IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Electric Power Grid Resilience to Cyber Adversaries: State of the Art

TIEN NGUYEN[1], SHIYUAN WANG[1], (Student Member, IEEE), MOHANNAD ALHAZMI[1,3], (Student Member, IEEE), MOSTAFA NAZEMI[1], (Student Member, IEEE), ABOUZAR ESTEBSARI[1,2], (Member, IEEE), and PAYMAN DEHGHANIAN[1], (Member, IEEE)

[1]Department of Electrical and Computer Engineering, The George Washington University, 800 22nd St NW, Washington, Suite 5900, DC 20052, USA.
[2]School of the Built Environment and Architecture, London South Bank University, 103 Borough Rd, London, SE1 0AA, UK.
[3]Electrical Engineering Department, College of Engineering, King Saud University, Riyadh 11421, Saudi Arabia.

Corresponding author: Payman Dehghanian (e-mail: payman@gwu.edu).

ABSTRACT The smart electricity grids have been evolving to a more complex cyber-physical ecosystem of infrastructures with integrated communication networks, new carbon-free sources of power generation, advanced monitoring and control systems, and a myriad of emerging modern physical hardware technologies. With the unprecedented complexity and heterogeneity in dynamic smart grid networks comes additional vulnerability to emerging threats such as cyber attacks. Rapid development and deployment of advanced network monitoring and communication systems on one hand, and the growing interdependence of the electric power grids to a multitude of lifeline critical infrastructures on the other, calls for holistic defense strategies to safeguard the power grids against cyber adversaries. In order to improve the resilience of the power grid against adversarial attacks and cyber intrusions, advancements should be sought on detection techniques, protection plans, and mitigation practices in all electricity generation, transmission, and distribution sectors. This survey discusses such major directions and recent advancements from a lens of different detection techniques, equipment protection plans, and mitigation strategies to enhance the energy delivery infrastructure resilience and operational endurance against cyber attacks. This undertaking is essential since even modest improvements in resilience of the power grid against cyber threats could lead to sizeable monetary savings and an enriched overall social welfare.

INDEX TERMS Cyber physical systems (CPS), cyber attack, intrusion detection system (IDS), false data injection attack (FDIA), energy management system (EMS), power grid resilience.

I. INTRODUCTION

SMART GRIDS have transformed the monitoring, control, and operation of bulk power grids via modern communication, signal processing and control technologies. While the smart grids allow for power networks to be effortlessly and wide-area monitored, the widespread deployment of modern information and communication technologies (ICTs) engenders a significant security concern and vulnerability to malicious cyber attacks: adversaries which may alter the underlying physical systems and processes, thereby potentially compromising the national security [1–3]. With the extensive integration of cyber infrastructure in smart grids is formed an expanded attack surface characterized by intensified complexity, heterogeneity and number of resources [4] (see Figure 1). This is evidenced by the frequency, complexity, and severity of cyber attacks targeting several key power system operational functions such as automatic generation control (AGC), state estimation (SE), and energy management systems (EMS) which have been globally observed to be on the rise in recent years [5]. Cyber attacks are malicious intrusions triggered by disrupting the cyber layers of the communication systems in the power grid. There are generally four types of attacks that the power grid may be vulnerable to: physical-only, cyber-only, cyber-enabled physical and physical-enabled cyber attacks [6]. Disruptions appear when either the system operator makes a detrimental error based on compromised sensor measurements or the power grid is remotely or directly controlled by a malicious intruder [7]. An intruder may be motivated to initiate a cyber attack for many reasons including financial benefits, large blackouts, or a combination of both [8]. The gravity of the attack is dependent on the resources the attacker has access to and the knowledge he/she possesses on the

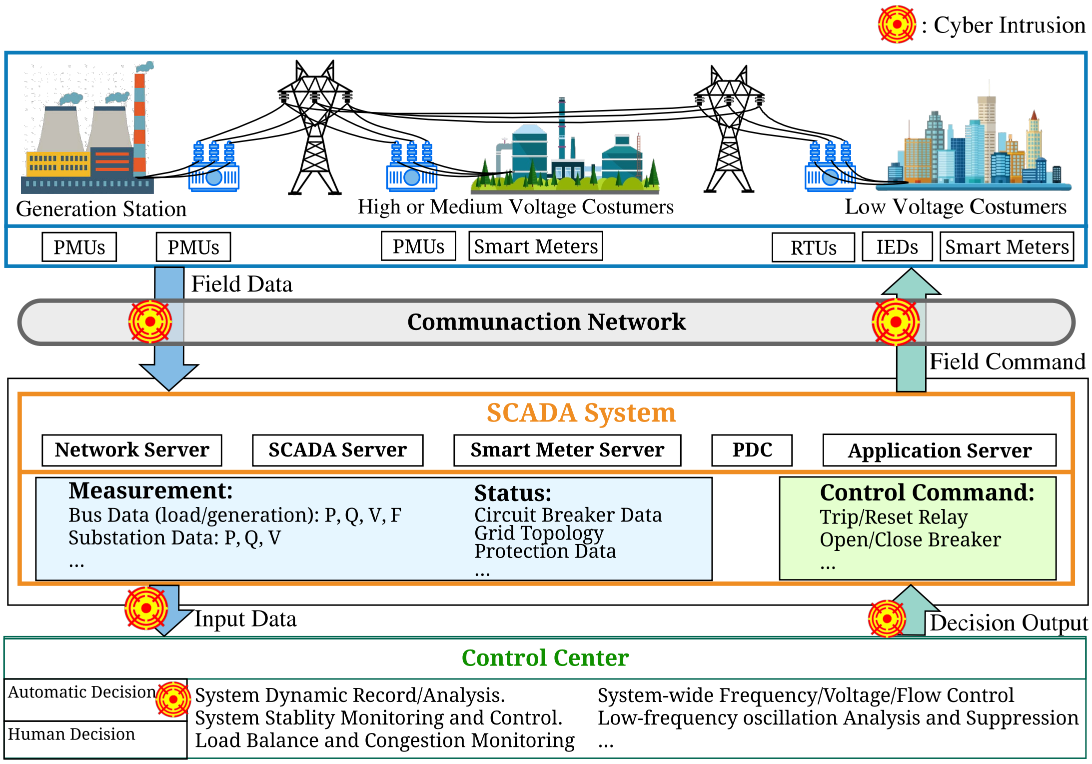


Figure 1: General view of the power grid cyber vulnerabilities.

system topology. The more accurate model the attacker has access to, the larger the deception attack that can be executed undetected [9]. Attackers may take advantage of their knowledge of the grid and launch *coordinated attacks* to critical substations in the network which may eventually cause brownouts/blackouts with significant techno-economic consequences [10]. From a realization perspective, a cyber attack can be considered measure-based or control-based. A *measure-based cyber attack* targets the tie-line flows and frequency measurements, i.e., the measurements PL45, PL69 and the system frequency being sent to the control center. A *control-based cyber attack* targets the area control error (ACE) values once they are sent from the AGC algorithm and before they arrive the designated substations. An attack can send the opposite-direction ramping commands to the generating units. Modifications to the ACE signals (e.g., a sign change of the ACE value) can lead to the generation ramping-up for load reduction and vice-versa [11].

Historically, there were reported incidents in which power systems and industrial control systems (ICS) had their systems cyber compromised. In the United States, the power grid was penetrated in 2009 by cyber spies and a key infrastructure was compromised by an undetected intrusion: Siemens supervisory control and data acquisition (SCADA) systems were attacked by computer worm Stuxnet. In 2010, Stuxnet was able to infiltrate Iran's Natanz nuclear fuel-enrichment facility which was a part of Iran's nuclear development project [12, 13]. In 2003, a cyber-attack penetrated a computer network at the Davis-Besse nuclear power plant located in the US [13]. There have also been reports that an experimental cyber attack was launched by researchers which caused a generator malfunction and self-destruct [14]. Energy theft is another common cyber attack practice in which the electric power is misused or "stolen" by a malicious intruder. Reports reveal that the United States loses $\sim$ \$6 billion due to energy theft alone while it accounts for $\sim$ \$25 billion loss by the electric companies globally [15]. Even advanced metering infrastructure (AMI) platforms, which are used to moderate the power flows in the grid, have been compromised and abused for energy theft. In 2009, the FBI reported a wide and organized energy theft scheme which may cost a utility company up to \$400 million annually following the deployment of AMIs [16, 17]. One major known attack was the cyber attack that occurred on the Ukrainian power grid, happened on December 23rd, 2015, where a third party from Russian security services illegally entered the SCADA systems and computers, and ultimately caused a blackout with massive consequences: a service outage that left 225,000 customers without electricity for 2-6 hours [18]. Such blackouts are detrimental in that they cause financial losses and disruptions in all aspects of our everyday life [19]. Hence, characterization, modeling, and assessment of the power grid cyber vulnerability and designing solutions to protect the grid and enhance its resilience against cyber adversaries is essential. This is because even modest improvements in resilience of the power

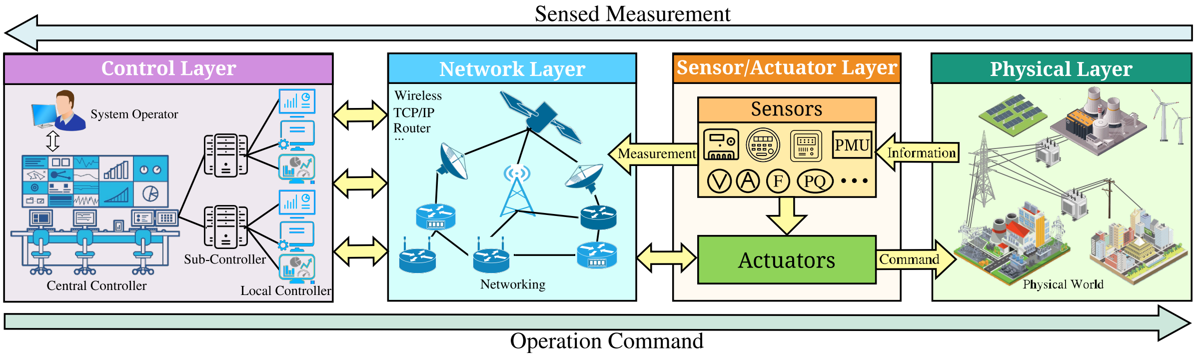


Figure 2: General architecture of a CPS with multiple layers.

grid against cyber threats (through advanced monitoring, efficient threat detection, and recovery algorithms) could lead to sizeable monetary savings and an enriched overall social welfare. More critically, it could help reduce undesirable social, psychological, and physical outcomes associated with the prolonged power outages resulting from cyber intrusions, e.g., premature death, injury, social unrest, etc.

Various studies have investigated the impact of cyber attacks against different day-to-day operation and control mechanisms in power grids, including but not limited to state estimation (SE), electricity markets, power system protection, renewable forecasts, and power system dynamics and control [1, 2, 20–31], among many others. A cyber-resilient power grid entails fault tolerance, fast response, recovery and reliability. Ensured resilience of the power grids against extremes does not only reduce the volume of outages, but also ensures that the grid timely responds to a variety of cyber catastrophes and man-made faults [32]. In the case of power transmission systems, difficulty in maintaining system security arises in that intelligence is only applied and available locally by protection systems and by central control through SCADA systems. In some cases, the central control system is slow to respond to cyber attacks and the protection systems are limited to a few local components [33]. There are many methods to model a cyber attack: an Unmanned Aerial Vehicle (UAV) trajectory plot can model the different paths it can take based on the type of the cyber attack and the impact the attack imposes on the power grid [34]. Attack trees can be devised to model many types of cyber attack scenarios encompassing all possible approaches an attacker may take [15, 35] or other methods such as Markov decision process (MDP) to enumerate all possible attack scenarios [36]. In order to model a control system, however, a graph-based topological network model or graph theory is proposed for a target control system. Integrated with logical connection information, it permits the implementation of a simple Prolog-based expert system to represent a device visibility path and allows assessment of the device vulnerability [37]. A classical mathematical model to describe the power transmission grid is commonly referred to as the structure-preserving power network model. It consists of dynamic swing equations for generator rotor dynamics and algebraic load-flow equations for power flow through network buses [22].

Aiming at reporting the existing state of knowledge on the topic, this paper is structured as follows: a background on cyber attacks including definitions, potential attack surfaces, and the impacts on bulk power grids are presented in Section II. Section III discusses the power grid resilience to cyber attacks and how the smart grid cyber layer should be characterized to resist cyber threats, ensuring the operational endurance and resilience. Section IV reviews some protection mechanisms in power systems against cyber adversaries to prevent failures, followed by Section V where mitigation solutions are reviewed. The paper will be concluded in Section VI with several concluding remarks.

II. CYBER ATTACKS: MODELING AND CLASSIFICATION

In this section, the root causes of cyber attacks and the attack surfaces are firstly reviewed to overview where in power grid such threats would emerge. The impacts of cyber attacks on power systems are next discussed, considering the technical failures and the consequent effects of triggering events.

A. CYBER ATTACK ROOT CAUSES AND SURFACES

The smart grid is a hybrid of power and communication systems, the latter of which renders vulnerabilities which can be compromised during a cyber attack; these vulnerabilities are confidentiality, integrity and availability (CIA) [38]. In today's standards, the power grid is characterized as a cyber-physical system (CPS) shown in Figure 2, which contains physical, sensor/actuator, network, control, and information layers. Manipulation of each layer is possible but does not necessarily mean an intrusion detection component or system needs to be applied in all layers. Information flows in between all layers as they operate only in tandem [39].

Cyber attacks appear in many different forms, where its most basic definition is man-made manipulation of the power grid and redirecting power flow to where it is unassigned by the network operator (see Table 1). As different interoperability layers of smart grids including physical, function, and business layers are interconnected through communication layer to exchange information,

Table 1: Potential Attack Surfaces in Power Grids

	Transmission System	Distribution System	Device	System	Attack Type
Data Concentrator (DC)	✓	✓		✓	FDIA/Delay/Jamming
SCADA	✓	✓		✓	FDIA/DOS
Control System	✓		✓	✓	FDIA/DOS
State Estimator	✓			✓	FDIA
Communication Channel	✓	✓		✓	DOS/Jamming/Delay
Power Market	✓			✓	FDIA/DOS/Delay
Remote Termial Unit (RTU)	✓	✓	✓		FDIA/DOS/Delay/Jamming
Phasor Measurement Unit(PMU)	✓	✓	✓		FDIA/Delay/Jamming
Programmable logic controller (PLC)	✓	✓	✓		FDIA/Delay/Jamming
Advanced Meter Infrastructure (AMI)		✓	✓		FDIA/Jamming
Intelligent Electronic Device (IED)		✓	✓		FDIA/Jamming

attack surfaces are wider than those listed in Table 1. However, in this table, the most common surfaces which have potential to be attacked in existing modern power systems are reviewed as a basis to identify the domain and the type of common attacks.

Some of the main common attacks are denial of service (DoS), false data injection attack (FDIA), energy theft [17], insertion of malware or worms, as well as physical damage of the power grid such as causing equipment to self destruct [14, 35, 40].

- DoS attacks are often realized when the attacker jams the communication channels, compromises the electronic devices, and attacks the routing protocols which ultimately lead to delays and congestion in the communication channels. Generally, a DoS attack restricts a legitimate user's access to the services and resources by flooding the communication network with unnecessary traffic [12, 41].
- FDIA scenarios are realized when an attacker injects false data, usually on a communication line between the field sensors and the control center, with the intent to deceive the network operator and even disturb the SE processes [8, 13]. FDIAs may result in a wide variety of outcomes depending on the intruder's intention, some of which include energy theft, miscalculation of locational marginal prices (LMP) for illegal market profits, and physical damage upon the network. FDIAs can affect the LMPs by misleading the SE which then adversely affects the contingency analysis procedures [42].
- Insertion of malware or worms can range in different types from malicious software which runs in backgrounds to slow down the operations of the electric utility computers to insertion of Trojan software to steal practical security certificates [40].

Cyber intrusion does not necessarily have to occur in the power system itself since it can originate from separate systems that interact frequently with the grid such as electric vehicle supply equipment (EVSE) [43]. In [40], a malware attack model is able to attack the electric vehicle (EV) infrastructure and its communication systems when EVs are plugged in for charging. In some instances, attacks can be undetectable such as malicious data injection attacks that alter the values of measurements without being detected, which may result in serious consequences [44].

From an engineering perspective, there is an opportunity for cyber attacks in smart power grids due to the proliferation and reliance on distributed advanced metering infrastructure (AMI) [45], intelligent electronic devices (IEDs) [46–56], and wireless and/or off-the-shelf communications components and systems across the power network. Such cyber infrastructure increases the system connectivity and autonomous decision-making by employing standardized information protocols that often have (or will have in the future) publicly documented vulnerabilities. Motivations for cyber attacks also abound. Market deregulation and privatization of the energy industry has increased the competition among energy providers to enhance consumer-centricity. Threats also exist in the form of dissatisfied utility insiders, electricity consumers, and cyber terrorists.

B. IMPACTS OF CYBER ATTACKS ON POWER GRID

Control systems are becoming more vulnerable as they get overwhelmingly coupled with modern information and communication technologies and the physical controllers in a CPS [57]. The critical equipment and systems which can be mainly affected or exploited during an attack are in the energy management systems (EMS) in transmission networks or distribution management systems (DMS) in distribution networks. Such platforms collect data from remote and distributed meters and sensors across the network and generate estimates of the system states at the intervals of roughly 15 minutes [46–51, 53, 55]. When false meter data is injected through a cyber attack, the EMS or DMS functions at the control center will be misled by the state estimators which may potentially make erroneous decisions on contingency analysis, power dispatch, and even billing actions [14]. The smart grid offers synchrophasor-based cyber security, which entails a CPS system that provides real-time data to the EMS in order to manage (monitor and control) the physical network [58–61]. However, the latest synchrophasor devices, e.g., phasor measurement units (PMUs), as well as digital fault records (DFRs) and protective relays with PMU functionality are susceptible to a wide range of errors [53, 60] including cyber attacks; this is even further challenging considering the fact that such equipment are intertwined with a large number of legacy devices that have little or no protection against cyber attacks [62]. In [34], the CPS security is analyzed where a deception attack compromises sensors, actuators and both sensors and actuators. The probability of FDIA to be launched successfully usually depends on two assumptions: (i) the attacker has control over some sensor nodes and (ii) the attacker has complete knowledge of the system or its exact topology at all moments during the attack [63]. Generally, the highest impact of an attack is realized when an intruder gains access to the supervisory control access points of SCADA systems and launches control actions [64]. The attacker may compromise raw data measurements which causes undetected errors to factor into estimates of state variables such as bus voltage angles and magnitudes. This can occur when the attacker takes advantage of small errors tolerated by SE algorithms. Ultimately, this severely threatens power system security [13]. Disturbances in SE can lead to increases in state estimates mean square errors (MSE) and changes in the real-time electricity market prices. The effect of invalid MSE can lead to network operators making wrong decisions and the changes in real-time electricity market prices can benefit only the attacker. [65]. With FDIAs, the power grid can suffer economic attacks, load redistribution attack, or energy deceiving attack. An *economic attack* is a type of FDIA which can affect operations of the deregulated electricity market which is comprised of two markets: the day-ahead market and the real-time market. An attacker can manipulate market prices for power and get monetary gains. A *load redistribution attack* is an attack which can affect power grid operation by attacking the security-constrained economic dispatch (SCED). The purpose of SCED is to minimize the total system operation cost; however, when the raw measurements are manipulated by an attacker, the SCED will result in an overload of the lines that will remain unnoticed by the system operator and ultimately causes large physical damages to the power grid. An *energy deceiving attack* affects the distributed energy routing process; essentially this is a scheme to determine the optimal energy routes for load demand or generation. When measured data has been tampered, it can cause erroneous energy demand or supply messages to initiate [13]. Overall, cyber attacks can impact four main aspects of the bulk power systems which are SE, AGC, voltage control, and energy market. FDIAs deceive the system operators to believe that the current operating conditions are secure both physically and economically when they actually are not [42], injection of false data can affect the stability and security of the system [66]. Spatiotemporal cyber-state correlations can be used to detect the FDIA. Potential anomalies can be detected by monitoring the temporal consistencies of the spatial correlations between state estimations [67].

Another way an intruder can affect the communication network is by attempting to connect and dial up to a remote terminal unit (RTU) or an IED which can allow them to wiretap telecommunications, perform a local-area network (LAN) or wide-area network (WAN) transmission shown in Figure 3. They could also attack the corporate information technology (IT) systems and gain backdoor access to the interconnected EMS or SCADA systems; internet service providers (ISP) and telecommunications are other sources they can attack. Some electric utility providers are dependent on corporate IT systems and this is how their interconnected SCADA systems greatly intensify the vulnerability of the electric power grid [37]. Similarly, AMI systems can be attacked. AMI includes smart meters, customer gateways, AMI communication network and head-end; AMI is considered a fundamental technology of smart grids for making two-way communications along with various other functions. However, there have been several potential vulnerabilities with AMI specifically the insertion of malicious software and disabling of metering systems [38].

Cyber attacks and intrusions can occur multiple times from a single origin and spread to different areas. A typical example is electric vehicle charge stations (EVCS) [43, 68–72]: when a consumer charges its EV at multiple stations, it is likely that malware can spread due to vehicle-to-infrastructure and EVSE communications. Essentially, an attack on an EV may spread to the power grid infrastructure starting from the EVSE and all the way up to the utility systems [40]. The integration of transportation and power systems may leave many open doors for hackers, especially in the interconnected environment, i.e., the EV infrastructure, including EVs, EVSE, meters and other roadside infrastructures and when deeply integrated with critical infrastructure systems [73–75].

III. POWER GRID RESILIENCE TO CYBER ATTACKS

The concept of resilience has become a well-researched topic in recent years as it mainly drives the swift detection and effective mitigation of the power grid against high-impact low-probability (HILP) events [76–78]. The word "resilience" is originated from the Latin word "resilire", reflecting "the ability to rebound" [32]. Power system resilience in the face of the devastating natural-driven HILP events has been studied widely in the literature [76–97]. The past research defines, quantifies, and categorizes the concept of resilience in many different ways. For instance, the National Infrastructure Advisory Council (NIAC) proposed a universal definition of infrastructure resilience in 2010: "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure depends on its ability to anticipate, absorb, adapt to and/or rapidly recover from a potentially disruptive event" [98]. In a similar attempt, [99] defines resilience as the system's ability to withstand the main interruption within acceptable degradation parameters and to recover within an acceptable time and composite risks and costs. An alternative definition of resilience is the ability to prepare for and adapt to changing conditions, featured with robustness and fast recovery [100]. The last but not the least interpretation of resilience could be

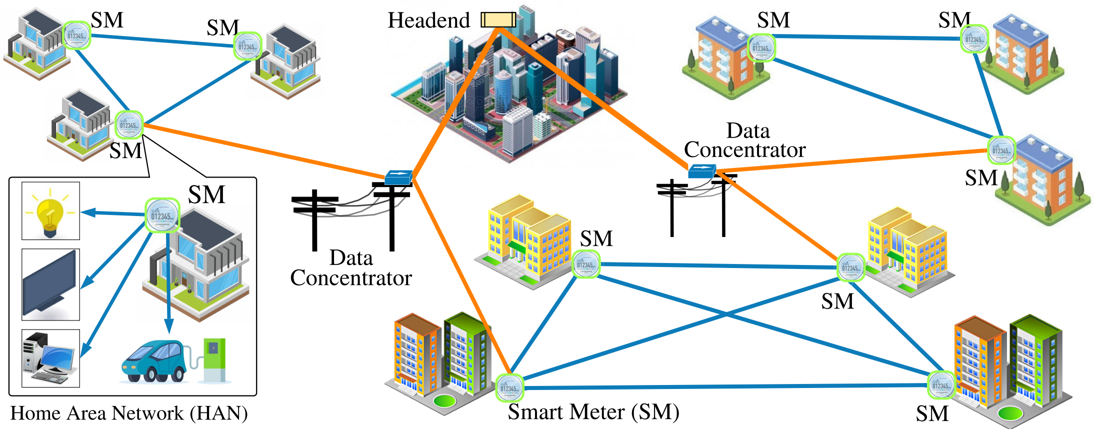


Figure 3: System view of advance metering infrastructures.

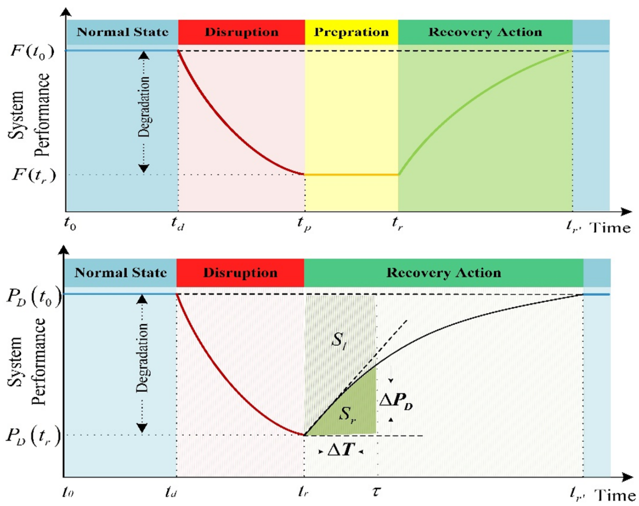


Figure 4: Power system transition states following a critical HILP disturbance: a proactive response and recovery strategy that can be implemented in an automated manner can minimize or bypass the preparation time when the event hits the power grid, thereby effectively boosting its resilience.

the system's ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events [101].

The power grid is required to supply the electric power continuously and reliably to end-users in general and critical lifeline infrastructures (e.g., water networks, oil and gas systems, communication systems, transportation networks, etc.) and mission-critical services (e.g., health sector, defense bases, etc.). The electric sector's approach to the protection of the grid critical infrastructure is generally known as "defense-in-depth", which contains prevention, preparation, response, and recovery for an inclusive range of credible hazards to electric grid operations. Resilience in power grids entails accurate threat detection, infrastructure vulnerability monitoring, and timely response and recovery (see Figure 4). Both "long-term" and "short-term" strategies for enhancing the grid resilience against extreme conditions have been addressed in the literature. In the former, enhancing the grid structural resilience is primarily the focus of concern and suggestions are toward deployment of the "grid hardening" plans through reinforcement, preventive maintenance of the critical assets, vegetation management, efficient allocation of flexible energy resources (e.g., storage units), etc. In the latter, improving the operational resilience is targeted through fast emergency response and remedial actions, defensive islanding, use of the micro-grids, etc.

The IT employed in industrial control systems (ICS) is cyber-vulnerable in general and can potentially impose direct impacts on the physical power grids. CPS will be the core component of many critical infrastructures, yet vulnerable to random failures and cyber attacks. Hence, it is critical to design, develop, and implement ICS and CPS with resilient cyber defense systems [12], i.e., integrating robust intrusion detection systems (IDS) to ensure the power grid resilience with countermeasures being taken effectively [39]. Energy theft is an important concern relating to smart grid implementation; while the implementation of AMI is used to mitigate energy theft, penetration tests have uncovered several vulnerabilities with smart meters [15, 17]. Deregulation of the electric power industry has unbounded generation and transmission systems which, in turn, allows for a broad range of participants to make decisions in the power sector. This is critical as an attack on the SCADA systems can disrupt and damage critical infrastructural operations, contaminate the ecological environment, cause major economic losses and, and even more dangerously, claim human lives [102]. In presence of all these challenges and vulnerabilities and the intensified number of access points and functionalities to tamper with [103] in highly-complex cyber-physical power grids, new strategies are needed to secure the entire network against malicious cyber intrusions [3, 97, 104–106].

The potential for achieving power system resilience depends highly on how preventive and corrective maintenance strategies are planned and implemented component-wise [107–112] and system-wide [113–127] as well as where and how the security measures and systems are deployed. Incorporating data and cyber infrastructure to the power grid exposes the system to many cyber security threats. The smart grids of the future with massive renewable resources and an expanded uncertainty set [128–130] will inherit not only the vulnerabilities of advanced communication systems but also the vulnerabilities of the legacy power system. Security mechanisms should be designed into the power grid with the goal of reducing vulnerabilities and mitigating their consequences [131]. Anomaly detection and root-cause analysis are essential for building resilient CPS since the grid may not know how to counteract the damage if it does not know what caused the damage. Accurately detecting anomalies and isolating their causes is important for applying appropriate proactive and preventive measures [57], [41], [66].

IV. CYBER ATTACK PROTECTION

Most methods for detecting cyber intrusions rely on outdated techniques that are originated from the IT domain and adopted in smart grids in an insufficient manner. Typically, the inherited techniques from power experts mainly focus on existing types of attacks, e.g., load redistribution [132], distributed DoS [133], etc. Real-time cyber vulnerability assessment in power systems brings new challenges due to the fact that the conventional techniques for cyber intrusion detection in dynamic power systems are computationally demanding to be applied in real-time.

Fundamentally, there are two types of attack detection and identification strategies widely researched in the literature: *static* and *dynamic*. Dynamic detection and identification outperform its static counterpart while possibly using fewer measurements. With a comprehensive assessment of the limitations in both static and dynamic detection and identification techniques, [22] proposes a provably-valid dynamic detection and identification procedure borrowing tools from the geometric control theory domains: the tools are comprised of geometrically designed residual filters. Cyber attack detection can be performed using relevant and high-fidelity data. Spotting slight anomalies in PMU data helps identify unobservable cyber attacks which can not be detected by existing technologies. In [134], a convex optimization-based decomposition approach utilizes the low-ranking property of PMU data to formulate an unobservable cyber attack identification problem as a matrix decomposition problem where the observed data matrix is the sum of the low-ranking PMU data and a linear projection of a column-spare matrix. The majority of the existing attack detection methods use measurements at one-time instance and only explore the spatial correlations whereas the convex-optimization decomposition method in [134] exploits the temporal correlations as well and can identify unobservable cyber-data attacks even when the system is dealing with the aftermath of disturbances.

Strategies to detect cyber intrusions are plentiful and endless since there is an expanded set of cyber attack surfaces and vectors to be able to manipulate the grid towards an intruder's favor. In [19], a new network-based cyber intrusion detection system (NIDS) uses multi-cast messages in substation automation systems (SASs) to monitor anomalies and malicious activities of multi-cast messages which are based on IEC 61850, generic object-oriented substation event (GOOSE) and sample value (SV). NIDS detects discrepancies and intrusions which violate the predefined security rules by using a specification-based algorithm. To detect energy theft, another common challenge in power systems, [17] uses normal and malicious data of consumer consumption patterns and a consumption pattern-based energy theft detector (CPBETD). This tool combined with the application of a Support Vector Machine (SVM) anomaly detector allows the algorithm to use silhouette plots to identify different distributions in the dataset and relies on distribution transformer meters to detect nontechnical loss (NTL) at the transformer level. In order to detect cyber intrusions in the system, it is essential to classify it for identification. Effective techniques to classify cyber attacks or anomalies are using SVMs and a variety of machine learning algorithms.

Detecting intrusions through the entire sector of the power network is challenging; in [135], a proposal of grouping network buses and designing filters for detection and isolation of faults addresses a feasible detection mechanism. In addition to grouping network buses, [135] suggests using the swing equation to model the power network which can be used in tandem with grouping power buses. Investigating system models and security requirements of AMIs to present an attack tree based threat model for AMI has shown an improvement in the detection accuracy and detection speed of intrusions in [15].

While cyber attacks may become prominent in the future, there are normal fault contingencies which occur in the system on a daily basis driven by environmental stressors and equipment failures. The system needs to be able to differentiate the difference between an intrusion attack and a natural discrepancy. In [136], a devised algorithm is implemented to accurately detect and locate faults in power systems in addition to identifying bad data using weighted least absolute value (WLAV). WLAV has the ability to reject bad data to reduce dimensionality. A Bayesian framework can also be utilized to unify different approaches of network detection based on random diffusions and algorithms which are based on network's spectral properties [137]. This algorithm detects threat networks using partial observations which can be optimal in the Neyman-Pearson sense and prepares the system for cyber intrusion attacks should they are launched in the future. A data-driven algorithm for online power grid topology change identification with PMUs is suggested in [58], where the proposed machine learning algorithm can differentiate the various types of faults in power grids and the topology switching actions initiated by the system operators or attackers.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2993233, IEEE Access

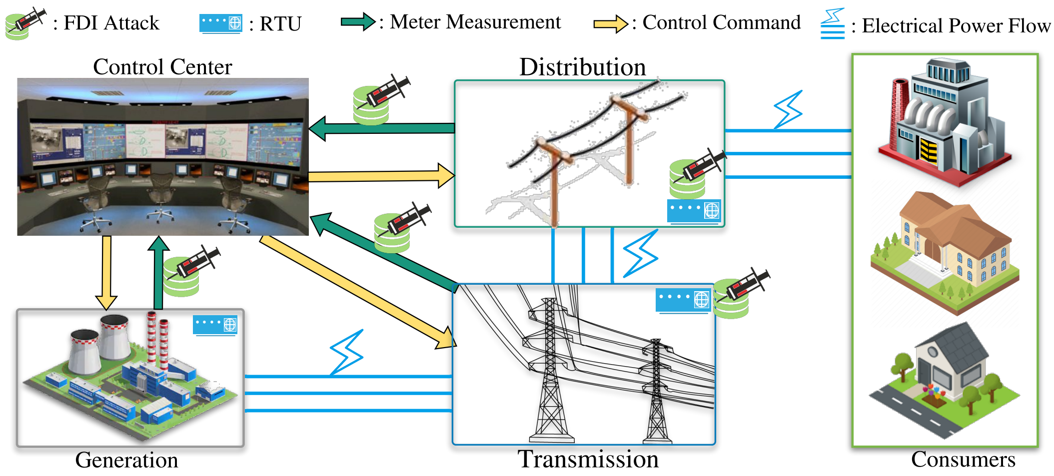


Figure 5: FDI attacks on state estimation in a power grids.

A. FDIA DETECTION

The FDIA problem is viewed as a matrix separation problem and two methods which are presently employed to solve this problem are nuclear norm minimization and low rank matrix factorization. These methods can recover lost or missing data in addition to detecting malicious attacks in the power grid. FDIA happens when an attacker injects false data, usually on a communication line between sensors and the control center with the intent to deceive the network operator and even disturb the SE processes [8, 13]. Reference [138] presents an approach using observer nodes to detect and isolate cyber attacks on network nodes and those on the communication links between the nodes. In order to minimize the computational complexity, observer nodes are reduced, while the observability of the system is not compromised. A perturbation-based approach is employed in [44] for detecting both fault-induced and maliciously-injected bad data in the power grid. This method probes the system by applying known perturbations and measuring the values elsewhere to find unexpected responses in terms of measurement values. [139] presents a mechanism for false data detection which notices the intrinsic low dimensionality of temporal measurements in power grids as well as the sparse nature of the FDIAs. Several research efforts discussed methods of building and detecting such an attack. Successful implementation of FDIAs commonly requires full knowledge of the network topology. [140] proposed a form of an attack without having complete information of the network topology. This can be done by using the kernel-independent component analysis to map the restricted data into a new Jacobian matrix, through which the undetectable attack is modeled [140]. [141] proposed an extreme learning machine (ELM) technique based on one-class-one-network (OCON) framework to detect any cyber threat on the AC state estimation. FDIA attacks are detected using Kullback-Leibler Distance in [142], where the accuracy of the detection mechanism is influenced by the predefined thresholds. A novel false data detection technique based on the separation of nominal power grid states and anomalies is discussed in [139]. [143] used an algorithm to ensure shorter decision time and a more promising FDIA detection accuracy by tracking the unfamiliar parameters and process multiple measurements at the same time.

Even though these techniques can prevent the system from FDIAs to some extent, smart intruders may be still able to damage the PMU (or RTU) measurements in power grids and bypass the bad data detection (BDD) mechanisms in SCADA systems and wide-area measurement system (WAMS) platforms [14, 144–154] (see Figure 5). This can be accomplished through manipulated measurements and injecting artificially generated data to the basic measurements in power grids [155–158]. An FDIA detection mechanism in smart meters is modeled in [159]. Correlation between the power system components and detection methods against smart grid intrusions is proposed in [160]. An efficient approach to protect the power system from FDIA is by implementing precautions in advance [161–164]. Robust SE algorithms against FDIA based on Markov chain theory and Euclidean distance metric are introduced in [165]. [26] modeled the FDIAs with multiple adversaries against one defender implemented in the smart grid. A game theoretic approach is used in [30] to study the interactions between the defender and the attacker in CPS. DoS attacks, random attacks, and FDIA intrusions are detected in [166] using Kalman filter by estimating the variables of the state processes and feeding them to either the χ^2 detector or euclidean detector. In order to detect the injected bad data by PMUs, [167] introduced a distributed host-based collaborative detection method using a conjunctive rule based majority voting algorithm to detect such an attack.

B. PHASOR MEASUREMENT UNIT PROTECTION

In order for protocols and measurements to be true, exact, and valid at all times with robustness against any external changes, they need to be protected in smart grids. Protecting

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2993233, IEEE Access

a set of basic key measurements and having PMU based protection mechanisms or secure PMU equipment [7, 13, 58, 134] can retain the fidelity of the measured data and accurate state estimates in a wide variety of smart grid applications using such measurements. When a set of measurements is protected, an attacker can not inject unobservable attacks without hacking into the protected units [134] and allowing themselves to be noticed. A distributed intrusion detection system can be deployed for smart grids to pinpoint cyber intrusions. This system contains an analyzing module (AM) and an intelligent module which communicates between three different cyber layers of home area network (HAN), the neighborhood area network (NAN) and the wide-area network (WAN) [38, 168].

It is estimated that in order to achieve a full power system observability, one typically needs to install PMUs at around one-third of the network buses; nevertheless, it is recognized that this is difficult and costly to achieve in the near future [169]. Therefore, one will have to estimate the state of the system with a hybrid of both PMUs and conventional measurements. This practice essentially leads to careful selections of PMU placement strategies in the power grid in order to minimize the SE errors. [169] optimizes PMU placement to increase the SE accuracy using an algorithm that is related to key property and submodularity which contributes to efficient greedy algorithms. An optimal PMU placement problem is interpreted as an optimal experiment design problem with a class of optimality criteria. In particular, the greedy PMU placement algorithm achieves at least 63 % of the optimal total variance reduction for typical power systems. Performing a vulnerability assessment is critical to ensure that power infrastructure cyber security is systematically evaluated. This proposed framework provides a measure to quantify system vulnerability and a planning tool to assist system analysts to identify bottlenecks in the system where improvements are most effective [64]. Similarly, a novel vulnerability measure is introduced in [170] to compare and prioritize different grid topologies against FDIAs with incomplete information of the grid's topology. This measure can potentially help build power grids that are less vulnerable against practical FDIAs when the attacker has limited information and launches an imperfect attack. In [3], discussions on how optimal placement of PMUs throughout the power network may lead to very accurate SE are provided. PMUs also provides advanced mechanisms in detecting stealthy attacks. Rerouting the topology of the power grid intensifies the complexity of the grid topology and is used as a defense mechanism against FDIAs which are undetectable via conventional means [63]. References [63, 171–178] suggest that leveraging defensive circuit breakers and simultaneously applying grid re-configuration practices can enhance the overall network efficiency, reliability, and security. This is achieved at minimum cost and by harnessing the network built-in flexibility only. Nevertheless, additions of circuit breakers may not be a viable security measure

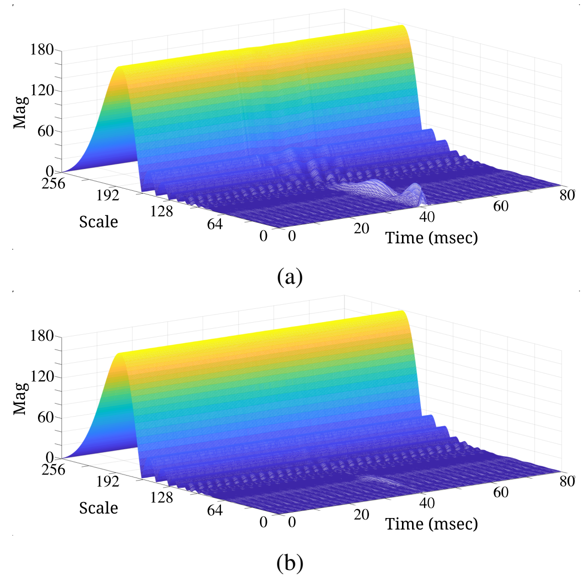


Figure 6: Simulation results in a IEEE 30-Bus system from [58], where (a) Transmission Line 2-4 is switched-off at $t = 30ms$ only, (b) Transmission Line 2-5 is switched-off at $t = 30ms$ only. Both features are extracted at Bus 6.

if the attacker has compromised a large set of sensor nodes and knows a large portion of the grid topology. In [58], advanced wavelet transform and machine learning analytics are embedded in existing PMUs, devices with PMU functionalities, or as a stand-alone sensor in power grids that can detect the malicious changes in network topology by an attacker (unwanted line switching operations). The waveform features corresponding to different topology changes are extracted as shown in Figure 6 which were used to detect and classify the associated line switching actions characterized through commutation jamming and/or FDIA scenarios.

Implementing different techniques to reduce the number of simulations and achieve a quicker SE allows for early event detection. This provides an opportunity for the network operators to be prepared for the potential adversarial cyber attacks since there will be additional time saved for the optimal response to be deployed (see Figure 7). Using a Principal Component Analysis (PCA) based dimensionality reduction of PMU data allows for raw data blocks to be processed quicker, thereby realizing an early detection of cyber disruptions [179, 180]. Similarly, [134] uses an unobservable cyber attack identification as a matrix decomposition problem which contains a sum of low-ranked matrices with a linear projection of a column-sparse matrix. Since low-dimensional structure of PMU data matrix is recently observed, the matrix decomposition problem has attracted more attention and has wide spread applications such as internet monitoring, medical imaging and image processing [134]. In [181], a similar technique is proposed which reduces the simulation run-time by incorporating Importance Sampling which is used to speed up simulations

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2993233, IEEE Access

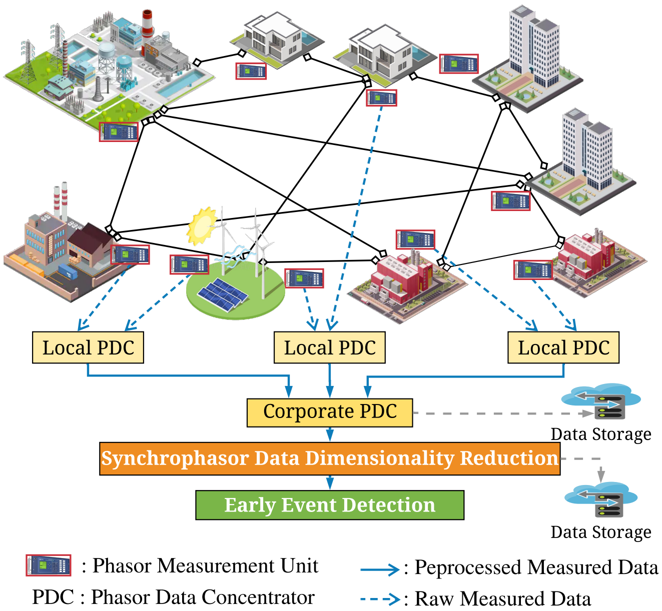


Figure 7: Early event detection mechanisms in power grids.

several orders of magnitudes compared to the standard simulation practices. This essentially increases the efficiency of simulations associated with Markovian models on highly dependable dynamic systems.

C. DETECTION USING MACHINE LEARNING

Machine learning and artificial intelligence techniques are more recently proposed and applied in power systems to identify disturbances and detect cyber attacks even through deception [62]. Recent advancement in deep learning (DL), a subcategory of machine learning that uses artificial neural networks to extract accurate features from raw data, brings about new solutions for data-driven attack detectors. In fact, DL approaches use feature learning techniques to extract novel features (aka signatures) in an unsupervised, self-guided manner. Given a set of measurement data, with raw features as the input, DL tries to crate and refine a set of algorithms to reproduce the same data set as the output. The generated algorithms try to minimize the difference between the input and the output so that the original data can be recovered directly from the generated features [97].

A machine-learned framework is created in [182] and refined with unsupervised feature learning to detect different types of cyber attacks in power systems. Stacked autoencoder-based unsupervised feature learning is proposed to capture useful and rich patterns hidden in the data to recognize the cyber attack, and achieve competitive results compared with detectors relying on detailed system information and human expertise. In [41], research was done to combine SVM with a variety of machine learning algorithms to find the most promising algorithm which can detect an adversarial intrusion. A robust spam filtering method is introduced in [183] using a hybrid method for rule-based processing and back-propagation neural network. In [184], different types of deep learning mechanisms, e.g. ANN, decision trees, etc., are tested to assess the cyber security of a particular IEEE test system. Reference [185] introduced a new model for malicious code detection using a new hybrid DL model. A decision support tool is proposed in [62] which enables power system operators to classify various types of attacks. In this paper, different types of classification algorithms are considered, e.g., OneR in which the optimal feature and rule is extracted based on the simplistic method [186], NNge which is a nearest-neighbor-like algorithm that classifies samples by comparing them to those which already have been observed and comparing the new examples to their surrounding data points [187], Random Forests which is an ensemble of tree predictors where each tree casts a vote for the most popular class on the input of a new instance [188]. In [189], an extended version of deep belief network (DBN) called conditional DBN (CDBN) was proposed to analyze the sequential PMU data in real-time and detect the existence of information corruption using auto-regressive (AR) data modeling scheme. In [190], the efficiency of the DL-based cyber-physical approach for FDIA detection is demonstrated. The proposed approach addresses both cyber (e.g., information corruption) and physical disruptions. Reference [191] used a scenario-based sparse cyber-attack model with incomplete network information to detect the possibility of data manipulation. In this paper, the results demonstrated that the proposed approach not only requires less assumption on system topologies and attack types, but also verifies the high detection accuracy of the adopted DL. Reference [192] compared the performance of three different DL approaches: (i) gradient boosting machines (GBM), (ii) generalized linear modelings (GLM), and (iii) distributed random forests (DRF). The numerical results justified that DL-based approaches can accurately detect FDIA scenarios against SE algorithms. Reference [8] proposed two DL techniques for FDIA detection in smart grids. The first model uses the multivariate Gaussian semi-supervised learning while the second model uses a measurement-based deviation analysis algorithm. Both models are used to identify anomalies in transmission networks. In [193], a new detection framework was proposed to develop a density ratio estimation (DRE) technique: an efficient countermeasure against cyber-attacks. Reference [194] proposes a DL-based model for FDIA detection in smart meter data utilizing a state vector estimator (SVE) and a DL-based identification (DLBI) algorithm. The model uses the historical data and tries to recognize a pattern to identify FDIA scenarios in real-time.

V. IMPACT MITIGATION AND RESTORATION

In industrial applications, strengthening industrial control systems (ICS) will protect different classes of infrastructure such as utilities and oil and gas facilities. The ICS is strengthened by designing an intrusion detection system contained in the cyber layer with a controller at the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2993233, IEEE Access

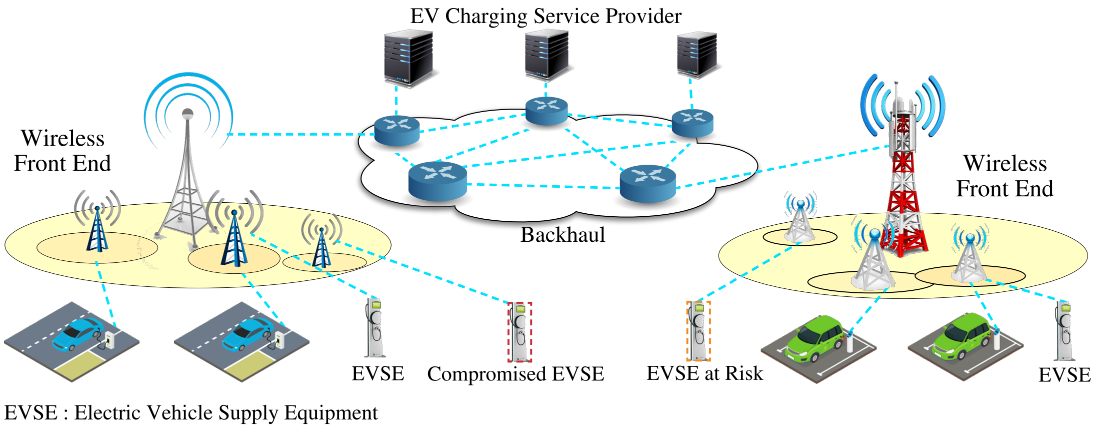


Figure 8: System architecture which supports EVSEs.

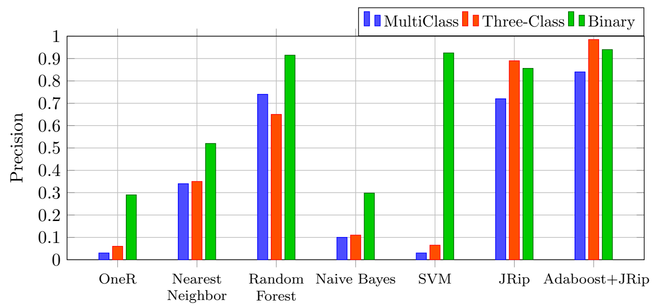


Figure 9: Precision results of various classifiers [62].

physical layer dynamic system [12]. Having a resilient smart grid entails both accurate and swift attack detection and timely response and recovery. This goal can be achieved by having distributed control agents that facilitate both attack detection and system recovery through iterative local processing and message transmission. These control agents are distributed across the grid, thereby characterizing distributed intelligence mechanisms [46, 58, 59, 104, 105, 195]. Limitations by a lack of information about cyber attacks can be partially removed by future research and development of the advanced testbeds for comprehensive testing and evaluations. Test beds are extremely useful tools for thorough evaluation of mitigation and economic strategies in response to cyber vulnerabilities [46, 53, 64].

Modeling vulnerabilities in power grids are critical for its survival under adversarial attacks. In order to create a network topology model of vulnerabilities, *device visibility* and *device vulnerability* need to be defined and quantified. The concept of device visibility path, with the use of a small Prolong application to assess the vulnerability level of a hypothetical target device, can help map the cyber vulnerabilities within a system, thereby enabling opportunities to fortify the network security where needed [37]. A model-based IDS for home area networks (HAN) is suggested in [131] by identifying the security challenges in HAN first and determining next how a Bayesian network intrusion detection system can be used in future HANs. In order to determine the IDS requirements for HAN, examination of the existing types of IDS is needed; there are signature IDS, anomaly-based IDS, and specification-based IDS, as in the following:

- *Signature-based IDS* usually has a database of predetermined attack patterns, known as signatures, and detects the intrusions by comparing the system behavior with these signatures.
- *Anomaly-based IDS* detects malicious activities with regards to deviations from statistically normal behavior in the system.
- *Specification-based IDS* also recognizes intrusions with regards to deviations from normal behaviors of the system. However, instead of statistical measurements, normal behaviors are characterized based on manually extracted specifications of the system.

Characterization of irreducible attacks or observable attacks with the compromise of two power injection meters is performed in [7] with the use of an efficiently designed algorithm to group all observable attacks. In addition, the deployment of secure PMUs is approached as a countermeasure against unobservable attacks. When cyber attacks occur, parts of the system will be compromised and it is important to isolate them quickly while ensuring a sufficient supply of power (through available equipment) to the system load points and mission-critical systems and services [40, 85, 88]. Reference [40] claims that EVs mobility contributes to attack propagation. Therefore, when an attack spreads via EVs, a mixed-integer linear programming (MILP) optimization problem is suggested that minimizes the risk of attack propagation while considering the EV loads, EV threat levels and demand profile in power distribution system (see Figure 8). In such a CPS ecosystem of EVs, isolating the compromised systems will mitigate the effect of a malware or worm while continuing to supply the services to the customers.

In order to mitigate the detrimental consequences of an adversarial cyber attack, one first step is to identify the attack itself. Classifying the attack and giving it an identity allows operators to understand what they are dealing with. In [62], different machine learning classifying algorithms were tested in order to determine the viability of using machine learning as a decision support for system operators; the results demonstrated in Figure 9 show that it is a viable approach but more research is needed for deployment in an operational environment and practical settings.

VI. CONCLUSION

This paper offers a detailed and comprehensive description of the links between the adversarial cyber attacks and power grid resilience, off-the-shelf cyber intrusion detection techniques, and what systems are or could be in place to protect the smart power grids against malicious cyber attacks. The mechanisms through which cyber attacks can impact the bulk power grid are reviewed to understand where and how to enhance and reinforce countermeasures to mitigate the attack consequences. Although there is a variety of cyber detection and protection methods already in place, this review highlighted the importance of considering cyber attacks in planning for resilience in power grids: strategies that entail both grid hardening practices for structural resilience as well as procedures for operational resilience; this is due to the recently more-frequent realization of emerging threats with no or very few similarities to those formerly-experienced incidents. While there might be found additional methods for detection, protection and mitigation against cyber attacks than those listed in this review and there will certainly be new schemes and measures in the future, this survey aimed to collect the state-of-the-art already-investigated or implemented solutions to provide a basis for future research and developments. Implementation of these various methods on testbeds and real-world environments will finally allow for improvements in monitoring, protection, mitigation, and resilience of the smart power grids against the looming threats of cyber adversaries.

References

[1] Y. Mo et al. "Cyber–physical security of a smart grid infrastructure". In: *Proceedings of the IEEE* vol. 100, no. 1 (2011), pp. 195–209.

[2] A. Sanjab and W. Saad. "Power System Analysis: Competitive Markets, Demand Management, and Security". In: *Handbook of Dynamic Game Theory* (2017), pp. 1–38.

[3] S. Cui et al. "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions". In: *IEEE Signal Processing Magazine* vol. 29, no. 5 (2012), pp. 106–115.

[4] J. Pacheco and S. Hariri. "IoT security framework for smart cyber infrastructures". In: *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W)*. IEEE. 2016, pp. 242–247.

[5] A. Ashok and M. Govindarasu. "Cyber attacks on power system state estimation through topology errors". In: *2012 IEEE Power and Energy Society General Meeting*. July 2012, pp. 1–8. DOI: 10.1109/PESGM.2012.6345091.

[6] J. Depoy et al. "Risk assessment for physical and cyber attacks on critical infrastructures". In: *MILCOM 2005-2005 IEEE Military Communications Conference*. IEEE. 2005, pp. 1961–1969.

[7] A. Giani et al. "Smart grid data integrity attacks: characterizations and countermeasures π". In: *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE. 2011, pp. 232–237.

[8] M. Esmalifalak et al. "Detecting stealthy false data injection using machine learning in smart grid". In: *IEEE Systems Journal* vol. 11, no. 3 (2014), pp. 1644–1652.

[9] A. Teixeira et al. "Cyber security analysis of state estimators in electric power systems". In: *49th IEEE Conference on Decision and Control (CDC)*. Dec. 2010, pp. 5991–5998. DOI: 10.1109/CDC.2010.5717318.

[10] A. Estebsari et al. "Techno-economic impacts of automatic undervoltage load shedding under emergency". In: *Electric Power Systems Research* vol. 131 (2016), pp. 168–177. ISSN: 0378-7796. DOI: https://doi.org/10.1016/j.epsr.2015.10.016. URL: http://www.sciencedirect.com/science/article/pii/S0378779615003120.

[11] A. Ashok et al. "Experimental evaluation of cyber attacks on Automatic Generation Control using a CPS Security Testbed". In: *2015 IEEE Power Energy Society General Meeting*. July 2015, pp. 1–5. DOI: 10.1109/PESGM.2015.7286615.

[12] Y. Yuan et al. "Resilient control of cyber-physical systems against denial-of-service attacks". In: *2013 6th International Symposium on Resilient Control Systems (ISRCS)*. IEEE. 2013, pp. 54–59.

[13] G. Liang et al. "A Review of False Data Injection Attacks Against Modern Power Systems". In: *IEEE Transactions on Smart Grid* vol. 8, no. 4 (July 2017), pp. 1630–1638. ISSN: 1949-3053. DOI: 10.1109/TSG.2015.2495133.

[14] O. Kosut et al. "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures". In: *2010 First IEEE International Conference on Smart Grid Communications*. IEEE. 2010, pp. 220–225.

[15] R. Jiang et al. "Energy-theft detection issues for advanced metering infrastructure in smart grid". In: *Tsinghua Science and Technology* vol. 19, no. 2 (Apr. 2014), pp. 105–120. ISSN: 1007-0214. DOI: 10.1109/TST.2014.6787363.

[16] S. McLaughlin et al. "AMIDS: A multi-sensor energy theft detection framework for advanced

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2993233, IEEE Access

metering infrastructures." In: *SmartGridComm*. 2012, pp. 354–359.

[17] P. Jokar; N. Arianpoo, and V. C. Leung. "Electricity theft detection in AMI using customers' consumption patterns". In: *IEEE Transactions on Smart Grid* vol. 7, no. 1 (2015), pp. 216–226.

[18] D. U. Case. "Analysis of the cyber attack on the Ukrainian power grid". In: *Electricity Information Sharing and Analysis Center (E-ISAC)* (2016).

[19] J. Hong; C.-C. Liu, and M. Govindarasu. "Detection of cyber intrusions using network-based multicast messages for substation automation". In: *ISGT 2014*. IEEE. 2014, pp. 1–5.

[20] A. Sanjab; W. Saad, and T. Başar. "Graph-Theoretic Framework for Unified Analysis of Observability and Data Injection Attacks in the Smart Grid". In: *arXiv preprint arXiv:1801.08951* (2018).

[21] Q. Zhu and T. Başar. "Robust and resilient control design for cyber-physical systems with an application to power systems". In: *2011 50th IEEE Conference on Decision and Control and European Control Conference*. IEEE. 2011, pp. 4066–4071.

[22] F. Pasqualetti; F. Dörfler, and F. Bullo. "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design". In: *2011 50th IEEE Conference on Decision and Control and European Control Conference*. IEEE. 2011, pp. 2195–2201.

[23] A. Ferdowsi et al. "Game theory for secure critical interdependent gas-power-water infrastructure". In: *2017 Resilience Week (RWS)*. IEEE. 2017, pp. 184–190.

[24] G. El Rahi et al. "Prospect theory for enhanced smart grid resilience using distributed energy storage". In: *2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE. 2016, pp. 248–255.

[25] Y. Liu; P. Ning, and M. K. Reiter. "False data injection attacks against state estimation in electric power grids". In: *ACM Transactions on Information and System Security (TISSEC)* vol. 14, no. 1 (2011), p. 13.

[26] A. Sanjab and W. Saad. "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective". In: *IEEE Transactions on Smart Grid* vol. 7, no. 4 (2016), pp. 2038–2049.

[27] L. Xie; Y. Mo, and B. Sinopoli. "Integrity data attacks in power market operations". In: *IEEE Transactions on Smart Grid* vol. 2, no. 4 (2011), pp. 659–666.

[28] A. Sanjab and W. Saad. "Smart grid data injection attacks: To defend or not?" In: *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE. 2015, pp. 380–385.

[29] Y. W. Law; T. Alpcan, and M. Palaniswami. "Security games for risk minimization in automatic generation control". In: *IEEE Transactions on Power Systems* vol. 30, no. 1 (2014), pp. 223–232.

[30] A. Sanjab and W. Saad. "On bounded rationality in cyber-physical systems security: Game-theoretic analysis with application to smart grid protection". In: *2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*. IEEE. 2016, pp. 1–6.

[31] F. Pasqualetti; F. Dörfler, and F. Bullo. "Attack detection and identification in cyber-physical systems". In: *IEEE transactions on automatic control* vol. 58, no. 11 (2013), pp. 2715–2729.

[32] A. Gholami; F. Aminifar, and M. Shahidehpour. "Front lines against the darkness: Enhancing the resilience of the electricity grid through microgrid facilities". In: *IEEE Electrification Magazine* vol. 4, no. 1 (2016), pp. 18–24.

[33] S. M. Amin and B. F. Wollenberg. "Toward a smart grid: power delivery for the 21st century". In: *IEEE power and energy magazine* vol. 3, no. 5 (2005), pp. 34–41.

[34] C. Kwon; W. Liu, and I. Hwang. "Security analysis for cyber-physical systems against stealthy deception attacks". In: *2013 American control conference*. IEEE. 2013, pp. 3344–3349.

[35] C.-W. Ten; G. Manimaran, and C.-C. Liu. "Cybersecurity for critical infrastructures: Attack and defense modeling". In: *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* vol. 40, no. 4 (2010), pp. 853–865.

[36] S. Zonouz et al. "SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures". In: *IEEE Transactions on Smart Grid* vol. 5, no. 1 (2013), pp. 3–13.

[37] D. C. de Leon et al. "Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack". In: *ACM Workshop on Scientific Aspects of Cyber Terrorism,(SACT)*. Citeseer. 2002.

[38] Y. Zhang et al. "Distributed intrusion detection system in a multi-layer network architecture of smart grids". In: *IEEE Transactions on Smart Grid* vol. 2, no. 4 (2011), pp. 796–808.

[39] S. Han et al. "Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges". In: *IEEE Systems Journal* vol. 8, no. 4 (Dec. 2014), pp. 1052–1062. ISSN: 1932-8184. DOI: 10.1109/JSYST.2013.2257594.

[40] S. Mousavian et al. "A risk-based optimization model for electric vehicle infrastructure response to cyber attacks". In: *IEEE Transactions on Smart Grid* vol. 9, no. 6 (2017), pp. 6160–6169.

[41] N. Chand et al. "A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection". In: *2016 International Conference on Advances in Computing,*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2993233, IEEE Access

Communication, & Automation (ICACCA)(Spring). IEEE. 2016, pp. 1–6.

[42] J.-W. Kang; I.-Y. Joo, and D.-H. Choi. "False data injection attacks on contingency analysis: Attack strategies and impact assessment". In: *IEEE Access* vol. 6 (2018), pp. 8841–8851.

[43] B. Wang et al. "Electrical Safety Considerations in Large Electric Vehicle Charging Stations". In: *IEEE Transactions on Industry Applications* vol. 55, no. 6 (2019), pp. 6603–6612.

[44] K. L. Morrow et al. "Topology perturbation for detecting malicious data injection". In: *2012 45th Hawaii International Conference on System Sciences*. IEEE. 2012, pp. 2104–2113.

[45] B. Wang et al. "New Reward and Penalty Scheme for Electric Distribution Utilities Employing Load-Based Reliability Indices". In: *IET Generation, Transmission & Distribution* vol. 12, no. 15 (2018), pp. 3647–3654.

[46] T. Becejac and P. Dehghanian. "PMU Multilevel End-to-End Testing to Assess Synchrophasor Measurements during Faults". In: *IEEE Power and Energy Technology Systems Journal* vol. 6, no. 1 (Mar. 2019), pp. 71–80.

[47] A. Razi-Kazemi and P. Dehghanian. "A Practical Approach to Optimal RTU Placement in Power Distribution Systems Incorporating Fuzzy Sets Theory". In: *International Journal of Electrical Power and Energy Systems* vol. 37, no. 1 (2012), pp. 31–42.

[48] P. Dehghanian; A. Razi-Kazemi, and M. Fotuhi-Firuzabad. "Optimal RTU Placement in Power Distribution Systems Using a Novel Method Based on Analytical Hierarchical Process (AHP)". In: *The 10th International IEEE Conference on Environmental and Electrical Engineering (EEEIC)*. 2011, pp. 1–6.

[49] M. Moeini-Aghtaie; P. Dehghanian, and S. H. Hosseini. "Optimal Distributed Generation Placement in a Restructured Environment via a Multi-Objective Optimization Approach". In: *16th Conference on Electric Power Distribution Networks (EPDC)*. 2011, pp. 1–6.

[50] A. Razi-Kazemi; P. Dehghanian, and G. Karami. "A Probabilistic Approach for Remote Terminal Unit Placement in Power Distribution Systems". In: *The 33rd IEEE International Telecommunications Energy Conference (INTELEC)*. 2011, pp. 1–6.

[51] P. Dehghanian; A. Razi-Kazemi, and G. Karami. "Incorporating Experts Knowledge in RTU Placement Procedure Using Fuzzy Sets Theory- A Practical Approach". In: *The 33rd IEEE International Telecommunications Energy Conference (INTELEC)*. 2011, pp. 1–6.

[52] M. Shojaei et al. "A New Look on the Automation of Medium Voltage Substations in Power Distribution Systems". In: *17th Conference on Electric Power Distribution Networks (EPDC)*. 2012, pp. 1–6.

[53] M. Kezunovic et al. "Life-Cycle Management Tools for Synchrophasor Systems: Why We Need Them and What They Should Entail". In: *The 2016 IFAC CIGRE/CIRED Workshop on Control of Transmission and Distribution Smart Grids*. CIGRE. 2016, pp. 1–6.

[54] T. Becejac; P. Dehghanian, and M. Kezunovic. "Probabilistic Assessment of PMU Integrity for Planning of Periodic Maintenance and Testing". In: *International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*. 2016, pp. 1–6.

[55] M. Kezunovic; P. Dehghanian, and J. Sztipanovits. "An Incremental System-of-Systems Integration Modelling of Cyber-Physical Electric Power Systems". In: *Grid of the Future Symposium, CIGRE US National Committee*. CIGRE. 2016, pp. 1–6.

[56] M. H. Rezaeian Koochi et al. "A Synchrophasor-based Decision Tree Approach for Identification of Most Coherent Generating Units". In: *The 44th Annual Conference of the IEEE Industrial Electronics Society (IECON)*. 2018, pp. 1–6.

[57] S. Krishnamurthy; S. Sarkar, and A. Tewari. "Scalable anomaly detection and isolation in cyber-physical systems using bayesian networks". In: *Proceedings of asme dynamical systems and control conference, san antonio, tx, usa*. 2014.

[58] S. Wang; P. Dehghanian, and B. Zhang. "A Data-Driven Algorithm for Online Power Grid Topology Change Identification with PMUs". In: *IEEE Power and Energy Society (PES) General Meeting*. 2019, pp. 1–5.

[59] S. Wang; P. Dehghanian, and Y. Gu. "A Novel Multi-Resolution Wavelet Transform for Online Power Grid Waveform Classification". In: *The 1st IEEE International Conference on Smart Grid Synchronized Measurements and Analytics (SGSMA)*. 2019, pp. 1–6.

[60] T. Becejac; P. Dehghanian, and M. Kezunovic. "Analysis of PMU Algorithm Errors During Fault Transients and Out-of-Step Disturbances". In: *IEEE Power and Energy Society (PES) Transmission & Distribution (T&D) Conference and Exposition Latin America*. 2016, pp. 1–6.

[61] T. Becejac; P. Dehghanian, and M. Kezunovic. "Impact of PMU Errors on the Synchrophasor-based Fault Location Algorithms". In: *48th North American Power Symposium (NAPS)*. 2016, pp. 1–6.

[62] R. C. B. Hink et al. "Machine learning for power system disturbance and cyber-attack discrimination". In: *2014 7th international symposium on resilient control systems (ISRCS)*. IEEE. 2014, pp. 1–8.

[63] K. Ly et al. "Approximate Power Grid Protection Against False Data Injection Attacks". In: *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure*

Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech). Nov. 2017, pp. 527–533. DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.97.

[64] C. Ten; C. Liu, and G. Manimaran. "Vulnerability assessment of cybersecurity for SCADA systems". In: *IEEE Transactions on Power Systems* vol. 23, no. 4 (2008), pp. 1836–1846.

[65] L. Jia; R. J. Thomas, and L. Tong. "On the nonlinearity effects on malicious data attack on power system". In: *2012 IEEE Power and Energy Society General Meeting*. July 2012, pp. 1–8. DOI: 10.1109/PESGM.2012.6345685.

[66] K. Chatterjee; V. Padmini, and S. A. Khaparde. "Review of cyber attacks on power system operations". In: *2017 IEEE Region 10 Symposium (TENSYMP)*. July 2017, pp. 1–6. DOI: 10.1109/TENCONSpring.2017.8070085.

[67] P. Chen et al. "Detection of false data injection attacks in smart-grid systems". In: *IEEE Communications Magazine* vol. 53, no. 2 (Feb. 2015), pp. 206–213. ISSN: 0163-6804. DOI: 10.1109/MCOM.2015.7045410.

[68] M. Moeini-Aghtaie et al. "PHEV's Centralized/Decentralized Charging Control Mechanisms: Requirements and Impacts". In: *The 45th North American Power Symposium (NAPS)*. 2013, pp. 1–6.

[69] B. Wang; P. Dehghanian, and D. Zhao. "Chance-Constrained Energy Management System for Power Grids with High Proliferation of Renewables and Electric Vehicles". In: *IEEE Transactions on Smart Grid* (2020), pp. 1–13.

[70] B. Wang et al. "Aggregated Electric Vehicle Load Modeling in Large-Scale Electric Power Systems". In: *IEEE Transactions on Industry Applications* (2020), pp. 1–14.

[71] P. Jamborsalamati et al. "Enhancing Power Grid Resilience through An IEC61850-based EV-Assisted Load Restoration". In: *IEEE Transactions on Industrial Informatics* vol. 16, no. 3 (Mar. 2020), pp. 1799–1810.

[72] B. Wang et al. "Adaptive Operation Strategies for Electric Vehicle Charging Stations". In: *IEEE Industry Applications Society (IAS) Annual Meeting*. 2019, pp. 1–7.

[73] M. A. Saffari et al. "Robust/Stochastic Optimization of Energy Arbitrage in Smart Microgrids using Electric Vehicles". In: *Electric Power Systems Research* vol. 174 (Sept. 2019), pp. 1–14.

[74] M. Moeini-Aghtaie et al. "Optimized Probabilistic PHEV Demand Management in the Context of Energy Hubs". In: *IEEE Transactions on Power Delivery* vol. 30, no. 2 (2015), pp. 996–1006.

[75] M. S. Misaghian et al. "Electric Vehicles Contributions to Voltage Improvement and Loss Reduction in Microgrids". In: *North American Power Symposium (NAPS)*. 2018, pp. 1–6.

[76] P. Dehghanian et al. "Predictive risk analytics for weather-resilient operation of electric power systems". In: *IEEE Transactions on Sustainable Energy* vol. 10, no. 1 (2019), pp. 3–15.

[77] P. Dehghanian; S. Aslan, and P. Dehghanian. "Maintaining electric system safety through an enhanced network resilience". In: *IEEE Transactions on Industry Applications* vol. 54, no. 5 (2018), pp. 4927–4937.

[78] B. Zhang; P. Dehghanian, and M. Kezunovic. "Optimal allocation of PV generation and battery storage for enhanced resilience". In: *IEEE Transactions on Smart Grid* vol. 10, no. 1 (2017), pp. 535–545.

[79] M. Nazemi et al. "Energy Storage Planning for Enhanced Resilience of Power Distribution Networks against Earthquakes". In: *IEEE Transactions on Sustainable Energy* vol. 11, no. 2 (Apr. 2020), pp. 795–806. ISSN: 1949-3029. DOI: 10.1109/TSTE.2019.2907613.

[80] M. Amirioun et al. "Metrics and quantitative framework for assessing microgrid resilience against windstorms". In: *International Journal of Electrical Power & Energy Systems* vol. 104 (2019), pp. 716–723.

[81] S. Wang et al. "Resilience-Assured Protective Control of DC/AC Inverters under Unbalanced and Fault Scenarios". In: *The 10th IEEE Power and Energy Society (PES) Conference on Innovative Smart Grid Technologies-North America (ISGT-NA)*. 2019, pp. 1–5.

[82] Z. Yang; P. Dehghanian, and M. Nazemi. "Enhancing Seismic Resilience of Electric Power Distribution Systems with Mobile Power Sources". In: *IEEE Industry Applications Society (IAS) Annual Meeting*. 2019, pp. 1–7.

[83] S. Wang et al. "A Machine Learning Approach to Detection of Geomagnetically-Induced Currents in Power Grids". In: *IEEE Industry Applications Society (IAS) Annual Meeting*. 2019, pp. 1–7.

[84] M. Babakmehr et al. "Sparse Representation-based Classification of Geomagnetically Induced Currents". In: *Clemson University Power Systems Conference*. 2020, pp. 1–6.

[85] Z. Yang et al. "Toward Resilient Solar-Integrated Distribution Grids: Harnessing the Mobility of Power Sources". In: *IEEE Power and Energy Society (PES) Transmission and Distribution (T&D) Conference and Exposition*. 2020, pp. 1–5.

[86] M. Nazemi and P. Dehghanian. "Seismic-Resilient Bulk Power Grids: Hazard Characterization, Modeling, and Mitigation". In: *IEEE Transactions on Engineering Management* (2020), pp. 1–17.

[87] S. Wang et al. "A Machine Learning Approach to Detection of Geomagnetically-Induced Currents in Power Grids". In: *IEEE Transactions on Industry Applications* vol. 56, no. 2 (Mar. 2020), pp. 1098–1106.

[88] Z. Yang; P. Dehghanian, and M. Nazemi. "Seismic-Resilient Electric Power Distribution Systems: Harnessing the Mobility of Power Sources". In: *IEEE Transactions on Industry Applications* (2020), pp. 1–10.

[89] M. Nazemi et al. "Multivariate Uncertainty Characterization for Resilience Planning in Electric Power Systems". In: *IEEE/IAS 56th Industrial and Commercial Power Systems (I&CPS) Technical Conference*. 2020, pp. 1–7.

[90] B. Zhang; P. Dehghanian, and M. Kezunovic. "Simulation of Weather Impacts on the Wholesale Electricity Market". In: *10th International Conference on Deregulated Electricity Market Issues in South Eastern Europe (DEMSEE)*. 2015, pp. 1–6.

[91] T. Dokic et al. "Risk Assessment of a Transmission Line Insulation Breakdown due to Lightning and Severe Weather". In: *The 49th Hawaii International Conference on System Science (HICSS)*. 2016, pp. 1–8.

[92] P. Dehghanian; S. Aslan, and P. Dehghanian. "Quantifying Power System Resiliency Improvement using Network Reconfiguration". In: *IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*. 2017, pp. 1–5.

[93] J. Su et al. "Distributed Wind Power Resources for Enhanced Power Grid Resilience". In: *The 51st North American Power Symposium (NAPS)*. 2019, pp. 1–6.

[94] D. Wang et al. "Power Grid Resilience to Electromagnetic (EMP) Disturbances: A Literature Review". In: *The 51st North American Power Symposium (NAPS)*. 2019, pp. 1–6.

[95] M. Babakmehr et al. "Artificial Intelligence-Based Cyber-Physical Event Classification for Islanding Detection in Power Inverters". In: *IEEE Journal of Emerging and Selected Topics in Power Electronics* (2020), pp. 1–11.

[96] S. Wang et al. "Advanced Control Solutions for Enhanced Resilience of Modern Power-Electronic-Interfaced Distribution Systems". In: *Journal of Modern Power Systems and Clean Energy* vol. 7, no. 4 (July 2019), pp. 716–730.

[97] B. Shinde et al. "Real-Time Detection of Critical Generators in Power Systems: A Deep Learning HCP Approach". In: *The 4th IEEE Texas Power and Energy Conference (TPEC)*. 2020, pp. 1–6.

[98] A. Berkeley; M. Wallace, and C. COO. "A framework for establishing critical infrastructure resilience goals". In: *Final Report and Recommendations by the Council, National Infrastructure Advisory Council* (2010).

[99] Y. Y. Haimes. "On the definition of resilience in systems". In: *Risk Analysis: An International Journal* vol. 29, no. 4 (2009), pp. 498–501.

[100] W. House. *Critical infrastructure security and resilience*. White House, 2013.

[101] S. L. Cutter et al. "Disaster resilience: A national imperative". In: *Environment: Science and Policy for Sustainable Development* vol. 55, no. 2 (2013), pp. 25–29.

[102] B. Zhu and S. Sastry. "SCADA-specific intrusion detection/prevention systems: a survey and taxonomy". In: *Proceedings of the 1st workshop on secure control systems (SCS)*. Vol. 11. 2010, p. 7.

[103] A. Giani et al. "The VIKING project: An initiative on resilient control of power networks". In: *2009 2nd International Symposium on Resilient Control Systems*. Aug. 2009, pp. 31–35. DOI: 10 . 1109 / ISRCS.2009.5251361.

[104] S. Wang; P. Dehghanian, and Y. Gu. "A Novel Multi-Resolution Wavelet Transform for Online Power Grid Waveform Classification". In: *The 1st IEEE International Conference on Smart Grid Synchronized Measurements and Analytics (SGSMA)*. 2019, pp. 1–6.

[105] S. Wang; L. Li, and P. Dehghanian. "Power Grid Online Surveillance through PMU-Embedded Convolutional Neural Networks". In: *IEEE Industry Applications Society (IAS) Annual Meeting*. 2019, pp. 1–7.

[106] S. Wang; P. Dehghanian, and L. Li. "Power Grid Online Surveillance through PMU-Embedded Convolutional Neural Networks". In: *IEEE Transactions on Industry Applications* vol. 56, no. 2 (Mar. 2020), pp. 1146–1155.

[107] P. Dehghanian; Y. Guan, and M. Kezunovic. "Real-Time Life-Cycle Assessment of High Voltage Circuit Breakers for Maintenance using Online Condition Monitoring Data". In: *IEEE Transactions on Industry Applications* vol. 55, no. 2 (2019), pp. 1135–1146.

[108] P. Dehghanian et al. "Security-Based Circuit Breaker Maintenance Management". In: *IEEE Power and Energy Society (PES) General Meeting*. 2013, pp. 1–5.

[109] Y. Guan et al. "Assessing Circuit Breaker Life Cycle using Condition-based Data". In: *IEEE Power and Energy Society (PES) General Meeting*. 2013, pp. 1–5.

[110] P. Dehghanian and M. Kezunovic. "Cost/Benefit Analysis for Circuit Breaker Maintenance Planning and Scheduling". In: *The 45th North American Power Symposium (NAPS)*. 2013, pp. 1–6.

[111] P. Dehghanian; Y. Guan, and M. Kezunovic. "Real-Time Life-Cycle Assessment of Circuit Breakers for Maintenance using Online Condition Monitoring

Data". In: *IEEE/IAS 54th Industrial and Commercial Power Systems (I&CPS) Technical Conference*. 2018, pp. 1–8.

[112] P. Dehghanian; T. Popovic, and M. Kezunovic. "Circuit Breaker Operational Health Assessment via Condition Monitoring Data". In: *The 46th North American Power Symposium*. 2014, pp. 1–6.

[113] S. Moradi et al. "A Mathematical Framework for Reliability-Centered Asset Management Implementation in Microgrids". In: *International Transactions on Electrical Energy Systems* (2018).

[114] H. Mirsaeedi et al. "Long-Term Maintenance Scheduling and Budgeting in Electricity Distribution Systems Equipped with Automatic Switches". In: *IEEE Transactions on Industrial Informatics* vol. 14, no. 5 (2018), pp. 1909–1919.

[115] M. Asghari Gharakheili; M. Fotuhi-Firuzabad, and P. Dehghanian. "A New Multi-Attribute Support Tool for Identifying Critical Components in Power Transmission Systems". In: *IEEE Systems Journal* vol. 12, no. 1 (2018), pp. 316–327.

[116] F. Pourahmadi; M. Fotuhi-Firuzabad, and P. Dehghanian. "Application of Game Theory in Reliability Centered Maintenance of Electric Power Systems". In: *IEEE Transactions on Industry Applications* vol. 53, no. 2 (2017), pp. 936–946.

[117] F. Pourahmadi; M. Fotuhi-Firuzabad, and P. Dehghanian. "Identification of Critical Generating Units for Maintenance: A Game Theory Approach". In: *IET Generation, Transmission & Distribution* vol. 10, no. 12 (2016), pp. 2942–2952.

[118] H. Sabouhi et al. "Identifying Critical Components of Combined Cycle Power Plants for Implementation of Reliability Centered Maintenance". In: *IEEE CSEE Journal of Power and Energy Systems* vol. 2, no. 2 (2016), pp. 87–97.

[119] H. Sabouhi et al. "Reliability Modeling and Availability Analysis of Combined Cycle Power Plants". In: *International Journal of Electrical Power and Energy Systems* vol. 79 (2016), pp. 108–119.

[120] R. Ghorani et al. "Identifying Critical Component for Reliability Centered Maintenance Management of Deregulated Power Systems". In: *IET Generation, Transmission, and Distribution* vol. 9, no. 9 (2015), pp. 828–837.

[121] P. Dehghanian et al. "A Comprehensive Scheme for Reliability Centered Maintenance Implementation in Power Distribution Systems- Part II: Numerical Analysis". In: *IEEE Transactions on Power Delivery* vol. 28, no. 2 (2013), pp. 771–778.

[122] P. Dehghanian et al. "A Comprehensive Scheme for Reliability Centered Maintenance Implementation in Power Distribution Systems- Part I: Methodology". In: *IEEE Transactions on Power Delivery* vol. 28, no. 2 (2013), pp. 761–770.

[123] P. Dehghanian et al. "Critical Component Identification in Reliability Centered Asset Management of Distribution Power Systems via Fuzzy AHP". In: *IEEE Systems Journal* vol. 6, no. 4 (2012), pp. 593–602.

[124] P. Dehghanian; M. Fotuhi-Firuzabad, and A. Razi-Kazemi. "An Approach for Critical Component Identification in Reliability-Centered Maintenance of Power Distribution Systems Based on Analytical Hierarchical Process". In: *The 21st International Conference and Exhibition on Electricity Distribution (CIRED)*. 2011, pp. 1–4.

[125] P. Dehghanian and M. Fotuhi-Firuzabad. "A Reliability-Oriented Outlook on the Critical Components of Power Distribution Systems". In: *The 9th IET International Conference on Advances in Power System Control, Operation, and Management (APSCOM)*. 2011, pp. 1–6.

[126] P. Dehghanian et al. "A Practical Application of the Delphi Method in Maintenance-Targeted Resource Allocation of Distribution Utilities". In: *The 13th International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*. 2014, pp. 1–6.

[127] F. Pourahmadi; M. Fotuhi-Firuzabad, and P. Dehghanian. "Identification of Critical Components in Power Systems: A Game Theory Application". In: *IEEE Industry Application Society (IAS) Annual Meeting*. 2016, pp. 1–6.

[128] J. Lai et al. "Broadcast Gossip Algorithms for Distributed Peer-to-Peer Control in AC Microgrids". In: *IEEE Transactions on Industry Applications* vol. 55, no. 3 (May 2019), pp. 2241–2251.

[129] F. Pourahmadi et al. "Dynamic Uncertainty Set Characterization for Bulk Power Grid Flexibility Assessment". In: *IEEE Systems Journal* vol. 14, no. 1 (Mar. 2020), pp. 718–728.

[130] M. Khoshjahan et al. "Harnessing Ramp Capability of Spinning Reserve Services for Enhanced Power System Flexibility". In: *IEEE Transactions on Industry Applications* vol. 55, no. 6 (Nov. 2019), pp. 7103–7112.

[131] P. Jokar. "Model-based intrusion detection for home area networks in smart grids". In: *University of Bristol, Bristol* (2012), pp. 1–19.

[132] D. I. Dogaru and I. Dumitrache. "Robustness of Power Systems in the Context of Cyber Attacks". In: *2017 21st International Conference on Control Systems and Computer Science (CSCS)*. IEEE. 2017, pp. 506–512.

[133] I. Dumitrache and D. I. Dogaru. "Smart grid overview: infrastructure, cyber-physical security and challenges". In: *2015 20th International Conference on Control Systems and Computer Science*. IEEE. 2015, pp. 693–699.

[134] M. Wang et al. "Identification of "unobservable" cyber data attacks on power grids". In: *2014*

IEEE International Conference on Smart Grid Communications (SmartGridComm). Nov. 2014, pp. 830–835. DOI: 10.1109/SmartGridComm.2014.7007751.

[135] H. Nishino and H. Ishii. "Distributed detection of cyber attacks and faults for power systems". In: *IFAC Proceedings Volumes* vol. 47, no. 3 (2014), pp. 11932–11937.

[136] F. Vosgerau et al. "Power system state and topology coestimation". In: *2010 IREP Symposium Bulk Power System Dynamics and Control - VIII (IREP)*. 2010, pp. 1–6.

[137] S. T. Smith et al. "Bayesian Discovery of Threat Networks". In: *IEEE Transactions on Signal Processing* vol. 62, no. 20 (Oct. 2014), pp. 5324–5338. ISSN: 1053-587X. DOI: 10.1109/TSP.2014.2336613.

[138] A. Teixeira; H. Sandberg, and K. H. Johansson. "Networked control systems under cyber attacks with applications to power networks". In: *Proceedings of the 2010 American Control Conference*. June 2010, pp. 3690–3696. DOI: 10.1109/ACC.2010.5530638.

[139] L. Liu et al. "Detecting false data injection attacks on power grid by sparse optimization". In: *IEEE Transactions on Smart Grid* vol. 5, no. 2 (2014), pp. 612–621.

[140] Y. Li and Y. Wang. "False data injection attacks with incomplete network topology information in smart grid". In: *IEEE Access* vol. 7 (2018), pp. 3656–3664.

[141] D. Xue; X. Jing, and H. Liu. "Detection of False Data Injection Attacks in Smart Grid Utilizing ELM-Based OCON Framework". In: *IEEE Access* vol. 7 (2019), pp. 31762–31773.

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

[143] Y. Huang et al. "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis". In: *IEEE Systems Journal* vol. 10, no. 2 (2014), pp. 532–543.

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

[145] O. Vuković and G. Dán. "Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks". In: *IEEE Journal on Selected Areas in Communications* vol. 32, no. 7 (2014), pp. 1500–1508.

[146] Y. Yamaguchi et al. "Cyber security analysis of power networks by hypergraph cut algorithms". In: *IEEE Transactions on Smart Grid* vol. 6, no. 5 (2015), pp. 2189–2199.

[147] Y. Zhang et al. "Power system reliability evaluation with SCADA cybersecurity considerations". In: *IEEE Transactions on Smart Grid* vol. 6, no. 4 (2015), pp. 1707–1721.

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

[149] S. Choi and A. S. Meliopoulos. "Effective real-time operation and protection scheme of microgrids using distributed dynamic state estimation". In: *IEEE Transactions on Power Delivery* vol. 32, no. 1 (2016), pp. 504–514.

[150] C. Murphy and A. Keane. "Local and remote estimations using fitted polynomials in distribution systems". In: *IEEE Transactions on Power Systems* vol. 32, no. 4 (2016), pp. 3185–3194.

[151] S. Bi and Y. J. A. Zhang. "Graph-based cyber security analysis of state estimation in smart power grid". In: *IEEE Communications Magazine* (2017).

[152] J. Zhao et al. "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks". In: *IEEE Transactions on Smart Grid* vol. 8, no. 4 (2015), pp. 1580–1590.

[153] Y. Weng et al. "Robust data-driven state estimation for smart grid". In: *IEEE Transactions on Smart Grid* vol. 8, no. 4 (2016), pp. 1956–1967.

[154] S. Maharjan et al. "Improved sample value adjustment for synchrophasor estimation at off-nominal power system conditions". In: *IEEE Transactions on Power Delivery* vol. 32, no. 1 (2016), pp. 33–44.

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

[156] O. Kosut et al. "Malicious data attacks on the smart grid". In: *IEEE Transactions on Smart Grid* vol. 2, no. 4 (2011), pp. 645–658.

[157] X. Liu et al. "Modeling of local false data injection attacks with reduced network information". In: *IEEE Transactions on Smart Grid* vol. 6, no. 4 (2015), pp. 1686–1696.

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

[159] X. Liu et al. "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure". In: *IEEE Transactions on Smart Grid* vol. 6, no. 5 (2015), pp. 2435–2443.

[160] P.-Y. Chen et al. "Detection of false data injection attacks in smart-grid systems". In: *IEEE Communications Magazine* vol. 53, no. 2 (2015).

[161] S. Bi and Y. J. Zhang. "Graphical methods for defense against false-data injection attacks on power

system state estimation". In: *IEEE Transactions on Smart Grid* vol. 5, no. 3 (2014), pp. 1216–1227.

[162] S. Bi and Y. J. Zhang. "Using covert topological information for defense against malicious attacks on DC state estimation". In: *IEEE Journal on Selected Areas in Communications* vol. 32, no. 7 (2014), pp. 1471–1485.

[163] J. M. Hendrickx et al. "Efficient computations of a security index for false data attacks in power networks". In: *IEEE Transactions on Automatic Control* vol. 59, no. 12 (2014), pp. 3194–3208.

[164] H. Sedghi and E. Jonckheere. "Statistical structure learning to ensure data integrity in smart grid". In: *IEEE Transactions on Smart Grid* vol. 6, no. 4 (2015), pp. 1924–1933.

[165] H. Karimipour and V. Dinavahi. "Robust massively parallel dynamic state estimation of power systems against cyber-attack". In: *IEEE Access* vol. 6 (2017), pp. 2984–2995.

[166] K. Manandhar et al. "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter". In: *IEEE transactions on control of network systems* vol. 1, no. 4 (2014), pp. 370–379.

[167] B. Li et al. "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system". In: *Journal of Parallel and Distributed Computing* vol. 103 (2017), pp. 32–41.

[168] B. Wang et al. "Electrical Safety Considerations in Large-Scale Electric Vehicle Charging Stations". In: *IEEE Transactions on Industry Applications* (2019), pp. 1–1. ISSN: 0093-9994. DOI: 10.1109/TIA.2019.2936474.

[169] Q. Li; R. Negi, and M. D. Ilić. "Phasor measurement units placement for power system state estimation: A greedy approach". In: *2011 IEEE Power and Energy Society General Meeting*. July 2011, pp. 1–8. DOI: 10.1109/PES.2011.6039076.

[170] M. A. Rahman and H. Mohsenian-Rad. "False data injection attacks with incomplete information against smart power grids". In: *2012 IEEE Global Communications Conference (GLOBECOM)*. Dec. 2012, pp. 3153–3158. DOI: 10.1109/GLOCOM.2012.6503599.

[171] P. Dehghanian and M. Kezunovic. "Probabilistic Decision Making for the Bulk Power System Optimal Topology Control". In: *IEEE Transactions on Smart Grid* vol. 7, no. 4 (2016), pp. 2071–2081.

[172] P. Dehghanian et al. "Flexible Implementation of Power System Corrective Topology Control". In: *Electric Power System Research* vol. 128 (2015), pp. 79–89.

[173] M. Alhazmi et al. "Power Grid Optimal Topology Control Considering Correlations of System Uncertainties". In: *IEEE/IAS 55th Industrial and Commercial Power Systems (I&CPS) Technical Conference*. 2019, pp. 1–7.

[174] M. Kezunovic et al. "Reliable Implementation of Robust Adaptive Topology Control". In: *The 47th Hawaii International Conference on System Science (HICSS)*. 2014, pp. 1–10.

[175] P. Dehghanian and M. Kezunovic. "Impact Assessment of Power System Topology Control on System Reliability". In: *IEEE Conference on Intelligent Systems Applications to Power Systems (ISAP)*. 2015, pp. 1–6.

[176] P. Dehghanian and M. Kezunovic. "Probabilistic Impact of Transmission Line Switching on Power System Operating States". In: *IEEE Power and Energy Society (PES) Transmission and Distribution (T&D) Conference and Exposition*. 2016, pp. 1–6.

[177] M. Alhazmi et al. "Power Grid Optimal Topology Control Considering Correlations of System Uncertainties". In: *IEEE Transactions on Industry Applications* vol. 55, no. 6 (Nov. 2019), pp. 5594–5604.

[178] M. Nazemi; P. Dehghanian, and M. Lejeune. "A Mixed-Integer Distributionally Robust Chance-Constrained Model for Optimal Topology Control in Power Grids with Uncertain Renewables". In: *13th IEEE Power and Energy Society (PES) PowerTech Conference*. 2019, pp. 1–6.

[179] L. Xie; Y. Chen, and P. R. Kumar. "Dimensionality Reduction of Synchrophasor Data for Early Event Detection: Linearized Analysis". In: *IEEE Transactions on Power Systems* vol. 29, no. 6 (Nov. 2014), pp. 2784–2794. ISSN: 0885-8950. DOI: 10.1109/TPWRS.2014.2316476.

[180] M. Wang et al. "A low-rank matrix approach for the analysis of large amounts of power system synchrophasor data". In: *2015 48th Hawaii International Conference on System Sciences*. IEEE. 2015, pp. 2637–2644.

[181] A. Goyal et al. "A unified framework for simulating Markovian models of highly dependable systems". In: *IEEE Transactions on Computers* vol. 41, no. 1 (Jan. 1992), pp. 36–51. ISSN: 0018-9340. DOI: 10.1109/12.123381.

[182] D. Wilson et al. "Deep learning-aided cyber-attack detection in power transmission systems". In: *2018 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE. 2018, pp. 1–5.

[183] C.-H. Wu. "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks". In: *Expert Systems with Applications* vol. 36, no. 3 (2009), pp. 4321–4330.

[184] N. V. Tomin et al. "Machine learning techniques for power system security assessment". In: *IFAC-PapersOnLine* vol. 49, no. 27 (2016), pp. 445–450.

[185] Y. Li; R. Ma, and R. Jiao. "A hybrid malicious code detection method based on deep learning".

In: *International Journal of Security and Its Applications* vol. 9, no. 5 (2015), pp. 205–216.

[186] R. C. Holte. "Very simple classification rules perform well on most commonly used datasets". In: *Machine learning* vol. 11, no. 1 (1993), pp. 63–90.

[187] B. Martin. "Instance-based learning: nearest neighbor with generalization [thesis". In: (1995).

[188] L. Breiman. "Random forests". In: *Machine learning* vol. 45, no. 1 (2001), pp. 5–32.

[189] G. W. Taylor. *Composable, distributed-state models for high-dimensional time series*. University of Toronto Toronto, 2009.

[190] J. Wei and G. J. Mendis. "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)*. IEEE. 2016, pp. 1–6.

[191] H. Wang et al. "Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks". In: *IEEE Transactions on Industrial Informatics* vol. 14, no. 11 (2018), pp. 4766–4778.

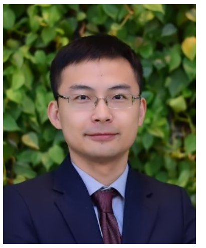
[192] M. Ashrafuzzaman et al. "Detecting stealthy false data injection attacks in power grids using deep learning". In: *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE. 2018, pp. 219–225.

[193] Y. Chakhchoukh et al. "Statistical outlier detection for diagnosis of cyber attacks in power state estimation". In: *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE. 2016, pp. 1–5.

[194] Y. He; G. J. Mendis, and J. Wei. "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism". In: *IEEE Transactions on Smart Grid* vol. 8, no. 5 (2017), pp. 2505–2516.

[195] A. Tajer et al. "Distributed joint cyber attack detection and state recovery in smart grids". In: *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE. 2011, pp. 202–207.

TIAN NGUYEN is currently pursuing B.Sc. degree in electrical engineering at the Department of Electrical and Computer Engineering, The George Washington University, Washington, D.C., USA. His research interests include power grid reliability, energy efficiency, and renewable integration.



SHIYUAN WANG (S'18) received the B.Eng degree in mechanical engineering from University of Science and Technology Beijing, China, in 2012; the M.Sc. degree in electrical engineering from The George Washington University, Washington, DC., USA, in 2014. He is currently pursuing the Ph.D. degree at the Department of Electrical and Computer Engineering, George Washington University, Washington, D.C., USA. His research interests include power system reliability and resiliency, smart grid and renewable energy, power grid harmonic analysis, and application of signal processing in energy analytics.

MOHANNAD ALHAZMI received the B.Sc. and M.Sc. degrees in electrical engineering from Umm Al-Qura University, Saudi Arabia in 2013 and The George Washington University, Washington D.C., USA, in 2017, respectively. He is currently pursuing his Ph.D. degree in the Department of Electrical and Computer Engineering at The George Washington University. His research interests include power system control, reliability and resiliency of power grids and critical infrastructure, cyber security and smart electricity grid applications.

MOSTAFA NAZEMI received the B.Sc. degree from K. N. Toosi University of Technology, Tehran, Iran, in 2015, and the M.Sc. degree from Sharif University of Technology, Tehran, Iran, in 2017, in electrical engineering and in energy systems engineering, respectively. He is currently pursuing the Ph.D. degree in electrical engineering at the Department of Electrical and Computer Engineering, George Washington University, Washington, D.C., USA. His research interests include power system resilience, power system planning and operation, energy optimizations, and smart electricity grid applications.

ABOUZAR ESTEBSARI received the Ph.D. degree in electrical engineering from Politecnico di Torino in Italy, in 2015 and pursued his research as a research fellow in this university. In 2016, he was with the E.ON. Energy Research Center at RWTH-Aachen University, in Germany, as a visiting scholar. Since August 2019, he has been a research scholar with the Department of Electrical and Computer Engineering in George Washington University, Washington, D.C., USA. From 2017 to 2020, he was an assistant professor at Politecnico di Torino, in Italy. He is currently an Assistant Professor at School of the Built Environment and Architecture in London South Bank University. His main research interests include power system security of supply and resiliency, smart grid applications, and multi-vector energy systems.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2993233, IEEE Access

PAYMAN DEHGHANIAN (S11, M17) is an Assistant Professor at the Department of Electrical and Computer Engineering in George Washington University, Washington, D.C., USA. He received the B.Sc., M.Sc., and Ph.D. degrees all in Electrical Engineering respectively from University of Tehran, Tehran, Iran, in 2009, Sharif University of Technology, Tehran, Iran, in 2011, and Texas A&M University, Texas, USA in 2017. His research interests include power system protection and control, power system reliability and resiliency, asset management, and smart electricity grid applications.

Dr. Dehghanian is the recipient of the 2013 IEEE Iran Section Best M.Sc. Thesis Award in Electrical Engineering, the 2014 and 2015 IEEE Region 5 Outstanding Professional Achievement Awards, and the 2015 IEEE-HKN Outstanding Young Professional Award.