IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 22, 2018, accepted November 2, 2018, date of publication November 9, 2018,
date of current version December 7, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2879996

A Survey on Power Grid Cyber Security: From Component-Wise Vulnerability Assessment to System-Wide Impact Analysis

XIAOGE HUANG, ZHIJUN QIN, (Member, IEEE), AND HUI LIU, (Senior Member, IEEE)
College of Electrical Engineering, Guangxi University, Nanning 530004, China

Corresponding author: Zhijun Qin (zjqin@ gxu.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 51767001.

ABSTRACT The now ubiquitous use of information technology poses a crucial challenge to the cyber security of power grid operations, one that has aroused serious concerns from both industry and academia. The state-of-the-art research either focuses on the vulnerability assessment of particular types of components or concentrates on the prevention and mitigation of cyber attacks from the power grid's perspective. Complete causal chains connecting component vulnerabilities to cyber attacks causing malicious system-wide effects are unclear, which hinders cyber-attack prevention and the consolidation of affected components. To bridge this research gap, this survey aims to study two issues that need further investigation. On one hand, the causal relationship between power grid component vulnerabilities and resulting cyber attacks has not been thoroughly explored. On the other hand, the evolvement of cyber attacks, from initial attempt to resulting serious consequences has not been resolved. To study these two issues, we first analyze various stakeholders and associated information flows in diverse applications in power grid operation. Second, we summarize the root cause of cyber attacks in the vulnerability of communication protocols. Third, a multi-stage model is proposed to describe the cyber vulnerabilities, which reveals potential attacks and their evolvement on power grid components at each stage, assesses the associated impact on the entire power grid, and elucidates possible countermeasures. With the above efforts, this survey establishes a complete causal chain from component-wise vulnerability to system-wide impact assessment for enhancing cyber security, and potential research directions for enhancing power grid cyber security are identified.

INDEX TERMS Cyber security, power grid component vulnerability, countermeasure, causal relationship, cyber attack evolvement.

I. INTRODUCTION

A. MOTIVATION AND RELATED WORK

The ever more frequent emergencies occurring due to cyber security issues, and their catastrophic effects on power grid operations, have aroused significant attention from both industry and academia. According to a report from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), cyber security failures was ranked first among all power grid incidents for frequency in 2013 and 2014 [1]. One recent real-world cyber attack that led to serious consequences serves as a strong reminder underscoring the importance of enhancing power grid cyber security. On December 23, 2015, the Supervisory Control and Data Acquisition (SCADA) system of the Ukrainian power grid lost its self-control capabilities due to an attack of malicious code, one that influenced at least three control zones [2]. This attack led to a blackout of seven 110-kV substations and twenty-three 35-kV substations. As a result, the power supply for over 80,000 users was interrupted. Therefore, research on this topic grows rapidly to cover the increasingly wide spectrum of technical challenges.

Power grids being compromised by large-scale continuous cyber attacks are low-probability and high-impact events. The prevention, mitigation, and restoration of cyber attack events need to be addressed in a holistic manner to enhance the resilience of power grid against these malicious attacks. The definition of power grid resilience [3]–[5], evaluation methodologies [6], [7], countermeasure strategies against cyber attacks, and restoration strategies to resume system functionality have been proposed. We notice that the cyber

security of power grids depends on the connection and the relationship between the cyber and physical infrastructure of power grid, the evolvement of cyber attacks from targeting power system components to causing system-wide impact plays the central role in both incident-focused viewpoint and post-incident learning viewpoint of power grid resilience [8].

To better understand the state-of-the-art of the research in power grid cyber security, several literature reviews have been published. References [9]–[11] provided reviews on system-wide cyber vulnerabilities and their effects on entire energy networks, while [12]–[16] primarily paid attention to the taxonomy of well-known cyber attacks on power grids. The authors of the latter reviews considered potential threats on various target domains (generation, transmission, distribution, etc.) and listed a number of countermeasures, which included risk assessments, detection methods, and mitigation to preserve the safe operation of the power grid. Some researchers have also conducted thorough reviews of cyber security issues in general cyber-physical system (CPS) [17]–[19], which described the structure, vulnerability, and cyber attacks of such systems (currently power grids are typical examples of CPS). Nonetheless, the above surveys were limited to exploring only certain research directions. Due to the lack of a causal chain from component-wise cyber vulnerabilities to potential attacks affecting entire systems, a comprehensive study is needed to advance the detection, mitigation, and prevention of cyber attacks on power grids.

We argue that, to augment the perspectives of the aforementioned surveys, two fundamental questions need further clarification: 1) the causal relationship between the vulnerabilities of power grid components and resulting cyber attacks should be thoroughly determined; and 2) the evolvement of cyber attacks, from initial attempt to resulting serious consequences must be understood. Resolving the above two questions will help identify a complete causal chain from component-wise vulnerabilities to system-wide consequences. Furthermore, modern power grid components should also involve the consideration of cyber security features and functions into their design process to resist cyber attacks more effectively [20]. Therefore, it is necessary to determine which components are vulnerable and understand the correspondence between these vulnerabilities and associated threats, which in turn guide the design of these components.

B. CONTRIBUTION AND PAPER ORGANIZATION

In an attempt to address the aforementioned questions, this work aims to: 1) provide a comprehensive landscape describing power grid cyber security challenges; 2) demonstrate potential cyber-attack risks on various stakeholders in power grid operations; 3) describe the root causes and possible consequences of various types of cyber attacks; and 4) summarize the taxonomy and scenarios of cyber attacks as well as discuss feasible countermeasures.

For sake of clarification, the major contribution of this survey is highlighted as follows. First, we establish a complete causal chain from the venerability of power grid components to the system-wide impact caused by realized cyber attacks. The major building blocks for concatenating such a causal chain are shown in Fig. 1, which provides a starting point for researchers to strengthen cyber security research and highlights the contribution of our survey. Second, in the light of the complete causal chain, state-of-the-art and potential research opportunities are discussed in detail to enhance the research of power grid cyber securities.

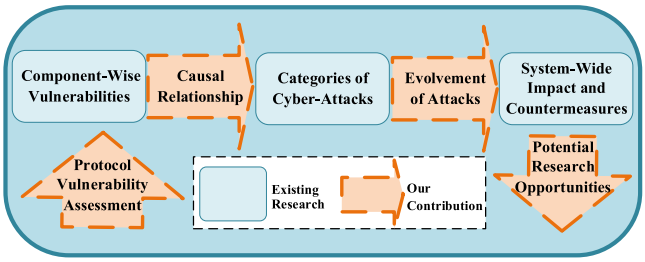

FIGURE 1. Building blocks to concatenate the causal chain of cyber attacks.

The remainder of this work is organized as follows. In section II, we demonstrate how information technology (IT) infrastructure plays an increasingly central role in power grid operations and provide a landscape for power grid cyber security challenges. In Section III, we summarize a wide spectrum of vulnerabilities in various communication protocols that exist among power grid components and the entire power grid. These vulnerabilities can be the starting point of cyber attacks. In Section IV, we investigate the taxonomy and effects of known attacks, the causal relationship between attacks and vulnerabilities, and the evolvement process of these attacks. In Section V, we discuss countermeasures for the aforementioned attacks and suggest research opportunities for further study. Finally, some concluding remarks and discussion are provided in section VI.

II. SIGNIFICANCE OF CYBER SECURITY FOR MODERN POWER GRIDS

To understand the significance of existing power grid cyber security needs, we provide an overview in this section that includes 1) the scope of cyber security required for power grids and 2) a landscape for power grid cyber security challenges.

A. THE SCOPE OF POWER GRID CYBER SECURITY

1) CYBER SECURITY IN A CYBER-PHYSICAL SYSTEM

The current operational paradigm of power grids, namely smart grids, contains the largest cyber-physical systems in the world. To scope the cyber security problem in power grids persuasively, it is necessary to scope the research directions in terms of a CPS.

A CPS usually refers to a system that integrates computing processes and physical processes, possesses advanced capability, adaptability, scalability, resiliency, safety, and security

characteristics [21]. Smart grids, modern medical equipment, and transportation control systems are all typical cyber-physical systems [22]. A CPS can be viewed as the integration of two types of components: 1) cyber components and 2) physical components. The physical components are the parts of the system that directly connect to the physical world. The remaining parts that interact with the physical world via communication media are cyber components. For example, field devices such as sensors that directly connect to the physical environment through an analog input belong to the physical component. On the other hand, remote terminal units (RTUs) that exist extensively in cyber-physical systems and connect with sensors or other field devices are considered, in most cases, to be cyber components. For this study, the CPS cyber security problem only refers to security issues affecting the cyber network and ignores the physical security of physical components.

2) THE CYBER SECURITY OF POWER GRIDS

Power grid components can be divided into two categories: 1) power applications and 2) supporting infrastructures [23]. Power applications refer to applications that interact with the physical word and fulfill basic tasks to satisfy the customers' energy demands, which are considered as the physical part of a power grid. For example, the transmission network, generators, and so on, which are responsible for preserving the quality of electricity provided to customers, belong to the power applications category. The cyber part of the supporting infrastructure category supports and sustains the daily operations of the power grid. This category includes monitoring systems, data acquisition and processing systems, and communication networks.

To solve cyber security issues for power grids, it is essential to maintain proper operation of all supporting infrastructure.

B. THE LANDSCAPE FOR POWER GRID CYBER SECURITY CHALLENGES

We argue that the explosive growth in two areas, namely the volume of communicating equipment used in supporting infrastructures and the number of various stakeholders in electricity markets, is the main reason for the growing cyber security challenge found in modern power grids. More communication equipment and stakeholders increase the opportunities for attackers to link to supporting infrastructures and to initiate cyber attacks. Based on the National Institute of Standards and Technology (NIST) seven-domain smart grid framework [24], we depict the landscape for these challenges that cause by additional communicating equipment in Fig. 2. Specifically, we add modern IT components, which depend on information interaction capabilities and needs, to expand the specific domain defined in NIST framework. The detailed of these infrastructures are explained as below.

1) ELECTRICITY MARKET

In many current electricity markets, the growing number of players and amount of vulnerable communication links are risk to the power grid. The number of gencos (generation companies), discos (distribution companies) and retailers have increased significantly [25]. In the traditional monopoly market model, generation and transmission networks were mostly owned by the same company, therefore their communications were conducted through a relatively secure intranet. However, the expansion of roles in power grids seen in the current model increases the difficulty of intranet communication [26], therefore attackers can acquire more opportunities to influence energy bidding and distributed energy resource aggregation through such modified operations in Internet communication.

2) OPERATIONS

The domain of Operations maintains the complicated network of communication devices and thus poses the greatest risk in all domains. The SCADA systems within the operation domain communicate with all other domains, therefore attacks against the SCADA network can result in severe consequences. By invading SCADA systems, attackers are able to alter the distribution of power flow and affect system state estimation. In addition, attackers may even seize control of SCADA networks, causing devastating failures throughout the power grid. The aforementioned Ukrainian blackout in 2015 is one example of this type of attack.

3) GENERATION SYSTEMS

Attackers invade generation systems to create chaos during equipment operation. This type of attack can cause a device to act at the wrong timing or simply not act at all. Another purpose of such attacks is to destroy the power balance between supply-side and demand-side. This situation is becoming more frequent due to the rise in number of renewable power plants [27]. Unlike traditional power plants, renewable power plants rely on energy sources at very distributed locations. For example, solar collectors are generally located around buildings or on rooftops, while bioenergy depends on specific environments such as farms. Such geographical distribution increases risk in attack on communication links. Additionally, the lower startup cost, wide distribution, and ease of construction of renewable power plants results in the number of such plants exceeding largely that of traditional power plants. The rise of distributed renewable power generation increases the number of communication equipment, making such generation systems inherently more vulnerable to cyber attacks.

4) DISTRIBUTION, CUSTOMER, AND SERVICE PROVIDER DOMAINS

The distribution, customer, and service provider domains are the primary targets for privacy attacks. Customer information systems, third-party providers, smart meters, and advanced monitoring infrastructure (AMI) are novel supporting infrastructures with two-way communication capabilities [28], while electric vehicles and smart houses are new products that collect a huge amount of private customer data. Attacks

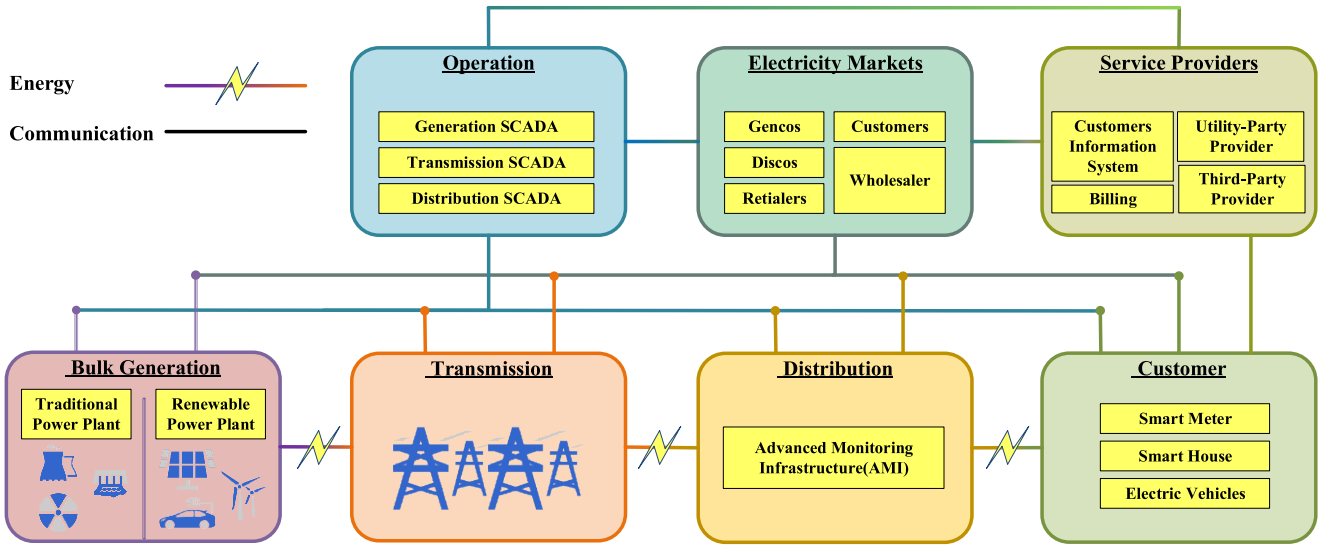

FIGURE 2. Novel expanded NIST power grid structure. Genco: generation companies; disco: distribution companies; SCADA: supervisory control and data acquisition

against any of these systems can lead to the leakage of customer information and results in inaccurate billing.

III. COMPONENT-WISE CYBER VULNERABILITY IN POWER GRIDS

As discussed in Section II, the implementation of wide-area communication across multiple components and various players in power grids poses a high risk of cyber attacks. However, information exchange and interoperability has been indispensable in power grid operations and it is difficult to improve cyber security by simply reducing communication. This circumstance calls for an innovative approach that eliminates the risk originated from the novel communication technology. Inspired by [29], we remark that there must be a strengthening of protocols used in existing communication technologies to improve cyber security in power grids.

In this section: 1) a general multi-stage model of a cyber attack is provided that describe the evolvement of the attack from initial probes to resulting consequences; and 2) the vulnerabilities inherent in various communication protocols used among power grid components and the entire power grid are summarized based on this multi-stage model.

A. GENERAL MULTI-STAGE MODEL OF A CYBER ATTACK

A typical cyber threat against supporting infrastructure consists of the following three stages: 1) interception and invasion, 2) attack preparation, and 3) launching the attack. The general multi-stage model of a cyber attack is depicted in Fig. 3. In Stage I, an attacker needs to intercept communication messages through encryption destruction after linking to a system, and invade this system through authentication forgery or through special internal channels that are independent of specific protocol vulnerabilities. In the second stage, obtaining access to the operating system is necessary

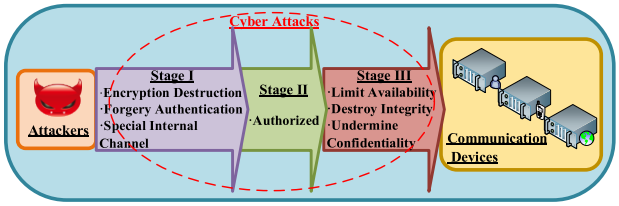

FIGURE 3. Genera l multi-stage model of a cyber attack.

to launch attacks, which requires the attacker to be authorized. In Stage III, the attacker achieves their attack intentions through three different operations: causing an impact on the availability of equipment, affecting the integrity of system data, or affecting the confidentiality of system data.

B. PROTOCOL VULNERABILITIES IN THE THREE STAGES OF A CYBER ATTACK

1) STAGE I: INTERCEPTION AND INVASION

In Stage I, the attacker's actions do not affect the normal operation of the power grid, and the only goal of the attacker is to invade the system or intercept data by intercepting signals from the communicating devices in the cyber system. Therefore, the most significant protocol vulnerabilities for this stage are as follows.

a. Authentication vulnerabilities: the authentication mechanism in the protocol for confirming the identity of the visitor is vulnerable to attackers. In this case, the attacker can successfully establish an access channel without disguising their identity.
b. Encryption vulnerabilities: the communication message possesses almost no leakage protection in the protocol. Once the communication signal is maliciously intercepted by the attacker, the attacker can extract

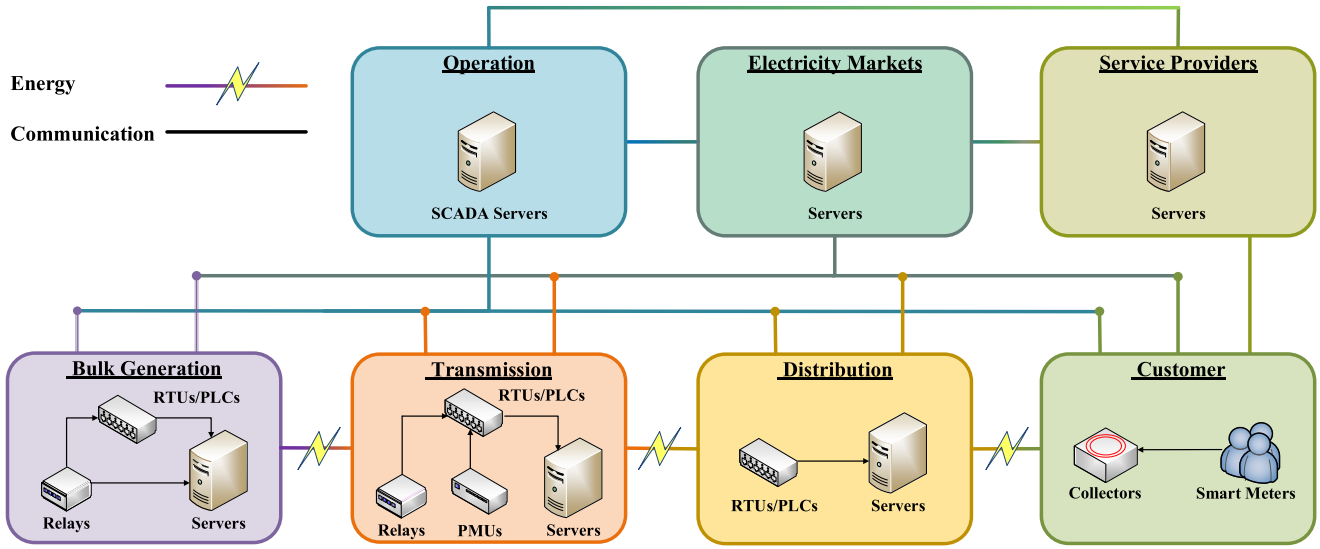

FIGURE 4. Potential effected components by cyber attacks in a power grid.

communication data between communication devices without cracking the encryption.

2) STAGE II: PREPARING FOR AN ATTACK

Once an access channel has been established, an attacker next prepares to conduct sabotage operations against a cyber system to achieve malicious purposes. The protocol vulnerabilities that are particularly prominent in this stage are:

c. Authorization management vulnerabilities: a communication protocol with this vulnerability is not capable of providing strong supervision over the behavior of visitors to the system. Attackers can exploit this vulnerability to expand their operations in the cyber system.

3) STAGE III: LAUCHING AN ATTACK

From the point of view of the effects of the attack, we can divide the potential intent of the attacker into three categories: targeting the integrity of the data received by the system; targeting the availability of system equipment; or targeting system data privacy. The protocol vulnerabilities for these three categories in this stage are:

d. Confidentiality protection vulnerabilities: this kind of protocol vulnerability provides an attacker the opportunity to read private information and illegally steal large amounts of data.

e. Integrity protection vulnerabilities: packets containing false data or incomplete data can be sent to or from the system through these vulnerable protocols.

f. Availability protection vulnerabilities: The attacker can use this protocol vulnerability to affect other devices through parameter modification, etc., which eventually results in the device losing control or failing to operate properly.

C. POTENTIAL EFFECTED COMPONENTS BY CYBER ATTACKS IN POWER GRIDS

To assist in recognizing power grid vulnerabilities, Fig. 4 depicts the numerous common and representative points in the power grid that may suffer cyber attacks. The figure shows the communication networks that can be exploited to communicate among the sub-systems in the aforementioned seven domains. The following components are vulnerable to cyber attacks within these domains:

- Protective relays are secondary protection devices that switch on/off the circuit by detecting the change of electrical signals (e.g., current and voltage), and use the IEC61850/Modbus communications protocol to receive real-time commands that determine their actions [9]. Relays are mainly distributed throughout bulk generation systems and the transmission system.
- Remote terminal units (RTUs) and power line communication (PLC) devices are common in power plants, the transmission network, and the distribution network, and are installed at remote sites to monitor, measure, and control field devices. These components depend on Modbus and DNP3 protocols to interact with other devices [17].
- The phasor measurement unit (PMU) performs synchronous phasor measurements and outputs, along with dynamic recording based on a standard clock signal in the transmission system. The communication standard IEEE 37.118 is implied in the synchronization data exchange process of PMUs [30].
- The smart meter is a modern client-side information collection device with two-way communication capabilities. One of the most widely used communication protocols for smart meters is Modbus [31].
- Servers in each domain interact with SCADA in operations and the market through numerous

TABLE 1. Protocol vulnerabilities in power grids.

Component	Domain	Protocol	Vulnerabilities			Reference
			Stage I	Stage II	Stage III	
RTU/PLC	Bulk generation, transmission, distribution	Modbus / DNP3	a,b	c	e,f	[32-36]
Relay	Bulk generation, transmission	IEC61850/Modbus	a,b		e,f	[37-41]
Smart meter	Customer	Modbus	a		e,f	[38, 42, 43]
PMU	Transmission	IEEE 37.118	a		d,e,f	[44, 45]
Server	Bulk generation, transmission, distribution, operation	IEC61850	a,b			[46, 47]
Note: the following letters are used to denote the vulnerabilities: a: vulnerable in authentication; b: vulnerable in encryption; c: vulnerable in authorization management; d: vulnerable in confidentiality protection; e: vulnerable in integrity protection; f: vulnerable in availability protection.						

communication channels, including WANs, Internet, LAN, FAN, and so on [18]. This wide assortment of communication paths contains many complicated protocols. The Internet-based protocol IEC61850 is taken as an example here.

D. COMPONENT-WISE VULNERABILITIES IN POWER GRIDS

We summarize the relationship between components, domains, protocols, and the vulnerabilities in Table 1. The vulnerability of each communication protocol is also separated by the stage of the attack to support the development of protection strategies and reveal potential attacks.

IV. FROM COMPONENT-WISE VULNERABILITY TO SYSTEM-WIDE IMPACT

We aim to develop the causal chain of the component vulnerability causing system-wide impact by cyber attacks. Although many researchers have studied the taxonomy of cyber attacks in the power grid, most of work did not construct a causal link between the cyber attack and a series of controllable cyber vulnerabilities, thus hindering the development of cyber-attack prevention. We argue that the obstacle to establishing this connection is a negligence in determining the evolvement of attacks.

Many cyber attacks on power grids have already occurred throughout the world and continue to occur, and most of them can be classified based on their *impact* on the confidentiality or the integrity of data, or on the availability of devices. However, such a classification provides little insight to capture the evolvement of cyber attacks.

Instead, we refer to these types of known attacks as *impact-based* attacks. Similarly, attacks classified based on protocol vulnerabilities are defined as *protocol-based* attacks. We observe that *impact-based* attacks evolve from a combination of multiple *protocol-based* attacks, as will be elaborated in the following subsections. *Impact-based* attacks, e.g., fake data injection attack, contain less information about the scenario of attack and only focus on the resulting impact of the attack on system data or devices. However, without clear understanding on how the attack scenario evolves from a *protocol-based* attack to an *impact-based* attack, it is substantially difficult for researchers to comprehensively link specific vulnerabilities with a given cyber attack and its effect on the system.

To improve this situation, this section 1) summarizes the causal relationship between *protocol-based* attacks and specific cyber vulnerabilities, 2) provides a taxonomy of *impact-based* attacks and their system-wide impact, and 3) infers the evolution of cyber attacks from the initial attempt to their significant system effects based on the scope and principle of the *protocol-based* attack.

A. PROTOCOL-BASED ATTACKS AND THEIR TARGETED VULNERABILITES

1) MAN-IN-THE MIDDLE ATTACK

This attack targets vulnerabilities in authentication and authorization management, i.e., within stages I and II in the multi-stage model of cyber attacks. Under this type of attack, there is a malicious attacker between two communication targets that may secretly relay or alter the communication message [48]. At best, the two sides in the communication can only identify the authenticity of the information and cannot prevent the middleman from falsifying or eavesdropping on the information they send out. This attack is common against protocols such as DNP3 [38], Modbus [38], and IEC61850 [49].

2) DENIAL OF SERVICE ATTACK

This attack targets vulnerabilities in availability protection within stage III in the multi-stage model of a cyber-attack. This type of attack interrupts the device's connection service, either temporarily or permanently, by flooding the target machine or resource with redundant requests to overload the system and prevent some or all legitimate requests from being satisfied [50]. This attack is ubiquitous in communication networks based on the Modbus [51], and DNP3 [52] protocols.

3) REPLAY ATTACK

This attack targets vulnerabilities in authentication during stage I. The malicious attacker records a piece of valid information from the transmission information, and then sends this valid information back to the service. This gives the attacker opportunities to pass through the authentication successfully. This type of attack targets communication systems based on Modbus [51], DNP3 [53], and IEC61850 [54] protocols.

4) INJECTION ATTACK

This attack targets integrity protection vulnerabilities within stage III. This form of attack is a crucial means for destroying the integrity of data in the system. With this attack, the attacker sends invalid data and commands that modify or partially delete data in the system. This type of attack usually occurs against communication channels based on DNP3 [55], IEC61850 [56], and IEEE C37.118 [57] protocols.

5) SPOOFING ATTACK

This attack targets authentication vulnerabilities during stage I of a cyber attack. Spoofing attacks occur where an unauthorized pass through the authentication is made by falsifying data. This situation is found in DNP3 [58], Modbus [37], IEC61850 [59], and IEEE C37.118 [57] *protocol-based* communication systems.

6) EAVESDROPPING ATTACK

This attack targets confidentiality protection vulnerabilities in stage III. The attacker secretly or stealthily captures data packets from the communication process, which can threaten the confidentiality of the system. Eavesdropping attacks have been seen in systems that rely on IEC61850 [60] and Modbus protocols [38].

7) MODIFICATION ATTACK

This attack targets vulnerabilities in integrity and availability protection within stage III. The attacker can achieve their goal by modifying data to threaten the availability of the device. This attack targets the communication protocols DNP3 [55], Modbus [38], IEC61850 [60], and IEEE C37.118 [45].

8) RECONNAISSANCE ATTACK

This attack is not directly aimed towards any one type of protocol vulnerability, but is a useful form of attack that assists other *protocol-based* attacks. Such attackers can capture communication content to discover potential vulnerabilities from the captured data so that more effective service disruption attacks can be launched. This kind of attack seek vulnerabilities in the DNP3 [61], IEC61850 [62], Modbus [63], and IEEE C37.118 [57] protocols.

B. TAXONOMY OF IMPACT-BASED ATTACKS AND SYSTEM-WIDE IMPACTS

1) INTEGRITY ATTACKS

The integrity attack works via maliciously inserting into the system and altering or deleting measurement parameters or commands to mislead the system [12]. This type of attack can be launched almost anywhere on the network, which lead to errors in electricity billing, dispatch, erroneous analysis, or even causing blackouts [64]. There are two forms of this attack: 1) attacks on state estimation and 2) data tampering that is not intended to influence state estimation.

a: ATTACKS ON STATE ESTIMATION

Integrity attacks on state estimation are known as a false data injection attack (FDIA). The state estimation of a power grid uses various measurement parameter data to estimate the current operating state of the system [65]. FDIA attackers mislead the system by modifying the measurement parameters used in the state estimation, which can produce estimates that are biased but difficult for operators to find.

The linearized DC model of a power grid's state estimation is described by

$$z = \boldsymbol{H}x + \boldsymbol{e}, \tag{1}$$

where $z = [P_k, Q_k, P_{k-m}, Q_{k-m}, V_k]^T$ refers to the measurement vectors originating from the measurement and acquisition devices in the system, $\boldsymbol{x} = [\theta_k, V_k]^T$ is the state vector, $\boldsymbol{H}$ is the Jacobian matrix corresponding to the topology of the power grid, and $\boldsymbol{e} \sim N(0,\sigma^2)$ is the noise in the state estimation, which is generated by errors in measurement, the communication process, or maliciously created by hackers and other attackers. The distribution of the noise $\boldsymbol{e}$ generally follows a Gaussian curve, and σ is its deviation.

The state of the system $\hat{\boldsymbol{x}}$ can be estimated by applying the weighted least square (WLS) method, calculated by

$$\hat{\boldsymbol{x}} = (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}z. \tag{2}$$

Here, $\boldsymbol{R}^{-1}$ is a diagonal matrix with diagonal elements $\boldsymbol{R}_{ii}^{-1} = \sigma^2$.

FDIA attackers create deviations in the state estimation by injecting poorly integrated measurement parameters $\hat{z}_{\boldsymbol{a}}$ into the system.

The estimation error caused by FDIAs is well concealed, as existing technologies mainly use bad data detection to prevent problematic data intrusion. The principle of this

method is to perform a threshold detection on $\ell 2$-norm of the measurement residual. When

$$\| z - \hat{z} \|^2 > \tau \tag{3}$$

is satisfied, where τ is a predetermined threshold, the assumption is that there is bad data in the measurement parameters. In this case,$\hat{z}$ is instead calculated using

$$\hat{z} \approx z + \boldsymbol{H}(\boldsymbol{x} - \hat{\boldsymbol{x}}). \tag{4}$$

However, FDIAs cannot be detected by traditional bad data detection. Assume $\hat{z}_a = z + \boldsymbol{a}$ is a modified data injected by attackers. If the attack satisfies the formula $\boldsymbol{a}=\boldsymbol{Hc}$, the attacker is able to deceive bad data detection due to the following condition (5) holds.

$$\begin{aligned} \| z_a - \hat{z} \|^2 &= \| z_a - \boldsymbol{H}\hat{x}_{bad} \|^2 \leq \tau \\ &= \| z + \boldsymbol{a} - \boldsymbol{H}(\hat{\boldsymbol{x}} + \boldsymbol{c}) \|^2 \\ &= \| z - \boldsymbol{H}\hat{x} + \boldsymbol{a} - \boldsymbol{H}c \|^2 \\ &= \| z - \boldsymbol{H}\hat{x} \|^2 \leq \tau \end{aligned} \tag{5}$$

Liu *et al.* [66] discovered this attack and pointed out that most FDIAs are concealed since they usually satisfy the condition $\boldsymbol{a}=\boldsymbol{Hc}$.

b: DATA TAMPERING ATTACKS

In most cases, tampering with the system's data is an important component for other types of attacks other than aiming to affect state estimation. Attacked points of data tampering are no longer limited in the measurement parameter of the power grid. For example, an attacker may affect the availability of the device by modifying the predetermined threshold.

2) CONFIDENTIALITY ATTACKS

Privacy attacks are prominently a confidentiality attack in power cyber systems, which mainly target the customer side of the system. With a large number of smart meters equipped with two-way communication capabilities installed in AMIs, the risk of customer privacy leakage increases dramatically. Today's AMIs connect more smart meters than ever, and service providers typically include a customer information system as part of the AMI. In this case, the malicious access of a smart meter can result in a large scale of customer data being exposed to privacy attackers. It is also possible for attackers to infer the electrical equipment contained within a house containing a smart meter and profile the customers' private life by analyzing the customers' electricity use. According to public records, private data leakage is viewed as one of the most prominent threats in customer-side systems [67].

In addition, databases are almost everywhere throughout the modern grid. Domains such as generation, distribution, and so on all have their own databases, which also have the potential to be the target of confidentiality attacks.

3) AVAILABILITY ATTACKS

This type of attack destroys the availability of devices by limiting their correct operation. Devices analyzed in this paper for their vulnerability to this type of threat include 1) relays, 2) RTUs, 3) and smart meters.

a: ATTACKS ON RELAYS

An attacker sends or tampers directly or indirectly with a relay's commands and preset thresholds to affect the relay's actions and limit its availability. The means used to launch such attacks on relays mainly involve: 1) compromising the relay, 2) sending commands to the relay through a compromised infrastructure to cause an incorrect operation, or 3) modifying the settings of distance protection scheme to cause rejections [68]. A relay directly controls energy transmission within its working range. An incorrect operation or rejection of the relay can thus cause disturbances in energy transfer and uneven distribution, resulting in partial short circuit failures. A series of pre-planned combinations of relay failures can cause power outages. There are also some strategies available for attackers to increase the destructiveness of relay attacks, such as random relay selection, area-based relay selection, and cascading-aware relay selection [69].

b: ATTACKS ON RTUs

Attacks on RTUs come in several forms. On one hand, some attacks attempt to compromise one or more RTUs and are used to post fake data and manipulate critical control commands. Another attack approach is to intercept data or commands sent from RTUs and forward the fabricated data to the control center. Malicious commands or data from key RTUs can then affect the judgment of the control center and induce mistakes in control.

c: ATTACKS ON SMART METERS

Device availability attacks on smart meters refer to sending incorrect information to the collector through a 'dark' smart meter to steal energy. Such electricity thefts have now become one of the most representative challenges for modern AMIs [70].

C. THE EVOLVEMENT OF CYBER ATTACKS: FROM PROTOCOL-BASED ATTACK TO IMPACT-BASED ATTACK

Impact-based attacks evolve from the coordination between a number of *protocol-based* attacks conducted in multiple stages of the cyber attack model. We can summarize the evolvement of cyber attacks according to the attack scope and its attack principles from *protocol-based*attack to *impact-based* attack. This evolution is illustrated in Fig. 5, and can be viewed as the potential path for cyber attacks to cause substantial impact on a system because of component vulnerabilities.

D. FROM COMPONENT-WISE VULNERABILITY TO SYSTEM-WIDE IMPACT

A clear understanding of the evolution of a cyber attack makes it easier to build a causal logical chain leading from specific component vulnerabilities to the actual cyber attack and resulting system-wide impact. By comparing Table 1 and Fig. 5, and the relationship between *protocol-based*attacks and the multi-stage model of cyber attacks, a causal relationship between the components, specific *protocol-based* attacks, and resulting system impact can be determined, as shown in Table. 2. The checked square on the Table. 2 indicates that this component is at risk to the corresponding attack.

V. COUNTERMEASURES FOR CYBER THREATS AND RESEARCH OPPORTUNITIES

Several constructive countermeasures for *impact-based* cyber attacks have been developed in literature, as will be summarized as follows. For ease of demonstration, we divide the countermeasures for various attacks into two broad categories: *prevention* and *detection*. And we also summarize the existing studies on the resilience of the power grid due to it is a significant aspect for the cybersecurity. This section also identifies some research gaps and opportunities.

A. EXISTING COUNTERMEASURES FOR IMPACT-BASED ATTACKS

1) INTEGRITY ATTACKS

a: PREVENTION STRATEGIES

Existing measures to prevent integrity attacks rely on reinforcing protection in specific areas or on specified

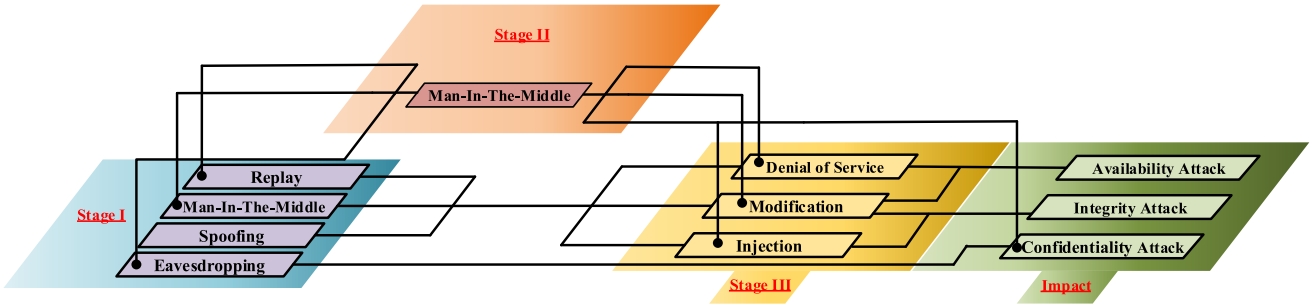

FIGURE 5. Evolvement of a cyber attack.

TABLE 2. Causal relationship from components to impacts.

Component	Protocol-Based Attack								Impact			Reference
	1	2	3	4	5	6	7	8	Availability	Integrity	Confidentiality	
RTU/PLC	✓	✓	✓	✓	✓		✓	✓	✓	✓		[37, 38, 51, 52, 53, 55, 58, 61, 63]
Relay	✓	✓	✓		✓		✓	✓	✓			[37, 38, 49, 51, 54, 59, 62, 63]
Smart Meter	✓	✓	✓		✓	✓	✓	✓	✓		✓	[37, 38, 51, 63]
PMU				✓	✓		✓	✓		✓		[45, 57]
Server	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	[49, 54, 56, 59, 60, 62]

Note: The types of protocol-based attack are denoted as follows: 1: man-in-the-middle attack; 2: denial of service attack; 3: replay attack; 4: injection attack; 5: spoofing attack; 6: eavesdropping attack; 7: modification attack; 8: reconnaissance attack.

components. Liu *et al.* [71] proposed a method of determining the least number of measurements to be protected in a way that minimizes the computational complexity, while [72], [73] reinforced the protection of a sufficient number of measurements that it would make it virtually impossible for an adversary to obtain sufficient measurement information to launch an attack.

b: DETECTION STRATEGIES

Integrity attack detection consists of developing methods that enable the system to alert system operators when the system is undergoing a malicious data attack. Khorshidi and Shabaninia [74] proposed a model to determine false data attack probability based on the theory that the malicious data injection causes an energy consumption increase in the estimation and optimization calculated via bat and firefly algorithms. The Kullback–Leibler distance (KLD) [75] is used to calculate the distance between two probability distributions derived from measurement variations, and the KLD gets bigger when FDIAs occur. In [76] and [77], quickest detection (sequential detection) based on adaptive CUSUM algorithms was exploited in a power grid, while [78] proposed a short-term state forecasting and texting forecast result method to detect integrity attacks. Deep learning technology has also been utilized for attack detection [79], [80]. Wang *et al.* [81] proposed an inference system which concerned with one type of data tempering attacks which named Alter-and-Hide attack. This attack threats substations through tampering the abnormal measurements to normal states.

2) AVAILABILITY ATTACKS

a: PREVENTION STRATEGIES

Zhang and Dong [69] proposed an improved scheme to strengthen the protection of P2P based relays. Chen *et al.* [82] provided a novel remedial pilot main protection scheme to protect relays, and Rahman *et al.* [83] exploited an innovative multi-agent scheme to maintain system security.

Reference [84] suggested detailed strategies for preventing malware attacks that aimed to compromise cyber targets, proposed protective measures such as system refinement, multi-factor authentication, and integrity monitoring, and specified the corresponding stages and tools to which each measurement was applied. Additionally, Powers [85] emphasized the importance of whitelist protection to improve system resistance towards availability attacks.

b: DETECTION STRATEGIES

Singh [86] simulated two RTU attack scenarios and detected attacks through a comparator domain. Reference Reference [87] developed a novel method to detect malicious data using topology information from the RTUs once the data was intercepted and modified, while [88] provided a method to simulate a relay attack and evaluated the impact.

In attack detection, Hink *et al.* [68] listed five machine-learning algorithms for detecting relay attacks. In [89], a hybrid network intrusion detection system for digital relay protection was proposed. References [90] and [91] provided methods to detect availability attacks and quantify the impact. A novel availability attack detection system based on a smart whitelist approach was proposed in [92].

3) CONFIDENTIALITY ATTACKS

a: PREVENTION STRATEGIES

To prevent data leakage, [93] established a trusted core network (TCN) to protect smart meters, and [94] summarized a privacy-preserving scheme to protect against privacy attacks.

b: DETECTION STRATEGIES

For determining attack detection direction, [95] proposed a smart meter compromise attack detection method, which relied on a ring architecture to maintain a high level of system security. A game-theory-based detection model was designed in [96], and [97] found hidden danger in malware attacks by using machine learning algorithms to search for executable files in an AMI.

4) THE ENHANCEMENT OF THE SYSTEM RESILIENCE

Besides the aforementioned detection and prevention strategies against cyber attacks, enhancement of power grid resilience to battle extreme conditions, i.e., power grid compromised by cyber attacks, has been proposed [98]. After the power grid is compromised by large-scale continuous malicious cyber attack, power grid operators will conduct multi-stage strategies to restore cyber security and to restore system functionality. These stages are resist & absorb, response & adapt, and recover [98]. A variety of research work has been conducted to propose operational strategies for resist & absorb stage [99], response & adapt stage [100], recover stage [101]. Countermeasures to improve the system resilience considering all three stages have been investigated in [102] and [103].

B. POSSIBLE DIRECTIONS FOR FUTURE RESEARCH

1) REINFORCEMENT OF COUNTERMEASURE

Existing countermeasures reflect the fact that state-of-the-art research in cyber power grids lacks the ability to prevent attacks. Judging from the number of published papers, the number of detection methods for various types of attacks is much greater than the number of preventive strategies. As a whole, there are still considerable research possibilities for improving the prevention of various attacks.

Additionally, we argue that the lack of research on prevention strategies is directly related to the mainstream classification perspective of cyber attacks, which is based on the consequences of the attack. When focus is mainly on the last stage of the attack model, it is difficult for researchers to establish a comprehensive framework for developing effective methods for preventing attacks. In contrast, if we put more effort to study the first two stages of the attack model, we can discover more efficient and effective prevention methods. Additionally, only a small number of countermeasures for *protocol-based* attacks have been applied to power grids, and the application of these existing methods against attacks for cyber attack prevention is also worthy of further attention.

2) VULNERABILITY ASSESSMENT AND REINFORCEMENT IN NEW PROTOCOLS

This paper only introduces four typical and widely-used communication protocols in power grids. However, due to the rapid advancement of communications technologies, a large number of new and upgraded protocols have been gradually applied to various parts of power grids. The new protocols also consist of vulnerabilities in various stages of the proposed attack model thus will be risky to certain types of attacks against them. An in-depth study of the new protocols being used in power grids is necessary and urgent.

3) DEVELOPMENT OF A DIAGNOSTIC SYSTEM FOR CYBER ATTACKS

Based on the proposed attack model, it is possible to infer the level of impact of *protocol-based* attacks that a power grid may suffer. The construction of a cyber-attacks diagnostic model that can diagnose *impact-based* attacks based on *protocol-based* attacks is feasible. A power grid possessing a self-diagnosis function during an attack can significantly improve the cyber security of the power grid.

4) DEALING WITH SPECIAL CHANNEL INVADERS

A small number of attackers simply invade systems illegally and do not depend on protocol vulnerabilities. For instance, such attackers may access the system through a leakage of information from internal communication channels. Thus, it is worthwhile to minimize the number of such intruders to ensure that continued research on protocol security is valuable and is not made irrelevant due to such system invasions.

5) ACCESS CONTROL IN COMMUNICATION SYSTEMS

With the expansion of the electricity market and the development of power grids, growth in the number of new communication roles in power grids is an inevitable trend. Despite this trend, it is important to maintain control over restricting the number of visits to a given cyber space. For example, whitelist management and limited access methods remain viable access control methods.

VI. CONCLUSIONS

To enhancing power grid resilience defending against malicious cyber attacks, it is prerequisite to clarify the connection and relationship of cyber and physical infrastructure of power grids. Nonetheless, the evolvement of cyber attacks from initial attempts to causing extensive impact on the physical part of power grid has not been thoroughly explored.

In this paper, we established the causal chain from component-wise vulnerabilities to system-wide impacts in the cyber security of power grids by surveying current state-of-the-art literature, enabling existing research to play a more powerful role in developing the prevention against cyber attacks on power grids. Our major contributions were threefold as below.

1) Protocol vulnerabilities were viewed as root vulnerabilities within the power grid's cyber network. A causal relationship between these vulnerabilities and protocol-based cyber attacks was established.
2) The evolution of a cyber attack from protocol-based attack to impact-based attack was described, capturing the attack scenario from initial attack on cyber components to impact the entire physical part of power

grids. Based on these results, known countermeasures for cyber attacks were summarized.

3) The research challenges discussed in this survey but not yet fully studied were identified as further research directions in damage prevention (or system hardening) against cyber attacks, including countermeasure reinforcement, new protocol analysis, diagnostic method for detecting cyber attacks, special invaders control, and communication system access control. We also remark that, in the power grid resilience perspective, quick recovery of cyber and physical infrastructure functionalities, efficient strategies to improve survivability under malicious cyber attacks, are also critical research areas that need further scrutiny.

REFERENCES

[1] U. S. Department of Homeland Security. (2014). *Industrial Control Systems Cyber Emergency Response Team*. [Online]. Available: https://ics-cert.us-cert.gov/

[2] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Nov. 2016.

[3] R. Arghandeh, A. V. Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renew. Sustain. Energy Rev.*, vol. 58, pp. 1060–1069, May 2016.

[4] S. M. Amin, "Electricity infrastructure security: Toward reliable, resilient and secure cyber-physical power and energy systems," in *Proc. IEEE PES Gen. Meeting*, Jul. 2010, pp. 1–5.

[5] Z. A. Collier, D. Dimase, S. Walters, M. M. Tehranipoor, J. H. Lambert, and I. Linkov, "Cybersecurity standards: Managing risk and creating resilience," *Computer*, vol. 47, no. 9, pp. 70–76, Jan. 2014.

[6] A. Gholami, T. Shekari, M. H. Amirioun, F. Aminifar, M. H. Amini, and A. Sargolzaei, "Toward a consensus on the definition and taxonomy of power system resilience," *IEEE Access*, vol. 6, pp. 32035–32053, Jun. 2018.

[7] F. He, J. Zhuang, N. S. V. Rao, C. Y. T. Ma, and D. K. Y. Yau, "Game-theoretic resilience analysis of Cyber-Physical Systems," in *Proc. IEEE 1st Int. Conf. Cyber-Phys. Syst., Netw., Appl. (CPSNA)*, Aug. 2013, pp. 90–95.

[8] Resilient America Roundtable, National Academy of Sciences of USA. (2014). *Expert Meeting: Improving Power System Resilience in the 21st Century*. [Online]. Available: http://sites.nationalacademies.org/PGA/ResilientAmerica/PGA_146736

[9] R. K. Pandey and M. Misra, "Cyber security threats—Smart grid infrastructure," in *Proc. Nat. Power Syst. Conf. (NPSC)*, Dec. 2016, pp. 1–6.

[10] J. E. Y. Rossebo, F. Fransen, and E. Luiijf, "Including threat actor capability and motivation in risk assessment for smart GRIDs," in *Proc. Cyber-Phys. Secur. Resilience Smart Grids (CPSR-SG)*, Apr. 2016, pp. 1–7.

[11] M. M. Pour, A. Anzalchi, and A. Sarwat, "A review on cyber security issues and mitigation methods in smart grid systems," in *Proc. SoutheastCon*, May 2017, pp. 1–4.

[12] X. Li, X. Liang, R. Lu, H. Zhu, X. Lin, and X. Shen, "Securing smart grid: Cyber attacks, countermeasures, and challenges," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38–45, Aug. 2012.

[13] C. Konstantinou, A. Keliris, and M. Maniatakos, "Taxonomy of firmware Trojans in smart grid devices," in *Proc. Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.

[14] K. Chatterjee, V. Padmini, and S. A. Khaparde, "Review of cyber attacks on power system operations," in *Proc. IEEE Region 10 Symp. (TENSYMP)*, Jul. 2017, pp. 1–6.

[15] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proc. Int. Conf. Internet Things 4th Int. Conf. Cyber, Phys. Social Comput.*, Feb. 2011, pp. 380–388.

[16] M. A. Douad and Y. Dahmani, "ARTT taxonomy and cyber-attack framewok," in *Proc. New Technol. Inf. Commun. (NTIC)*, Jan. 2016, pp. 1–6.

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

[18] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 13–27, 2016.

[19] A. Burg, A. Chattopadhyay, and K. Y. Lam, "Wireless communication and security issues for cyber–physical systems and the Internet-of-Things," *Proc. IEEE*, vol. 106, no. 1, pp. 38–60, Jan. 2018.

[20] P. E. Weerathunga and A. Cioraca, "The importance of testing smart grid IEDs against security vulnerabilities," in *Proc. Annu. Conf. Protective Relay Eng. (CPRE)*, May 2017, pp. 1–21.

[21] U.S. National Science Foundation. (2018). *Cyber-Physical Systems (CPS)*. [Online]. Available: https://www.nsf.gov/pubs/2018/nsf18538/nsf18538.htm

[22] K.-D. Kim and P. R. Kumar, "Cyber–physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, pp. 1287–1308, May 2012.

[23] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Oct. 2011.

[24] F. Rahimi and A. Ipakchi, "Demand response as a market resource under the smart grid paradigm," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 82–88, Jun. 2010.

[25] J. Morsali, K. Zare, and M. T. Hagh, "MGSO optimised TID-based GCSC damping controller in coordination with AGC for diverse-GENCOs multi-DISCOs power system with considering GDB and GRC non-linearity effects," *IET Gener. Transmiss. Distrib.*, vol. 11, no. 1, pp. 193–208, Jan. 2017.

[26] D. Kirschen and G. Strbac, *Fundamentals of Power System Economics*. Hoboken, NJ, USA: Wiley, 2006, pp. 76–78.

[27] A. Purvins, I. T. Papaioannou, I. Oleinikova, and E. Tzimas, "Effects of variable renewable power on a country-scale electricity system: High penetration of hydro power plants and wind farms in electricity generation," *Energy*, vol. 43, no. 1, pp. 225–236, Jul. 2012.

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

[29] Y. Xu, Y. Yang, T. Li, J. Ju, and Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control systems," in *Proc. IEEE Conf. Energy Internet Energy Syst. Integr. (EI2)*, Jan. 2018, pp. 1–6.

[30] M. N. Agostini, A. O. Pires, M. Dalmas, L. B. de Oliveira, and S. L. Zimath, "Analysis and simulation of dynamic performance of PMU according to IEEE C37.118.1-2011 standard," in *Proc. Develop. Power Syst. Protection (DPSP)*, May 2016, pp. 1–5.

[31] S. Cao, Q. Zhu, and H. Liu, "PROFIBUS-based reading method of smart meter's data," *J. Comput. Appl.*, vol. 33, no. 5, pp. 1248–1250, Sep. 2013.

[32] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, "DNPSec: Distributed network protocol version 3 (DNP3) security framework," in *Advances in Computer, Information, and Systems Sciences, and Engineering*. Dordrecht, The Netherlands: Springer, 2007, pp. 227–234.

[33] I. Darwish, O. Igbe, O. Celebi, T. Saadawi, and J. Soryal, "Smart grid DNP3 vulnerability analysis and experimentation," in *Proc. IEEE 2nd Int. Conf. Cyber Secur. Cloud Comput.*, Jan. 2016, pp. 141–147.

[34] H. Wi, J. H. Lee, and O. Yi, "Study on data security in industrial control system through modbus RTU protocol vulnerability attack," in *Proc. Symp. Korean Inst. Commun. Inf. Sci.*, Jan. 2018, pp. 78–80.

[35] X. Lv, L. Jiang, and H. Meng, "Cyber threats and intrusion detection for MODBUS-based SCADA system," *Comput. Eng. Appl.*, vol. 53, no. 24, pp. 122–128, Dec. 2017.

[36] G. Gilchrist, "Secure authentication for DNP3," in *Proc. Power Energy Soc. Gen. Meeting*, Aug. 2008, pp. 1–3.

[37] R. Nardone, R. J. Rodríguez, and S. Marrone, "Formal security assessment of Modbus protocol," in *Proc. Internet Technol. Secured Trans. (ICITST)*, Feb. 2017, pp. 142–147.

[38] Z. Drias, A. Serhrouchni, and O. Vogel, "Taxonomy of attacks on industrial control protocols," in *Proc. Int. Conf. Protocol Eng. (ICPE) Int. Conf. New Technol. Distrib. Syst. (NTDS)*, Oct. 2015, pp. 1–6.

[39] I. Ali, M. S. Thomas, and S. Gupta, "Sampled values packet loss impact on IEC 61850 distance relay performance," in *Proc. IEEE Innov. Smart Grid Technol.-Asia (ISGT Asia)*, Jan. 2014, pp. 1–6.

[40] H. Wang, Z. Cai, Z. Su, and Z. Zhu, "The analysis of relay protection communication mechanism based on IEC61850," in *Proc. Adv. Power Syst. Autom. Protection*, Apr. 2012, pp. 223–227.

[41] D. Chen, Z. Yang, and G. Xiang, "Research and implementation on function sequence visualization of relay protection based on IEC61850," *Power Syst. Control Protection*, vol. 44, no. 22, pp. 182–186, Nov. 2016.

[42] R. C.-W. Phan, "Authenticated modbus protocol for critical infrastructure protection," *IEEE Trans. Power Del.*, vol. 27, no. 3, pp. 1687–1689, Jul. 2012.
[43] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur, "Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed," in *Proc. Commun. Quality Rel. (CQR)*, May 2015, pp. 1–6.
[44] K. E. Martin *et al.*, "IEEE Standard for synchrophasors for power systems," *IEEE Trans. Power Del.*, vol. 13, no. 1, pp. 73–77, Jan. 1998.
[45] R. Khan, K. Mclaughlin, D. Laverty, and S. Sezer, "Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Nov. 2016, pp. 1–5.
[46] J. Chai and S. Liu, "Cyber security vulnerability assessment for smart substations," in *Proc. Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Dec. 2016, pp. 1368–1373.
[47] N. Liu, J. Zhang, H. Zhang, and W. Liu, "Vulnerability assessment for communication network of substation automation systems to cyber attack," in *Proc. IEEE/PES Power Syst. Conf. Expo.*, Apr. 2009, pp. 1–7.
[48] Y. Yang *et al.*, "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems," in *Proc. Sustain. Power Gener. Supply (SUPERGEN)*, Apr. 2013, pp. 1–8.
[49] B. J. Kang *et al.*, "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," in *Proc. Emerg. Technol. Factory Automat. (ETFA)*, Sep. 2015, pp. 1–8.
[50] Department of Homeland Security. (2013). *Understanding Denial-of-Service Attacks*. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-015
[51] J. M. Taylor and H. R. Sharif, "Security challenges and methods for protecting critical infrastructure cyber-physical systems," in *Proc. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, Sep. 2017, pp. 1–6.
[52] T. Mander, R. Cheung, and F. Nabhani, "Power system DNP3 data object security using data sets," *Comput. Secur.*, vol. 29, no. 4, pp. 487–500, Jun. 2010.
[53] R. Amoah, S. Camtepe, and E. Foo, "Securing DNP3 broadcast communications in SCADA systems," *IEEE Trans. Ind. Informat.*, vol. 12, no. 4, pp. 1474–1485, Aug. 2016.
[54] P. E. Nordbø, "Cyber security in smart grid stations," in *Proc. Conf. Exhib. Elect. Distrib. (CIRED)*, Dec. 2013, pp. 1–4.
[55] S. East, J. Butts, M. Papa, and S. Shenoi, "A taxonomy of attacks on the DNP3 protocol," in *Critical Infrastructure Protection III*. Berlin, Germany: Springer, 2009, pp. 67–81.
[56] R. Macwan *et al.*, "Collaborative defense against data injection attack in IEC61850 based smart substations," in *Proc. Power Energy Soc. Gen. Meeting (PESGM)*, Nov. 2016, pp. 1–5.
[57] Y. Yang *et al.*, "Intrusion detection system for network security in synchrophasor systems," in *Proc. Inf. Commun. Technol. (IETICT)*, Oct. 2013, pp. 246–252.
[58] R. Amoah, S. Camtepe, and E. Foo, "Formal modelling and analysis of DNP3 secure authentication," *J. Netw. Comput. Appl.*, vol. 59, pp. 345–360, Jun. 2015.
[59] L. E. D. Silva and D. V. Coury, "A new methodology for real-time detection of attacks in IEC 61850-based systems," *Elect. Power Syst. Res.*, vol. 143, pp. 825–833, Nov. 2016.
[60] T. A. Youssef, M. El Hariri, N. Bugay, and O. A. Mohammed, "IEC 61850: Technology standards and cyber-threats," in *Proc. Int. Conf. Environ. Elect. Eng. (EEEIC)*, Sep. 2016, pp. 1–6.
[61] I. A. Siddavatam and F. Kazi, "Security assessment framework for cyber physical systems: A case-study of DNP3 protocol," in *Proc. IEEE Bombay Section Symp. (IBSS)*, Sep. 2015, pp. 1–6.
[62] Y. Yang *et al.*, "Cybersecurity test-bed for IEC 61850 based smart substations," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Oct. 2015, pp. 1–5.
[63] A. G. Voyiatzis, K. Katsigiannis, and S. Koubias, "A modbus/TCP Fuzzer for testing internetworked industrial systems," in *Proc. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Oct. 2015, pp. 1–6.
[64] E. Hossain, Z. Han, and H. V. Poor, *Smart Grid Communications and Networking*. Cambridge, U.K.: Cambridge Univ. Press, 2012, pp. 297–302.
[65] F. C. Schweppe and D. B. Rom, "Power system static-state estimation, part II: Approximate model," *IEEE Trans. Power App. Syst.*, vol. PAS-89, no. 1, pp. 125–130, Jan. 1970.
[66] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Trans. Inf. Syst. Secur.*, Jan. 2009, pp. 21–32.
[67] F. G. Mármol, C. Sorge, O. Ugus, and G. M. Pérez, "Do not snoop my habits: Preserving privacy in the smart grid," *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 166–172, May 2012.
[68] R. C. B. Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *Proc. Int. Symp. Resilient Control Syst. (ISRCS)*, Aug. 2014, pp. 1–8.
[69] J. Zhang and Y. Dong, "Cyber attacks on remote relays in smart grid," in *Proc. Conf. Commun. Netw. Secur. (CNS)*, Dec. 2017, pp. 1–9.
[70] S. Mclaughlin, D. Podkuiko, and P. Mcdaniel, "Energy theft in the advanced metering infrastructure," in *Proc. World Forum Internet Things (WF-IoT)*, Jan. 2009, pp. 176–187.
[71] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1802–1810, Jul. 2017.
[72] 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," in *Proc. 1st Workshop Secure Control Syst. CPSweek*, Jan. 2010, pp. 1–9.
[73] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1244–1253, Sep. 2013.
[74] R. Khorshidi and F. Shabaninia, "A new method for detection of fake data in measurements at smart grids state estimation," *IET Sci. Meas. Technol.*, vol. 9, no. 6, pp. 765–773, Aug. 2015.
[75] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.
[76] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, Jun. 2016.
[77] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.
[78] J. Zhao, G. Zhang, M. L. 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 Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, Jul. 2017.
[79] J. Wei and G. J. Mendis, "A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids," in *Proc. Cyber-Phys. Secur. Resilience Smart Grids (CPSR-SG)*, Oct. 2016, pp. 1–6.
[80] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid.*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.
[81] C. Wang, C.-W. Ten, Y. Hou, and A. Ginter, "Cyber inference system for substation anomalies against alter-and-hide attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 896–909, Mar. 2017.
[82] L. Chen *et al.*, "Remedial pilot main protection scheme for transmission line independent of data synchronism," *IEEE Trans. Smart Grid*, to be published.
[83] M. S. Rahman, A. M. T. Oo, M. A. Mahmud, and H. R. Pota, "A multi-agent approach for security of future power grid protection systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Nov. 2016, pp. 1–5.
[84] B. Min and V. Varadharajan, "Design and analysis of security attacks against critical smart grid infrastructures," in *Proc. Int. Conf. Eng. Complex Comput. Syst.*, Oct. 2014, pp. 59–68.
[85] J. Powers, R. Smith, Z. Korkmaz, and H. Ahmed, "Whitelist malware defense for embedded control system devices," in *Proc. Saudi Arabia Smart Grid (SASG)*, Apr. 2016, pp. 1–6.
[86] P. Singh, S. Garg, V. Kumar, and Z. Saquib, "A testbed for SCADA cyber security and intrusion detection," in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, Sep. 2015, pp. 1–6.
[87] J. Kim and L. Tong, "On topology attack of a smart grid," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Apr. 2013, pp. 1–6.
[88] C. Konstantinou and M. Maniatakos, "Impact of firmware modification attacks on power systems field devices," in *Proc. Int. Conf. Smart Grid Commun. (SmartGridComm)*, Mar. 2016, pp. 283–288.
[89] G. Koutsandria, V. Muthukumar, M. Parvania, S. Peisert, C. McParland, and A. Scaglione, "A hybrid network IDS for protective digital relays in the power transmission grid," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Jan. 2015, pp. 908–913.

[90] V. K. Singh, A. Ozen, and M. Govindarasu, "Stealthy cyber attacks and impact analysis on wide-area protection of smart grid," in *Proc. North Amer. Power Symp. (NAPS)*, Nov. 2016, pp. 1–6.
[91] N. Boumkheld, M. Ghogho, and M. El Koutbi, "Intrusion detection system for the detection of blackhole attacks in a smart grid," in *Proc. Int. Symp. Comput. Bus. Intell. (ISCBI)*, Nov. 2016, pp. 1–14.
[92] F. Skopik, I. Friedberg, and R. Fiedler, "Dealing with advanced persistent threats in smart grid ICT networks," in *Proc. ISGT*, May 2014, pp. 1–5.
[93] K. O. Detken, C. H. Genzel, C. Rudolph, and M. Jahnke, "Integrity protection in a smart grid environment for wireless access of smart meters," in *Proc. Int. Symp. Wireless Syst. Conf. Intell. Data Acquisition Adv. Comput. Syst.*, Nov. 2014, pp. 79–86.
[94] L. Lyu, Y. W. Law, J. Jin, and M. Palaniswami, "Privacy-preserving aggregation of smart metering via transformation and encryption," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Sep. 2017, pp. 472–479.
[95] M. H. Yaghmaee, Q. A. Frugh, and M. Bahekmat, "Monitoring approach for detection compromise attacks in smart meter," in *Proc. 22nd Int. Conf. Exhib. Elect. Distrib. (CIRED)*, Dec. 2013, pp. 1–4.
[96] M. Shange, J. Lin, X. Zhang, and C. Xu, "A game-theory analysis of the rat-group attack in smart grids," in *Proc. IEEE 9th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process. (ISSNIP)*, Jun. 2014, pp. 1–6.
[97] V. Babu and D. M. Nicol, "Detection of x86 malware in AMI data payloads," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Mar. 2016, pp. 617–622.
[98] Z. Bie, Y. Lin, G. Li, and F. Li, "Battling the extreme: A study on the power system resilience," *Proc. IEEE*, vol. 105, no. 7, pp. 1253–1266, Apr. 2017.
[99] Q. Zhu and T. Başar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Proc. 50th IEEE Conf. Decis. Control Eur. Control Conf.*, Mar. 2012, pp. 4066–4071.
[100] S. Paul, A. Parajuli, M. R. Barzegaran, and A. Rahman, "Cyber physical renewable energy microgrid: A novel approach to make the power system reliable, resilient and secure," in *Proc. IEEE Innov. Smart Grid Technol. Asia (ISGT-Asia)*, Dec. 2016, pp. 659–664.
[101] H. Lin *et al.*, "Self-healing attack-resilient PMU network for power system operation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1551–1565, May 2018.
[102] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389–1407, Jul. 2017.
[103] S. Mehrdad, S. Mousavian, G. Madraki, and Y. Dvorkin, "Cyber-physical resilience of electrical power systems against malicious attacks: A review," *Current Sustain. Renew. Energy Rep.*, vol. 5, no. 1, pp. 14–22, Mar. 2018.

XIAOGE HUANG was born in Guangxi, China. He received the bachelor's degree in electrical engineering from Guangxi University, Nanning, China, in 2018. In 2014, he joined the Guangxi key Laboratory of Power System Optimization and Energy Technology as a Research Assistant. His major research interests include machine learning, deep learning, and power system optimization.

ZHIJUN QIN (S'11–M'15) received the B.E. and M.S. degrees (Hons.) from the Huazhong University of Science and Technology, Wuhan, China, in 2000 and 2003, respectively, and the Ph.D. degree from The University of Hong Kong, Hong Kong, in 2015, all in electrical engineering. From 2015 to 2016, he was a Post-Doctoral Research Fellow with The University of Hong Kong. He was the major algorithm developer and among the key contributors of a decision support software tool entitled System Restoration Navigator, which was developed under the support of Electric Power Research Institute, USA, from 2010 to 2016.

He is currently an Associate Professor with Guangxi University. His research interests include power system resilience, renewable energy integration, cyber security of cyber-physical system, optimal power flow, and power system dynamics.

HUI LIU (M'12–SM'17) received the M.S. and Ph.D. degrees in electrical engineering from the College of Electrical Engineering, Guangxi University, China, in 2004 and 2007, respectively.

He was with Jiangsu University as a Faculty Member from 2007 to 2016 and was with Tsinghua University as a Post-Doctoral Fellow from 2011 to 2013. He visited the Energy Systems Division, Argonne National Laboratory, Argonne, IL, USA, from 2014 to 2015. He joined the College of Electrical Engineering, Guangxi University, in 2016, where he is currently a Professor. His research interests include power system optimization, power system stability and control, electric vehicles, integrated energy systems, and demand response. He is an Associate Editor of the IEEE Access. He is also a reviewer for more than 20 journals.