International Journal of Information Security
https://doi.org/10.1007/s10207-022-00594-7

SURVEY

Classifying resilience approaches for protecting smart grids against cyber threats

Andrew D. Syrmakesis[1] · Cristina Alcaraz[2] · Nikos D. Hatziargyriou[1]

Abstract
Smart grids (SG) draw the attention of cyber attackers due to their vulnerabilities, which are caused by the usage of heterogeneous communication technologies and their distributed nature. While preventing or detecting cyber attacks is a well-studied field of research, making SG more resilient against such threats is a challenging task. This paper provides a classification of the proposed cyber resilience methods against cyber attacks for SG. This classification includes a set of studies that propose cyber-resilient approaches to protect SG and related cyber-physical systems against unforeseen anomalies or deliberate attacks. Each study is briefly analyzed and is associated with the proper cyber resilience technique which is given by the National Institute of Standards and Technology in the Special Publication 800-160. These techniques are also linked to the different states of the typical resilience curve. Consequently, this paper highlights the most critical challenges for achieving cyber resilience, reveals significant cyber resilience aspects that have not been sufficiently considered yet and, finally, proposes scientific areas that should be further researched in order to enhance the cyber resilience of SG.

Keywords Smart grids · Cyber-physical systems · Resilience · Cyber threats

1 Introduction

The growing concerns about climate change and the ever-increasing needs for electrical energy dictate changes in the conventional power system, in order to make it more reliable, efficient and eco-friendly. For this purpose, both research and industry communities in several parts of the world (e.g., USA, E.U., China, Australia, etc.) [1,2] focus their efforts on "smartening" the grid, in order to effectively accommodate the needs of all users, i.e., producers, consumers and prosumers. One of the key features of smart grids (SG) is the wide integration of information and communication technologies (ICT) in electrical energy functionalities.

✉ Cristina Alcaraz
alcaraz@lcc.uma.es

Andrew D. Syrmakesis
asirmakesis@power.ece.ntua.gr

Nikos D. Hatziargyriou
nh@power.ece.ntua.gr

[1] School of Electrical and Computer Engineering, National Technical University of Athens (NTUA), Athens, Greece

[2] Computer Science Department, University of Malaga, Campus de Teatinos s/n, 29071 Malaga, Spain

ICT brings numerous benefits, but also critical security challenges that emerge by the digital transformation of the power grid [3,4]. The wide variety of ICT applications in the SG exposes many vulnerable spots which pave the way for different types of cyber attacks. For instance, SG uses a group of heterogeneous communication technologies, such as ZigBee, wireless mesh networks, cellular network communication and power-line communication [5]. Their complex interconnections along with the possible protocol incompatibilities can result in serious security gaps. In addition, the operation of power systems is still heavily dependent on proprietary and legacy technologies, such as conventional supervisory control and data acquisition (SCADA) systems whose design did not originally account for security measures. As a consequence, they expose the system to many risks [6]. Moreover, unlike ordinary ICT infrastructures, securing modern power systems is more challenging due to their strict operational requirements and their criticality level [7].

Successful cyber attacks against Cyber-Physical Systems (CPS) have been already recorded, like the well-known case in Ukraine's power system in December 2015. This large-scale incident is extensively reported by SANS institute and Electricity Information Sharing and Analysis Center (E-

Published online: 06 May 2022

ISAC) and power companies [8]. The coordinated attack consisted of malware installation via spear phishing emails, unauthorized access and SCADA system hijacking, which opened several circuit breakers remotely to interrupt the electricity supply to consumers. It also involved denial-of-service (DoS) attacks on telephone systems to prevent customers from emergency reporting to the operators. The outcome of this attack affected approximately 225,000 customers. Another notorious software, called Stuxnet, was uncovered in 2010 [9]. Stuxnet worm targeted the hosts of specific Siemens industrial control systems that were running on Windows environment, and it mainly affected Iranian nuclear facilities [10]. For this reason, protecting SG systems from such malicious actions is currently an active research area [11], relevant for governments [3], international organizations such as European Union Agency for Cybersecurity (ENISA) [4], National Institute of Standards and Technology (NIST) [11,12] and the academic community.

So far, several defense mechanisms have been proposed in the literature by the ICT community and power system research communities. Most of this related work is presented in this paper and is classified according to the resilience techniques given by NIST in [13] and the resilient states described in [14]. More specifically, the methodology of the paper is as follows: In Sect. 3, a collection of several methods that increase the cyber resilience of SG and CPS in general is presented. Each method is briefly analyzed to identify the key points of its approach. In this way, it is clarified which resilience technique of NIST is applied at each method in order to group them accordingly, based on these techniques. This type of classification forms the different subsections of Sect. 3, which are dedicated to the aforementioned resilience techniques. Finally, these techniques are mapped to the different resilience states presented in [14]. This mapping can be found at the introduction of each subsection of Sect. 3.

The challenges of cyber resilience emerge in different parts of the SG, including communication, software and end system security and the stability of control algorithms. This paper focuses on communication security. This is due to the fact that the resilience techniques described by NIST, which form the basis of the proposed classification, focus on communication security challenges. In a more general context, some research works dealing with the other aspects of SG cyber resilience are also included.

In the literature, there are different research works that present methods for cyber resilience enhancement of CPS and draw interesting conclusions from them. For example, the goal of [15] is to identify trends and recent results on the proposed responses of CPS to cyber attacks and to highlight limitations and open problems. In [16], the existing methods for cyber resilience enhancement of CPS (redundancy, fault tolerance, security) are presented based on an extensive literature study. However, to the authors' view, none of them is making a practical classification for the cyber resilience of SG in order to propose a research guide, as the present work does. Particularly, the main contributions of this paper can be summarized as follows:

- This work contains a state-of-the-art collection of scientific works related to the cyber resilience of SG and CPS in general.
- These scientific works are classified according to the formal resilience techniques defined by NIST.
- These resilience techniques and the related scientific works in turn are mapped to the typical resilient states. This type of mapping offers a new perspective to the researchers regarding the cyber resilience of SG.
- Finally, the main challenges toward the cyber resilience of SG are highlighted and directions for future research are drawn, based on the study of the presented methods.

The remainder of this paper is structured as follows: Sect. 2 defines the terms of SG, CPS and resilience in power systems, analyzes the typical resilience curve and introduces the cyber resilience techniques identified by NIST. In Sect. 3, the related work is briefly analyzed and classified based on the cyber resilience techniques of NIST and the main phases of the standard resilience curve. Section 4 presents the current open issues and research challenges within the resilience field. It also adds the current trends to address future research. Finally, Sect. 5 provides the conclusions and outlines the future work.

2 Preliminary terminologies and background

2.1 Definitions of smart grids and cyber-physical systems

There have been several definitions for SG by international organizations, such as ENISA. Moreover, CPS is a broad term that refers to a wide variety of ICT systems connected to the physical world. Therefore, at this point it is important to clearly define these terms in order to clarify our view about them to the reader.

International organizations have provided the following definitions for the SG: ENISA considers the SG as an upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added [17]. NIST defines the SG as the addition and integration of various digital computing and communication technologies and services with the power delivery infrastructure [18]. Our view of the SG is aligned with these definitions, i.e., it is a power grid that serves the supply driven infrastructure created by

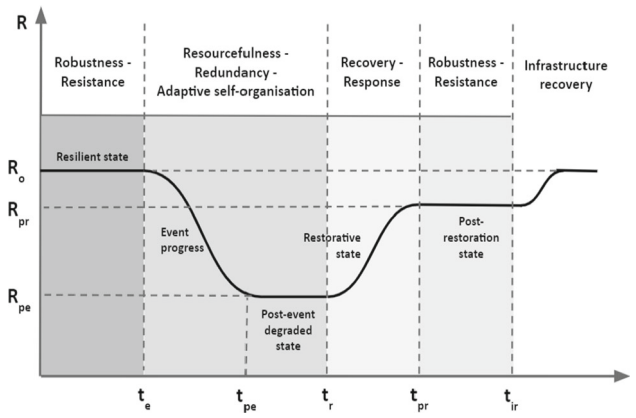

Fig. 1 Resilience curve [14]

renewable energy supplies and this is enabled by smart components with more communications links added.

According to [19], CPS are an integration of computational and physical processes. In CPS, embedded computers and networks monitor and control the physical processes, usually with feedback loops. The physical processes in these systems affect the computations and vice versa. Authors are aligned with this definition and perceive SG as a subset of CPS. Therefore, while this work is mainly focused on the cyber resilience of SG, it also includes few cyber resilience methods that may be applicable to other CPS, e.g., automobile cruise control, water treatment processes, etc.

2.2 Resilience relevance in the power sector

Cybersecurity can be regarded as one of the main aspects of the general concept of resilience. In [14], resilience is defined as "*the ability of a system to withstand, absorb and rapidly recover from an external, high-impact, low-probability devastating event, like an extreme weather event or a cyber attack*". Figure 1 presents the typical resilience curve [14] of a power system. This curve illustrates how the performance of the system evolves over time in an event that degrades its state. This is useful in order to understand the different resilience states along with their main defense characteristics, such as robustness/resistance, resourcefulness/redundancy and adaptive self-organization.

The different resilience states are characterized in [14] by a certain resilience metric, which expresses quantitatively the system reliability or power quality, e.g., the number of customers affected or the number of residents in a population impacted. For the sake of clarity and observing the curve of Fig. 1, these metrics are described as follows:

- *Resilient state* at this state, a well-designed power system could deter the success of a launched cyber attack. Configuring a secure and intrusion-tolerant grid at this stage provides a high resilience level which is capable of preventing unauthorized access and successful attacks.
- *Post-event degraded state* in case of an unplanned event, e.g., a cyber attack or a power outage, the performance of the power system might degrade; the percentage of this degradation depends on the impact of the attack and the preventive measures that have been applied. Key resilience techniques help reduce the impact of the attack and facilitate the progress to restoration state. For example, redundancy provides operational flexibility to the power system by offering additional resources. It should be noted that the duration of this state can be very short, thus transforming the trapezoidal shape of the resilience curve to triangular.
- *Restorative state* at this state, the compromised power system has managed to mitigate the cyber attack and it gradually returns to its normal condition. Its recovery is almost fully completed. For example, after an accomplished attack, the power grid should modify its functionality, allocate alternative resources and optimally restore affected components or applications.
- *Post-restoration state* this is the state where the recovery process has been completed and the power system is again operational. Nevertheless, its resilience level R_{pr} might be lower than its initial value R_o. Operational recovery refers to bringing back the system into a state that is operational, while infrastructure recovery refers to the restoration of the resilience level of the system to its initial value. For example, if all replicas of a SCADA master are compromised, restoring at least one of them will make the system operational again. However, all the replicas of the SCADA master have to be restored in order to reach the initial resilience level of the system.

At this point, it is important to explain the meaning of the different variables depicted in Fig. 1:

- R_o: initial resilience value,
- R_{pe}: resilience value after a successfully completed cyber attack,
- R_{pr}: resilience value after attack mitigation,
- t_e: starting time of the cyber attack,
- t_{pe}: end time of the cyber attack,
- t_r: starting time of the attack mitigation,
- t_{pr}: end time of attack mitigation and
- t_{ir}: starting time of infrastructure recovery.

In the following section, a brief overview of the NIST reference techniques for cyber resilience [13] is presented.

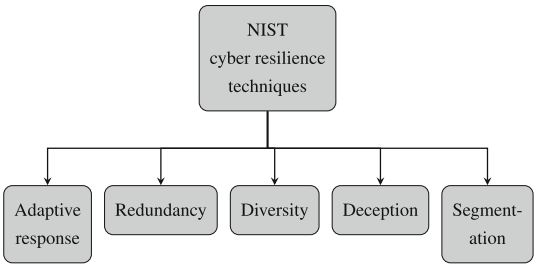

Fig. 2 Cyber resilience techniques according to NIST

2.3 Resilience techniques according to NIST

NIST recently published a Special Publication (SP-800-160), titled as "*Developing Cyber Resilient Systems: A Systems Security Engineering Approach*" [13], which identifies a set of fourteen cyber resilience techniques. Each technique includes a set of standard methodologies and practices which aim to design attack-resilient systems. In this work, recently published approaches are classified according to the NIST techniques shown in Fig. 2. These techniques are described in the remainder of this section:

- *Adaptive response* this technique involves timely and appropriate response to an attack by reconfiguring some of the system components to alter their functionalities or modify the allocation of the resources. These changes have to be made without interrupting the operation of the system.
- *Segmentation* it prioritizes operations and resources according to their criticality and trustworthiness in order to separate the most vulnerable or attractive ones and secure them accordingly. Segmentation can take place before the system is activated or dynamically, while the system operates.
- *Redundancy* it embraces the presence of multiple, protected instances of critical units (called "replicas"), including hardware, information and functions, eliminates single points of failure and allows the system to survive even after a successful cyber attack. Redundancy also refers to the preservation of additional, alternative communication resources. The constant synchronization of replicas is essential at this point.
- *Diversity* this technique refers to heterogeneity in terms of design, architecture or technology so as to make it difficult for adversaries to exploit common vulnerabilities.
- *Deception* it is implemented by hiding important assets, intentionally providing misleading information or misdirecting adversaries to imitations of the actual elements of the system. Deceiving adversaries may prevent them from causing substantial damage to the system, even when they have managed to invade.

3 Resilience methods and classification

This section addresses the different research works proposed in the literature to increase the resilience of SG against cyber attacks. Each of these works is explained to some extent and is associated with: (i) the cyber resilience technique mentioned in Sect. 2.3 and (ii) the appropriate state of the resilience curve

These relevant works are selected to demonstrate the feasibility of the proposed classification.

3.1 Adaptive response

Adaptive response is a widely adopted cyber resilience technique for the protection of the applications of the SG. It is considered as an active way of defense, since the system is modified in real time, and in such a way that the impact of the attack is mitigated. This process involves the capability of the system to automatically adjust its functionality or resource allocation when a cyber attack is identified in order to avoid operational disruptions. More specifically, adaptive response involves:

- *Dynamic reconfiguration* alters the behavior of system components without interrupting services; e.g., dynamically change the controller functionality or traffic routes.
- *Dynamic resource allocation* changes the allocation of the resources without terminating critical processes.

Studies that use the adaptive response technique are generally applied at the resilient state, post-event degraded state and restorative state. This measure is used after the detection of an attack or the identification of compromised resources, and aims at bringing the system to a resilient state. Figure 3 shows the methods that utilize adaptive response to achieve resilience against cyber attacks in power grids. Some related studies are also presented bellow.

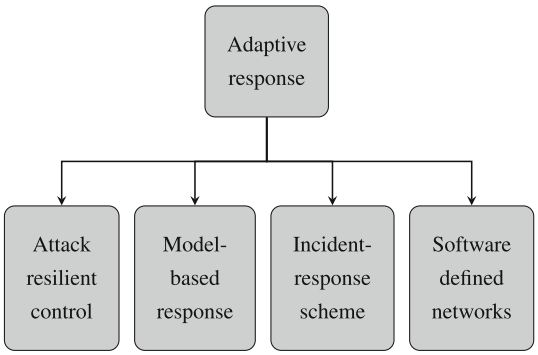

Fig. 3 Methods for adaptive response

3.1.1 Attack-resilient control

Various intelligent control mechanisms have been developed as an adaptive response to adversaries. They ensure stable operation for the power system in the event of an attack and provide security at the application layer [20].

In [21], an extra module to the physical control model is added which is called commensurate response (CR). This technique tackles setpoint attacks, which affect the input signal of the controller of the plant, and actuation attacks, which directly affect the output signal of the controller of the plant; it does not consider attacks on sensors [15]. With the CR module, the rise time of the model (the amount of time the system needs to reach its steady state) can be controlled on-demand. As a result, data integrity attacks can be delayed and possibly prevented, due to the intentional slow down of the response of the system. The proposed solution is evaluated by using a case study on automobile cruise control. The system is exposed to data integrity attacks, and it is demonstrated that the CR module improves the cyber resilience of the system.

An attack-resilient control scheme for distributed energy resources (DER) is presented in [22]. The traditional DER unit and its feedback control is integrated with a sliding mode observer (SMO), which is a nonlinear control method, in order to decrease the impact of a cyber attack. The SMO module is inserted between the output and the control input of the DER plant and is capable of estimating the attack signal that is generated by adversaries. The original and correct output data can be retrieved by removing the attack signal estimation from the corrupted measurements of the DER plant. For evaluation, a detailed nonlinear, switch model of a three-phase converter-base DER is used, considering the following attack scenarios: DoS, replay attack and bias injection.

In [23], an attack-resilient framework for energy management system (EMS) is presented. This framework is composed of a data-driven, attack detection module and a resilient control policy which focuses on preserving the stability of the physical system during and after an attack. The resilient control policy depends on a virtual sensor, implemented in the supervisory controller using a Kalman filter, which eliminates the impact of the corrupted measurements on the system. The performance of the proposed framework is evaluated using a reduced-order model of a real EMS site and simulated attacks.

There are several studies that utilize attack-resilient control in CPS in general, in order to provide a resilient system against attacks. These approaches could be potentially introduced in power system applications in the future. For instance, in [24] compressed sensing techniques are applied to estimate the state of the plant during attacks. Numerical simulations have been conducted using the IEEE 14-bus power network in MATLAB. In [25], an attack-resilient state estimator is proposed that is applied on the cruise control of an electric, unmanned vehicle. It is demonstrated that the attacker cannot destabilize the system by exploiting the difference between the model used for state estimation and the real physical dynamics of the system. In [26], a control method based on a recursive filtering algorithm is implemented against specific sensor attacks. This technique estimates the states of the system by leveraging the redundant information in the controller. Both [25] and [26] methods are evaluated using the LandShark, an electric unmanned ground vehicle [27].

3.1.2 Model-based response

To mitigate cyber attacks, a common practice in CPS is the replacement of affected measurements with approximated ones. Approximated measurements usually derive from a representative model that captures the behavior of the physical system for a given control signal as input. This approach is considered a model-based response, since it takes advantage of such a model and uses its output as a response against cyber attacks. A typical control diagram of a simplified CPS that uses model-based response is shown in Fig. 4. The "Model" module, which is a representative model of the physical system, operates in parallel with the "Plant" module, which is the physical system, and they simultaneously receive the control signal u. Afterward, "Sensors" communicate with "Plant" to collect its y measurements, while the "Model" produces an estimation $\hat{y}$ of these measurements. Both y and $\hat{y}$ signals are sent to the "Detector" in order to decide if the actual measurements have been affected and pass the proper $\tilde{y}$ to the controller. Finally, the "Controller" receives a reliable $\tilde{y}$ signal and along with the "Actuator", they compute the right u signal. The aforementioned steps are constantly repeated to keep controlling and protecting the "Plant".

An approach that considers model-based response is presented in [28]. In this work, a representative linear model is developed that can emulate the actual behavior of the

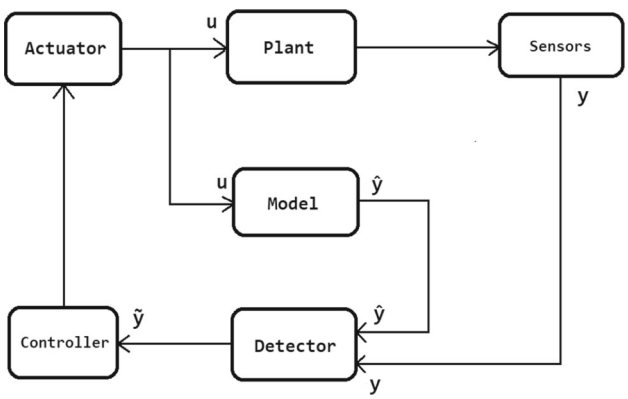

Fig. 4 Typical model-based response

physical system under investigation. This model is obtained by linearizing the Tennessee Eastman process control system model [29] (which is also used for evaluation purposes) about the steady-state operating conditions. The detection method derives from the comparison of the expected output signal, which is produced by the aforementioned linear model, with the measured output signal. Any deviation from a predefined threshold raises an alarm which, in turn, activates the response mechanism. The proposed response mechanism replaces the measurements from the compromised sensor with a measurement sequence that the linear model generates. Similarly, in [30], a SCADA system with software-defined network (SDN) assistance is presented, which replaces compromised measurements with estimated ones. For evaluation, an extension of the MiniCPS [31] is developed in order to provide SDN functionalities for both supervisory and field networks.

In [32], data integrity attacks are mitigated by using the mean value of the area control error (ACE) forecast instead of the standard ACE equation of the automatic generation control (AGC), when an intrusion is identified. The method is validated using a three-area power system model, where its parameters are provided but its simulation software is missing. In the same vein, an algorithm is proposed in [33] that estimates which sensor data links have been affected to identify the attack. If the attack is identified, then the power export deviation is accounted for the ACE computation; otherwise, an attack-mitigating state estimation program is launched. This algorithm is validated by experiments on a physical 16-bus power system testbed and PowerWorld [34] simulations based on a 37-bus power system model.

In [35], a data clearing method based on conditional deep belief networks (CDBNs) is investigated as a real-time response. Observations indicate a high correlation among the measurements of phasor measurement units (PMUs) that belong to the same cluster of a hierarchical, cyber-physical, multi-agent control environment. The agent with the highest inertia generator in a cluster is termed the lead agent, while the others are referred to as secondary. By feeding historical data into two identical CDBNs, one for the measurements of the leader agent and the other for the measurements of the secondaries, the actual behavior of the system can be predicted. Thus, if the outputs of the two CDBNs agree there is no report of an attack, alternatively, measurements are replaced by the ones deriving from the secondary agent with the highest reputation metric. This method is evaluated by modeling the 39-bus New England test system in MATLAB/Simulink. The authors expand their work in [36] which is focused on the detection of false data injection (FDI) attacks.

Another study that considers deep learning algorithms in order to predict the measurements of a load frequency control (LFC) system under a DoS attack is presented in [37]. In this work, a real-time data prediction algorithm is provided, which is a combination of a deep autoencoder and an extreme learning machine (ELM) algorithm. This prediction algorithm estimates the data that are lost due to the DoS attack so as to keep the LFC system in a normal and operational state. This method is evaluated in MATLAB/Simulink by using the single-, two- and three-area LFC models provided in [38].

3.1.3 Incident response scheme

There are techniques that propose an attack response policy as a defensive strategy when an attack on the system has been identified. This response policy may involve individual steps, such as discarding traffic and component isolation, or a general process with multiple steps, such as system reconfiguration, protection of vulnerable targets and system shutdown, among others. There are also schemes that generate this policy on-demand, either before the activation of the system or in real time.

In [39], an autonomously self-protecting SCADA system with three layers of security measures is suggested. The first line of defense uses historical observations of the controlled variables and selected security features of the SCADA system in order to predict if the next state of the system is dangerous. The future performance of the system is predicted by the autoregressive integrated moving-average (ARIMA) forecasting model [40]. Furthermore, there is a hybrid intrusion detection system (IDS) based on anomaly and signature detection techniques, such as Naive Bayes classifier and a set predefined rules. Finally, if the system is compromised, a multi-criteria analysis controller is implemented to propose an appropriate response. The proposed defense scheme is evaluated by a water storage tank which is modeled in a laboratory-scale control system in Mississippi State University SCADA Security Laboratory.

Game theory is another scientific field that can provide defensive strategies against attackers. Game models can be run offline and reveal which are the optimal responses depending on the adversary's moves. For example, in [41–43] sequential game between an adversary and a SCADA administrator is formulated in order to analyze their interactions in case of cyber attack. Both the attacker's and the defender's moves are predefined, and the payoff matrix is constructed with the intention of representing a real-world scenario. By using the backward induction process to find the subgame perfect Nash equilibrium of the whole game, a decision-making analysis derives that can be adopted by the operator as an attack response scheme. The proposed approach is analyzed using the case study of a SCADA system sensor network, but it is not evaluated with any simulation.

A typical study that uses a game theory method to apply active response against cyber attacks is presented in [44]. In this work, the investigated attacks can cause transient insta-

bility to synchronous generators by stealthily compromising DER actuators. As a defensive strategy, a noncooperative, differential game is modeled that discovers the countermeasure vector. This vector describes which policy should be followed at each state by unaffected DER control signals in order to suppress attacks on actuators. This work can also serve as vulnerability assessment, since it reveals the individual security risk of the DER. For evaluation, an IEEE ten-machine 39-bus system is implemented in MATLAB/Simulink under various settings.

In [45], a zero-sum game is modeled that can represent the decision-making process between a sensor node and an adversary who launches DoS attacks. This methodology can be applied both offline, for a scheduled strategy, and in real time, if the necessary information about previous states is available. The method is not evaluated in any platform.

3.1.4 Software-defined networking

SDN is a flexible technology that differs from traditional networks in the context of programmability. The core idea behind SDN is to transfer the network traffic decisions from hardware, like network switches, to a programmable environment, like SDN controllers [46]. The main benefit of this approach is that the controller can take optimal decisions about the forwarding responsibilities of the network, due to its flexibility and complete overview of the state of the system.

An integration of SDN with network virtualization is presented in [47]. This integration can monitor the data exchange and dynamically configure the data traffic of a SG according to certain QoS policies. Programmability of SDN facilitates the process of communication link restoration by discovering alternative, available topologies. For evaluation, a virtualized network is simulated within a single physical machine using OpenStack [48] to create multiple entities in VMs and OpenvSwitch [49,50] to provide the functionality of SDN. In [51], a centralized controller dynamically manages data flows across the nodes by constantly monitoring the components of the network. The controller is simulated and evaluated by using NOX controller [52] and OpenvSwitch. In [53], a microgrid is integrated with SDN to ensure real-time route reconfiguration, considering the latency requirements and rate limitation of the network. For evaluation, a hardware-in-the-loop environment is used that includes OPAL-RT [54], OpenFlow switches and a microgrid central controller (MGCC), which is based on a campus microgrid at the University of Connecticut.

A defense scheme for a SDN-based SG environment is described in [55], which is applied but not limited to substation components. The idea is that the system can identify which communication links are more likely to be attacked by adversaries with the link failure learning (LFL) algorithm. Therefore, the traffic is dynamically rerouted via the SDN controller, based on the most reliable communication links. LFL is implemented with a multi-armed bandit approach (MAB) algorithm, a classic reinforcement learning example, where the SDN controller is constantly informed from the switches about link failures and rewards the most resilient communication paths. For evaluation, a substation environment that implements the IEC 61850 standard is considered using Mininet 2.3, RYU SDN controller 4.22 and OpenFlow 1.3 compatible switches.

In [56], the problem of link flood attacks in a IEC 61850-based substation communication network is considered. A security score model of an IEC 61850 network, initially proposed in [57], is enhanced by taking into account the criticality of each device in the SG network. The resilience of the substation against link flood attacks is increased through the SDN architecture. Using the threat mitigatory module of the OpenFlow controller and the security score, the system is able to respond with an effective mitigation scheme against attacks without affecting the functionality of the SG. Also, the system can detect malicious behavior via the threat detector module of the SDN. The model is evaluated in an experimental global environment for network innovations (GENI) [58] testbed, characterized by wide area network dynamics and realistic traffic scenarios to address IEC 61850 network attacks.

3.2 Segmentation

The purpose of the segmentation technique is to segregate the components and functions of the system (e.g., sensors in power grid) according to criticality or trustworthy levels. In this way, the system operators can effectively spend their security resources, follow a specific recovery sequence, isolate security functions from non-security functions, etc. Therefore, segmentation may entail:

- *Predefined segmentation* defines resource sets based on their criticality so that they can be protected separately before the system is activated.
- *Dynamic segmentation* modifies the configuration of protected segments while the system is operating.

This resilience technique is mainly applied to the resilient state, but may also be applied to the restorative state. When the segmentation technique is applied to assist recovery processes, it is performed in offline mode, before the system is activated, to ensure that critical components will be protected separately. In this way, the resilience level of the system is increased. Figure 5 shows algorithms and technologies used for segmentation against cyber attacks in power grids. Some related studies are presented in the following subsections.

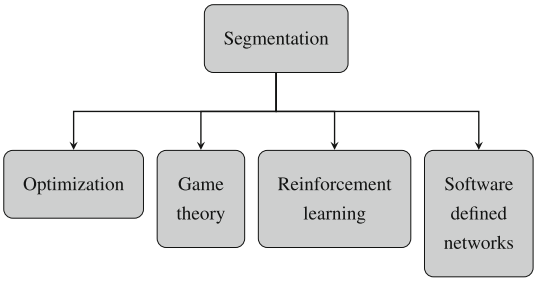

Fig. 5 Methods for segmentation

3.2.1 Optimization methods

In order to properly discover the critical parts in power systems, it is important to define a vulnerability metric for each element and sort them accordingly. This type of ranking is used by the system operator to define critical and non-critical segments in the SG. This is a typical optimization problem where the goal is to minimize or maximize a value; e.g., vulnerability metric, subject to certain constraints, or security budget.

For example, in [59] the chances of a successful false data injection attack on smart meters are investigated, under a limited budget. This method searches for all sets of meters that can bypass the bad data detection defense and classifies them as *target sets*. With the *target sets*, the *vulnerability index* metric for every meter is constructed, which measures the amount of attack vectors in which a protected meter appears and the damage caused by a hijacked meter. Finally, meters are ranked based on their *vulnerability index* and the top-k affordable ones are protected. The performance of this method is evaluated by simulating FDI attacks against IEEE 14-bus, 30-bus, 57-bus, 118-bus and 300-bus systems.

3.2.2 Game theory

Game theory models have been also proposed for discovering the most critical parts in a power system, similar to the optimization methods described in Sect. 3.2.1. By developing an attacker/defender game, game theory models can conduct a vulnerability analysis for the power system under investigation. In this way, the system operators can discover which parts of the power system are more likely to be targeted and can secure them accordingly. Vulnerability analysis can also contribute to the development of security guidelines in case of successful cyber attacks, as a defensive response against them.

In [60], a strictly competitive game is designed that approximates the interaction between attacker and defender in case of FDI attacks against power system state estimation. In this way, the least-budget defense strategy is designed to make power systems immune to FDI attacks. Then, an extension to the proposed problem is considered, where the number of protected meters is limited, making the proposed method feasible for real-life applications. Simulations have been performed on several IEEE test power systems (IEEE 9-bus, 14-bus, 30-bus, 118-bus, and 300-bus), using MATPOWER [61], to verify the scalability of the proposed approach.

3.2.3 Reinforcement learning

A common approach for optimally recovering different components of the power grid is to develop reinforcement learning algorithms. Reinforcement learning is a process that allows a software agent to adopt optimal behavior by interacting with a dynamic environment via trial-and-error [62]. The majority of the proposed methods attempt to find an optimal strategy to self-heal the system under specific restrictions, e.g., recovery time or cost.

A Q-learning technique is implemented in [63], that models the importance of the communication links and finds the optimal set of links for recovery under a limited budget. For evaluation, large-scale failures are simulated in MATLAB in order to compare the proposed recovery strategy with other ones. In [64], Q-learning is applied to discover an optimal link/node recovery sequence in feasible time. The simulation results are demonstrated on three benchmarks under the IEEE 300-bus system. In [65], the optimal re-closing time of power transmission lines after a successful cyber attack is investigated using a deep reinforcement learning method. For validation, the recovery strategy is compared with two alternative ones for different scenarios within a simulated, modified 9-bus system, whose parameters are provided.

Reinforcement learning can also be leveraged to keep the system at a resilient state. In [66], cognitive radio network technology is considered for the SG, which is suitable for wide area monitoring without additional cost. To make it difficult for an attacker to accomplish a jamming attack, the transmitter and the receiver follow a MAB approach to choose the most likely available and jamming-free channels to communicate. Successful acknowledgment signal is a metric that determines whether a selected channel combination in the strategies of the transmitter and the receiver will be rewarded or not. In the long term, channels with the highest potential of being available are chosen for communication. The performance of the proposed scheme is measured by the average throughput and the similarity of the secondary users' knowledge on the channel availability, but the details of the experimental environment are not provided.

3.2.4 Software-defined networking

The disconnection of compromised elements in a PMU network is suggested in [67] in order to prevent a cyber attack from further expansion. This utility adopts a SDN architec-

ture since reconfiguration of switches is easier with such a technology. Isolating a set of interconnected units though may cause data loss from functional PMUs and phasor data concentrators (PDCs) and affect critical functionalities such as state estimation. Therefore, discovering new communication links to reconnect PMUs and PDCs with the control center using the dynamic nature of a SDN makes the system capable of self-recovery. Furthermore, an integer linear program is formulated along with a heuristic algorithm to boost self-healing procedure, taking system requirements into consideration. The proposed defense scheme is evaluated by MATLAB simulations in both IEEE 30-bus and 118-bus systems.

3.3 Redundancy

Redundancy, as a cyber resilience technique, uses additional resources of critical components in order to reduce the possibility of information or services loss. Namely, the main idea when redundant systems are deployed is to eliminate single points of failures, like a single SCADA master. Thus, it is more difficult for adversaries to launch a successful cyber attack because they have to compromise several different parts of the system, making it more resilient. It is important to mention that the redundancy technique replicates multiple systems of the same kind, whereas diversity, as we will discuss later, uses multiple systems of a different kind but with similar functionality. Different approaches and examples of redundancy mechanisms include the following:

- *Backup* keeps backups of important elements of the system to restore them when an attack has been launched.
- *Additional capacity* reserves extra capacity for information storage in terms of space, processing in terms of MHz/GHz or communication, e.g., additional bandwidth.
- *Replication* duplicates hardware/software components while keeping their main operational functions synchronized all the time. To achieve this, it is necessary to maintain one or more alternate processing units, maintain a redundant secondary system, etc.

This widely used resilience technique entails the inclusion of additional resources, as backup support, before the system is activated in order to leverage them in case of a successful cyber attack. As a result, it is mainly applied to the resilient state to boost the resilience level of the system. There are also studies that are applied to the restorative state, but this research field is still at its infancy. In Fig. 6, algorithms and technologies that contemplate redundancy to achieve resilience against cyber attacks in power grids are depicted. Various studies that comprise the aforementioned strategy are presented below.

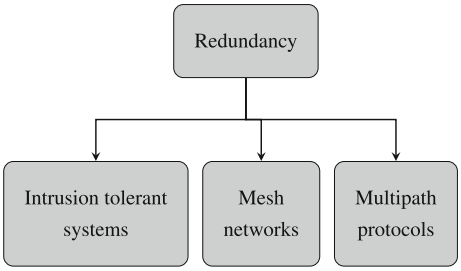

Fig. 6 Methods for redundancy

3.3.1 Intrusion-tolerant systems

In [68], an extra layer to the conventional SCADA architecture is added to increase its survivability against cyber attacks. This new layer consists of a filtering unit (FU) which serves as a rule-based, malicious packet detector between the master and slave units of a SCADA system to decide whether a command should be executed or not. In this sense, the master device communicates with the slave device through the FU via an encrypted Modbus protocol. In order to tackle the problem of a concurrent corruption of the master and the FU, the single FU is replaced by a mesh of N filtering units. This topology boosts the resilience of a SCADA system because adversaries have to compromise at least K different filtering units (where $K > N$) to execute their attack. This architecture is validated in a laboratory environment which replicates the process network of a typical power plant [69].

In [70], a survivable architecture for the master unit of a SCADA system is proposed by including an intrusion-tolerant replication system which is implemented with the Prime replication protocol [71,72]. The main objective of this work is the elimination of the issues that emerge due to the architectural difference between the SCADA system and the intrusion tolerant replication systems. For evaluation, the replication engine is integrated with a real SCADA master product for electricity distribution and a proxy is developed to integrate SCADA master with an RTU.

An intrusion-tolerant SCADA system is proposed in [73]. This architecture (called "Spire") tackles the attacks against systems that use the prime intrusion-tolerant replication engine for the master unit of a SCADA system. Moreover, it provides proactive recovery with periodical replica reboot, operating system-level diversity and network-level intrusion tolerance by running the spines messaging framework which offers link redundancy among control centers and substations. The different topologies that the replicas of the SCADA master form are thoroughly investigated in order to discover the most suitable ones based on the attack case, bearing in mind the Byzantine fault tolerance requirements. Spire is deployed in a real wide area cloud environment to evaluate its ability to support the timeliness requirements of the power grid and has participated in a red-team exercise.

A system that also adds redundancy and diversity techniques to enhance its resilience against spoofing attacks is presented in [74]. In a standard wide area monitoring system (WAMS) that uses PMUs, a single Global Positioning System (GPS) receiver timestamps every metering unit. On the contrary, in the proposed architecture each PMU (or cluster of PMUs) operates under its own GPS receiver in order to preserve the synchronization of WAMS in case of successful spoofing attacks against synchrophasors. Time synchronization among GPS receivers is achieved with network time protocol (NTP) [75]. For the experiments, two PMUs with a power grid that works at 60 Hz are used but the type of the testbed (real or simulated) is not clarified.

In [76], an intrusion-tolerant architecture for SDN-assisted critical infrastructures with a redundant controller is presented. Although this approach chooses an election-based consensus system that is well known for its tolerance against Byzantine faults, its drawback is that it cannot meet the strict functional requirements of the critical infrastructures. The integration of the system with an intermediate broker addresses this issue. The intermediate broker stores the necessary information about status and request packets and communicates with every SDN controller operating in parallel. Furthermore, it keeps all controller replicas informed about the status of the network and thus, any delay caused by synchronization is eliminated. This architecture is not evaluated with any simulation.

3.3.2 Mesh networks

There are several studies that recommend the design of multihop mesh networks to tackle congestion and DoS attacks. In this sense, a distributed middleware architecture is presented in [77] that leverages redundant gateway nodes to reroute congested traffic caused by a cyber attack. Here, alternative paths are evaluated based on quality-of-experience (QoE) criteria. The proposed architecture is validated in two cases using a real-time co-simulation test system of NS3 and MATLAB/Simulink. Similarly, in [78] rules inspired by flocking theory are developed for effective network routing in case of data traffic congestion. This work is improved in [79], which focuses on a multicast route decision scheme capable of efficiently compensating the bandwidth consumption with the end-to-end latency. Both of them are employing MATLAB/Simulink for their simulations.

In [80], a middleware is proposed as a complementary communication channel between the master and slave units of a SCADA system. Among others, a peer-to-peer (P2P) middleware technology is used to meet the large-scale design requirements of the SCADA system. The system is hardened via path redundancy, which provides an abundance of communication links for the transferred data and data replication, which increases the data availability throughout the communication network. In case of a node crash, sensor messages can be obtained from the P2P overlay network and data corruption can be prevented by identifying a message with a replica stored in the P2P network. A simulation-based evaluation is followed using the OMNet++ [81], a discrete event simulator.

Another attack-resilient architecture that leverages mesh networking is proposed in [82]. This architecture includes a power distribution network composed of smart meters that communicate with local controllers which, in turn, are supervised by substation controllers. Local controllers are connected with each other in mesh topology in order to maintain high data delivery rate in case of successful jamming attacks. When such an attack is detected, local controllers send the channel hopping sequences to the smart meters. Then, smart meters select which local controller to choose at each time step in order to make it difficult for jammers to learn these sequences. Also, this work is extended in [83] to further reduce the effects of a jamming attack. In this updated version, a retransmission packet strategy between smart meters and local controllers is utilized to record lost packets and resend them. This framework is evaluated by simulating a smart grid communication subsystem in MATLAB 2013b.

In [84], a redundancy-based restoration mechanism is designed for a network infrastructure. This infrastructure consists of three layers, where a fog-based architecture provides the necessary redundancy in order to protect specific cyber-physical control devices. The main idea is the link replication with the assistance of fog computing in order to keep the control of the system active all the time. To achieve this in time, a forecasting method that predicts a possible threat is proposed based on k-means and k-nearest neighbor algorithms. Two case studies that consider different attack strategies have been implemented in MATLAB for evaluation.

3.3.3 Multipath protocols

In [85], an extension of the multipath TCP (MPTCP) transportation protocol is employed for WAMS to mitigate the impact of DoS/DDoS attacks. Particularly, MPTCP establishes multiple transmission control protocol (TCP) connections between two nodes via different network interfaces, called subflows. In this work, subflows between PMUs and PDCs are randomly opened and closed over a certain amount of time. Thus, a successful attack on network resources is inadequate because of the limited life span of connections. Data are transmitted successfully with path redundancy and experiments indicate that this mechanism respects the latency constraints of WAMS. A significantly improved version of this work, in terms of performance and resilience, is outlined in [86]. For evaluation, the NorNet testbed [87] is

used which consists of a collection of multihomed nodes distributed throughout Norway.

3.4 Diversity

Unlike redundancy, diversity deploys multiple, heterogeneous elements that serve the same purpose but share unique features among them; e.g., multiple communication links of different types. Diversity was introduced to tackle the fate sharing problem of replicas [88] that is caused by the redundancy technique. If an attacker manages to compromise one replica, it is highly likely to affect all of them [84]. Furthermore, an adversary might spend valuable resources on a diversified system or could apply significant effort to inappropriate targets. This technique can be considered as complementary to redundancy since there are several studies where these techniques coexist and support one another. Different approaches and examples of diversity are presented below:

- *Synthetic diversity* diverse software/hardware implementations to generate a variety of instances.
- *Design diversity* use alternative designs to provide equivalent functionality.
- *Path diversity* offer multiple independent paths for control and communications.

Similar to redundancy, diversity is configured in offline mode to make it difficult for adversaries to exploit redundant systems if some replicas are compromised. Hence, this resilience technique can be applied at the resilient state. There are also studies that are used at the restorative state, but this research field is still at its infancy. Figure 7 depicts the methods that use the diversity technique to achieve resilience against cyber attacks in power grids. In the following subsections, studies apply the aforementioned methods are presented.

3.4.1 Intrusion-tolerant systems

Some of the intrusion-tolerant systems described in Sect. 3.3 apply the diversity technique alongside redundancy [68,70,73,84]. For instance, in [68] design-level diversity is used by deploying each filtering unit on a different operating system with alternate configurations. Similarly, in [73], diversity is applied with different operating systems but is also extended to application level, where the compiler generates different types of software with same functionality. In [70], diversity is achieved by incorporating a single operating system with address space layout randomization (ASLR) [89]. Moreover, this defensive method offers support for automatic software generation at compilation time [90] and for an individual private key as a requirement to send sensitive

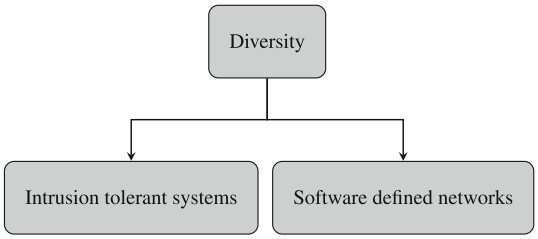

Fig. 7 Methods for diversity

Table 1 Synthetic diversity

Intrusion-tolerant systems	
Operating system level	Different types of OS
	ASLR
Application level	N-version programming [91,92]
	Compiler-based software diversification

information from each replica. A summary of these synthetic level diversity methods is depicted in Table 1.

3.4.2 Software-defined networking

The problem of compromised communication links can be tackled with path diversity. If a communication link is compromised, then another backup path of a different technology can be used. Path diversity is usually facilitated by a SDN-based system due to its flexibility [93]. Thus, diversity along with adaptive response is a suitable combination of cyber resilience techniques, widely adopted by research community. For example, in [94] the SDN controller automatically alters flow tables when a wired communication link has failed and the traffic is redirected through a backup wireless interface. This approach is tested on a simulated environment which is an integration of Mininet with NS-3 [95] network simulator.

In [96], the capabilities of SDN are used to improve the resilience of communication across different substations. By combining communication path diversity and the functionalities of SDN, an additional wireless network interface is deployed that acts as an auxiliary passage when wired connections suffer from disturbances. In this work, NS-3 is integrated with the Mininet environment to emulate the interconnections between substations. This is an interesting point for experimental purposes since real substation facilities are not always available or practical. The method is evaluated by measuring end-to-end packet and recovery delay for user datagram protocol (UDP) and TCP connections for several topologies.

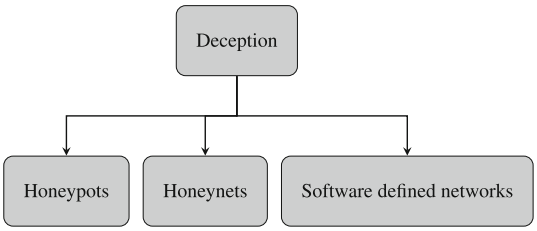

Fig. 8 Methods for deception

3.5 Deception

A common method to protect critical parts of an ICT infrastructure when unauthorized access to the system has been granted is to mislead the intruders. This technique is called deception. With this technique, the system operator tries to misdirect or delay the adversaries in order to keep a track of their behavior and their methods, hide critical assets from them, waste their resources, and ultimately, force them to launch an attack to the wrong target. Different approaches and examples of deception are presented below:

- *Misdirection* enables decoy units or environments, e.g., honeypots, to attract the activities of the adversaries.
- *Misinformation* intentionally provides misleading information to attackers.

Intentional exposure of resources which are similar to the critical ones is a preventive technique to enhance the resilience level of SG. As a result, deception is associated with the resilient state. In Fig. 8, the most representative deception methods to achieve resilience against cyber attacks in power grids are shown. Moreover, recent studies that apply deception technique are presented in the following subsections.

3.5.1 Honeypots

The concept of honeypot is to emulate the operation of a real computer system in order to learn the behavior of the attackers and distract them from more valuable resources [97]. Honeypots can be grouped into two general categories: production honeypots that protect an organization and research honeypots that are used to gather information [98]. Research honeypots are designed to gain information about the attackers. They are mainly deployed by research organizations, such as universities and security research companies. This work focuses on research honeypots.

In the literature, research honeypots have been proposed in order to gather information about the motives and tactics of adversaries. For example, the crysys PLC (CryPLH) [99] is a high-interactive honeypot that emulates a commercial Siemens Simatic S7-300 PLC. An enhanced version of CryPLH can be found in [100], where many bugs of the initial environment have been eliminated. For evaluation, CryPLH was implemented in a laboratory setup along with the real PLC device. Both of them were publicly accessible to verify if they are indistinguishable from the perspective of attackers. Moreover, a low-interaction honeypot (called SHaPe) is introduced in [101], which is specialized in substation automation systems. The performance of SHaPe in not evaluated by any simulation or experiment.

Conpot [102] is another low-interactive SCADA honeypot that aims to collect intelligence about the motives and methods of adversaries. To evaluate the SCADA honeypot Conpot, a virtualized image was created in [103] and used in multiple Amazon Web Services' (AWS) zones. For the purposes of the honeypot analysis, an in-depth review of both the Guardian AST gas pump monitoring system and default Siemens S7-200 ICS was performed together with a brief analysis of the IPMI - 371 and Kamstrup - 382 smart meter SCADA devices.

3.5.2 Honeynets

In order to develop honeypot solutions that can adequately emulate a large-scale system such as SG, honeynets have been proposed in the literature. Honeynet is a set of interconnected honeypots where each honeypot individually delivers a particular task.

A honeynet system that is composed of different honeypot substations has been implemented in [104]. These honeypot substations communicate with a virtual power grid in order to give the attackers the sense of a realistic topology which can be used as a decoy. A proof-of-concept implementation is presented along with its preliminary evaluation. The implementation includes open-source tools, namely VirtualBox [105] for host and device vitualization, Mininet [106] for network emulation and SoftGrid [107] for integrated cyber-physical simulation.

Another honeynet is described in [108]. In this work, a single substation is emulated which is composed of honeypots simulating the human machine interface (HMI) and intelligent electronic devices (IEDs). This framework is evaluated by simulating the power flow of an electric grid with GridLABD from Pacific Northwest National Laboratory. GridLABD comprises multiple substations and emulates the IEC 61850 digital communications protocol by extending Conpot honeypot.

In [109,110], an architecture with multiple honeypot instances is deployed. It is designed to imitate industrial communication protocols, such as Modbus and IEC 60870-5-104, for tracking the processes of malicious activities. Moreover, this implementation is expanded in [111] to cover more industrial communication protocols. This framework and its implementation were evaluated through experiments

that were carried out using the Amazon EC2 cloud environment. The protocols exposed are Modbus, DNP3, ICCP, IEC-104, SNMP (v1/2/3), TFTP and XMPP and the duration of the experiments was 28 days.

3.5.3 Software-defined networking

SDN is again another technology that can implement deception techniques, specifically when it is used in conjunction with honeypots. For example, a honeypot network is introduced in [112] which is identical to the field network under investigation. When the IDS of the system identifies an adversary, it informs the SDN controller to properly modify the flow tables in order to relocate the attacker and lead them to the honeypot. With this approach, the attacker can be isolated from the actual process without affecting its performance. The proposed framework is evaluated within a network of physically separated virtual machines (VM) using Mininet, MiniCPS and ONOS [113].

Moreover, the incident response system for the water treatment SCADA system, previously presented in [30], can also use SDN for deception technique. According to this work, another potential incident-response strategy to mitigate an attack is to mislead an adversary to a honeypot when an attack has been detected. The traffic is headed toward the honeypot when it is selected by the preconfigured incident response policy of the SDN controller.

4 Research challenges and open issues

The previous analysis of existing methods that enhance the cyber resilience of SG reveals the difficulties that are encountered during the design of such methods, the relevant topics that are not covered in the literature and the algorithms or technologies that could be potentially considered in the future. This section is dedicated to the cyber resilience challenges of SG that have been identified from the analysis of Sect. 3. Research gaps and directions about future research are also given in this section.

4.1 Research challenges

4.1.1 Operational requirements

From the analysis of Sect. 3, it is clearly illustrated that the SG differs from traditional energy systems (power grids that are not integrated with ICT technology) in that their operational requirements [7] (e.g., response time, measurement accuracy, etc.) are strict. Therefore, a proposed cyber resilience solution cannot be considered reliable if it violates the operational requirements of the SG, regardless of its effectiveness. For instance, if a defensive mechanism manages to redirect the important information in a compromised system but fails to deliver it on time, then it is not useful for SG.

To address this challenge, any proposed defense should validate that the operational limits are followed. This can be achieved via extensive experiments which demonstrate that, when the defense mechanism is activated, the system remains still operational. Moreover, for better evaluation these experiments should be performed on a real testbed.

4.1.2 SDN limitations

The analysis in Sect. 3 shows that there are several methods that use SDN to increase the cyber resilience of SG. Nevertheless, there are still aspects in SDN technology that have not been sufficiently considered. For example, the SDN controller is the key part of this technology since it is responsible for the network management. This means that if it fails, the entire system will stop operating, and therefore, it is considered as a single point of failure (SPoF). Designing systems with SPoFs is a bad practice in general and they should be heavily protected by system engineers or, ideally, eliminated. Moreover, the computational cost of traffic rerouting SDN solutions often fails to comply with a crucial requirement in automation scenarios of critical infrastructures—to incur minimal overhead, as well as zero interference in case of failure.

Another critical aspect is the selection of the protocol that will enable the SDN technology. Many of the methods described in Sect. 3 are utilizing SDN based on OpenFlow protocol. OpenFlow is a protocol that enables SDN controllers to determine the path of network packets across a network of switches. Until recently, the terms OpenFlow and SDN were nearly interchangeable. However, OpenFlow has drawbacks that prevent the smooth integration of SDN with the SG environment. For example, Internet service providers cannot choose specific OpenFlow functions (although not all of them are always needed) and thus, costs are high. Moreover, each new OpenFlow version requires a network switch vendor that supports the protocol, making it vendor-dependent.

4.1.3 Collaborative resilience

As given in Table 2, standard ICT technologies and software components such as intrusion-tolerant systems, mesh networks, SDN and honeypots dominate the techniques of redundancy, diversity and deception—some of them adding an important economic burden. Their techniques are mainly deployed before the cyber attack takes place and aim to make it difficult for the adversary to affect the system components or data. The other family of mechanisms, which derives from the power system community, tends to have a more active role in terms of resilience, once the system is compromised. This

Table 2 Overview of methods

Paper	Resilience		
	Method	Technique	State
[21–23]	Attack-resilient control	Adaptive response	Restorative state
[24–26]	Attack-resilient control	Adaptive response	Post-event degraded state
[28,30,32,33,35,37]	Model-based response	Adaptive response	Post-event degraded state
[39,41,43–45]	Incident response scheme	Adaptive response	Resilient state
[47,56]	SDN	Adaptive response	Resilient state
[51,53,55]	SDN	Adaptive response	Restorative state
[59]	Optimization	Segmentation	Resilient state
[60]	Game theory	Segmentation	Resilient state
[66]	Reinforcement learning	Segmentation	Resilient state
[63–65]	Reinforcement learning	Segmentation	Restorative state
[67]	SDN	Segmentation	Resilient state
[68,70,73,74,76]	Intrusion-tolerant systems	Redundancy	Resilient state
[77–80,82]	Mesh networks	Redundancy	Resilient state
[84]	Mesh networks	Redundancy	Restorative state
[85,86]	Multipath protocols	Redundancy	Resilient state
[68,70,73]	Intrusion-tolerant systems	Diversity	Resilient state
[84]	Intrusion-tolerant systems	Diversity	Restorative state
[94,96]	SDN	Diversity	Resilient state
[99–103,114,115]	Honeypots	Deception	Resilient state
[104,108–111]	Honeynets	Deception	Resilient state
[30,112]	SDN/Honeypot	Deception	Resilient state

is reasonable if we consider the fact that computer systems generally transit between known, discrete states contrary to power systems, where their dynamic nature poses stability issues.

Given this, a critical challenge at this point is how to harmonically combine computer science and power system solutions to provide defense in depth with multiple levels of cyber resilience. Methods that would integrate these different solutions into a uniform one could significantly enhance the cyber resilience of SG.

4.1.4 Distinction between cyber attack and plant failures

Cyber attacks and plant failures are two different types of unplanned events that both have a negative impact on the SG. Identifying whether a degradation in the performance of the SG is due to a cyber attack or plant failure is important in order to apply the proper countermeasures. Moreover, proposed methods that tackle a cyber attack are not necessarily appropriate for plant failures and vice versa. For example, the typical model-based response that is demonstrated in Fig. 4 has been widely adopted in the academic literature to mitigate cyber attacks against the SG, but it might fail when the actual signal is affected by a plant failure.

However, this distinction is a very challenging task and has been rarely addressed [116]. It is advisable for researchers to put their efforts toward the distinction between cyber attacks and plant failures in order to apply the proper recovery methods. The special features of each unplanned event have to be investigated in order to distinguish the one from the other.

4.2 Open issues

In Sect. 3, a variety of methods that aim to make SG more cyber resilient are briefly analyzed. Nevertheless, there are still pending issues that have not been sufficiently considered and thus, they become interesting open issues which are worth investigation. This section is dedicated to these open issues.

4.2.1 Standardization

It has been already discussed that SG is a highly complex infrastructure, where many heterogeneous technologies constantly cooperate altogether. In this sense, achieving high levels of cyber resilience in SG is a multifaceted issue. Cyber resilience of SG can benefit from the development of a set of general standards that would settle common cyber resilience definitions for SG, classify relevant problems and propose

possible solutions or recommendations. While such mature guidelines have been already proposed in the ICT domain [13], the standardization efforts in CPS are still in progress. For example, while DERs are increasingly used in SG, they often fail to meet the critical infrastructure protection security requirements [117–119] established by the North American Electric Reliability Corporation (NERC) in [120].

The development of such a framework is not a trivial task. There are strict operational limits in SG which are critical obstacles toward the standardization of its cyber resilience. Moreover, several industries, corporations, organizations, institutes, etc., are involved with the SG and have different approaches toward its different aspects. This lack of consensus further complicates the establishment of a unified guide about the cyber resilience of SG.

4.2.2 SG restoration

As shown in Figs. 3, 4, 5, 6, 7 and 8 and Tables 2 and 3, the majority of the included techniques mainly aim to protect the system at the resilient state. On the other hand, the research efforts toward the post-event degraded state and the restorative state of the resilience curve of [14] are limited. It should also be noted that, to the knowledge of the authors, there are no techniques in the literature that deal with the post-restoration state.

The few works that are involved with the latter stages of the resilience curve (restorative and post-restoration states) create a significant research gap in the literature. This is reasonable if we consider their challenging nature. Developing algorithms or designing architectures that can automatically restore SG requires deep understanding about the behavior of the adversaries and in some cases human intervention might be necessary. Nevertheless, significant effort should be put on this subject in order to provide the power sector with a holistic protection against cyber threats.

4.3 Future directions

This section presents and analyzes the scientific areas that should be further researched in order to enhance the cyber resilience of SG. These areas arise naturally from the in-depth analysis of Sect. 3.

4.3.1 Deep learning (DL)

In Sect. 3, several ML applications that have enhanced cyber resilience of SG are presented, especially when adaptive response and segmentation techniques take place. Nevertheless, authors believe that DL, which is a promising ML subfield, has not been sufficiently investigated for the cyber resilience of SG. For instance, autoencoders [121] and deep belief networks [122] are two types of DL algorithms that can extract high-level, complex features of the given input in order to learn the behavior of SG controllers more accurately. Recurrent neural networks (RNNs) and, specifically, long short-term memory (LSTM) [123] are DL models that perform well in classification and prediction tasks based on time series data and thus are suitable for IDS or measurement estimation. Graph convolutional networks (GCNs) [124] learn the features of the given data, which are represented as a graph, by inspecting its neighboring nodes. In the literature, there are significant efforts [125,126] that consider system topology to represent the power grid as a graph in order to apply a GCN architecture. More specifically, DL models should be implemented in the future in order to:

1. Create more reliable and accurate IDS;
2. Construct more attack-resilient SG controllers;
3. Learn the behavior of the controllers of the SG to replace them in cases of emergency for the majority of the expected cyber attacks; and
4. Optimize decision-making processes, e.g., (i) select appropriate attack response, and (ii) choose alternative, reliable communications paths, etc.

Despite their usefulness in several challenging tasks, ML/DL algorithms have significant drawbacks that complicate their practical implementation. First of all, these algorithms require a large amount of data for their training phase which makes them computationally demanding models (either in terms of time or infrastructure cost). Furthermore, adversarial machine learning is a critical threat against these algorithms. Adversarial ML exploits the fact that ML/DL models usually draw their testing and training data from the same underlying distribution. In this way, adversaries attempt to cause malfunctions to ML/DL models by providing deceptive inputs to them. For example, poisoning attack is a typical attack during the training phase that attempts to modify the statistical characteristics of the training dataset [127]. Regarding the testing phase, in [128] it is observed that imperceptive perturbations to the images can fool DL models into providing misclassifications and in [129], adversarial examples are generated by appending noise to the original image along the gradient directions. These limitations and threats have to be carefully considered when ML/DL models are applied.

Finally, while ML-based controllers often demonstrate better performance compared to conventional controllers, they might behave unpredictably in unforeseen events that are not covered by the initial training dataset. This is a fundamental issue and has to be carefully handled by ML/DL model designers. To tackle this challenge, periodic retraining of the proposed ML/DL models is advisable with new data that are collected over time in order to include more unplanned events and newly identified threats.

Table 3 Resilience techniques versus states

States	Techniques				
	Adaptive response	Segmentation	Redundancy	Diversity	Deception
Resilient state	✓	✓	✓	✓	✓
Post-event degraded state	✓				
Restorative state	✓	✓			
Post-restoration state					

4.3.2 OpenFlow alternatives

Though OpenFlow was one of the first widely used protocols for enabling SDN, it fails to meet all the distinct requirements of SG for cyber resilience due to its limitations, as illustrated in Sect. 4.1.2. Therefore, alternative approaches to OpenFlow have recently received significant attention. For instance, in [130] P4 is proposed, which is a data plane programming language. In contrast to OpenFlow, the data plane functionalities described with P4 are not fixed by the hardware. Vendors provide an abstraction model of the networking devices, the P4 architecture model, and a target specific P4 compiler. Since multiple targets can have the same architecture, programs can be ported. Moreover, P4 is designed to be protocol-independent. The P4 programmer specifies the header formats and field names of the required protocols in the program which are in turn interpreted and processed by the compiled program and target device. Consequently, these features of P4 can assist the communication of the SDN with the heterogeneous technologies of SG.

NETCONF [131] is another management protocol used to configure network devices. The abstraction level which offers, can assist the management of the different technologies within SG. Its operations are realized on top of a remote procedure call (RPC) paradigm. The NETCONF protocol uses an Extensible Markup Language (XML)-based data encoding for the configuration data and the protocol messages. The NETCONF protocol can be separated into four layers:

- *Secure transport layer* provides the actual communication between client (controller) and server (network device);
- *Message layer* defines the encoding of the remote procedure calls;
- *Operations layer* defines a set of basic operations; and
- *Content layer*.

Clearly, the aforementioned approaches are not the only ones that can be utilized as alternatives to OpenFlow, but they can become an interesting pivotal point for investigation toward the enhancement of SDN functionalities.

4.3.3 Parallel redundancy protocol and high-availability seamless redundancy

Since SG is considered a critical infrastructure, it requires the minimum recovery time possible when a successful cyber attack has been achieved. The IEC 61850 (the default standard for industrial automation networks) uses the Ethernet technology and introduces its own challenges and requirements [132,133]. Regarding the network infrastructure, the recently published IEC 61850-90-4 [134] has adopted parallel redundancy protocol (PRP) and high-availability seamless redundancy (HSR), both defined in the IEC 62439-3, as the preferred Ethernet-based protocols for station bus and process bus in substations. They offer almost-zero recovery time and frame loss protection in the presence of a cyber attack or grid failure in general.

The PRP is an IEC standard providing redundant Ethernet. Under PRP, each node is connected to two separated, parallel, fail-independent local area networks (LANs). A transmitter sends two copies of the same packet over each LAN and when a receiver acquires a packet, it accepts the first copy and discards the duplicate. Thus, if both networks are operational, it is ensured that the information will reach its destination. This provides zero recovery time in case of a single failure, so no data are lost.

High-availability seamless redundancy (HSR) is a standard which covers the need for reliable Ethernet. The core of HSR functionality is its topology, which typically is a ring. The source node duplicates all the frames it has to deliver and sends them simultaneously to their destination, utilizing two independent paths (clockwise and counterclockwise). If either one of the paths is broken, due to link or node failure caused by a cyber attack, the frames are still capable of reaching their destination.

The drawback of PRP is its high network cost, compared with a single non-redundant network. An HSR ring provides the same level of redundancy with a lower cost. The advantage of PRP, when compared with HSR, is that normal non-PRP-aware nodes can be connected to the network without special hardware, like RedBox in HSR. However, these single attached nodes can communicate only with the nodes connected into the same LAN and they cannot leverage the

redundancy. Furthermore, there are studies [135] that experimentally demonstrate the failure of these protocols to actually achieve zero recovery time in realistic scenarios. If these protocols do not meet the strict operational requirements of electric power substations (their order of magnitude varies between 4 and 12 ms, [135,136]), the electrical system will perform poorly, e.g., delays in the exchange of teleprotection messages lead to damages by short circuits. Therefore, it is apparent that there is still room for improvement regarding these protocols and their deployment in a substation environment. This integration will, in turn, increase the resilience of SG against cyber threats.

4.3.4 Emerging technologies

Designing a cyber resilient system that follows the strict operational limits of SG can be achieved with various advanced algorithms and technologies. Nevertheless, there is always a bottleneck to the improvements that these approaches can offer. Therefore, research effort should be also put on low-level technological approaches like improving the medium with which the information is transmitted. These approaches have a direct impact on the performance of the system, without the need of any special algorithm or methodology that will optimally manage the available resources.

A highly promising technology for the reinforcement of the cyber resilience of SG is the fifth generation of mobile networks, known as 5G networks [137]. The key features of 5G networks are the use of millimeter-wave signals and the high-frequency operation, which allow them to support greater bandwidth, lower latency and a vast number of devices (e.g., IoT and smart devices), turning 5G and Beyond 5G (B5G) into an ideal solution toward a more cyber resilient SG [138]. The low latency and increased bandwidth will enable the addition of security mechanisms without violating operational requirements. Moreover, 5G networks can provide continuous availability and security of the SG applications through cyber monitoring, grid self-healing and data re-routing, facilitating the re-connection of nodes and the 24/7 control.

Apart from this, the current computing paradigms are also good approaches to delegate computational loads. Edge, fog and cloud computing services could assist in resilience tasks [139,140], such as maintaining and determining new routes in real time and processing recovering states or data, without significantly impacting the operational performance of the underlying system. This impact could possibly vary, depending on the paradigm. Last but not least, digital twins correspond to a simulation tool that could ideally identify security vulnerabilities and estimate possible threat states to develop suitable response/restoration solutions in the application context [141]. This kind of simulation tool can be combined with the aforementioned technologies (artificial intelligence, edge computing and B5G) to create resilient solutions that work in real time [142], since digital twins can recompute values of the physical context.

Many of these technologies are in their infancy, posing different research issues such as the trustworthy degree in the delegation of services; the level of precision in the estimations, predictions or simulations; the degree of reliability; and the degree of QoS and security in the response or restoration processes. This also means that these technologies can introduce new vulnerabilities and security risks that have to be considered.

4.3.5 Lessons learned

Table 4 corresponds the resilience techniques and resilience states with the proposed future directions. This subsection is dedicated to the conclusions that are drawn from this table and can be used as a research guidance for future works. First of all, deep learning algorithms can be implemented throughout the whole resilience curve and mainly facilitate adaptive response and segmentation techniques. This is rea-

Table 4 Future directions for resilience techniques and states

States	Techniques				
	Adaptive response	Segmentation	Redundancy	Diversity	Deception
Resilient state	Deep learning	Deep learning	PRP	PRP	Cloud, edge, fog computing
	Digital twins		HSR	HSR	
			5G(B5G)	5G(B5G)	
Post-event degraded state	Deep learning				
Restorative state	Deep learning	Deep learning	5G(B5G)	5G(B5G)	
	Digital twins		Cloud, edge, fog computing	Cloud, edge, fog computing	
Post-restoration state	Deep learning		5G(B5G)	5G(B5G)	
	Digital twins		Cloud, edge, fog computing	Cloud, edge, fog computing	

sonable due to the close relation of the power sector with these techniques and the wide application of deep learning in power systems. On the other hand, redundancy, diversity and deception techniques are mainly computer-oriented and can be facilitated by emerging computing/communication technologies and specialized protocols.

Regarding the resilience states, it should be noted that the future directions presented in this section can be also applied in post-restoration state. This is quite important, considering that very few works deal with this state, as depicted in Table 3. Furthermore, these future directions can be applied to every resilience state. For instance, cloud, fog and edge computing can provide additional infrastructures to the SG in order to assist it in preserving its initial resilience level (resilient state), maximize its resilience level after an attack (post-event degraded state), recover it, e.g., using alternative nodes or links (restorative state) and, finally, keep it almost at normal operating point before it is fully recovered.

5 Conclusion and future work

Cyber threats against modern power control systems and their mitigation are crucial tasks to consider. There are numerous studies that propose defensive methods in order to prevent an attack or to detect malicious behavior. The latter is a widely studied field of research, in contrast to studies that attempt to make the SG more resilient against cyber attacks. This paper offers an overview of the current approaches that enhance the cyber resilience of SG and provides an extended discussion about current challenges, open issues and future directions. These approaches are grouped according to the cyber resilience techniques defined in the NIST SP 800-160 [13]. These techniques in turn are associated with the different states of the typical power system resilience curve defined in [14]. The result is a taxonomy that can assist researchers in investigating the cyber resilience of SG. It can also help them identify some promising future research areas and technologies in this field.

As future research, we intend to investigate methods that combine the capabilities of the ICT technology along with dynamic functionalities of the power system control solutions. An example of such a technique is the application of the SDN technology to the power system controls for the cyber resilience enhancement of SG. We consider it a potential intersection of ICT and power systems applications, suitable for the restorative state of cyber resilience. Nonetheless, we will also leverage the benefits of the emerging technologies described in Sect. refemergingtechnologies, given that they deserve further attention.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature. Funding for open access charge: Universidad de Málaga / CBUA.

Code availability Not applicable.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. U.S. Department of Energy, Grid Modernization and the Smart Grid. https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid
2. European Commission, European Technology Platform SmartGrids; Vision and Strategy for Europe's Electricity Networks of the Future. https://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf
3. U.S. Department of Energy, Cybersecurity. https://www.energy.gov/national-security-safety/cybersecurity
4. European Union Agency for Cybersecurity (ENISA), Smart Grids. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids?tab=details
5. Gungor, V.C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., Hancke, G.P.: Smart grid technologies: communication technologies and standards. IEEE Trans. Industr. Inf. **7**(4), 529–539 (2011)
6. Gunduz, M.Z., Das, R.: Cyber-security on smart grid: threats and potential solutions. Comput. Netw. **169**, 107094 (2020)
7. Alcaraz, C., Lopez, J.: Analysis of requirements for critical control systems. Int. J. Crit. Infrastruct. Protect. (IJCIP) **5**(137–145), 2012 (2012)
8. Case, D.U.: Analysis of the cyber attack on the Ukrainian power grid. Electr. Inf. Sharing Anal. Center (E-ISAC) **388**, 1–29 (2016)
9. Falliere, N., Murchu, L.O., Chien, E.: W32 stuxnet dossier White paper. W32. stuxnet dossier. White paper, Symantec Corp **5**(6), 29 (2011)
10. Karnouskos, S.: Stuxnet worm impact on industrial cyber-physical system security. In: IECON 2011—37th Annual Conference of the IEEE Industrial Electronics Society, pp. 4490–4494 (2011)
11. National Institute of Standards and Technology: Framework for improving critical infrastructure cybersecurity. Technical Report, NIST (2018)

12. Pillitteri, V.Y., Brewer, T.L.: Guidelines for smart grid cybersecurity. Technical Report (2014)
13. Ross, R., Pillitteri, V., Graubart, R.D., Bodeau, D.J., Rosalie, M.: A Systems Security Engineering Approach, Developing Cyber Resilient Systems (2019)
14. Panteli, M., Mancarella, P.: The grid: stronger, bigger, smarter? Presenting a conceptual framework of power system resilience. IEEE Power Energy Mag. **13**(3), 58–66 (2015)
15. Cómbita, L.F., Giraldo, J., Cárdenas, A.A., Quijano, N.: Response and reconfiguration of cyber-physical control systems: a survey. In: 2015 IEEE 2nd Colombian Conference on Automatic Control (CCAC), pp. 1–6 (2015)
16. Mihalache, S.F., Pricop, E., Fattahi, J.: Resilience enhancement of cyber-physical systems: a review. Power Syst. Resil. 269–287 (2019)
17. European Union Agency for Cybersecurity (ENISA), ENISA Smart Grid Security Recommendations. https://www.enisa.europa.eu/publications/ENISA-smart-grid-security-recommendations
18. Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N., Wollman, D.: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0, 2021-02-18 00:02:00 (2021)
19. Lee, E.A.: Cyber physical systems: design challenges. In: 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), pp. 363–369 (2008)
20. Sridhar, S., Hahn, A., Govindarasu, M.: Cyber-physical system security for the electric power grid. Proc. IEEE **100**(1), 210–224 (2012)
21. Zheng, Z., Jin, S., Bettati, R., Reddy, A.L.N.: Securing cyber-physical systems with adaptive commensurate response. In: 2017 IEEE Conference on Communications and Network Security (CNS), pp. 1–6 (2017)
22. Gholami, S., Saha, S., Aldeen, M.: A cyber attack resilient control for distributed energy resources. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), pp. 1–6 (2017)
23. Paridari, K., O'Mahony, N., El-Din Mady, A., Chabukswar, R., Boubekeur, M., Sandberg, H.: A framework for attack-resilient industrial control systems: attack detection and controller reconfiguration. Proc. IEEE **106**(1), 113–128 (2018)
24. Fawzi, H., Tabuada, P., Diggavi, S.: Secure estimation and control for cyber-physical systems under adversarial attacks. IEEE Trans. Autom. Control **59**(6), 1454–1467 (2014)
25. Pajic, M., Weimer, J., Bezzo, N., Tabuada, P., Sokolsky, O., Lee, I., Pappas, G.J.: Robustness of attack-resilient state estimators. In: 2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), pp. 163–174 (2014)
26. Bezzo, N., Weimer, J., Pajic, M., Sokolsky, O., Pappas, G.J., Lee, I.: Attack resilient state estimation for autonomous robotic systems. In: 2014 IEEE/RSJ international conference on intelligent robots and systems, pp. 3692–3698 (2014)
27. Black-I Robotics LandShark UGV. https://www.blackirobotics.com/landshark-ugv/
28. Cárdenas, A.A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., Sastry, S.: Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS '11, pp. 355–366. ACM, New York (2011)
29. Ricker, N.L.: Model predictive control of a continuous, nonlinear, two-phase reactor. J. Process Control **3**(2), 109–123 (1993)
30. Murillo Piedrahita, A.F., Gaur, V., Giraldo, J., Cárdenas, A.A., Rueda, S.J.: Leveraging software-defined networking for incident response in industrial control systems. IEEE Softw. **35**(1), 44–50 (2018)
31. Antonioli, D., Tippenhauer, N.O.: MiniCPS: a toolkit for security research on CPS networks. In: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy, pp. 91–100 (2015)
32. Sridhar, S., Govindarasu, M.: Model-based attack detection and mitigation for automatic generation control. IEEE Trans. Smart Grid **5**(2), 580–591 (2014)
33. Tan, R., Nguyen, H.H., Foo, E.Y.S., Yau, D.K.Y., Kalbarczyk, Z., Iyer, R.K., Gooi, H.B.: Modeling and mitigating impact of false data injection attacks on automatic generation control. IEEE Trans. Inf. Forensics Secur. **12**(7), 1609–1624 (2017)
34. PowerWorld, 2016. http://www.powerworld.com/
35. Wei, J., Mendis, G.J.: A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids. In: 2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG), pp. 1–6 (2016)
36. He, Y., Mendis, G.J., Wei, J.: Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans. Smart Grid **8**(5), 2505–2516 (2017)
37. Li, Y., Zhang, P., Ma, L.: Denial of service attack and defense method on load frequency control system. J. Franklin Inst. **356**(15), 8625–8645 (2019)
38. Bevrani, H.: Robust power system frequency control (2014)
39. Chen, Q., Abdelwahed, S.: A model-based approach to self-protection in SCADA systems. In: 9th International Workshop on Feedback Computing (Feedback Computing 14) (2014)
40. Zhu, X., Shen, M.: Based on the ARIMA model with grey theory for short term load forecasting model. In: 2012 International Conference on Systems and Informatics (ICSAI2012), pp. 564–567 (2012)
41. Hewett, R., Rudrapattana, S., Kijsanayothin, P.: Cyber-security analysis of smart grid SCADA systems with game models. In: Proceedings of the 9th Annual Cyber and Information Security Research Conference, CISR '14, pp. 109–112. Association for Computing Machinery, New York (2014)
42. Rubio, J.E., Cristina, A., Javier, L.: Game theory-based approach for defense against apts. In: 18th International Conference on Applied Cryptography and Network Security (ACNS'20), vol. 12147, pp. 297–320. Springer (2020)
43. Hewett, R., Rudrapattana, S., Kijsanayothin, P.: Smart grid security: deriving informed decisions from cyber attack game analysis. In: 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 946–951 (2014)
44. Srikantha, P., Kundur, D.: A DER attack-mitigation differential game for smart grid security analysis. IEEE Trans. Smart Grid **7**(3), 1476–1485 (2016)
45. Li, Y., Shi, L., Cheng, P., Chen, J., Quevedo, D.E.: Jamming attacks on remote state estimation in cyber-physical systems: a game-theoretic approach. IEEE Trans. Autom. Control **60**(10), 2831–2836 (2015)
46. Belmonte Martin, A., Marinos, L., Rekleitis, E., Spanoudakis, G., Petroulakis, N.E.: Threat landscape and good practice guide for software defined networks/5g (2015)
47. Al-Rubaye, S., Kadhum, E., Ni, Q., Anpalagan, A.: Industrial Internet of Things driven by SDN platform for smart grid resiliency. IEEE Internet Things J. **6**(1), 267–277 (2019)
48. OpenStack. https://www.openstack.org/
49. OpenvSwitch. http://openvswitch.org/
50. OpenFlow. https://www.opennetworking.org/
51. Zhang, X., Wei, K., Guo, L., Hou, W., Wu, J.: SDN-based resilience solutions for smart grids. In 2016 International Conference on Software Networking (ICSN), pp. 1–5 (2016)
52. Gude, N., Koponen, T., Pettit, J., Pfaff, B., Casado, M., McKeown, N., Shenker, S.: NOX: towards an operating system for networks. ACM SIGCOMM Comput. Commun. Rev. **38**(3), 105–110 (2008)

53. Ren, L., Qin, Y., Wang, B., Zhang, P., Luh, P.B., Jin, R.: Enabling resilient microgrid through programmable network. IEEE Trans. Smart Grid **8**(6), 2826–2836 (2017)
54. OPAL-RT Technologies. https://www.opal-rt.com/
55. Rehmani, M.H., Akhtar, F., Davy, A., Jennings, B.: Achieving resilience in SDN-based smart grid: a multi-armed bandit approach. In: 2018 4th IEEE conference on network softwarization and workshops (NetSoft), pp. 366–371 (2018)
56. Maziku, H., Shetty, S.: Software defined networking enabled resilience for IEC 61850-based substation communication systems. In: 2017 International Conference on Computing, Networking and Communications (ICNC), pp. 690–694 (2017)
57. Premaratne, U., Samarabandu, J., Sidhu, T., Beresh, R., Tan, J.: Security analysis and auditing of IEC61850-based automated substations. IEEE Trans. Power Deliv. **25**(4), 2346–2355 (2010)
58. GENI. Exploring networks of the future. https://www.geni.net/
59. Fan, J., Khazbak, Y., Tian, J., Liu, T., Cao, G.: Mitigating stealthy false data injection attacks against state estimation in smart grid. In: 2018 IEEE Conference on Communications and Network Security (CNS), pp. 1–9 (2018)
60. Deng, R., Xiao, G., Lu, R.: Defending against false data injection attacks on power system state estimation. IEEE Trans. Ind. Inf. **13**(1), 198–207 (2017)
61. Zimmerman, R.D., Murillo-Sánchez, C.E., Thomas, R.J.: MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans. Power Syst. **26**(1), 12–19 (2011)
62. Kaelbling, L.P., Littman, M.L., Moore, A.W.: Reinforcement learning: a survey. J Artif. Intell. Res. **4**, 237–285 (1996)
63. Jia, H., Gai, Y., Zheng, H.: Network recovery for large-scale failures in smart grid by reinforcement learning. In: 2018 IEEE 4th International Conference on Computer and Communications (ICCC), pp. 2658–2663 (2018)
64. Zhang, Y., Wu, J., Chen, Z., Huang, Y., Zheng, Z.: Sequential node/link recovery strategy of power grids based on q-learning approach. In: 2019 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1–5 (2019)
65. Wei, F., Wan, Z., He, H.: Cyber-attack recovery strategy for smart grid based on deep reinforcement learning. IEEE Trans. Smart Grid **11**, 2476–2486 (2019)
66. Niu, J., Ming, Z., Qiu, M., Hai, S., Zonghua, G., Qin, X.: Defending jamming attack in wide-area monitoring system for smart grid. Telecommun. Syst. **60**(1), 159–167 (2015)
67. Lin, H., Chen, C., Wang, J., Qi, J., Jin, D., Kalbarczyk, Z.T., Iyer, R.K.: Self-healing attack-resilient PMU network for power system operation. IEEE Trans. Smart Grid **9**(3), 1551–1565 (2018)
68. Fovino, I.N., Carcano, A., Masera, M.: A secure and survivable architecture for SCADA systems. In: 2009 Second International Conference on Dependability, pp. 34–39 (2009)
69. Fovino, I.N., Masera, M., Leszczyna, R.: ICT security assessment of a power plant, a case study. In: Proceeding of the Second International Conference on Critical Infrastructure Protection. Citeseer (2008)
70. Kirsch, J., Goose, S., Amir, Y., Wei, D., Skare, P.: Survivable SCADA via intrusion-tolerant replication. IEEE Trans. Smart Grid **5**(1), 60–70 (2014)
71. Kirsch, J.: Intrusion-tolerant replication under attack. Citeseer (2010)
72. Amir, Y., Coan, B., Kirsch, J., Lane, J.: Prime: byzantine replication under attack. IEEE Trans. Depend. Secure Comput. **8**(4), 564–577 (2011)
73. Babay, A., Tantillo, T., Aron, T., Platania, M., Amir, Y.: Network-attack-resilient intrusion-tolerant SCADA for the power grid. In: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 255–266 (2018)
74. Garofalo, G., Di Sarno, C., Coppolino, L., D'Antonio, S.: A GPS spoofing resilient WAMS for smart grid. In: European Workshop on Dependable Computing, pp. 134–147. Springer (2013)
75. Hinden, R., Deering, S.: Internet protocol version 6 (IPv6) addressing architecture. Technical Report, RFC 3513 (2003)
76. Kurtz, F., Wietfeld, C.: Advanced controller resiliency in software-defined networking enabled critical infrastructure communications. In: 2017 International Conference on Information and Communication Technology Convergence (ICTC), pp. 673–678 (2017)
77. Wu, Y., Wei, J., Hodge, B.: A distributed middleware architecture for attack-resilient communications in smart grids. In: 2017 IEEE International Conference on Communications (ICC), pp. 1–7 (2017)
78. Wei, J., Kundur, D.: A flocking-based model for DoS-resilient communication routing in smart grid. In: 2012 IEEE Global Communications Conference (GLOBECOM), pp. 3519–3524 (2012)
79. Wei, J., Kundur, D.: GOAliE: goal-seeking obstacle and collision evasion for resilient multicast routing in smart grid. IEEE Trans. Smart Grid **7**(2), 567–579 (2016)
80. Germanus, D., Khelil, A., Suri, N.: Increasing the resilience of critical scada systems using peer-to-peer overlays. In: International Symposium on Architecting Critical Systems, pp. 161–178. Springer (2010)
81. Pongor, G.: OMNeT: objective modular network testbed. In: MASCOTS: Proceedings of the International Workshop on Modeling, Analysis, and Simulation On Computer and Telecommunication Systems, pp. 323–326 (1993)
82. Hongbo, L., Yingying, C., Chuah, M.C., Jie, Y.: Towards self-healing smart grid via intelligent local controller switching under jamming. In: 2013 IEEE Conference on Communications and Network Security (CNS), pp. 127–135 (2013)
83. Liu, H., Chen, Y., Chuah, M.C., Yang, J., Poor, H.V.: Enabling self-healing smart grid through jamming resilient local controller switching. IEEE Trans. Depend. Secure Comput. **14**(4), 377–391 (2017)
84. Alcaraz, C.: Cloud-assisted dynamic resilience for cyber-physical control systems. IEEE Wirel. Commun. **25**(1), 76–82 (2018)
85. Demir, K., Suri, N.: Towards DDoS attack resilient wide area monitoring systems. In: Proceedings of the 12th International Conference on Availability, Reliability and Security, pp. 1–7 (2017)
86. Demir, K., Nayyer, F., Suri, N.: MPTCP-H: a DDoS attack resilient transport protocol to secure wide area measurement systems. Int. J. Crit. Infrastruct. Prot. **25**, 84–101 (2019)
87. Dreibholz, T.: The NorNet Testbed for Multi-Homed Systems—Introduction and Status. Princeton University, Princeton (2014)
88. Tanha, M., Hashim, F., Subramaniam, S.: Secure and self-healing control centers of critical infrastructures using intrusion tolerance. IJ Netw. Secur. **17**(4), 365–382 (2015)
89. Shacham, H., Page, M., Pfaff, B., Goh, E.-J., Modadugu, N., Boneh, D.: On the effectiveness of address-space randomization. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, pp. 298–307 (2004)
90. Franz, M.: Eunibus pluram: massive-scale software diversity as a defense mechanism. In: Proceedings of the 2010 New Security Paradigms Workshop, pp. 7–16 (2010)
91. Avizienis, A.: The N-version approach to fault-tolerant software. IEEE Trans. Softw. Eng. **11**(12), 1491–1501 (1985)
92. Knight, J.C., Leveson, N.G.: An experimental evaluation of the assumption of independence in multiversion programming. IEEE Trans. Softw. Eng. **12**(1), 96–109 (1986)
93. Li, Y., Chen, M.: Software-defined network function virtualization: a survey. IEEE Access **3**, 2542–2553 (2015)
94. Aydeger, A., Akkaya, K., Uluagac, A.S.: SDN-based resilience for smart grid communications. In: 2015 IEEE Conference on

Network Function Virtualization and Software Defined Network (NFV-SDN), pp. 31–33 (2015)
95. NS-3. https://www.nsnam.org/
96. Aydeger, A., Akkaya, K., Cintuglu, M.H., Uluagac, A.S., Mohammed, O.: Software defined networking for resilient communications in Smart Grid active distribution networks. In: 2016 IEEE International Conference on Communications (ICC), pp. 1–6 (2016)
97. Spitzner, H.L.: Catching the insider threat. In: 19th Annual Computer Security Applications Conference, 2003. Proceedings, pp. 170–179 (2003)
98. Spitzner, L.: Honeypots: Tracking Hackers, vol. 1. Addison-Wesley, Reading (2003)
99. Buza, D.I., Juhász, F., Miru, G., Félegyházi, M., Holczer, T. CryPLH: protecting smart energy systems from targeted attacks with a PLC honeypot. In: International Workshop on Smart Grid Security, pp. 181–192. Springer (2014)
100. Holczer, T., Félegyházi, M., Buttyán, L.: The design and implementation of a PLC honeypot for detecting cyber attacks against industrial control systems (2015)
101. Kołtyś, K., Gajewski, R.: Shape: a honeypot for electric power substation. J. Telecommun. Inf. Technol. **4**, 37–43 (2015)
102. Rist, L.: Introducing Conpot (2013)
103. Jicha, A., Patton, M., Chen, H.: SCADA honeypots: an in-depth analysis of Conpot. In: 2016 IEEE Conference on Intelligence and Security Informatics (ISI), pp. 196–198 (2016)
104. Mashima, D., Chen, B., Gunathilaka, P., Tjiong, E.L.: Towards a grid-wide, high-fidelity electrical substation honeynet, year=2017. In: 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 89–95
105. Virtualbox. https://www.virtualbox.org/
106. Mininet. http://mininet.org/
107. Gunathilaka, P., Mashima, D., Chen, B.: Softgrid: a software-based smart grid testbed for evaluating substation cybersecurity solutions. In: Proceedings of the 2nd ACM workshop on cyber-physical systems security and privacy, pp. 113–124 (2016)
108. Redwood, O., Lawrence, J., Burmester, M.: A symbolic honeynet framework for SCADA system threat intelligence. In: Critical Infrastructure Protection IX, pp. 103–118. Springer, Berlin (2015)
109. Serbanescu, A.V., Obermeier, S., Yu, D.: A flexible architecture for Industrial Control System honeypots. In: 2015 12th International Joint Conference on e-Business and Telecommunications (ICETE), vol. 04, pp. 16–26 (2015)
110. Serbanescu, A.V., Obermeier, S., Yu, D.-Y.: A scalable honeynet architecture for industrial control systems. In: E-Business and Telecommunications, pp. 179–200. Springer, Berlin (2016)
111. Serbanescu, A.V., Obermeier, S., Yu, D.-Y.: ICS threat analysis using a large-scale honeynet. In: 3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015) 3, pp. 20–30 (2015)
112. Salazar, L., Cardenas, A.: Enhancing the Resiliency of Cyber-Physical Systems with Software-Defined Networks, pp. 15–26 (2019)
113. ONOS. https://opennetworking.org/onos/
114. Pothamsetty, V., Franz, M.: SCADA HoneyNet Project: Building Honeypots for Industrial Networks (2005)
115. Simões, P., Cruz, T., Proença, J., Lehto, M., Monteiro, E., Neittaanmäki, P.: Specialized honeypots for SCADA systems. In: Cyber Security: Analytics, Technology and Automation, pp. 251–269. Springer, Berlin (2015)
116. Ye, J.: Estimation of false data injection attacks for load frequency control systems. J. Phys. Conf. Ser. **2076**(1), 012093 (2021)
117. de Carvalho, R.S., Saleem, D.: Recommended functionalities for improving cybersecurity of distributed energy resources. In: 2019 Resilience Week (RWS), vol. 1, pp. 226–231 (2019)
118. Cedric, C., Ifeoma, O., Patricia, C., Jay, J.: Cyber security assessment of distributed energy resources. In: 2017 IEEE 44th Photovoltaic Specialist Conference (PVSC), pp. 2135–2140 (2017)
119. Qi, J., Hahn, A., Xiaonan, L., Wang, J., Liu, C.-C.: Cybersecurity for distributed energy resources and smart inverters. IET Cyber-Phys. Syst. Theory Appl. **1**(1), 28–39 (2016)
120. NERC CIP Standards. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
121. Ng, A., et al.: Sparse Autoencoder. CS294A Lecture Notes, vol. 72, pp. 1–19 (2011)
122. Hinton, G.E.: Deep belief networks. Scholarpedia **4**(5), 5947 (2009)
123. Graves, A., Schmidhuber, J.: Framewise phoneme classification with bidirectional LSTM and other neural network architectures. Neural Netw. **18**(5–6), 602–610 (2005)
124. Kipf, T.N., Welling, M.: Semi-supervised classification with graph convolutional networks. arXiv:1609.02907 (2016)
125. Chen, K., Hu, J., Zhang, Y., Yu, Z., He, J.: Fault location in power distribution systems via deep graph convolutional networks. IEEE J. Sel. Areas Commun. **38**(1), 119–131 (2020)
126. Wang, D., Zheng, K., Chen, Q., Luo, G., Zhang, X.: Probabilistic power flow solution with graph convolutional network. In: 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), pp. 650–654 (2020)
127. Biggio, B., Fumera, G., Roli, F.: Security evaluation of pattern classifiers under attack. IEEE Trans. Knowl. Data Eng. **26**(4), 984–996 (2014)
128. Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., Fergus, R.: Intriguing properties of neural networks. arXiv:1312.6199 (2013)
129. Tramèr, F., Kurakin, A., Papernot, N., Goodfellow, I., Boneh, D., McDaniel, P. Ensemble adversarial training: attacks and defenses. arXiv:1705.07204 (2017)
130. Bosshart, P., Daly, D., Gibb, G., Izzard, M., McKeown, N., Rexford, J., Schlesinger, C., Talayco, D., Vahdat, A., Varghese, G., et al.: P4: programming protocol-independent packet processors. ACM SIGCOMM Comput. Commun. Rev. **44**(3), 87–95 (2014)
131. Enns, R., Bjorklund, M., Schoenwaelder, J., Bierman, A.: Network Configuration Protocol (NETCONF) (2011)
132. Skeie, T., Johannessen, S., Brunner, C.: Ethernet in substation automation. IEEE Control Syst. Mag. **22**(3), 43–51 (2002)
133. Marshall, P.S., Rinaldi, J.S.: Industrial Ethernet. ISA (2004)
134. PRICE CODE: Communication networks and systems for power utility automation–part 90-4: Network engineering guidelines
135. Uchôa, L., Quincozes, S., Vieira, J.L., Passos, D., Albuquerque, C., Mosse, D.: Analysis of smart grid fault recovery protocols. In: NOMS 2020—2020 IEEE/IFIP Network Operations and Management Symposium, pp. 1–8 (2020)
136. IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation. IEEE Std 1646-2004, pp. 1–36 (2005)
137. Sofana Reka, S., Tomislav, D., Pierluigi, S., Sahaya Prabaharan, S.R.: Future generation 5G wireless networks for smart grid: a comprehensive review. Energies **12**(11), 2140 (2019)
138. De Dutta, S., Prasad, R.: Security for smart grid in 5G and beyond networks. Wirel. Pers. Commun. **106**(1), 261–273 (2019)
139. Diovu, R.C., Agee, J.T.: A cloud-based openflow firewall for mitigation against DDoS attacks in smart grid AMI networks. In: 2017 IEEE PES PowerAfrica, pp. 28–33 (2017)
140. Prokhorenko, V., Ali Babar, M.: Architectural resilience in cloud, fog and edge systems: a survey. IEEE Access **8**, 28078–28095 (2020)
141. Saad, A., Faddel, S., Youssef, T., Mohammed, O.A.: On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks. IEEE Trans. Smart Grid **11**(6), 5138–5150 (2020)

142. Lopez, J., Rubio, J.E., Cristina, A.: Digital Twins for Intelligent Authorization in the B5G-enabled Smart Grid. IEEE Wirel. Commun. **28**, 48–55 (2021)