (CPSs) are smart systems that include engineered interacting networks of physical and computational components [1]. The comprehensively interconnected and integrated systems contribute new functionalities to enable technological development in critical infrastructures, such as electric power systems, water networks, transportation, home automation, and health care. A CPS encompasses complex systems of control, awareness, computing, and communication. The complexity and heterogeneity have indicated the potential challenges to the security and resilience of CPSs. The interconnection of bulk physical layer components is challenging the protection against inherent physical vulnerabilities therein. On the other hand, cyber-integration, which relies on network communication and the internet of things (IoT) based devices, requires extraordinary investments in security designs and upgrades against unanticipated threats from cyberspace [2]. A cyber-physical attack is defined as a security breach in cyberspace that adversely affects the physical space of a CPS. [3]. Cyber-physical attacks compromise the confidentiality, integrity, and availability of information by coupling cyber and physical spaces in a CPS. In the past decades, several noteworthy cyber-physical attacks have been reported in the industry, facilitating synergistic efforts from industry practitioners and research communities towards a new CPS security era [4]. The first proclaimed cyber-physical attack dated back to 1982 in the Siberian wilderness, where attackers manipulated the pipeline control software, which led the valves' control to misbehave, resulting in severe crossing of pressure limits and eventually a massive explosion [5]. In 2003, the Slammer worm invaded the control system of the David-Besse nuclear plant in Ohio through a contractor's network, which disabled the supervisory system for 5 hours [6]. In June 2010, a cyber worm dubbed Stuxnet struck the Iranian nuclear fuel enrichment plant by utilizing four zero-day vulnerabilities and digitally signed certificates to bypass intrusion detection. The targets were the programmable logic controllers in the supervisory control and data acquisition (SCADA) system [7]. The Stuxnet maliciously alternated the frequency of electrical current powering the centrifuges and then switched them between high and low speeds at intervals for which the machines were not designed [8]. In December 2015, a coordinated cyberattack compromised three Ukrainian electric power distribution companies. Thirty substations suffered blackout for about three hours, resulting in wide-area power outages affecting approximately 225,000 customers. BlackEnergy3 malware was used to steal the authorized users' virtual private network credentials, and a telephonic denial-of-service (DoS) attack was executed to frustrate reports of outages [9].

The smart grid landscape, arguably one of the most complex CPSs in history, is undergoing a radical transformation. Particularly, increased renewable energy resources, demand diversification, and integration of information and communication technologies (ICTs) [10]. The cyber-physical smart grid (CPSG) that has organized a universal cyberinfrastructure interwoven with the bulk physical systems is susceptible to cyber-physical attacks. A wide variety of motivations exist

[1]The Mike Wiegers Department of Electrical and Computer Engineering, Kansas State University, Manhattan, KS 66506 USA

This material is based upon work supported in part by the U.S. National Science Foundation under Grant No. 1929147, and in part by the U.S. Department of Energy under Award No. DE-EE0008767.

Corresponding author: Hongyu Wu (e-mail: hongyuwu@ksu.edu).

Digital Object Identifier: 10.1109/ACCESS.2021.3058628

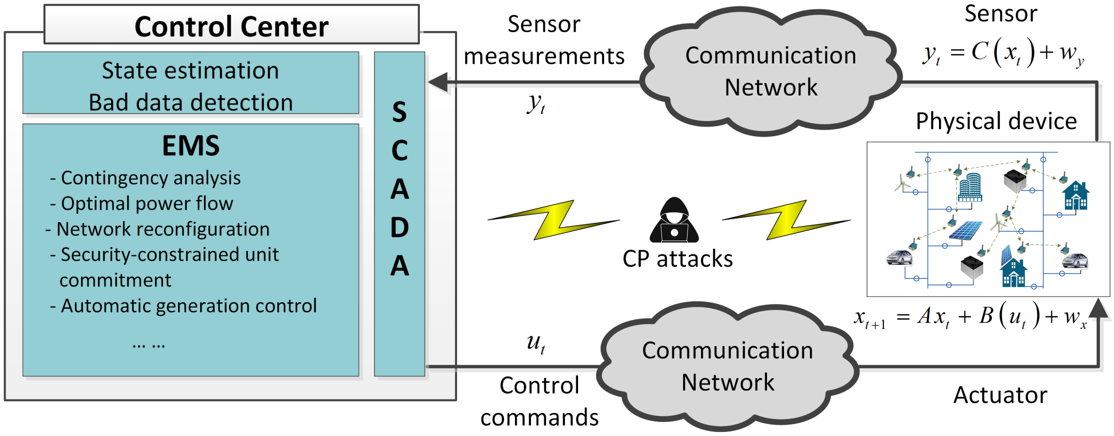


Fig. 1: Illustration of cyber-physical attacks on smart grid. This paper focuses on reviewing attacks that target either the EMS within the control center or physical devices in the field. Defense mechanisms against those attacks are also discussed.

for launching such an attack in the smart grid, ranging from economic reasons, to terrorism, to a grudge (a disgruntled employee [11]). A large body of recent work has been dedicated to addressing the cyber-physical security of smart grids, with many warnings becomes prominent [12]–[15] and new vulnerabilities are continuously unveiled [16]. Regarding cyber and physical security, neither of them alone can provide broad solutions without incorporating the other. In this regard, the investigations of the cyber-physical attacks and the developments of effective defense strategies are still incomprehensive. Thereby, it has become paramount to keep up with the latest progress along the research frontier of smart grid security, especially from a joint perspective of cyber and physical security.

This paper tries to bridge this gap by providing a comprehensive review of cyber-physical threat models and defense mechanisms. Over the last five years, several survey and review papers on the cyber-physical security of the smart grid have been published. Table I lists a comparison between this paper and other works in terms of the publication year, smart grid models, attack taxonomy, technological focus, challenges and opportunities, and the review scope.

The contributions of this paper, as illustrated in Table 1, are four-fold. First, a discrete-time nonlinear time-invariant system is proposed to represent a CPSG by using the state-space representation. Such a high-level abstraction is a useful strategy to form the foundation and generalize a defense analysis across all attack types. Second, the state-of-the-art cyber-physical attack models are summarized based on the proposed abstraction and categorized according to the control-feedback loop segment each attack involves. This new taxonomy provides the grid operator with intuitive situational awareness on how to enhance the system's cyber-physical security. Third, cyber-physical security of the smart grid is an extremely hot research topic, and a lot of good works have been published every year. Therefore, it is a much needed effort to keep up with the progress and furnish a concise summary and a clear categorization for readers to understand the current state-of-the-art. In order to provide a timely review, this paper surveys the most recent publications, including 78 in the last five years (i.e., 2016-2020) 49 of which were published in the past three years (i.e., 2018-2020). A thorough review of the cutting-edge defense approaches such as data-driven machine learning, moving target defense, and watermarking is provided. Finally, the challenges and opportunities of future CPSGs are discussed, which may shed light on cyber-physical security issues that the next-generation smart grid needs to tackle.

The remainder of this paper is organized as follows. The unified cyber-physical security model of the smart grid is proposed in Section II. The current state-of-the-art in attack models and defense mechanisms are surveyed in Sections III and IV, respectively. The challenges and opportunities with respect to the cyber-physical security of the smart grid are discussed in Section V. The concluding remarks are drawn in Section VI.

II. Smart Grid Cyber-Physical Security

A. *State-space representation of power grid control model*

A CPSG is a monolithic system with electricity generation, transmission, and distribution sectors [27]. The physical systems are interconnected through transmission lines and substations deployed in the field. The integration and coordination of heterogeneous components require reliable capabilities on information, computation, and communication. These requirements rely on a ubiquitous cyberinfrastructure interwoven with the physical systems. Measurements and commands are constantly generated and transmitted through communication channels. A CPSG consists of physical devices, actuators, sensors, communication channels, and a centralized control center equipped with a state estimator, a bad data detector, and an energy management system (EMS), as shown in Fig. 1.

We describe the CPSG as a discrete-time nonlinear time-invariant system by using a state-space representation as follows:

$$x_{t+1} = A(x_t) + B(u_t) + w_t \tag{1}$$

TABLE I: A Comparison of Related Literature

Ref.-Yr	CPSG model	Taxonomy	Attack types	Challenge and opportunity	Scope (attack or defense)	Technological focus
[17]-2015	Conceptual model	N/A	DoS	Yes	Both attack and defense	Informational
[18]-2015	Conceptual model	Layers (physical, MAC, network, application)	CIA triad attacks	Yes	Attack only	Both informational and operational
[19]-2016	N/A	CPSG components	CIA triad attacks	No	Attack only	Informational
[20]-2016	Abstract model	Security objectives (Confidentiality, integrity, availability)	CIA triad attacks	No	Both attack and defense	Both informational and operational
[21]-2016	N/A	Layers (communication, measurement, control)	DoS, wrapping, phishing attacks	No	Attack only	Both informational and operational
[2]-2016	Abstract model	Layers (generation, transmission, distribution)	Control, measurement attacks	Yes	Both attack and defense	Both informational and operational
[22]-2017	N/A	N/A	Malware	Yes	Attack only	Informational
[23]-2018	Abstract model	Source of threats	Technical and non-technical attacks	No	Attack only	Both informational and operational
[24]-2018	N/A	Attack behavior	Interruption, interception, modification, fabrication attacks	No	Both attack and defense	Both informational and operational
[25]-2019	Mathematical model (linear time invariant)	Spatial–temporal hiddenness	FDI, topology attack, DoS, replay attack, Stuxnet, dynamic attack	No	Both attack and defense	Both informational and operational
[26]-2020	Conceptual model	Security objectives (Confidentiality, integrity, availability)	CIA triad attacks	Yes	Both attack and defense	Informational
This paper-2021	Mathematical model (nonlinear time invariant)	Control and feedback loop (control, measurement, control-measurement)	Aurora, pricing attacks, AGC attacks, FDI, Topology attacks, GPS-spoofing, Line-outage masking, Stuxnet-like attacks	Yes	Both attack and defense	Both informational and operational

$$y_t = C\left(x_t\right) + v_t \tag{2}$$

where $x_t \in \mathbb{R}^n$ and $y_t \in \mathbb{R}^m$ are system state and measurements at time interval t, respectively; m is the number of measurements; n is the number of system states (usually $m \geq n$). Typically, system measurements include nodal net injections, line power flows, line current phasors, and bus voltage phases from the emerging phasor measurement units (PMUs). System states include bus voltage magnitudes and angles. $A\left(\bullet\right)$ denotes a system state function; $B\left(\bullet\right)$ is a control function; $C\left(\bullet\right)$ is a nonlinear measurement function; $w_x \in \mathbb{R}^n$ and $w_y \in \mathbb{R}^m$ are system operating noise and measurement noise, respectively. The measurement function is reliant on the specific measurement type and involves the power system network topology and parameters, such as line impedance and transformer tap ratios. The noise is generally assumed to be Gaussian distributed with a covariance matrix $R \in \mathbb{R}^{m\times m}$. The received sensor measurement data, which are called raw data, cannot be utilized directly by the EMS and must be processed by state estimation (SE) and bad data detection (BDD).

B. Cyber-physical security concerns

The wide-area field sensors and communication channels are exposed to an increased level of cyber threats. As shown in Fig. 1, the communication networks are vulnerable to adversaries who can manipulate the control and measurement signals. For countermeasures, the National Electric Sector Cybersecurity Organization Resource (NESCOR) has conducted impact analyses and assessment of data integrity attacks against the wide-area monitoring, protection, and control (WAMPAC) systems [28], in which a dozen attack scenarios are discussed with the corresponding failure scenarios, including line trip, improper synchronous closing, and control actions that create undesirable states. For instance, the WAMPAC.2 scenario indicated that the network equipment could be leveraging to spoof WAMPAC messages [28]. A threat agent may perform a spoofing attack and inject messages in WAMPAC network equipment (router, switch, etc.). The altered messages involve measurement that goes into the WAMPAC algorithms or control command to PMUs or phasor data concentrators (PDCs). The WAMPAC.4 scenario leverages the compromised PDC authentication to manipulate the measurement data. Such compromise may be due to a backdoor or network sniffing, which allows the malicious introduction of false measurement data. The altered data can trigger actions when none are necessary or fail to take action when needed. Meanwhile, The WAMPAC.8 scenario shows an attacker can insert malware in PMU/PDC firmware to alter measurements. When the altering action is triggered, significant effort or cost is invested in troubleshooting the systems given the lack of measurement consistency, followed by equipment replacement [28].

Figure 2 illustrates the cyber-physical attacks and their corresponding targets. Following the WAMPAC scenarios prescribed in [28], we summarize the cyber-physical attacks in CPSGs in the following three categories:

1) Control signal attacks: By relying on the ability to bypass the data authentication and integration examinations, control signal attacks aim at acquiring the physical device authority and then operate it at the attacker's will. This type of attack is usually designed to target mission-critical devices in power systems such as automatic generation control (AGC), relays, smart inverters, flexible AC transmission system (FACTS) devices, and circuit breakers. To achieve the adversaries' malicious goals effectively, adversaries likely have the knowledge about the target device (e.g., inverter P-Q setpoints, generator ramping limits, line flow limits). Despite the study of N-1 contingency for loss of a generator or transmission line, researchers show that by exploiting the clustering-based vulnerability, simultaneous attacks against the elaborately identified, most vulnerable devices may cause cascading failures [29]. Control attacks can achieve significant consequences in a short period. However, the lack of coordinated masks in the feedback measurement makes the attacks unhidden to detection methods.
2) Measurement attacks: These attacks focus on manipulating the sensor measurement data transferred through the communication channels or falsifying the remote terminal units (RTU) in the field. Physical communication links are usually compromised to deliver falsified messages (e.g., false data injection attacks, GPS spoofing, and replay attacks). Depending on the attackers' capabilities, they may change the firmware of devices, eavesdrop measurements for reconnaissance, and control sensors for reporting tampered measurements. For example, an attacker may change the Domain Name Systems (DNS) server of the device gateway to an attacker-controlled DNS server [30]. By doing this, DNS hijacking attacks can be implemented to control the device-remote server interactions. Once an attacker controls the communication between the gateway and the remote server, all the measurement reports are going to be sent to the malicious server instead of the legitimate server. In addition, traditional DoS or a Black Hole can block the packets in the network, decreasing the system's situational awareness. This type of attack may disable the system operator's situational awareness to cover intrusions or induce inappropriate operations according to the falsified system state based on the manipulated measurements.
3) Control-signal-measurement attacks: This type of attack is also called control-measurement-loop attacks, in which adversaries launch coordinated attacks on both the control signals and measurements. The control signal attack may cause immediate physical layer consequences, while the measurement attacks such as replay attacks can disguise the ongoing control signal attack. The manipulated measurements can pass existing anomaly detection mechanisms in the system. Existing research revealed that attackers might utilize the control-measurement-loop attack [31] (e.g., line outage masking attacks, Stuxnet attacks) to enhance the stealthiness of control signal attacks by masking the attack consequences as well as deceiving the attack detection and mitigation mechanism. For instance, the notorious Stuxnet attack [32], [33] targeted the SCADA systems and caused substantial damage to the centrifuge of a nuclear plant. A Stuxnet attack can compromise the programmable logic controllers and give unexpected commands while returning normal operation system measurements to the SCADA.

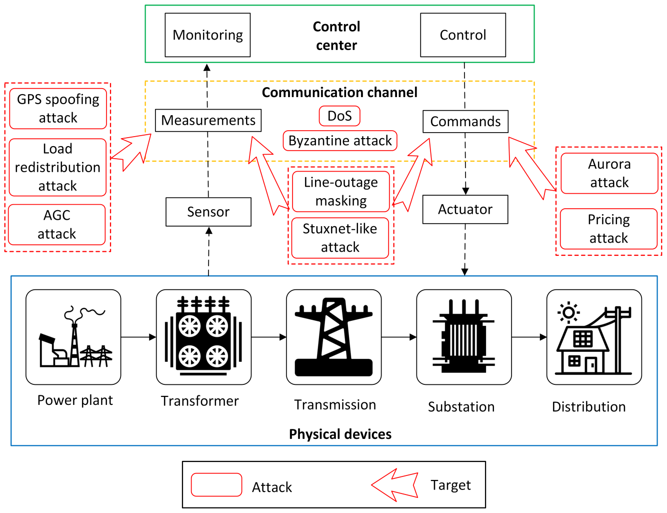


Fig. 2: Cyber-physical attacks and their targets reviewed in this paper.

III. Cyber-Physical Attacks

Analyzing vulnerabilities of a CPSG has attracted increasing attention in the last few years. The general approach is to study specific attacks against a particular system component. A CPSG consists of information technologies (IT) and operational technologies (OT). IT refers to the application of networks that deal with the data and the flow of digital information. In contrast, OT refers to technology that monitors and controls specific devices such as the SCADA system. IT and OT are merging together, known as IT-OT convergence, and the boundary between them has become blurry. This paper primarily focuses on the OT attacks and defense approaches in a smart grid. Several attack behaviors against the IT systems of a CPSG are briefly reviewed in Subsection A. Then, the OT attacks are discussed in greater detail in the rest of this section. Figure 2 shows the attacks and their targets surveyed in this paper.

A. Data Availability Attacks

Since wireless communication is commonly used in a CPSG, adversaries can launch attack schemes against the communication channel. In this paper, we classify the attacks that impede data availability as IT attacks. For example, Byzantine attacks against communication networks such as cognitive radio networks and mobile Adhoc networks were discussed in [34], [35]. These attacks are launched by compromised insider nodes to affect the trusted routing, which in turn reduces the overall network performance. After intrusion, a selfish sensing node can report falsified channel sensing results and increase its own gains at the cost of performance degradation of other honest nodes. Typically, attackers intentionally launch Byzantine attacks for two attack objectives. The first objective is vandalism, where attackers report channel vacancy when the sensing results indicate that the channel is busy. The second objective is exploitation, where attackers can access the idle channel exclusively by sending channel busy information when their sensing results indicate that the channel is idle. Attackers can pursue attack utility maximization of the above objectives [36].

Compared with Byzantine attacks that hinder the data availability by degrading the communication channel, DoS is another notorious attack that blocks the normal data transfer by occupying the communication channel with junk data. In a CPSG, the objective of a DoS attack is to disrupt the communication between a control center and sensors or actuators in the field. DoS attackers are not required to have the knowledge of the CPSG configuration or the ability to manipulate the control or measurement data in the communication channel. The attack consequence is that system operators can easily notice the attack due to the loss of measurement data. However, the operators cannot mitigate the attack since they cannot send control signals to the actuators. An example of the DoS attacks is the incident of the Ukrainian electric power companies discussed earlier. In [37], Qin et al. considered how to damage the system performance most severely when launching a DoS attack against the state estimation over the packet-dropping network environment. They presented an optimal attack schedule that maximizes the trace of the average expected estimation error covariance. In [38], Zhang et al. proposed a scenario that a DoS attacker with attack cost constraint jams the sensor-to-estimator communication channel. The authors formulated an optimization problem that balances the destruction on the cost of system control and the cost of attack in an infinite time horizon concurrently.

B. Control Signal Attacks

1) Aurora attacks: The aurora generator vulnerability was originally tested by the Idaho National Laboratory, where a hypothetical attacker maliciously opens and re-closes the circuit breaker of a generator by injecting a series of compromised control commands [39]. When disconnected from the power grid, the generator becomes desynchronized. The aurora attack is designed to re-close the breaker when the system and generator slip out of synchronism before the protection system responds to the attack. Since generator protection elements are intentionally delayed preventing unnecessary tripping, attackers typically get a 15-cycle window to re-close the breaker before any protection device kicks in [40]. The physical damage to the generator is caused by the variation of electrical power output from the generator and the incremental generator rotating speed during the aurora attack. Each time the breakers are re-closed, the difference of frequency and phase angle between the main grid and the generator may result in high torque and currents, which can ultimately damage the generator [41].

A scoring methodology with vulnerability ranking criteria to find the most vulnerable breakers for an aurora attack has been presented in [42]. In [43], modeling and an impact analysis of aurora attack targeting microgrid point of common coupling (PCC) and synchronous generator breakers were examined. The classic sync-check relays for coping with aurora attacks can lead to unintentional islanding in a microgrid, which is forbidden by the IEEE 1547 Standard [44]. The authors demonstrated that an attacker could successfully damage the microgrid synchronous generator by attacking the PCC breaker of a microgrid connected to the main grid.

2) Pricing attacks: Demand-response programs have been drawing more attention from retail-markets to increase the efficiency of the power grid. In a basic form, demand-response is a control mechanism where the control signals are the incentives. Tan et al. [45] introduced a pricing attack by performing scaling (sending the scaled value of the true price) and delay (sending old prices) attacks on the price signals. Giraldo et al. [49] further improved the attack by modeling an attacker who aims to increase the mismatch between the generated and the consumed power by compromising the communication channel and deploying an attack time series to manipulate the price signal. In contrast to one-snapshot attacks, where the attackers inject malicious data only once, Maharjan et al. [47] considered attacks capable of injecting false pricing information at any moment and repeatedly over a long-time duration. The power mismatch caused by the long-term attacks can lead to over-generation, economic losses, and poor power quality. To quantify the impact of the repeated attacks, the authors proposed a sensitivity analysis method. In their analysis, the authors utilized a z-transform sensitivity function to model the dynamics of the system.

Zhang et al. [46] analyzed the vulnerabilities in transactive energy systems. In such a system, the home controllers at the end-user react to the price signal sent by the transactive market and return bid information automatically. Data exchanged between the prosumer and the market agent can be manipulated by attackers. The authors extended the pricing attack using malware to inject both malicious bidding prices and quantities from prosumers. Under these attacks, the market-clearing price was manipulated, and the energy consumption of each individual prosumer was affected, which in turn adversely influenced the overall demand on the distribution feeders. Two attack scenarios were studied in [46], where the first scenario aimed at compromising the reliability of the system by manipulating the bid price to some extreme values, while the second scenario aims at making profits over time by manipulating the bid price within limits to avoid being detected. Note that prosumers know these bid limits from the service agreement. If the attacker manipulates the signals such that they are out of the limits, the manipulation will become

TABLE II: Control Signal Attack

Control signal attack	**Target**	**Objective**	**Means**	**Consequence**	**Mathematical expression**
Aurora attack [41], [44], [45]	Generators in power plants, microgrid synchronous generators	Cause damage to generators, motors, and transformers	Intentionally open and close a breaker or PCC breaker	Electromagnetic torque and current fluctuations	Control command injection u_t^a
Pricing attack [46]–[48]	Price signal, transactive energy systems bid signal	Mismatch between the generated and the consumed power, profitability	Manipulate the price signal, bid prices and bid quantities	System emergencies (e.g., line and transformer overload), economic losses	Price signal manipulation λ_t^a, bid price manipulation b_i^a, bid quantity manipulation q_i^a

obvious [47]. In contrast to the first scenario, the attack in the second scenario has a small impact on the total load, which makes it difficult to be detected. Table II summarizes the existing works on the control signal attacks.

C. Measurement Attacks

1) AGC attacks: The Automatic generation control is a wide-area frequency control application in interconnected power grids. It ensures system frequency remains within the acceptable bounds and limits the tie-line power flow between adjacent control areas to their scheduled values. AGC relies on power flow and frequency measurements from remote sensors to calculate the area control error (ACE). The ACE represents the power exchange error and the system frequency error between the real system state and the scheduled state. Based on the ACE, automated control commands on AGC generators are computed once every few seconds. However, existing measurement validation techniques such as the state estimation typically run once every a few minutes, which cannot accommodate the second-level frequency of AGC. Therefore, the lack of measurement validation or attack detection mechanism makes AGC susceptible to measurement attacks. Moreover, AGC is a highly automated system that requires minimal supervision and intervention by system operators. Once compromised, it may rapidly cause a power imbalance in the system [48].

Sridhar et al. [50] injected four adverse measurements, i.e., scaling, ramp, pulse, and random attacks, to demonstrate their impacts on the physical system stability and the market operation. In scaling attacks, measurements are modified to higher/lower values during the entire duration of the attack. Ramp attacks gradually increase or decrease original measurements over time. Pulse attacks modify measurements through temporally spaced short pulses. Random attacks add random values to true measurements. In an attack scenario to jeopardize system stability, the attacker's goal is to cause a rapid decline in the system frequency to trigger under-frequency load shedding. In the other attack scenario to manipulate the market operation and make a profit by generating more power, the attack involves modification of generator operating points identified by the security-constrained economic dispatch (SCED). In this case, the attacker is a utility that wants to generate more power than the dispatched schedule without being detected. The attacker injected fabricated tie-line power and system frequency measurements to force ACE miscalculation, forcing generators in the targeted area to ramp down. Meanwhile, the attacker ramped up its own generator, thereby generating more than the operating point suggested by SCED. As an increased generation in the attacker's area compensated for a decrease in the targeted area, the system frequency was kept.

Similarly, the four types of attacks discussed above were studied by Chen et al. [51] to implement the AGC attack strategy targeting explicitly at the load frequency control. Tan et al. [48] considered that the grid frequency is a global parameter that can be easily verified. They assumed there exist upper and lower bounds, known by the attackers, as stealthiness constraints for any injected attack vector to pass the data quality checks. The stealthiness constraints limit the attack vector magnitude and make the attacker unable to cause an unsafe frequency deviation in a single AGC cycle. Thus, Chen et al. [51] focused on attacks on power flow measurements using a continuous false data injection attack over multiple AGC cycles to overcome the stealthiness constraints. They defined a metric to assess the effectiveness of their attacks, i.e., Time-to-Emergency (TTE), as the time from the onset of an attack to the first time instant when the average frequency deviation of the system is out of the threshold (e.g., 0.5 Hz) in their case study. They optimized their proposed attack by minimizing the TTE and satisfied the stealthiness constraints simultaneously; therefore, leaving the shortest time period for the system to counteract.

2) FDI attacks: False Data Injection (FDI) attacks against state estimation, and bad data detection is one of the hottest topics in the smart grid. It was first presented by Liu et al. [52], [53] with DC system models. The authors assumed that the attacker knows the topology and network parameters of the entire power system and has the capability of manipulating the data measurements from the meters. An FDI attack can cheat the power system state estimation, which is the basis of many power system applications, such as contingency analysis, and economic dispatch [54], [55]. Falsified state estimation results could potentially mislead the operation and the auto-control mechanism of the EMS. The consequences of such attacks include economic loss, unstable system states, and even system voltage collapse [56]. Liang et al. [57] introduced an FDI attack that can induce physical line overflows. By considering the EMS sequential data processing functionalities, their optimized attack vector resulted in line overload when the false measurements cause generation re-dispatch. Elaborately constructed attack vectors can bypass bad data detection by keeping consistent with physical laws like Kirchhoff's circuit laws. The construction of the FDI attack vector a in DC models obey (3):

$$a = H\dot{x} \tag{3}$$

where H is the measurement matrix; $\dot{x}$ is the estimated state deviation due to the attack; and $\hat{x}_{attack} = \hat{x} + \dot{x}$. Therefore, the malicious measurements $Z_a = Z + a$ will get the same BDD residual r as the original measurements Z do.

Hug et al. further investigated the FDI attack in AC state estimation [58]. Unlike the DC model, where the elements in the measurement matrix H are constant, the relationship between the measurements and the states become non-linear in AC systems. The attack vector is derived as:

$$a = H(\hat{x} + \dot{x}) - H(\hat{x}) \tag{4}$$

where $\hat{x}$ is the estimated state; $\dot{x}$ is the change in the estimated state. The BDD residual under such an attack is determined by the covariance matrix, the malicious measurements, and the estimated states after the attack. Since the attack vector is noiseless, the residual after the attack is not greater than the original residual; thus, the attack is hidden. Note that the construction of AC FDI attacks requires the estimated states, as shown in (4).

The state-of-the-art research on FDI attacks is on weakening the assumption that the attacker has the full knowledge of the system network information (i.e., H and $H(\bullet)$ are known to the attackers). However, the attacker has limited ability to hack into meters. In this case, the attacker can only access some specific measurements due to the different physical protection of the meters [59]. The limited access to meters leads to a subset of research works generating attack vectors by minimizing the number of manipulated measurements. For an attacker, minimizing the number of attacked meters, as shown in (5), can reduce the risk of being detected and the attack cost.

$$\alpha_k = \min_{x} \|Hx\|_0 \tag{5}$$

where α_k denotes the minimum objective value, $\|\bullet\|_0$ is the cardinality of a vector. Such a problem is proven to be NP-hard and non-convex; thus, it is often solved by mixed-integer linear programming (MILP) methods [60]. By exploiting the sparsity of H in the power system on account of physical topology, Sou et al. [60] proposed a min-cut polynomial time approximate algorithm, which is faster but still as accurate as the MILP method. Wang et al. [61] simplified the original problem by solving the relaxed L1-norm problem for sparse attack construction. Due to recent studies, the L0-norm minimization can be relaxed to L1-norm minimization for sparse attack evaluation [62], [63]. Recall that the construction of a perfect AC FDI attack requires the knowledge of estimated states. In reality, however, an adversary cannot obtain the same estimated state as the operators. To close the gap, Zhao et al. [64] provided a sufficient condition to an imperfect FDI attack. By satisfying this condition, an imperfect attack vector can avoid being detected.

3) Blind FDI attacks: Recently, FDI attacks with little to no information inspired researchers to construct blind FDI attacks without explicit knowledge of the power grid topology. Some researchers proved that such attacks exist and can further decrease the attack cost. Kim et al. [65] presented the subspace method to learn the system operating subspace from measurements and launch attacks accordingly. Their subspace method did not require any system parameter information and depended on partial sensor measurements. In 2015, Yu et al. [66] studied the problem of blind FDI attack which makes inferences from the correlations of the line measurements. The construction of the attack utilizes the principal component analysis (PCA) [67] approximation method to transform the observation vector (a set of possibly correlated measurement variables z) into a set of linearly uncorrelated variables, $\tilde{x}$, called principal components. In the proposed attack model [66], attackers first collect some historical measurement data and run the PCA transformation. The PCA matrix, $H_{PCA} \in \mathbb{R}^{m\times n}$, is introduced by the dimensionality reduction of PCA, m is the number of measurements, and n is the number of principal components. The attacker can generate the stealthy blind FDI attack vector $a = H_{PCA}\dot{x}$ with an arbitrary $n \times 1$ non-zero vector $\dot{x}$. The attack was proven stealthy in the noiseless condition, and the noise will slightly degrade the performance of the attack.

In cases where attackers have the topology information needed, Rahman and Mohsenian-Rad [68] proved that an attack could estimate H by collecting offline topology data manually (e.g., getting access to the grid topology maps through intruders or utility company employees), and online measurements data (deploying attacker's sensors and PMUs). Another approach exploits the relationship between the publicly available locational marginal prices (LMPs) and the Lagrange multipliers of the network-constrained economic dispatch. Thus, LMPs components can unveil the topology information. Kekatos et al. [69] developed a regularized maximum likelihood estimator (MLE) to recover the grid Laplacian from the LMPs. A convex optimization problem was solved using an iterative alternating direction method of multipliers (ADMM) based algorithm. In the scenario where the loads vary within a small range, the topology information can be embedded into the correlations among power flow measurements. Esmalifalak et al. [70] proposed an independent component analysis (ICA) algorithm to speculate the matrix H from power flow measurements. Higgins et al. [71] proposed a data prepossessing before the ICA process. The proposed data classification is through T-distributed stochastic neighbor embedding (T-SNE) for dimensional reduction. Despite of the above cases where attackers can obtain the topology information, attackers are also able to construct FDI attacks with limited topology information. Deng et al. [72] demonstrated that the adversary could launch unobservable FDI attacks to modify the state variable on a bus if they know the susceptance of every transmission line that is incident to that bus.

Meanwhile, attackers can launch effective and unidentifiable FDI attacks based on data-driven strategies [73]. Data-driven methods, especially machine learning based approaches, are an essential branch of cyber-physical attacks on the smart

TABLE III: Measurement Signal Attack

Control signal attack	**Target**	**Objective**	**Means**	**Consequence**	**Mathematical expression**
AGC attack [48], [50], [51]	Automatic generation control	Rapid decline in the system frequency	ACE manipulation	Under-frequency load shedding	Measurement injection y_t^a
FDI attack [52]–[61]	State estimation based BDD	Incorrect estimated state	Measurement manipulation	CPSG functional failure	Measurement injection y_t^a
Blind FDI attack [65], [66], [68]–[70], [72]–[74]	State estimation based BDD	Incorrect estimated state	Measurement manipulation	CPSG functional failure	Measurement injection y_t^a
LR attack [75]–[81]	State estimation based BDD	Incorrect estimated state	Realistic measurement manipulation	CPSG functional failure	Realistic measurement injection y_t^a
Topology attack [82], [83]	Topology estimation	Incorrect topology estimation	Measurement manipulation	Incorrect topology state	Measurement injection y_t^a
Spoofing attack [84], [85]	PMU	Manipulating PMU measurements	GPS signal manipulation	Incorrect location and time stamp	Measurement injection y_t^a

grid. Chen et al. [73] assumed an attacker who has little knowledge of the power system and is unable to estimate important parameters from observations. The attacker can only perform attacks and online learning iteratively to search for an optimal strategy. The optimal attack strategy was modeled as a partially observable Markov decision process (POMDP). Which, however, was impossible to be solved. Thus, the attacker could obtain an approximately optimal strategy through a Q-learning algorithm with the nearest sequence memories (NSM). Markwood et al. [74] proposed a measurement matrix estimation attack, which was termed as a topology leaking attack. When the attacker knows the historical bus power injections and relative voltage phase angles, the measurement matrix H can be estimated. In cases where attackers can not distinguish the eavesdropped measurement corresponding to the current system topology, Higgins et al. [71] proposed an unsupervised learning method to cluster the data set via the density based spatial clustering of application with noise (DBSCAN) algorithm.

4) Load Redistribution Attacks: In 2011, Yuan et al. [75] defined a special type of false data injection attacks, namely load redistribution (LR) attacks. By considering the characteristics of the power system and the attacker's capability, limited access to specific meters is available to LR attackers. Unlike original FDI attacks with a strong assumption that the attacker has access to all the meters in the system, LR attacks only manipulate the injection measurements of load buses and line power flow measurements. Centralized generator measurements and zero load bus injection measurements are not attackable. In other words, LR attacks are realistic false data injection attacks. Liu et al. [76] proposed a local LR attack, which does not require the network parameter information of the whole system. They defined non-attacking regions, attacking regions, and boundary buses that connect these two types of regions. According to their research, an attacker, without knowing the network information of the entire power system, can launch a successful local load redistribution attack with only the knowledge of the network information (topology and line admittance) of the attacking region. This is done by keeping the same phase angle variations at all boundary buses.

Researchers have been recently focused on revealing the specific attack consequences. Che et al. [78] analyzed the mechanism that the attacker can implicitly identify the targeted initial contingency as a system weak point, then leverage such weak point to implement LR attacks to cause physical damages to the system. Under the impact of the load attack vector, the SCED enforces the line flow limits based on the incorrect power flow state. When the generators are following the dispatch commands sent from the SCED, severe transmission overloads can be caused [86]. Xiang et al. [80] quantified the impact of LR attack on the long-term power supply reliability by proposing a power system reliability evaluation model. The proposed Monte Carlo simulation based assessing method considers LR attacks that can cause load curtailment. Fu et al. [81] presented an attacker who does not pursue a temporary profit but the most tripped lines during the cascading process by coordinating LR attacks with physical attacks. As the main cause of cascading failure is a physical attack, the system operator will always try to prevent cascading failure by re-dispatching the system back to a security operation point. This is when LR attacks come into play to disrupt and mislead the re-dispatching by causing the maximum line overloading. Fu's case study showed that the LR enhanced coordinated attack is more serious than a single physical attack causing cascading attacks. Zhang et al. [77] extended the LR attack to AC distribution systems by presenting a net load redistribution attack (NLRA), which aims at misleading the distribution system state estimation to observe illusory voltage violations. Measurements from prosumer buses with behind-the-meter distributed energy resources (DER) can be manipulated by an NLRA. Choeum et al. [79] proposed an LR attack against the conservation voltage reduction (CVR) in distribution systems with DERs. The presented adversary injects malicious load data into the advanced metering infrastructure network and misleads the CVR to come up with an abnormal control signal for the voltage regulator and smart inverter set points. The CVR results are consequently distorted, which cause an increase in active power flow from the substation.

TABLE IV: Control-Signal-Measurement Attacks

Control signal attack	Target	Objective	Means	Consequence	Mathematical expression
Line outage masking attack [88]–[92]	Topology estimation	Measurement manipulation to mask line-outage	Measurement manipulation	Voltage violation and line overflow	Measurement injection y_t^a
Stuxnet-Like Attack [93], [94]	Communication channel	Incorrect control and measurement signal	Control signal and measurement manipulation	Stealthy malicious control commands	Control command injection u_t^a and measurement injection y_t^a

5) Topology Attacks: In 2013, Kim et al. [82] proposed topology attacks in distinguishing from the FDI attack. The main difference between the topology attack and the FDI attack is that the topology attack manipulates the estimated topology state (switch and breaker states) instead of the estimated system state (power injection, power flow). A topology attack is achieved by manipulating both the meter measurement data and the network data, which can be represented as binary bits indicating on and off states of various switches and line breakers. The attack vector in a DC model is shown in (6):

$$a = (\bar{H} - H)x \tag{6}$$

where H and $\bar{H}$ are the measurement matrices before and after the attack, respectively. When the measurement is noiseless, the system state x can be replaced with a function of measurements to generate the attack vector. However, the estimated state $\hat{x}$ is required when considering measurement noise.

Note that both DC and AC attack vectors previously mentioned in this subsection require full knowledge of network information to construct the measurement matrices and functions. In reality, this may not be possible. Therefore, a topology attack with local network information [82], [87] has been studied. Kim et al. [82] considered a weak attacker who has access to a few local meters only. The authors proposed line removal attacks, i.e., the adversary tries to remove lines from the actual network topology and mislead the operator that the line is disconnected. Liu et al. [87] observed the existing topology attacking model has two practical issues. The first issue is that there is no limit on the attacking amounts for load measurements at buses. The second issue is that attackers have limited capability to obtain necessary information. Thus, the authors proposed a local topology attack model to determine the feasible attack region by obtaining less network information.

6) GPS Spoofing Attack: In CPSGs, spoofing attacks on PMUs are conducted via global position system (GPS) spoofing, where the adversary produces artificial GPS signals. Two attack approaches, i.e., source ID mix attacks and time stamp attacks, are studied based on the spatio-temporal characterization of the GPS signals. A source ID mix attack is that attackers can exchange the location information of measurement data among different PMU's channels without altering the measurement values. This type of attack places the measured data into wrong positions in associated data servers. Cui et al. [84] demonstrated the impact of source ID mix spoofing on the wide-area monitoring systems (WAMS) and the wide-area damping control. By swapping the signals of two buses, the WAMS estimated the disturbance at a location far away from the correct location; the damping control failed, and the system frequency kept dropping. The other type of GPS spoofing attack is called time stamp attack, also known as time synchronization attacks (TSAs), which aim to maliciously introduce erroneous time stamps, thereby inducing a wrong phase angle in the PMU measurements [83]. Risbud et al. [85] formulated an optimization problem to identify the most vulnerable PMUs to construct a TSA. The vulnerability was quantified by the state estimation error, and a greedy algorithm was utilized to solve the problem.

D. Control signal measurement Attacks

1) Line Outage Masking Attacks: The recent attack on the Ukrainian power grid [95], which affected both the physical infrastructure and the situational awareness at the control center, is drawing more attention from researchers. A novel line outage masking attack was proposed [88]–[92], where an adversary attacks an area by physically disconnecting some lines from the attacked area (i.e., remotely open the circuit breakers) to occur short-term damage like voltage violation and line overflow, and then mask the measurements within the attacked area by DoS or FDI attacks. Such attacks combine both control and measurement layer attacks to cause immediate failure and block the operator's awareness at the same time, which may lead to cascading failures.

Deng et al. [92] presented two coordinated cyber-physical attacks (CCPAs) to mask the line outage, namely replay and optimized CCPA. To construct the replay CCPA, attackers alter the meter readings on all the branches to force the active power flow measurements after the line outage to be the same as the power flow measurements from a normal state. The replay CCPA is extremely costly, and the actual system state is not consistent with the manipulate measurements, which makes it detectable by independently known-secure PMUs. The optimized CCPA neutralizes the impact of the line outage on the BDD residual. Soltan et al. [88] proved that finding the set of line failures after data distortion and data replay masking attack is an NP-hard problem, based on the operator's knowledge of the phase angle measurement before and after the attack as well as the line admittance matrix. Li et al. [96], [97] proposed to conduct two-step cyberattacks that mask line outages resulting from the physical attacks. The cyberattacks are decomposed into two steps, which include a topology-preserving attack as the first step, followed by the load redistribution attack (if the first step is not feasible). More specifically, the topology attack masks line outages caused by physical attacks while the load redistribution attack keeps the total load unchanged and redistributes the line flow to bypass the state estimation-based detection. Chung et al. [91] further improved the masking approach by deploying a line-removing FDI attack (topology attack) that misled the SCADA system with a fake outage in another position. After the real line outage attack, the topology attack region is then selected to re-dispatch the power flow. The attack vector is generated in an AC model with local network information and the capability to manipulate the measurement within the attacked area.

2) Stuxnet-Like Attacks: Traditional Stuxnet attacks inject the malicious control commands to the actuators and, meanwhile, corrupt the sensor readings to cover the ongoing attack. To avoid being detected, Stuxnet attacks require the attacker's capabilities of replaying all the measurements during the steady state of the system. Forensic analysis of Stuxnet attacks [93] has shown the feasibility of a very targeted and highly sophisticated cyberattack. Moreover, with some modifications, Stuxnet can be tailored as a platform for targeting other systems e.g., automobile or power systems.

Tian et al. [94] defined Stuxnet-like attacks against secondary voltage control, which assume the attacker has write access to both the control signal and sensor measurement. The cyber-physical system dynamic is described as a discrete-time linear time-invariant (LTI) model. In the presence of an attack, the system dynamics are as follows:

$$x_a(t+1) = Ax_a(t) + Bu_a(t) + w(t) \tag{7}$$

$$y_a(t) = Cx_a(t) + v(t) \tag{8}$$

where the notations are similar to those in (1) and (2) with an exception that the subscript a denotes the under attack status. The attacker knows the state transit matrix A, the control matrix B, and the measurement matrix C. Variable u_a is the contaminated control signal received by the actuators; y_a is the manipulated sensor measurement received by the control center; x_a denotes the system state. Functions $w(t)$ and $v(t)$ respectively denote the process and sensor noises. This Stuxnet-like attack is only implemented on a converged system, where the control center expects unchanged system states. The attacker needs to judge whether the system has converged, according to the eavesdropped control signal and measurement data.

IV. Cyber-Physical Defense

Cyber-physical defense is absolutely the focus of ongoing research efforts, where a massive number of works have already been published in the literature. In this section, we first categorize cyber-physical defense approaches into temporally-relevant and spatially-relevant approaches. Further, several state-of-the-art cyber-physical defense approaches in the CPSG, including securing measurement sensors, model and algorithmic enhancement, data-driven approaches, moving target defense, and watermarking, are reviewed.

A. temporally- and spatially-relevant DETECTION

In a temporally-relevant detection, the current system state is estimated by prior estimated state, measurement, and control signal. At time t, the estimated measurement $\hat{y}\left(t\right)$ and the residual $\delta\left(t\right)$ are shown as:

$$\hat{y}\left(t\right) = L_1\left(\hat{X}\left(t-1\right), U\left(t-1\right), Y\left(t-1\right)\right) \tag{9}$$

$$\delta\left(t\right) \overset{\Delta}{=} y\left(t\right) - \hat{y}\left(t\right) \tag{10}$$

where $L_1\left(\bullet\right)$ is an abstract function; $\hat{X}\left(t-1\right) = \left[\hat{x}\left(t-1\right)\cdots\hat{x}\left(0\right)\right] \in \mathbb{R}^{n\times t}$ is the set of the prior estimated state; $U\left(t-1\right) = \left[u\left(t-1\right)\cdots u\left(0\right)\right] \in \mathbb{R}^{l\times t}$; $Y\left(t-1\right) = \left[y\left(t-1\right)\cdots y\left(0\right)\right] \in \mathbb{R}^{m\times t}$. After the estimation, if the calculated residual is larger than a pre-defined threshold, the detection method will signal an alert. Among all temporally-relevant approaches, the most widely used method is the Kalman filter based state estimator and the chi-squared test [98]–[100]. The Kalman filter based estimator minimizes the variance of the estimated state, given the previous observations. The chi-squared test [101] is commonly used to detect anomalies.

The spatially-relevant detection method estimates the system by the correlation between different sensors in one time-interval only. A power system state estimator and the residual-based BDD is an example of the spatially-relevant detection approach. An essential of this estimation is measurement filtering, which utilizes the measurement data redundancy to increase the measurement accuracy. At time t, the estimated system state is calculated based on the measurement from the same time interval,

$$\hat{x}\left(t\right) = L_2\left(y\left(t\right)\right) \tag{11}$$

where $L_2\left(\bullet\right)$ is an abstract function. From equation (2), the estimated measurement is shown as:

$$\hat{y}\left(t\right) = C\left(\hat{x}\right). \tag{12}$$

The residual-based alarm mechanism is also implemented in spatial-relevance detection. One notable difference is that in a temporally-relevant detection, the estimated measurement is calculated from prior system state (9); however, in a spatially-relevant detection, the estimation is based on the current state (12).

B. Securing measurement sensors

As previously mentioned, the majority of attacks require, more or less, the attacker's knowledge about the system control and measurement signal. An assessment in [30] has shown that the major cybersecurity concerns range from exploiting well-known protocols to the leakage of confidential information. Therefore, one natural approach is to select and protect critical control or measurement signal strategically.

Bobba et al. [55] explored the detection of false data injection by protecting a set of critical sensor measurements and a method to verify the values of strategically selected state variables. The authors demonstrated that an attack aims to construct an attack vector such that it avoids specific measurements and state variables that are protected and verified.

From the defender's perspective, the operator should select the sets of the protected measurements and the verified state to ensure that an adversary cannot find a stealthy attack vector. Thus, FDI attacks could always be detected. The trade-off here is that the protection and verification of a large number of measurements and state variables could be costly.

Phasor measurement units have recently attracted researchers' attention due to their ability to provide measurement redundancy and assist in FDI detection. Zhao et al. [64] developed a robust FDI attack detection method by checking the statistical consistency of measurements from a limited number of secured PMUs. In the proposed detector, short-term measurement forecasting [102] was advocated to enhance the PMU data redundancy. Giani et al. [103] proposed that it is sufficient to place $p+1$ known secure PMUs at carefully chosen buses to neutralize a collection of p cyberattacks. Since then, the optimal PMU placement has been researched to detect the stealthy FDI attacks with the least PMUs. Qi et al. [104] formulated the optimal PMU placement as an optimization problem, which maximizes the determinant of the empirical observability Gramian matrix. Pal et al. [105] presented an integer linear programming methodology for the PMUs placement scheme while considering realistic cost and practical constraints. Sarailoo et al. [106] adopted synchrophasor availability (SA) on all buses as a constraint and then minimized the number of PMUs. The SA is the fraction of time on average the bus voltage synchrophasor is correctly present. As mentioned in Section III, the synchronization between PMUs requires GPS signals, which are vulnerable and can be attacked [107]–[109]. Fan et al. [110] proposed a cross-layer detection against simultaneous GPS spoofing attacks towards multiple PMUs.

C. modeling and algorithmic enhancement

Another category of defense approaches is on the improvement of the detection models and algorithms. Huang et al. [111] proposed an adaptive cumulative sum (CUSUM) algorithm, which detects the adversary fast while maintaining a low detection error rate. Liu et al. [112] proposed a false data detection mechanism that utilized the intrinsically low-dimensional power grid measurements and the sparse nature of FDI attacks. The detection problem is formulated as a matrix separation problem and is solved by two methods: the nuclear norm minimization and low-rank matrix factorization. Gu et al. [113] proposed a detection method to detect FDI attacks by tracking the dynamics of measurement variations. They utilized the Kullback-Leibler distance (KLD) to calculate the distance between two probability distributions, i.e., historical measurements and suspicious measurements, to detect the FDI attacks. Zhao et al. [114] proposed a short-term state forecasting method considering the temporal correlation to calculate the approximate prior system measurements. The consistency between the forecasted and received measurements is checked by a statistics-based test method. From the consistency test result, a detection metric is constructed by the infinity and the L_2-norm-based measurement residual analysis. Ashok et al. [115] showed that the existing CPS defense focuses on either redundant measurements or the cybersecurity of sensors and communication channels. These offline approaches make specific assumptions about the attacks and systems, which are restrictive. One solution of PMUs placement or security mechanism may no longer be adequate under another system configuration. Therefore, the author proposed an online anomaly detection that covers broad attack scenarios. The proposed method leverages online information obtained from load forecasts, generation schedules, and real-time data from PMUs to detect anomaly measurements.

D. data-driven approaches

Another noteworthy category of defense approaches is on data-driven machine learning methods that have been gaining traction due to the following two salient advantages:

1) The construction of the data-driven approaches does not depend on the network topology; and
2) This approach is usually sensitive to time-variance measurement, which can be very effective in detecting one time interval stealthy FDI attacks created based on the spatial-relationship of CPSGs.

The use of supervised learning classifiers as alternate FDI detectors was proposed by Ozay et al. [116] in 2015. Supervised machine learning based binary-classifiers were presented to check the distance between ”secured” and ”attacked” measurements. With the distance information, attacks can be recognized by the learning algorithms. Yan et al. [117] proposed to implement the learning based false data classifiers as a secondary detector after the residual-based BDD. They designed FDI detectors with three widely used supervised learning based classifiers, including support vector machine, k-nearest neighbor, and extended nearest neighbor. The proposed detectors are capable of detecting stealthy FDI attacks that can bypass the residual-based BDD. Sakhnini et al. [118] tested three classification techniques with different heuristic feature selection techniques. The authors concluded that the support vector machine and the k-nearest neighbor algorithms could get better accuracy than the artificial neural network. However, the artificial neural network is expected to have better performance on larger systems at a higher computational cost. The recent breakthrough in computing provides the foundation for ”deep” neural network. Niu et al. [119] developed a smart grid anomaly detection framework based on a neural network. The recurrent neural network with a long short-term memory cell is deployed to capture the dynamic behavior of power systems. According to the captured behavior, the estimated measurements are calculated and compared with the observed measurements. If the residual between the observed and the estimated measurements is greater than a given threshold, an attack is detected.

As for reinforcement learning based methods, Chen et al. [73] proposed a BDD method based on Kernel density estimation. By using historical records, the measurements can be estimated. The effectiveness of the proposed detection method relies on the abundance of integrated records of normal operations of the power grid. When an attack vector is injected consistently, the tempered measurements could be used for the

Kernel density estimation analysis. Thus, the proposed BDD detection method could fail. Other than the studies that contribute to attack detection, Li et al. [120] proposed a defense methodology that recovers the real measurements to maintain uninterrupted state estimation under FDI attacks. The proposed method utilized a generative adversarial network based data model which captures the deviations from ideal measurements and then generates correct data to replace the manipulated data. Besides the aforementioned defense approaches that protect the transferred measurement data, the defense on the communication channel is vital. One of the cutting-edge wireless communication technologies used in the smart grid is the cognitive radio, which is motivated by the ever-increasing demand for high data rates in the face of limited spectral resources. Ding et al. [121] introduced a spectrum attacker who can inject attack data into the honest spectrum sensor to mislead the fusion center to lower the spectrum utilization. Moreover, the authors show that the kernel K-means clustering (KMC) algorithm yields better performance than the KMC algorithm in the detection of spectrum attacks. However, high-quality clean training data are too expensive or too difficult to obtain in some cases. Xie et al. [122] proposed a convex framework to provide robust classification and training in improving the anomaly-resistant against sensor failures (i.e., falsified channel sensing resulting in Byzantine attacks) in which possibly anomalous samples occur in the training set. Qin et al. [123] proposed a low-rank matrix completion based malicious user detection framework for the secure cooperative spectrum sensing with a lower data acquisition cost.

E. Moving Target Defense

The aforementioned operational defense approach is either computationally complex or somewhat passive. As an emerging technique, moving target defense (MTD), is originally proposed to enhance network security [124]. It proactively changes the system configuration so that it reduces the attack surface and increases the uncertainty about the network system. With the properly arranged MTD perturbation, the attacker's knowledge about the system is always outdated. This approach increases the barriers for the attackers to launch stealthy attacks. MTD has recently been introduced in the physical layer of the cyber-physical power system (CPPS) to provide proactive defense, which is an advantage over the traditional remedial defense. Comparing with the MTD in the cyber-layer network system, MTD in CPPS is very complex as it requires the physical dispatch of control, measurements, or device properties.

The concept of MTD was first introduced into the physical layer of the power system by Morrow et al. [125] and Davis et al. [126]. In general, MTD utilizes distributed flexible AC transmission system (D-FACTS) devices to actively modify impedance perturbations to invalidate attackers' knowledge about the power system configurations, which is essential for constructing stealthy attacks. Table V summarizes the existing works on MTD, where the superscript "AC" or "DC" indicates the corresponding AC or DC model used.

There are two essential steps in the construction of an MTD, namely MTD planning and MTD operation. First, in the MTD planning, a utility needs to install D-FACTS devices on an appropriately identified subset of transmission lines, namely solving the problem of D-FACTS placement. Arbitrary placement and full placement are the two simplest D-FACTS placement strategies. Arbitrary placement randomly selects a subset of lines to install D-FACTS devices [127]. Full placement is the most expensive method in which D-FACTS devices are installed on every transmission line [128]. However, the detection effectiveness of MTDs under these two placements is not considered. Max-rank placement [129], [130] can make MTDs achieve the maximum rank of the composite matrix (i.e., max-rank MTDs), a metric of the detection effectiveness. Spanning-tree placement proposed in [131] installs D-FACTS devices on the lines which form a spanning tree of the system. MTDs under spanning-tree placement is effective to detect single-bus, uncoordinated multiple-bus, and coordinated multiple-bus FDI attacks.

After the allocation of D-FACTS devices, the system operator/defender needs to continuously determine the D-FACTS setpoints under different load conditions in the MTD operation. The MTD operation includes four methods. First, random selection is the simplest operation method without any computational overhead, in which the D-FACTS setpoints are randomly perturbed [127]. As D-FACTS devices are originally used to control the power flow, OPF-based operation methods integrate the D-FACTS devices into the optimal power flow model to minimize the system losses or generation costs [129], [132], [133]. Neither the random selection method nor OPF-based operation methods consider the detection effectiveness. Thus, these two methods must be constructed in the D-FACTS placements, which ensure the detection effectiveness, such as the max-rank placements. Second, the optimization-based operation takes both the economic cost and the detection effectiveness into account, in which the metric of detection effectiveness is maximized or taken as constraints [128], [130]. Finally, the hidden MTD operation method delicately selects D-FACTS setpoints such that all measurements remain the same after MTD is applied [134]–[136]. In this case, vigilant attackers cannot detect the MTD in place using BDD. To find suitable placement for hidden MTD operation, authors in [135] enumerate all placement combinations, while authirs in [136] use the max-rank placement in [130], with the help of protected meters.

In the literature, there are three important concerns to evaluate the performance of MTD. First, attack detection effectiveness is the most important metric for a defense algorithm. As not all MTDs are effective in detecting FDI attacks, the feasibility and the limitation of MTD is discussed in [131]. Many works focus on improving the attack detection effectiveness of MTDs though the MTD planning [129]–[131], [136] and MTD operation [128], [132], [135]. Two metrics are proposed to measure the detection effectiveness of MTD, namely the Lebesgue measure [132] and the rank of the composite matrix [128]–[130], [135]. The composite matrix rank is superior to the Lebesgue measure in the evaluation of MTD detection effectiveness since it demonstrates the inherent nature of MTD on FDI attack detection and provides an explicit objective for constructing an effective MTD. Authors

TABLE V: Moving Target Defense in CPSG

MTD Algorithm	MTD planning	MTD operation	Characteristics
Random MTD [127]$^{\text{DC}}$	Arbitrary placement	Random selection	Detection effectiveness is not considered
OPF-based MTD [132]$^{\text{DC}}$, [133]$^{\text{AC}}$	N/A	OPF-based operation	Minimize generation cost and guarantee detection effectiveness [132]
Hidden MTD [135]$^{\text{DC}}$, [134]$^{\text{AC}}$, [136]$^{\text{DC}}$	Placement enumeration [135]; max-rank placement using protected meters [136]	Random selection subject to hidden condition [135]	MTD has max-rank and is hidden to alert attacker, but [136] uses extra protected sensors
Spanning-tree MTD [131]$^{\text{DC}}$	Spanning-tree placement	Random selection	Covers all buses, but max-rank MTD is not ensured
Max-rank MTD [128]$^{\text{DC}}$, [130]$^{\text{DC}}$, [129]$^{\text{DC, AC}}$	Full placement [128], max-rank placement [129], [130]	Optimization-based operation [128]; ACOPF-based operation [129]	Minimizes system losses [128] or generation costs [129]. Guarantees max-rank MTD based on numerical methods [128], [130] or graph-theory methods [129]

in [129] proved the rank of the composite matrix could be merely determined by D-FACTS placement, as long as no D-FACTS devices work in idle-states. In addition, the number of buses covered by D-FACTS devices and the incremental line reactance introduced by D-FACTS devices also impact the MTD detection effectiveness [131]. However, there is no metric proposed to measure this impact.

Second, the cost of the MTD application is a must-concern for a utility. The cost consists of the planning cost and the operation cost. In the planning cost, the number of D-FACTS devices used in MTD determines the capital cost and labor fee. Max-rank placement in [129] uses the minimum number of D-FACTS devices to achieve the maximum rank of the composite matrix. In the operation cost, the D-FACTS setpoints impact the generation cost and system losses, as these setpoints can change power flow in the system. Thus, OPF-based operation methods can be used to reduce the MTD operation cost in both AC and DC models. To integrate the OPF-based operation methods into the EMS, an interior-point solver proposed in [133] can solve these methods within seconds.

Third, the hiddenness of MTDs provides a superior function as it makes the MTD stealthy to attackers. Vigilant attackers use BDD to detect the existence of MTD before launching any attacks. If attackers detect any MTD in place, they may stop FDI attacks and invest more resources to launch data exfiltration attacks to obtain the latest system configuration [135]. Hidden MTDs can mislead these attackers to launch detectable attacks based on incorrect line parameters. In summary, a desirable MTD would be a hidden MTD with maximal detection effectiveness and low cost.

F. Watermarking

Watermarking is originally used to identify the ownership of noise-tolerant signals such as audio, video, or image data. It also can be used to check the integrity and authenticity of a signal. The first use of watermarking to defend the replay attack employed in Stuxnet was introduced by [98], [137], where the physical watermarking as a control-theoretic method to authenticate the correct control operation was proposed. Although existing tools like cryptography can provide authentication, physical watermarking is more effective against physical attacks or insiders who are usually authenticated users. The concept is that by injecting a known noise as a probe input of the system, an expected effect of such input should be found in the true measurement output due to the system dynamics. Thus, if the attacker is unaware of the watermarking, the injected attack will be detected by a chi-squared detector. Weerakkody et al. [99] considered a more adversarial attacker who has access to a subset of real-time control and sensing signals. The physical watermarking approach is extended to show the ability to counter a more intelligent adversary. Since introducing a random probe signal into the system could clearly affect the operating cost, Miao et al. [138] proposed an optimization method for the trade-off between cost-centric and security-centric controllers. Despite the detection capability, the physical watermarking needs to inject perturbation as a probe into the system, which may affect the system performance. Moreover, the physical watermarking detection sensitivity is usually related to the probe signal magnitude. Thus, to increase the detection performance, the defender has to sacrifice the optimal system performance.

Satchidanandan et al. [139] extended the physical watermarking to dynamic watermarking in a noisy dynamical system. The authors introduced independent and identically distributed random variables to actuator nodes, namely privately imposed excitation. The actual realization of the time-sequence excitation is superimposed on the control input from an honest actuator. The author assumed that the control policy is in place, and the excitation is only known by the honest actuator itself. The proposed dynamic watermarking can ensure that a malicious sensor is constrained to distorting the process noise by at most a zero-power signal by implementing the correlation detector. Ferdowsi et al. [140] proposed a deep learning framework for dynamic watermarking of IoT signals. The framework is based on the long short-term memory blocks to extract stochastic features from IoT signals and watermarks the features inside the original signal. This dynamic extraction enables eavesdropping attack detection since the attacker will not be able to extract the watermarked information.

Watermarking can also be used for attack identification in CPSG. Liu et al. [128] designed a reactance perturbation-based scheme to identify originally covert FDI attacks on power system state estimation. The term originally covert

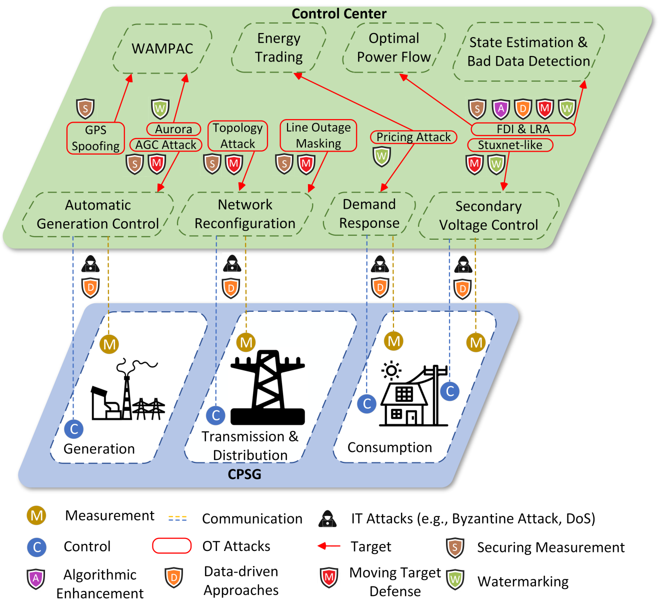


Fig. 3: Infographic of attack and defense mechanisms in smart grid.

attack refers to the stealth of the attack prior to reactance perturbation. The authors proved that the originally covert attack (constructed with original measurement matrix H_0) is detectable and identifiable in a reactance perturbation with a new measurement matrix H if and only if the rank of $[\mathrm{H}_0\ \mathrm{H}]$ is equal to $2(n-1)$, where n is the number of buses. Zhang et al. [141] proposed an attack identification approach for GPS spoofing attacks (GSAs) against PMUs. They performed a probing technique on each PMU in parallel to determine the locations of spoofed PMUs and the ranges of GSA phase shifts under the assumption that the PMU in a substation is secure.

The attack models reviewed in Section III and the defense mechanisms surveyed in Section IV are summarized in Fig. 3. The two-layer model in this figure is a graphic form of the CPSG model abstracted in Section II-A. In Fig. 3, each attack on smart grid functionalities is shown with corresponding counter-measurements labeled next to it.

V. Opportunities and Challenges

Despite the tremendous research efforts reviewed in this work, cyber-physical security challenges remain to be thoroughly addressed. Critical power system functionalities such as market operation, advanced metering, and network operation may also face attacks. Meanwhile, the potential implications of these attacks remain to be further investigated. In addition, the emerging applications, including time of use, demand response, and large-scale electric vehicles, will have strong impacts on the smart grid and may also become targets of cyber-physical attacks in the future. In this section, we highlight four critical challenges and opportunities in the field of smart grid cyber-physical security that deserve further research efforts.

A. Cyber-physical security in distribution systems on the grid edge

A CPSG is a critical infrastructure with an enormous number of complicated devices. Cyber-physical attack and defense simulations are necessary to estimate their performance, though it is impossible to implement most experiments on a real-world power grid. However, the existing cyber-physical studies focus primarily on transmission systems, while the work on the three-phase unbalanced distribution systems with low system observability is significantly under-researched. A growing number of distribution systems on the grid edge are experiencing significant penetration of DERs. The emerging power-electronic-device-based electric vehicles, local energy storage, and demand-response have also contributed to the system dynamics and complexity. Fully taking into account the new dynamics and complexity in low-observability distribution systems is quite challenging in the context of cyber-physical security. More research efforts are therefore necessary in distribution systems on the grid edge.

On the other hand, conventional, discrete-time, model-based simulations are accepted by researchers [142]. However, the traditional power system simulation tools may not be suitable for studying the distribution grid with increasing complexity and cyber-physical concerns. There has been a growing need to use continuous-time simulation with hardware in the loop (HIL) capabilities. In [143], the authors developed a SCADA security testbed, which integrates a real-time immersive network simulation environment with PowerWorld. The authors in [144] developed a testbed with PowerWorld and OPNET. A platform equipped with GridLAB-D and NetSim has been used for power systems and communication network simulation in [145]. Due to time-domain analysis complexity, these simulation platforms cannot run in real-time or perform HIL simulation. In a broader sense, the real-time simulation reflects the exact dynamic behavior of a CPSG, and the HIL ensures precise operation as the real devices. While these two functionalities are usually unavailable with the current simulation structure, development on the real-time simulation testbed with HIL largely remain to be conducted.

B. Interdependence

Studying the CPSG security issues relies on the interdependence of both the cyber layer and the physical layer. The attack detection requires advanced communication technologies to transfer data from the physical devices to the control center. On the other hand, most cyber-physical attack schemes have taken advantage of this interdependence to launch attacks in the cyber layer and induce physical damages. For future research in this area, cyber-physical interdependence needs to be comprehensively explored. For instance, the physical attacks on cybersecurity have been under-investigated, and the threats can be devastating when the dependence of physical systems is exploited by an attacker [2]. Another cyber-physical interdependence that has been largely ignored is simulation software. Traditional software is developed to simulate or emulate either communication networks (e.g., OPNET, NS2, OMNET) or physical power systems (e.g., RTDS, DSATools, PSS/E, PowerWorld). Such software cannot provide realistic cyber-physical environments [146]. Additionally, the interdependence between CPSGs and other critical infrastructures, such as communication, water, and transportation networks, ought to be researched in the context of cyber-physical attacks against CPSGs.

C. Attack coordination

In real-word CPSG, sequential outages are the most common causes of blackouts [147], e.g., the 2003 Northeast Blackout [148] and the 2011 Southwest Blackout [149]. If a series of attacks can trigger such events, then an intimidating cyber-physical security risk will be worthy of attention. In Section III, we discussed the line outage masking attack, one of the popular methods among coordinated attacks. Meanwhile, most researchers assume that the cyberattack vector is injected simultaneously with the physical damage in the existing research. This assumption may be validated in a specific condition, such as the system is in a steady state. However, the general circumstances in which the attackers cannot promise timely cyberattack injection with respect to the system dynamic have remained to be considered. However, the timing and ordering of coordinated attacks can also have an impact on the eventual damages. With an elaborate schedule, not only will concurrence be relaxed, but the damage may be amplified. On the other hand, from a defender's perspective, analyzing the coordinated attacks on CPSG based on temporal-topological correlation can help to restore the complete attack path and identify the intent of the attacks [150].

D. Attack identification and mitigation

In future power systems, an attack detector will be an indispensable tool for detecting and identifying anomalous measurements. Without reliable attack identification, it is hard to implement a mitigation process with pertinence. While detecting attacks is computationally straightforward, identifying the attack location and strategy is computationally challenging [151]. For instance, bad data cannot be identified once belonging to the critical sets of measurements, also known as bad data groups, because they cause the same normalized residuals for each element of the set [152]. Another problem is that existing state estimation based algorithms in transmission systems are not suitable for unbalanced distribution systems with high r/x ratios [153]. With the aforementioned issues, few solutions have been proposed for the identification of attacks. In addition, rather than brutally getting rid of identified compromised measurements, how best to mitigate the adverse effect of those attacks is also a very challenging issue depending on particular operation and controls of a CPSG.

VI. Conclusion

A CPSG relies on the cooperation of both cyber and physical layer functionalities. The ubiquitous threat to the entire smart grid's large attack surface makes it necessary to comprehensively analyze and classify attacks. This paper provides a CPPS operation model and addresses the associated vulnerabilities targeted by an attacker. We classify the existing attack approaches against different components based on the CPPS model. A review of the cutting-edge operational defense approaches was presented to summarize and categorize the state-of-the-art in the field, ranging from the state estimation based detector to the emerging moving target defense and watermarking methods. As smart grid technologies become more prevalent and more physical devices are connected to the cyber-physical infrastructures, significant attack surfaces are introduced, as well as a wide range of opportunities and challenges. Four challenges were highlighted in the investigation of smart grid cyber-physical security. Our survey provides insights that future research efforts must target a new set of cyber-physical security concerns, including real-time risk modeling and simulation, risk mitigation, and coordinated attack defense.

References

[1] C.-P. S. P. W. Group *et al.*, "Framework for cyber-physical systems: Volume 1, overview, version 1.0," *NIST Special Publication*, pp. 1500–201, 2017.

[2] 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, 2016.

[3] G. Loukas, "1 - a cyber-physical world," in *Cyber-Physical Attacks*, G. Loukas, Ed. Boston: Butterworth-Heinemann, 2015, pp. 1 – 19. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128012901000011

[4] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyberphysical system security for the electric power grid," vol. 100, no. 1, pp. 210–224. [Online]. Available: http://ieeexplore.ieee.org/document/6032699/

[5] T. C. Reed, *At the abyss: an insider's history of the Cold War*. Presidio Press, 2005.

[6] T. L. Hardy, *Software and System Safety*. AuthorHouse, 2012.

[7] P. Shakarian, "Stuxnet: Cyberwar revolution in military affairs," p. 11.

[8] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2 2011.

[9] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 7 2017.

[10] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, 1 2010, event: IEEE Power and Energy Magazine.

[11] J. Rost and R. L. Glass, *Disgruntled Employees and Sabotage*, 2011, pp. 189–212.

[12] F. M. Cleveland, "Cyber security issues for advanced metering infrastructure (ami)." 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 7 2008, pp. 1–5, iSSN: 1932-5517.

[13] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, 5 2009, event: IEEE Security Privacy.

[14] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, 1 2010, event: IEEE Security Privacy.

[15] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *2010 First IEEE International Conference on Smart Grid Communications*. IEEE, 2010, pp. 226–231.

[16] S. N. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6522–6530, 2019.

[17] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. Al Ali, "Smart grid cyber security: Challenges and solutions," in *2015 International conference on smart grid and clean energy technologies (ICSGCE)*. IEEE, 2015, pp. 170–175.

[18] A. Procopiou and N. Komninos, "Current and future threats framework in smart grid domain," in *2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*. IEEE, 2015, pp. 1852–1857.

[19] R. K. Pandey and M. Misra, “Cyber security threatssmart grid infrastructure,” in *2016 National Power Systems Conference (NPSC)*. IEEE, 2016, pp. 1–6.

[20] A. Sanjab, W. Saad, I. Guvenc, A. Sarwat, and S. Biswas, “Smart grid security: Threats, challenges, and solutions,” *arXiv preprint arXiv:1606.06992*, 2016.

[21] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, and C.-F. Covrig, “A survey on the critical issues in smart grid technologies,” *Renewable and Sustainable Energy Reviews*, vol. 54, pp. 396–405, 2016.

[22] P. Eder-Neuhauser, T. Zseby, J. Fabini, and G. Vormayr, “Cyber attack models for smart grid environments,” *Sustainable Energy, Grids and Networks*, vol. 12, pp. 10–29, 2017.

[23] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, “Smart grids security challenges: Classification by sources of threats,” *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, pp. 468–483, 2018.

[24] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, “Review of internet of things (iot) in electric power and energy systems,” *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 847–870, 2018.

[25] T. Liu, J. Tian, J. Wang, H. Wu, L. Sun, Y. Zhou, and X. Guan, “Integrated security threats and defense of cyber-physical systems,” *Acta Automatica Sinica*, vol. 45, no. 1, pp. 5–24, 2019.

[26] M. Z. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” *Computer Networks*, vol. 169, p. 107094, 2020.

[27] A. J. Wood, B. F. Wollenberg, and G. B. Shebl, *Power Generation, Operation, and Control*. John Wiley & Sons, 12 2013.

[28] None, None, “National Electric Sector Cybersecurity Organization Resource (NESCOR),” Tech. Rep. 1163840, Jun. 2014. [Online]. Available: http://www.osti.gov/servlets/purl/1163840/

[29] J. Yan, Y. Zhu, H. He, and Y. Sun, “Multi-contingency cascading analysis of smart grid based on self-organizing map,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 646–656, 4 2013, event: IEEE Transactions on Information Forensics and Security.

[30] Y. Dafalla, B. Liu, D. A. Hahn, H. Wu, R. Ahmadi, and A. G. Bardas, “Prosumer nanogrids: A cybersecurity assessment,” *IEEE Access*, vol. 8, pp. 131 150–131 164, 2020, event: IEEE Access.

[31] R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[32] T. M. Chen, “Stuxnet, the real start of cyber warfare?[editor’s note],” *IEEE Network*, vol. 24, no. 6, pp. 2–3, 2010.

[33] N. Falliere, L. O. Murchu, and E. Chien, “W32. stuxnet dossier,” *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, 2011.

[34] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, “Byzantine attack and defense in cognitive radio networks: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1342–1363, 2015.

[35] A. Geetha and N. Sreenath, “Byzantine attacks and its security measures in mobile adhoc networks,” *Intl Journal of Computing, Communications and Instrumentation Engineering (IJCCIE 2016)*, vol. 3, no. 1, pp. 42–47, 2016.

[36] G. Ding, J. Wang, Q. Wu, L. Zhang, Y. Zou, Y.-D. Yao, and Y. Chen, “Robust spectrum sensing with crowd sensors,” *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3129–3143, 2014.

[37] J. Qin, M. Li, L. Shi, and X. Yu, “Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks,” *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1648–1663, 2017.

[38] H. Zhang and W. X. Zheng, “Denial-of-service power dispatch against linear quadratic control via a fading channel,” *IEEE Transactions on Automatic Control*, vol. 63, no. 9, pp. 3032–3039, 2018.

[39] M. Zeller, “Common questions and answers addressing the aurora vulnerability,” *Schweitzer Engineering Laboratories Report*, 2011.

[40] M. Zeller, “Myth or reality does the aurora vulnerability pose a risk to my generator?” in *2011 64th Annual Conference for Protective Relay Engineers*, 2011, pp. 130–136.

[41] “Ieee standard for salient-pole 50 hz and 60 hz synchronous generators and generator/motors for hydraulic turbine applications rated 5 mva and above,” *IEEE Std C50.12-2005*, pp. 1–45, 2006.

[42] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, “Modeling cyber-physical vulnerability of the smart grid with incomplete information,” *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 235–244, 3 2013.

[43] M. F. Arani, A. A. Jahromi, D. Kundur, and M. Kassouf, “Modeling and simulation of the aurora attack on microgrid point of common coupling,” in *2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*. IEEE, 2019, pp. 1–6.

[44] “Ieee approved draft standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces - amendment 1 to ieee std 1547-2018 to provide more flexibility for adoption of abnormal operating performance category iii,” *IEEE P1547a/D1.4, January 2020*, pp. 1–17, 3 2020.

[45] R. Tan, V. Badrinath Krishna, D. K. Yau, and Z. Kalbarczyk, “Impact of integrity attacks on real-time pricing in smart grids,” 2013, p. 439450.

[46] Y. Zhang, V. V. G. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn, and S. Suresh, “Cyber physical security analytics for transactive energy systems,” *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 931–941, 3 2020.

[47] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, “Dependable demand response management in the smart grid: A stackelberg game approach,” *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 120–132, 3 2013, event: IEEE Transactions on Smart Grid.

[48] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, “Modeling and mitigating impact of false data injection attacks on automatic generation control,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1609–1624, 7 2017, event: IEEE Transactions on Information Forensics and Security.

[49] J. Giraldo, A. Crdenas, and N. Quijano, “Integrity attacks on real-time pricing in smart grids: Impact and countermeasures,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2249–2257, 9 2017.

[50] S. Sridhar and M. Govindarasu, “Model-based attack detection and mitigation for automatic generation control,” *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, 3 2014.

[51] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, “Novel detection scheme design considering cyber attacks on load frequency control,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1932–1941, 5 2018, event: IEEE Transactions on Industrial Informatics.

[52] Y. Liu, N. Peng, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS ’09. New York, NY, USA: Association for Computing Machinery, 2009, p. 2132. [Online]. Available: https://doi.org/10.1145/1653662.1653666

[53] Y. Liu, N. Peng, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[54] B. M. Horowitz and K. M. Pierce, “The integration of diversely redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems,” *Systems Engineering*, vol. 16, no. 4, pp. 401–412, 2013, _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/sys.21239.

[55] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, “Detecting false data injection attacks on dc state estimation,” vol. 2010, 2010.

[56] Z. Wang, Y. Chen, F. Liu, Y. Xia, and X. Zhang, “Power system security under false data injection attacks with exploitation and exploration based on reinforcement learning,” *IEEE Access*, vol. 6, pp. 48 785–48 796, 2018, event: IEEE Access.

[57] J. Liang, L. Sankar, and O. Kosut, “Vulnerability analysis and consequences of false data injection attack on power system state estimation,” *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3864–3872, 2016.

[58] G. Hug and J. A. Giampapa, “Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks,” *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 9 2012.

[59] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, “A review of false data injection attacks against modern power systems,” *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 7 2017.

[60] K. C. Sou, H. Sandberg, and K. H. Johansson, “Electric power network security analysis via minimum cut relaxation.” 2011 50th IEEE Conference on Decision and Control and European Control Conference, 12 2011, pp. 4054–4059, iSSN: 0743-1546.

[61] H. Wang, J. Ruan, G. Wang, B. Zhou, Y. Liu, X. Fu, and J. Peng, “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, 11 2018, event: IEEE Transactions on Industrial Informatics.

[62] J. Liang, L. Sankar, and O. Kosut, “Vulnerability analysis and consequences of false data injection attack on power system state estimation,” *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3864–3872, 2016.

[63] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. Vincent Poor, “Distributed models for sparse attack construction and state

vector estimation in the smart grid," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, 2012, pp. 306–311.

[64] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 4868–4877, 2018.

[65] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," *IEEE Transactions on Signal Processing*, vol. 63, no. 5, pp. 1102–1114, 3 2015, event: IEEE Transactions on Signal Processing.

[66] Z.-H. Yu and W.-L. Chin, "Blind false data injection attack using pca approximation method in smart grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1219–1226, 5 2015.

[67] "Principle component analysis: Springer series in statistics," in *Principal Component Analysis*, I. T. Jolliffe, Ed. New York, NY: Springer New York, 2002, pp. 1–9. [Online]. Available: https://doi.org/10.1007/0-387-22440-8_1

[68] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids." 2012 IEEE Global Communications Conference (GLOBECOM), 12 2012, pp. 3153–3158, iSSN: 1930-529X.

[69] V. Kekatos, G. B. Giannakis, and R. Baldick, "Grid topology identification using electricity prices." 2014 IEEE PES General Meeting | Conference Exposition, 7 2014, pp. 1–5, iSSN: 1932-5517.

[70] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid." 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), 10 2011, pp. 244–248.

[71] M. M. Higgins, D. F. Teng, and P. T. Parisini, "Stealthy mtd against unsupervised learning-based blind fdi attacks in power systems," *arXiv preprint arXiv:2004.07004*, 2020.

[72] R. Deng and H. Liang, "False data injection attacks with limited susceptance information and new countermeasures in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1619–1628, 2019.

[73] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "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, 3 2019, event: IEEE Transactions on Smart Grid.

[74] I. Markwood, Y. Liu, K. Kwiat, and C. Kamhoua, "Electric grid power flow model camouflage against topology leaking attacks." IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, 5 2017, pp. 1–9.

[75] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 6 2011.

[76] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 7 2014.

[77] H. Zhang, B. Liu, and H. Wu, "Net load redistribution attacks on nodal voltage magnitude estimation in ac distribution networks," in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, 2020, pp. 46–50.

[78] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Transactions on Power Systems*, vol. 34, no. 2, pp. 1513–1523, 3 2019, event: IEEE Transactions on Power Systems.

[79] D. Choeum and D. Choi, "Vulnerability assessment of conservation voltage reduction to load redistribution attack in unbalanced active distribution networks," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[80] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power system reliability evaluation considering load redistribution attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 889–901, 2017.

[81] J. Fu, L. Wang, B. Hu, K. Xie, H. Chao, and P. Zhou, "A sequential coordinated attack model for cyber-physical system considering cascading failure and load redistribution," in *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, 2018, pp. 1–6.

[82] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1294–1305, 7 2013.

[83] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the gnss spoofing threat and countermeasures," *ACM Computing Surveys*, vol. 48, no. 4, pp. 1–31, 5 2016.

[84] Y. Cui, F. Bai, Y. Liu, P. L. Fuhr, and M. E. Morales-Rodrguez, "Spatio-temporal characterization of synchrophasor data against spoofing attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5807–5818, 9 2019, event: IEEE Transactions on Smart Grid.

[85] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to gps spoofing," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3535–3548, 7 2019, event: IEEE Transactions on Smart Grid.

[86] L. Che, X. Liu, and Z. Li, "Fast screening of high-risk lines under false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4003–4014, 2018.

[87] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2617–2626, 11 2017.

[88] S. Soltan, M. Yannakakis, and G. Zussman, "React to cyber attacks on power grids," *IEEE Transactions on Network Science and Engineering*, vol. 6, no. 3, pp. 459–473, 7 2019.

[89] S. Soltan and G. Zussman, "Expose the line failures following a cyber-physical attack on the power grid," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 1, pp. 451–461, 3 2019.

[90] S. Soltan, P. Mittal, and H. V. Poor, "Line failure detection after a cyber-physical attack on the grid using bayesian regression," *IEEE Transactions on Power Systems*, vol. 34, no. 5, pp. 3758–3768, 9 2019.

[91] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, Y. Zhang, and C.-K. Wen, "Local cyber-physical attack for masking line outage and topology attack in smart grid," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4577–4588, 7 2019.

[92] R. Deng, P. Zhuang, and H. Liang, "Ccpa: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420–2430, 9 2017.

[93] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2011, pp. 4490–4494.

[94] J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, "Moving target defense approach to detecting stuxnet-like attacks," *IEEE Transactions on Smart Grid*, pp. 1–1, 2019.

[95] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.

[96] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2260–2272, 9 2016, event: IEEE Transactions on Smart Grid.

[97] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Analyzing locally coordinated cyber-physical attacks for undetectable line outages," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 35–47, 2018.

[98] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *2009 47th annual Allerton conference on communication, control, and computing (Allerton)*. IEEE, 2009, pp. 911–918.

[99] S. Weerakkody, Y. Mo, and B. Sinopoli, "Detecting integrity attacks on control systems using robust physical watermarking." 53rd IEEE Conference on Decision and Control, Dec. 2014, pp. 3757–3764, iSSN: 0191-2216.

[100] D. Simon, "Kalman filtering with state constraints: a survey of linear and nonlinear algorithms," *IET Control Theory & Applications*, vol. 4, no. 8, pp. 1303–1318, 2010.

[101] R. K. Mehra and J. Peschon, "An innovations approach to fault detection and diagnosis in dynamic systems," *Automatica*, vol. 7, no. 5, pp. 637–640, 1971.

[102] Y. Chakhchoukh, V. Vittal, and G. T. Heydt, "Pmu based state estimation by integrating correlation," *IEEE Transactions on Power Systems*, vol. 29, no. 2, pp. 617–626, 2013.

[103] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures." 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), 10 2011, pp. 232–237.

[104] J. Qi, K. Sun, and W. Kang, "Optimal pmu placement for power system dynamic state estimation by using empirical observability gramian," *IEEE Transactions on Power Systems*, vol. 30, no. 4, pp. 2041–2054, 7 2015, event: IEEE Transactions on Power Systems.

[105] A. Pal, A. K. S. Vullikanti, and S. S. Ravi, "A pmu placement scheme considering realistic costs and modern trends in relaying," *IEEE Transactions on Power Systems*, vol. 32, no. 1, pp. 552–561, 1 2017, event: IEEE Transactions on Power Systems.

[106] M. Sarailoo and N. E. Wu, "Cost-effective upgrade of pmu networks for fault-tolerant sensing," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 3052–3063, 5 2018, event: IEEE Transactions on Power Systems.

[107] Q. Yang, D. An, and W. Yu, "On time desynchronization attack against ieee 1588 protocol in power grid systems." 2013 IEEE Energytech, 5 2013, pp. 1–5.

[108] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, 3 2013, event: IEEE Transactions on Smart Grid.

[109] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Domnguez-Garca, "Spoofing gps receiver clock offset of phasor measurement units," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3253–3262, 8 2013, event: IEEE Transactions on Power Systems.

[110] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against gps spoofing attacks on pmus in smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2659–2668, 11 2015, event: IEEE Transactions on Smart Grid.

[111] Y. Huang, H. Li, K. A. Campbell, and Z. Han, "Defending false data injection attack on smart grid network using adaptive cusum test." 2011 45th Annual Conference on Information Sciences and Systems, 3 2011, pp. 1–6.

[112] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, 3 2014, event: IEEE Transactions on Smart Grid.

[113] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 9 2015, event: IEEE Transactions on Smart Grid.

[114] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1580–1590, Jul. 2017, event: IEEE Transactions on Smart Grid.

[115] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1636–1646, May 2018, event: IEEE Transactions on Smart Grid.

[116] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1773–1786, 2016.

[117] J. Yan, B. Tang, and H. He, "Detection of false data attacks in smart grid with supervised learning," in *2016 International Joint Conference on Neural Networks (IJCNN)*, 2016, pp. 1395–1402.

[118] J. Sakhnini, H. Karimipour, and A. Dehghantanha, "Smart grid cyber attacks detection using supervised learning and heuristic feature selection," in *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, 2019, pp. 108–112.

[119] X. Niu, J. Li, J. Sun, and K. Tomsovic, "Dynamic detection of false data injection attack in smart grid using deep learning," in *2019 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2019, pp. 1–6.

[120] Y. Li, Y. Wang, and S. Hu, "Online generative adversary network based measurement recovery in false data injection attacks: A cyber-physical approach," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2031–2043, 2020.

[121] G. Ding, Q. Wu, Y.-D. Yao, J. Wang, and Y. Chen, "Kernel-based learning for statistical signal processing in cognitive radio networks: Theoretical foundations, example applications, and future directions," *IEEE Signal Processing Magazine*, vol. 30, no. 4, pp. 126–136, 2013.

[122] T. Xie, N. M. Nasrabadi, and A. O. Hero, "Learning to classify with possible sensor failures," *IEEE Transactions on Signal Processing*, vol. 65, no. 4, pp. 836–849, 2016.

[123] Z. Qin, Y. Gao, and M. D. Plumbley, "Malicious user detection based on low-rank matrix completion in wideband spectrum sensing," *IEEE Transactions on Signal Processing*, vol. 66, no. 1, pp. 5–17, 2017.

[124] E. Al-Shaer, Q. Duan, and J. H. Jafarian, "Random host mutation for moving target defense," A. D. Keromytis and R. Di Pietro, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 310–327.

[125] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology perturbation for detecting malicious data injection." 2012 45th Hawaii International Conference on System Sciences, Jan. 2012, pp. 2104–2113, iSSN: 1530-1605.

[126] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense." 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Nov. 2012, pp. 342–347.

[127] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," the First ACM Workshop. Scottsdale, Arizona, USA: ACM Press, 2014, pp. 59–68, [Online; accessed 2020-05-16]. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2663474.2663482

[128] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying fdi attacks in power system state estimation," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, pp. 763–776, 8 2018, event: IEEE Journal of Selected Topics in Signal Processing.

[129] B. Liu and H. Wu, "Optimal d-facts placement in moving target defense against false data injection attacks," *IEEE Transactions on Smart Grid*, pp. 1–1, 2020, event: IEEE Transactions on Smart Grid.

[130] Z. Zhang, R. Deng, D. K. Yau, P. Cheng, and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2320–2335, 2019.

[131] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using d-facts devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 854–864, 2 2020.

[132] S. Lakshminarayana and D. K. Yau, "Cost-benefit analysis of moving-target defense in power grids," *IEEE Transactions on Power Systems*, 2020.

[133] B. Liu, L. Edmonds, H. Zhang, and H. Wu, "An interior-point solver for optimal power flow problem considering distributed facts devices," in *2020 IEEE Kansas Power and Energy Conference (KPEC)*, 2020, pp. 1–5.

[134] B. Liu, H. Wu, A. Pahwa, F. Ding, E. Ibrahim, and T. Liu, "Hidden moving target defense against false data injection in distribution network reconfiguration," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2018, pp. 1–5.

[135] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2208–2223, 3 2019.

[136] Z. Zhang, R. Deng, D. K. Yau, P. Cheng, and J. Chen, "On hiddenness of moving target defense against false data injection attacks on power grid," *ACM Transactions on Cyber-Physical Systems*, vol. 4, no. 3, pp. 1–29, 2020.

[137] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 93–109, 2 2015, event: IEEE Control Systems Magazine.

[138] F. Miao, M. Pajic, and G. J. Pappas, "Stochastic game approach for replay attack detection," in *52nd IEEE conference on decision and control*. IEEE, 2013, pp. 1854–1859.

[139] B. Satchidanandan and P. R. Kumar, "Dynamic watermarking: Active defense of networked cyber–physical systems," *Proceedings of the IEEE*, vol. 105, no. 2, pp. 219–240, 2016.

[140] A. Ferdowsi and W. Saad, "Deep learning-based dynamic watermarking for secure signal authentication in the internet of things," in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–6.

[141] Y. Zhang, J. Wang, and J. Liu, "Attack identification and correction for pmu gps spoofing in unbalanced distribution systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 762–773, 1 2020, event: IEEE Transactions on Smart Grid.

[142] J. Bélanger, P. Venne, and J.-N. Paquin, "The what, where and why of real-time simulation," *Planet Rt*, vol. 1, no. 1, pp. 25–29, 2010.

[143] C. Davis, J. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "Scada cyber security testbed development," in *2006 38th North American Power Symposium*. IEEE, 2006, pp. 483–488.

[144] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of scada control systems (tasscs)," in *ISGT 2011*. IEEE, 2011, pp. 1–7.

[145] T. Strasser, M. Stifter, F. Andrén, and P. Palensky, "Co-simulation training platform for smart grids," *IEEE Transactions on Power Systems*, vol. 29, no. 4, pp. 1989–1997, 2014.

[146] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in rtds and opnet," in *2014 North American Power Symposium (NAPS)*. IEEE, 2014, pp. 1–6.

[147] M. H. Athari and Z. Wang, "Impacts of wind power uncertainty on grid vulnerability to cascading overload failures," *IEEE Transactions on Sustainable Energy*, vol. 9, no. 1, pp. 128–137, 2017.

[148] A. Muir and J. Lopatto, "Final report on the august 14, 2003 blackout in the united states and canada: causes and recommendations," *US–Canada Power System Outage Task Force, Canada*, 2004.

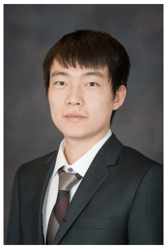
[149] F. E. R. Commission *et al.*, "Arizona-southern california outages on september 8, 2011: Causes and recommendations," *FERC and NERC Staff, Apr*, 2012.

[150] L. Wang, Z. Qu, Y. Li, K. Hu, J. Sun, K. Xue, and M. Cui, "Method for extracting patterns of coordinated network attacks on electric power cps based on temporal–topological correlation," *IEEE Access*, vol. 8, pp. 57 260–57 272, 2020.

[151] F. Pasqualetti, F. Dörfler, and F. Bullo, "A divide-and-conquer approach to distributed attack identification," in *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE, 2015, pp. 5801–5807.

[152] F. Fusco, "General bad data identification and estimation in the presence of critical measurement sets," in *2014 IEEE PES General Meeting— Conference & Exposition*. IEEE, 2014, pp. 1–5.

[153] A. Primadianto and C.-N. Lu, "A review on distribution system state estimation," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3875–3883, 2016.



Hang Zhang (S'2020) received his B.S. and M.S. degree in Electrical and Computer Engineering at Kansas State University, Manhattan, KS, USA in 2017 and 2018, respectively. He is currently pursuing the Ph.D. degree in Electrical and Computer Engineering at Kansas State University, Manhattan, KS, USA. His research interests include cyber-physical security and resiliency of power systems, machine learning, and renewable energy.

Bo Liu (S'18) received his B.S. and M.S. degree in Electrical Engineering from Harbin Institute of Technology, China in 2013 and 2015, respectively. He is currently working toward the Ph.D. degree in Electrical and Computer Engineering at Kansas State University, Manhattan, KS, USA. His current research interests include cyber-physical security of power systems, smart grid technologies, machine learning, and state estimation in smart grids.

Hongyu Wu (SM'15) received the B.S. degree in Energy and Power Engineering and the Ph.D. degree in Control Science and Engineering from Xi'an Jiaotong University, Xi'an, China, respectively. He is an Assistant Professor and a Michelle Munson-Serban Simu Keystone Research Faculty Scholar with the Department of Electrical and Computer Engineering, Kansas State University (K-State), Manhattan, KS, USA. He is a National Science Foundation EPSCoR research fellow and a team member in the IEEE-NERC Security Integration Project. Before joining K-State, he was a Research Engineer with Power Systems Engineering Center, National Renewable Energy Laboratory, Golden, CO, USA. From 2011 to 2014, he was a Postdoctoral Researcher with the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, IL, USA. His research interests include cyber-physical security of smart grids, power system planning, operation and energy management, as well as grid integration of renewable energy.