Current Sustainable/Renewable Energy Reports (2018) 5:14–22
https://doi.org/10.1007/s40518-018-0094-8

ENERGY MARKETS (R SIOSHANSI AND S MOUSAVIAN, SECTION EDITORS)

Cyber-Physical Resilience of Electrical Power Systems Against Malicious Attacks: a Review

Sarmad Mehrdad[1] · Seyedamirabbas Mousavian[2] · Golshan Madraki[2] · Yury Dvorkin[3]

Published online: 25 January 2018

Abstract

Purpose of Review In this paper, we study the literature on cyber-physical security of electrical power systems. The paper is intended to address the security strengths and weaknesses of the electrical power systems against malicious attacks.

Recent Findings The concept of holistic resilience cycle (HRC) is introduced to improve cyber-physical security of electrical power systems. HRC is a systematic view to the security of the power systems, characterized by its four stages as closely interconnected and explicable only by reference to the whole. HRC includes four stages of prevention and planning, detection, mitigation and response, and system recovery.

Summary Power systems are evolving from traditional settings towards more autonomous and smart grids. Cyber-physical security is critical for the safe and secure operations of the power systems. To achieve a higher security level for power systems, the research community should follow a systematic approach and consider all stages of the holistic resilience cycle in addressing security problems of the power systems.

Keywords Cyber-physical security · Holistic resilience cycle · Cyber attacks · Physical attacks · False data intrusion attacks · Internet of things

Introduction

Safe and secure operation of the electrical power systems is a critical challenge and ranks as the highest priority of the stakeholders of the electricity markets. Besides inevitable malfunctions of the power grid components, deliberate disruptions caused by malicious attacks put the security of the power systems at high risk. Integration of the intelligent devices into the power grid operations has made the power grid increasingly reliant on the information and communication technologies. The integrated cyber-physical nature of the modern power systems has created a large and complex infrastructure that necessitates advanced cyber and physical security mechanisms. In this paper, we introduce the concept of the holistic resiliency cycle (HRC) that emphasizes the necessity of considering the power systems security problem holistically.

HRC is a systematic view to the security of the power systems, characterized by its four stages as closely interconnected and explicable only by reference to the whole. HRC includes four stages: (i) prevention and planning, (ii) detection, (iii) mitigation and response, and (iv) system recovery. We review the literature on cyber-physical security of the power systems and analyze them based on the HRC stages. The goal of the paper is to study the weaknesses and strengths of the power systems literature from the HRC perspective and enlighten the future research directions that enhance the cyber-physical security of power systems.

This article is part of the topical collection on *Energy Markets*

✉ Seyedamirabbas Mousavian
amir@clarkson.edu

Sarmad Mehrdad
mehrdas@clarkson.edu

Golshan Madraki
gmadraki@clarkson.edu

Yury Dvorkin
dvorkin@nyu.edu

[1] Mechanical and Aeronautical Engineering Department, Clarkson University, Potsdam, NY, USA

[2] David D. Reh School of Business, Clarkson University, Potsdam, NY, USA

[3] Electrical and Computer Engineering, NYU Tandon School of Engineering, Brooklyn, NY, USA

The rest of the paper is organized as follows. Section II investigates the physical security of power systems. Section III addresses the cyber security of power systems and evaluates the power systems resiliency against such attacks. Section IV reports our conclusions.

Physical Security of Power Systems

A report from Wall Street Journal revealed that 274 deliberate attacks to the power grid components occurred in 2011–2014 [1]. Physical attacks on power systems components not only disrupt the power supply to customers but also cause substantial economic burdens for the other stakeholders of the power sector such as utility companies, transmission system operators, and distribution system operators [2]. As a case in point, 17 large-scale power transformers were damaged in a recent attack to a substation in California on April 16, 2013, which also cost 27 days of repair time [2]. Damages to the critical power grid components may cause cascading outages and even blackouts [3]. Different protection mechanisms have been discussed to enhance the physical security of power grids. Intrusion detection devices, access controls, lighting, fencing, cameras, sensors, and buffer zone security are suggested as protection mechanisms with lower reliability and moderate cost investments [2]. A communication mechanism can be devised to alarm guards/police to accelerate the response time to intrusions and reduce the potential attack damages. More reliable protection mechanisms such as undergrounding or double circuiting of transmission lines require much higher investment costs [2]. Hence, protection of all grid components against physical attacks is impractical and economically un- justifiable.

Power grid resilience against physical attacks has attracted the interests of the research community as well. Salmeron et al. [4] proposed a bilevel mathematical model to identify the most disruptive attack scenario given that the attackers have resource limitations. Similarly, Donde et al. [5, 6] developed screening algorithms to identify contingencies that cause severe damage to the power grid. These proposed models identify the critical components for protection such that the damage caused by the most disruptive attack would reduce if the protection plan is implemented. The authors in [7–9] developed a variety of trilevel optimization models within the defender-attacker-defender framework for power network defense considering different scenarios and contingencies. These models devise the best resiliency plan when the attacker plots his attack with the perfect knowledge of the protected components. Multilevel optimization problems are complicated to solve. Salmeron et al. [10] applied decomposition methods to effectively solve such large-scale protection optimization models. Furthermore, a variety of game theory models, such as static games, leader-follower games, zero-sum Markov games, are proposed in [11–17] to tackle the defender-attacker problems for enhanced power systems physical security.

From the HRC perspective, the existing research on physical security of power systems has focused on the prevention and planning stage while taking into account mitigation of damages and response to potential attacks. The common shortcoming in these studies is the assumption that the protected components will be completely secure and no longer at risk, which limits the application of these models in the real world. Future research needs to address this issue and provide a more reliable solution. Furthermore, the widespread structure of the power grids makes the detection of a physical attack prior to its occurrence next to impossible unless protected with sensors, cameras, or guards. Last but not the least, the recovery stage of HRC on physical attacks has been barely studied in the literature. On a similar topic, power system recovery after natural disasters has been well studied that could be used as a benchmark for studying the power system recovery after physical attacks.

Cyber Security of Power Systems

Smart grid advancements have made cyber security a critical challenge for power systems operators. Data availability, data integrity, and data confidentiality are the main elements of cyber resiliency. Cyber attackers target these elements to manipulate the data being communicated for control and operations of the power systems in order to tamper with the grid, interrupt the safe operations of the power grid, gain financial advantage, or even damage the power grid physical structure. Many researchers, computer scientists in particular, have investigated prevention methods that keep cyber intruders away from the network devices and databases. Suo et al. [18•] reviewed and analyzed the state-of-the-art on cyber attack prevention technologies including encryption mechanisms, communication security, protecting sensor data, and cryptographic algorithms. To evaluate the state of cyber security of power systems from the HRC point of view, we further investigate methods and mechanisms proposed in the power systems literature for detection, response and mitigation, and recovery. In the next section, cyber attacks on power systems are studied and classified into two clusters: direct attacks and indirect attacks. Direct attacks target power systems databases and components whereas indirect attacks take advantage of the mutual dependency of power systems and Internet of things (IoT).

Direct Cyber Attacks to Power Systems

Direct cyber attacks are classified into four groups based on their functions as discussed below.

Data Intrusion Attacks

Data intrusion attacks are the most common group of cyber attacks threatening the security of power systems. Control mechanisms detect bad data caused by routine malfunctions of power systems devices such as imperfect measurements obtained from faulty sensors. However, a cyber attacker could gain access to power systems databases and shrewdly tamper with data such that the control center mechanisms cannot detect the anomaly. In general, there are three major types of data intrusion attacks, false data injection (FDI) attacks, load redistribution attacks (LRA), and denial of service attacks (DoS).

In FDI attacks, introduced by Liu et al. [19], the attacker gains access to the current power systems configurations and manipulates the stored data and measurements in order to lead power systems operators toward making wrong and potentially harmful decisions. Mousavian et al. [3] showed how FDI attacks to the optimal power flow (OPF) module could cause overloaded transmission lines and result in power outages and physical damages. The authors used artificial neural networks to develop a detection algorithm against FDI attacks on OPF module [3]. The authors in [20] analyzed FDI attacks on the state estimation module and provided a new detection algorithm using the state variable distribution. Similarly, Li et al. [21] studied the injection of malicious data to the monitoring meters of the state estimation and developed a sequential detection method using the generalized likelihood ratio. Furthermore, Moslemi et al. [22] utilized the near chordal sparsity of the power grid to obtain the associated maximum likelihood function and detect FDI attacks on the state estimation. Liu et al. [23] combined features of the network traffic flow of information and power systems physical laws to create a detection model called abnormal traffic-indexed state estimation for a higher detection rate of FDI attacks to the state estimation.

Khalid et al. [24] studied FDI attacks on transmission systems and proposed a multisensor track-level fusion based prediction model to improve the resiliency of the transmission systems against such attacks. Phasor measurement units (PMU) can measure synchronized phasors of bus voltages and currents of transmission lines in real time for better observability of the power grid [25]. A PMU takes about 30 to 120 measurements per second and sends its measurements to a phasor data concentrator (PDC) through a wireless communication network [26, 27]. PMUs, supposedly the trusted sensors of obtaining measurements for better resiliency and observability of the transmission systems, have been the target of the FDI attacks as well [28–30]. The authors in [30] presented a detection method using the majority voting algorithm in order to identify the compromised PMU which sends anomaly measurements. Waghmare et al. [31] proposed a two-stage detection method against FDI attacks to PMUs, which applies principal component analysis to reduce the high-dimensional datasets and use the support vector machine (SVM) method. SVM has also been used to detect FDI attacks to SCADA control system [32]. Similarly, He et al. [33] used deep learning methods and historical measurements data to detect FDI attacks on SCADA in real time.

A new class of FDI has been introduced in [34] as stealthy false data injection (SFDI) attacks. SFDI manipulates the gross errors from the measurement matrices such that the attack is undetectable by current detection schemes of the state estimation. Ashok et al. [35] has developed a detection algorithm against SFDI attacks on state estimation, which utilizes synchrophasor measurements, load forecasts, and generation schedules. Mohammadpourfard et al. [36] assumed that injecting false data into the system causes a deviation on the probability distribution of the state vector and proposed an unsupervised method for detecting SFDI on state estimation. Yang et al. [37] proposed a method to detect SFDI attacks on PMUs, in which neighborhood of sensors would detect the attack by constantly checking the state of the nodes and sending the rightness signals to the neighboring nodes. This method detects FDI in a smaller neighborhood of nodes, instead of the entire system, which gives the system operators the advantage of less computational complexity and faster detection. Mousavian et al. [38•] took one step further and developed a risk mitigation response to SFDI attacks to PMUs. They developed a mixed integer linear programming model that avoids or optimally slows down the propagation of cyber attacks while keeping the power systems observable. A similar study has been conducted for responding to SFDI attacks in the electric vehicles power stations network [39, 40]. Lin et al. [41] extended the response model to PMU networks, discussed in [38•] and proposed a self-healing strategy for PMU networks. Load redistribution attacks, introduced in [42], is a special case of the SFDI attacks in which the attacker manipulates the loads data collected for state estimation such that the sum of the errors calculated by the state estimation remains minimal [42]. There are two approaches for the adversary to commit LRA, immediate and delayed attacking goals. The immediate attacking goal is to maximize the power systems operations cost immediately after the attack whereas the delayed attacking goal is to gradually overload the power lines, while the attack remains undetected and redistributes the load to maximize the operations cost at a certain time after the attack [42]. Yuan et al. [42, 43] developed detection models against LRAs. A related research revealed that an attacker do not need to obtain complete information about the network to execute LRA and remain undetected [44]. A game-theoretic approach is proposed and developed to present an optimal defense strategy against LRAs [45]. Furthermore, the authors in [46] quantified the influence of LRAs by modeling these intrusions as a semi-Markov model.

Denial of service attacks are a class of data intrusion attacks, in which the adversary inserts artificial loads to the

service source such that the normal trend of service will be no longer accessible to legitimate requests. The first DoS attack is committed in 1997 by Khan C. Smith during a DEF CON hacking conference, which disrupted access to the internet for more than an hour in the Las Vegas Strip. Distributed denial of service (DDoS) attack is an advanced version of DoS. The DDoS attack is initiated from multiple adversaries/nodes simultaneously such that shutting down one adversary does not stop the attack and further differentiating the legitimate and artificial service requests is next to impossible.

Wang et al. [47] developed a novel method for preventing DoS attacks. This method, called Honeypot Game Model, introduces honeypots in the automated metering infrastructure (AMI) as decoys to gather information about attack and prevent it. Accordingly, an optimal defense strategy will be implemented by analyzing the interaction between the attacker and the defender using the Bayesian-Nash equilibria. Diovu et al. [48] proposed a method for preventing and also mitigating the impacts of DDoS. This method uses a firewall which is leveraged by the cloud computing technology and reduces the data computation and data storing burden of the automated metering infrastructure.

Lu et al. [49] proposed a detection algorithm against DDoS attacks. In this detection method, a pair of probes are being sent from the service source to the service request node. Then, the Fourier-to-Time reconstruction algorithm is executed to verify the legitimacy of the service request based on the gap between the probes. Varalakshmi and Selvi [50] proposed a defense mechanism using an information divergence scheme to detect and discard the adversary's artificial requests. Srikanthra and Kundur [51] showed that DoS attacks have the potential to disrupt the overall grid even if they are perpetrated on just a subset of cyber communication nodes. They proposed a collaborative reputation-based topology configuration to enable other nodes to converge quickly for maintaining the dynamic stability, while a subset of nodes is under attack. Liu et al. [52] designed a response mechanism to such attacks. They designed a communication subsystem capable of self-healing, when jammed under attack, to mitigate the impacts of the DoS attacks. This subsystem is designed via an intelligent local switching controller. The purpose of this subsystem is to collect sufficient readings from smart meters by local controllers to estimate the state of the system. Furthermore, Clela et al. [53] proposed a defense scheme based on a rule-based feedback control for mitigating the impacts of DoS attacks on islanded microgrids. Liu et al. [52] developed a communication subsystem with the enhanced self-healing ability to respond to cyber attacks, while keeping the system operating with the minimum impact on its service level. Similarly, authors in [51] proposed a relatively similar method for responding to DDoS attacks imposed on a subset of nodes in the system, in which the remaining nodes maintain their dynamic stability and keep the system away from the total failure.

Non-Technical Loss Fraud

Non-technical loss (NTL) fraud, also known as theft attacks, is intended to manipulate the attacker's consumption data. Theft attacks are less likely to be detected due to its supposedly small impacts comparing to the entire operations of the power grid. However, the financial burden of theft attacks is significantly high. The annual cost of theft attacks is close to 6 billion dollars in the USA [54] and 25 billion dollars worldwide [55].

Pasdar and Mirzakuchaki [56] proposed a detection algorithm in 2007 that sends test signals at high frequency to consumers and calculates the impedance of the related connections. A similar approach along with the real-time tracking of consumers at all times was introduced in [57, 58]. The authors in [59] investigated the theft attack on AMI and proposed a detection method called AMI intrusion detector system (AMIDS). AMIDS tracks both cyber and physical consumption data and meter audit logs to identify the electricity fraud. The authors in [60] proposed a two- stage detection method that clusters high risk consumers and then monitors their consumption profile. Villar-Rodriguez et al. [61] utilized the time series analysis and probabilistic data mining to detect theft attacks. Due to the large scale of the problem, machine learning is extensively used to develop detection algorithms, which monitor the usage profile of the consumers and identify the electricity consumption fraud based on anomalies in the usage patterns [62–67].

Time Delay Attacks

Time delay attack, introduced in 2014 by Sargolzaei et al. [68], interferes with the control signal. Receiving the control signal at the right time is of great importance and crucial for controlling the system. A time delay attack simply creates a delay for the control signal to reach the control center. Hence, the control center uses the measurement data of a period ago to control the current performance of the system, which could make the system unstable and prone to damaging attacks. Sargolzaei et al. [69] proposed a prevention method for time delay attacks on load frequency control. Furthermore, Shafique and Iqbal [70] developed a controller for load frequency control based on linear matrix inequalities and utilizing the Lyapnov-Krasovskii functional-based delay-dependent stability criteria. Sargolzaei et al. [71] developed a detection algorithm against time delay attacks in mobile ad hoc networks. The time delay attacks are relatively new and research in this area is still evolving.

Replay Attacks

Replay attacks, also known as Sybil attacks, take advantage of a false identity in the network. Two nodes of the communication network send each other specific signals to verify their identities. Replay attacker remains hidden in the communication network and eavesdrops on the communication channel until the identifying signal is exchanged. The replay attacker takes advantage of the obtained identifier signal from one node to pretend it is a trusted node in the network. This situation is like someone steals a social security number and uses it to mislead credit card companies for issuing a credit card. To the best of our knowledge, this type of attacks mostly has targeted the vehicular networks, sensor networks, and social networks. Due to the interdependence of the smart grid, electric transportation systems, and wireless sensor networks (WSN), we study the Sybil attacks as well.

In 2006, Piro et al. [72] analyzed replay attacks on ad hoc networks and suggested that mobility in the system can be used to enhance the system security rather than being the point of vulnerability. They showed that Sybil attack can be detected even with a single node by having the system nodes passively monitor the traffic. Later in 2008, Lv et al. [73], developed another detection method against Sybil attacks, in which the signal strength sensed by multiple sensors and their distance are utilized for detection. They showed that a Sybil attack happened when two different identities appear to have nearly the same position. Rabieh et al. [74] took another approach for detection of Sybil attacks in vehicular ad hoc network (VANET). In this approach, the attacker's vehicle, known as Sybil vehicle, claims to have multiple identities. The attacker may use these fake identities for various reasons such as faking the traffic flow. The Sybil attack will be detected since the Sybil vehicle has fake locations and cannot respond to the challenge signal sent by the detection algorithm to the claimed location. Sharma et al. [75] proposed an alternative method for VANETs security against Sybil Attacks and used a generation of dynamic certificates to change the identifying signals dynamically assuming that the adversary does not know the protocol of changing the certificates. Sarigiannidis et al. [76] proposed a rule-based detection system, known as RADS, to monitor and detect Sybil attacks on large-scale WSNs. This approach is based on the ultra-wideband ranging-based detection algorithm. RADS operates in a distributed manner and does not require sharing information between the nodes, which decreases the computational burden and expedites the detection process. More detection algorithms against Sybil attacks have been proposed in literature [77–80].

Indirect Cyber Attacks to Power Systems

The Internet of things is a system of interrelated computing devices, mechanical and digital machines, objects, animals, or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interactions. The IoT has provided cyber attackers with the opportunity to tamper with the power grid throughout the internet. The IoT attacks on power systems follow two approaches, load altering attacks throughout the direct load control (DLC) programs and targeting the data centers and computational loads [81••]. In load altering attacks, the attacker takes advantage of the dependency of demand side management programs on the internet and compromises the command signals to take over the operation of the residential and industrial load, which are supposed to be controlled by DLC programs. Alternatively, the attacker may hack to a numerous vulnerable consumers' devices, such as injecting false electricity prices, in order to influence their load behavior [82]. The false command signal or the injected price signal would increase (or decrease) the individual loads of the consumers and abruptly changes the aggregated load [81••]. Aside from the potential financial gains for the attacker and loss for the consumers, the abrupt changes of load may cause severe damages such as circuit overflow, voltage problems, tripping the transmission lines, damages to consumers' equipment, or even shutting down the power grid temporarily. Amini et al. [83, 84] proposed a dynamic load altering attack, in which the attacker is not only interested in the sudden spike of the aggregated load but also controls the timing of the spike. The main goal of the dynamic load altering attack is for the attacker to monitor the effect of the attack and shrewdly adjust the outcomes of the attack for achieving the maximum damage to the power grid and its operations. The authors developed a detection algorithm against dynamic load altering attacks [85].

Alternatively, the attacker may target only a very selected group of consumers and yet cause spikes on the aggregated load. The consumption of electricity at the IT sector such as Google and Microsoft data centers is growing rapidly. It is expected that the IT sector demand for electricity increases from 2 to 5% of the total consumption in the USA over the next decade [86]. As a case in point, Microsoft's data center in Quincy, WA, consumes 48 MW, which is the equivalent of 40,000 residential loads [81••]. The notion of cloud computing and selling computation power as utility expedited the growth of the IT sector and therefore their power consumption [87]. The computational load of a data center could change quickly and directly increase its power consumption. This elasticity of data centers' loads and their direct dependency to the computational loads make data centers an attractive target for power systems attackers. Attackers may use the internet to increase the computational loads of data centers by requesting bogus computational tasks and therefore increase the load of the power grid abruptly.

Discussion and Conclusions

From the HRC perspective, the existing research on physical security of power systems has focused on the prevention and planning stage, while taking into account mitigation of damages and responses to potential attacks. The common shortcoming in this area is the assumption that the protected components will be completely secure and no longer at risk, which limits the application of these models in the real world. Future research needs to address this issue and provide a more reliable solution. The recovery stage of HRC on physical attacks has been barely studied in the literature. On a similar topic, power system recovery after natural disasters has been well studied that could be used as a benchmark for studying the power system recovery after physical attacks.

Our HRC analysis highlights a few concerns on the cyber security of power systems, which should be tackled by researchers in the future. First, the bulk of research on cyber security relates to the prevention mechanisms, outlined in [18•], and developing detection algorithms against the variety of cyber attacks discussed. The other two stages of the HRC perspective, response and recovery, have been barely studied in the literature. The Response and recovery are two major steps after cyber attack detection to mitigate risks and damages and restore the system to its normal operations. The fact that power systems are evolving to smart and autonomous grids puts more emphasis on the importance of the response and recovery for the safe and secure operations of the future power systems. Secondly, the research on cyber security of power systems has followed a micro-level approach

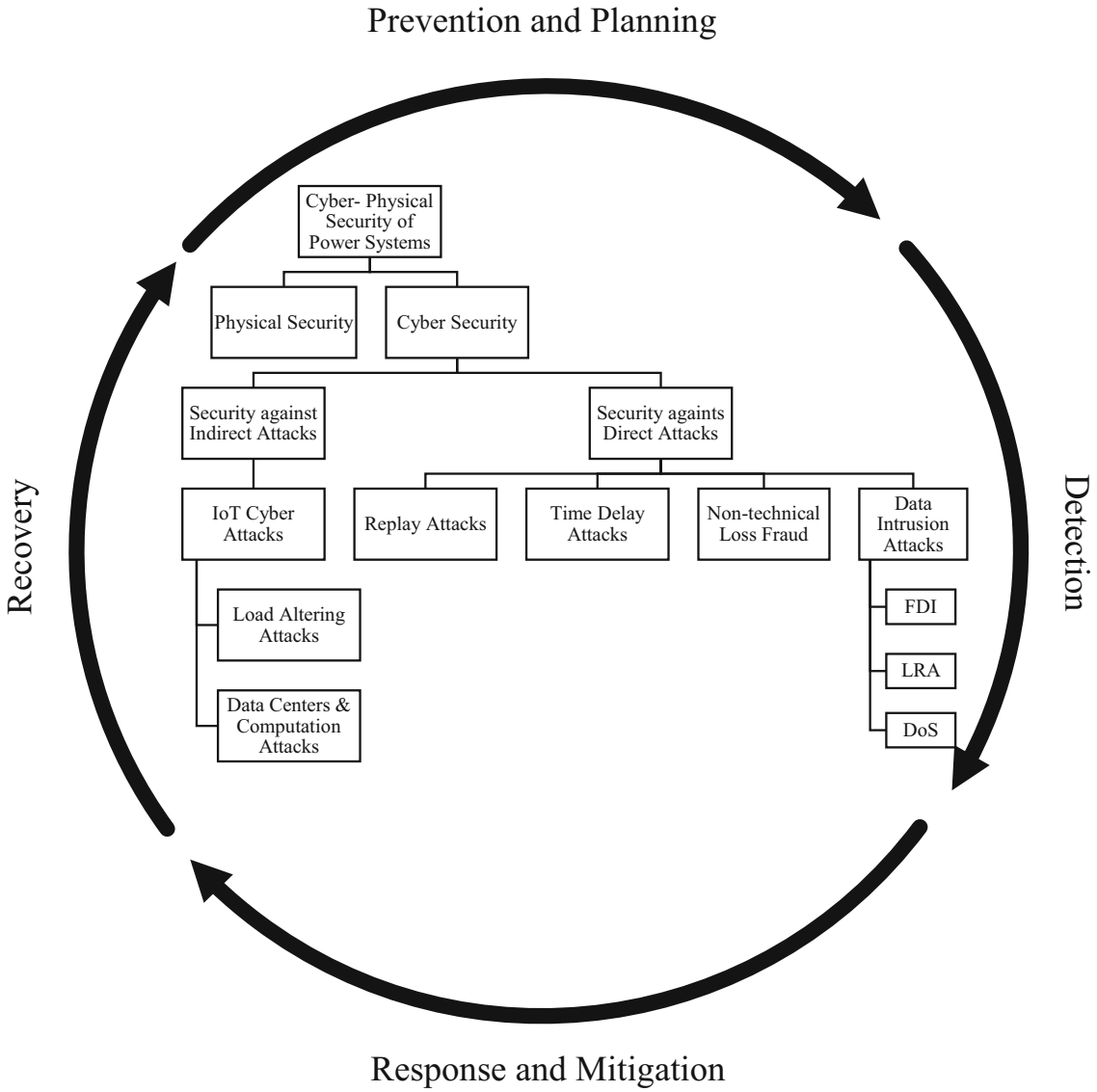

Fig. 1 Holistic resiliency cycle

that caused a gap and disconnections among the stages of the holistic resilience cycle. As a case in point, most of the proposed detection mechanisms are developed against a certain type of attack for a certain module under certain assumptions. This shortcoming limits the application of these models in the real world and could create more vulnerabilities in the system. It is critical to study cyber problems of power systems systematically, i.e., from the prevention to the recovery, in order to address the problem entirely and refrain cyber attackers from system vulnerability opportunities. Figure 1 summarizes our conclusions schematically.

Compliance with Ethical Standards

Conflict of Interest The authors declare that they have no conflicts of interest.

Human and Animal Rights and Informed Consent This article does not contain any studies with human or animal subjects performed by any of the authors.

References

People of particular interest, published recently, have been highlighted as:
- • Of importance
- •• Of major importance

1. Smith R. Assault on california power station raises alarm on potential for terrorism. [Online]. 2014. Available: http://www.wsj.com/articles/.
2. Nezamoddini N, Mousavian S, Erol-Kantarci M. A risk optimization model for enhanced power grid resilience against physical attacks. Electr Power Syst Res. 2017;143:329–38. https://doi.org/10.1016/j.epsr.2016.08.046.
3. Mousavian S, Valenzuela J, Wang J. Real-time data reassurance in electrical power systems based on artificial neural networks. Electr Power Syst Res. 2013;96:285–95. https://doi.org/10.1016/j.epsr.2012.11.015.
4. Salmeron J, Wood K, Baldick R. Analysis of electric grid security under terrorist threat. IEEE Trans Power Syst. 2004;19(2):905–12. https://doi.org/10.1109/TPWRS.2004.825888.
5. Donde V, Lopez V, Lesieutre B, Pinar A, Yang C, Meza J. Identification of severe multiple contingencies in electric power networks. In Proceedings of the 37th Annual North American Power Symposium, 2005. IEEE. 2005.
6. Donde V, Lopez V, Lesieutre B, Pinar A, Yang C, Meza J. Severe multiple contingency screening in electric power systems. IEEE Trans Power Syst. 2008;23(2):406–17. https://doi.org/10.1109/TPWRS.2008.919243.
7. Brown G, Carlyle M, Salmeron J, Wood K. Defending critical infrastructure. Interfaces. 2006;36(6):530–44. https://doi.org/10.1287/inte.1060.0252.
8. Alguacil N, Delgadillo A, Arroyo JM. A trilevel programming approach for electric grid defense planning. Comput Oper Res. 2014;41:282–90. https://doi.org/10.1016/j.cor.2013.06.009.
9. Yao Y, Edmunds T, Papageorgiou D, Alvarez R. Trilevel optimization in power network defense. IEEE Trans Syst Man Cybern Part C Appl Rev. 2007;37:712–8.
10. Salmeron J, Wood K, Baldick R. Worst-case interdiction analysis of large-scale electric power grids. IEEE Trans Power Syst. 2009;24(1):96–104. https://doi.org/10.1109/TPWRS.2008.2004825.
11. Holmgren AJ, Jenelius E, Westin J. Evaluating strategies for defending electric power networks against antagonistic attack. IEEE Trans Power Syst. 2007;22(1):76–84. https://doi.org/10.1109/TPWRS.2006.889080.
12. Chen G, Dong ZY, Hill DJ, Xue YS. Exploring reliable strategies for defending power systems against targeted attacks. IEEE Trans Power Syst. 2011;26(3):1000–9. https://doi.org/10.1109/TPWRS.2010.2078524.
13. Cappanera P, Scaparra MP. Optimal allocation of protective resources in shortest-path networks. Transp Sci. 2011;45(1):64–80. https://doi.org/10.1287/trsc.1100.0340.
14. Ma CYT, Yau DK, Lou X, Rao NS. Markov game analysis for attack-defense of power networks under possible misinformation. IEEE Trans Power Syst. 2012;28(2):1676–86.
15. Donde V, Lopez V, Lesieutre B, Pinar A, Yang C, Meza J. Identification of severe multiple contingencies in electric power networks. In Proceedings of the IEEE 37th Annual North American Power Symposium. 2005. p. 59–66.
16. Pinar A, Reichert A, Lesieutre B. Computing criticality of lines in power systems. In IEEE International Symposium onCircuits and Systems. 2007. p. 65–68.
17. Correa GJ, Yusta JM. Grid vulnerability analysis based on scalefree graphs versus power flow models. Electr Power Syst Res. 2013;101:71–9. https://doi.org/10.1016/j.epsr.2013.04.003.
18. • Suo H, Wan J, Zou C, Liu J. Security in the internet of things: a review. In International Conference on Computer Science and Electronics Engineering, Hangzhou. 2012. p. 648–651. **This review provides details on the state-of-the-art on cyber attack prevention technologies including encryption mechanisms, communication security, protecting sensor data, and cryptographic algorithms**.
19. Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. In Proceedings of the 16th ACM conference on Computer and communications security. ACM. 2009. p. 21–32.
20. Li Y, Wang Y. State summation for detecting false data attack on smart grid. Int J Electr Power Energy Syst. 2014;57:156–63. https://doi.org/10.1016/j.ijepes.2013.11.057.
21. Li S, Yilmaz Y, Wang X. Quickest detection of false data injection attack in wide-area smart grids. IEEE Trans Smart Grid. 2015;6(6):2725–35. https://doi.org/10.1109/TSG.2014.2374577.
22. Moslemi R, Moslemi R, Velni JM. A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids. IEEE Trans Smart Grid, vol. PP. 2017; 1–1.
23. Liu T, Sun Y, Liu Y, Gui Y, Zhao Y, Wang D, et al. Abnormal traffic-indexed state estimation: a cyberphysical fusion approach for smart grid attack detection. Futur Gener Comput Syst. 2015;49:94–103. https://doi.org/10.1016/j.future.2014.10.002.
24. Khalid HM, Peng JC-H. Immunity toward data-injection attacks using multisensor track fusion-based model prediction. IEEE Trans Smart Grid. 2015;8:697–707.
25. Zhu S, Wu L, Mousavian S, Roh JH. An optimal joint placement of PMUs and flow measurements for ensuring power system observability under N-2 transmission contingencies. Int J Electr Power Energy Syst. 2018;95:254–65. https://doi.org/10.1016/j.ijepes.2017.08.025.
26. Mousavian S, Valenzuela J, Wang J. A two-phase investment model for optimal allocation of phasor measurement units considering

transmission switching. Electr Power Syst Res. 2015;119:492–8. https://doi.org/10.1016/j.epsr.2014.10.025.
27. Mousavian S, Feizollahi MJ. An investment decision model for the optimal placement of phasor measurement units. Expert Syst Appl. 2015;42(21):7276–84. https://doi.org/10.1016/j.eswa.2015.05.041.
28. Zhao J, Zhang G, Jabr RA. Robust detection of cyber attacks on state estimators using phasor measurements. IEEE Trans Power Syst. 2017;32(3):2468–70. https://doi.org/10.1109/TPWRS.2016.2603447.
29. Deng R, Zhuang P, Liang H. Ccpa: coordinated cyberphysical attacks and countermeasures in smart grid. IEEE Trans Smart Grid. vol. PP. 2017; 1–1.
30. Li B, Lu R, Wang W, Choo K-KR. Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. Journal of Parallel and Distributed Computing. 2017;103:32–41. https://doi.org/10.1016/j.jpdc.2016.12.012.
31. Waghmare S, Kazi F, Singh N. Data driven approach to attack detection in a cyber-physical smart grid system. In Indian Control Conference (ICC). IEEE. 2017.
32. Maglaras LA, Jiang J, Cruz TJ. Combining ensemble methods and social network metrics for improving accuracy of ocsvm on intrusion detection in scada systems. Journal of Information Security and Applications. 2016;30:15–26. https://doi.org/10.1016/j.jisa.2016.04.002.
33. He Y, Mendis GJ, Wei J. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. IEEE Trans Smart Grid, vol. PP. 2017; 1–1.
34. Anwar A, Mahmood AN, Pickering M. Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements. J Comput Syst Sci. 2017;83(1):58–72. https://doi.org/10.1016/j.jcss.2016.04.005.
35. Ashok A, Govindarasu M, Ajjarapu V. Online detection of stealthy false data injection attacks in power system state estimation. Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation, vol. PP. 2016; 1–1.
36. Mohammadpourfard M, Sami A, Seifi AR. A statistical unsupervised method against false data injection attacks: a visualization-based approach. Expert Syst Appl. 2017;84:242–61. https://doi.org/10.1016/j.eswa.2017.05.013.
37. Yang W, Lei L, Yang C. Event-based distributed state estimation under deception attack. Neurocomputing, vol. PP. 2017; 1–1.
38.• Mousavian S, Valenzuela J, Wang J. A probabilistic risk mitigation model for cyber-attacks to pmu networks. IEEE Trans Power Systems. 2015. **The authors investigated a probabilistic risk mitigation response to cyber attacks to PMU networks after detection of the attack. The article is the first one in the literature that addressed how to respond to cyber attacks to power systems after detection of the attack**;30(1):156–65. https://doi.org/10.1109/TPWRS.2014.2320230.
39. Mousavian S, Erol-Kantarci M, Ortmeyer T. Cyber attack protection for a resilient electric vehicle infrastructure. San Diego: IEEE Globecom Workshops (GC Wkshps); 2015. p. 1–6.
40. Mousavian S, Erol-Kantarci M, Wu L, Ortmeyer T. A riskbased optimization model for electric vehicle infrastructure response to cyber attacks. IEEE Trans Smart Grid. PP(99); s1–1.
41. Lin H, Chen C, Wang J, Qi J, Jin D, Kalbarczyk Z, Iyer RK. Self-healing attack-resilient pmu network for power system operation. IEEE Transactions on Smart Grid, vol. PP. 2016; 1–1.
42. Yuan Y, Li Z, Ren K. Modeling load redistribution attacks in power systems. IEEE Transactions on Smart Grid. 2011;2(2):382–90. https://doi.org/10.1109/TSG.2011.2123925.
43. Yuan Y, Li Z, Ren K, Quantitative analysis of load redistribution attacks in power systems. IEEE Transactions on Parallel and Distributed Systems. 2012;23(9):1731-38. https://doi.org/10.1109/TPDS.2012.58.
44. Liu X, Li Z. Local load redistribution attacks in power systems with incomplete network information. IEEE Transactions on Smart Grid. 2014;5(4):1665–76. https://doi.org/10.1109/TSG.2013.2291661.
45. Xiang Y, Wang L. A game-theoretic approach to optimal defense strategy against load redistribution attack. In IEEE Power & Energy Society General Meeting. IEEE. 2015.
46. Xiang Y, Ding Z, Zhang Y, Wang L. Power system reliability evaluation considering load redistribution attacks. IEEE Transactions on Smart Grid. 2017;8:889–901.
47. Wang K, Du M, Maharjan S, Sun Y. Strategic honeypot game model for distributed denial of service attacks in the smart grid. IEEE Transactions on Smart Grid. 2017;8(5):2474–82. https://doi.org/10.1109/TSG.2017.2670144.
48. Diovu RC, Agee JT. A cloud-based openflow firewall for mitigation against ddos attacks in smart grid ami networks. In PowerAfrica, 2017 I.E. PES. IEEE. 2017.
49. Lu W-Z, Gu W-X, Yu S-Z. One-way queuing delay measurement and its application on detecting ddos attack. J Netw Comput Appl. 2009;32(2):367–76. https://doi.org/10.1016/j.jnca.2008.02.018.
50. Varalakshmi P, Selvi ST. Thwarting ddos attacks in grid using information divergence. Futur Gener Comput Syst. 2013;29(1):429–41. https://doi.org/10.1016/j.future.2011.10.012.
51. Srikantha P, Kundur D. Denial of service attacks and mitigation for stability in cyber-enabled power grid. In 2015 I.E. Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE. 2015.
52. Liu H, Chen Y, Chuah MC, Yang J, Poor HV. Enabling self-healing smart grid through jamming resilient local controller switching. IEEE Transactions on Dependable and Secure Computing. 2015;14:377–91.
53. Chlela M, Mascarella D, Joos G, Kassouf M. Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks. IEEE Trans Smart Grid, vol. PP. 2017; 1–1.
54. Salinas S, Li M, Li P. Privacy-preserving energy theft detection in smart grids: a p2p computing approach. IEEE Journal on Selected Areas in Communications. 2013;31(9):257–67. https://doi.org/10.1109/JSAC.2013.SUP.0513023.
55. Jiang R, Lu R, Wang Y, Luo J, Shen C, Shen XS. Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Sci Technol. 2014;19(2):105–20. https://doi.org/10.1109/TST.2014.6787363.
56. Pasdar A, Mirzakuchaki S. A solution to remote detecting of illegal electricity usage based on smart metering. In 2nd International Workshop on Soft Computing Applications, 2007. SOFA. IEEE. 2007.
57. Deb S, Bhowmik PK, Paul A. Remote detection of illegal electricity usage employing smart energy meter—a current based technique. In IEEE PES Innovative Smart Grid Technologies—India (ISGT India). IEEEx. 2011.
58. Bat-Erdene B, Lee B, Kim M-Y, Ahn T, Kim D. Extended smart meters-based remote detection method for illegal electricity usage. IET Generation, Transmission & Distribution. 2013;7(11):1332–43. https://doi.org/10.1049/iet-gtd.2012.0287.
59. McLaughlin S, Holbert B, Zonouz S, Berthier R. Amids: a multi-sensor energy theft detection framework for advanced metering infrastructures. In Third International Conference on Third International Conference on, 2012.
60. Jokar P, Arianpoo N, Leung VCM. Electricity theft detection in ami using customers consumption patterns. IEEE Transactions on Smart Grid. 2016;7:2016–226.
61. Villar-Rodriguez E, Ser JD, Oregi I, Bilbao MN, Gil-Lopez S. Detection of non-technical losses in smart meter data based on load curve profiling and time series analysis. Energy. 2017;137:118–28. https://doi.org/10.1016/j.energy.2017.07.008.

62. Nagi J, Yap KS, Tiong SK, Ahmed SK, Mohammad AM. Detection of abnormalities and electricity theft using genetic support vector machines. In IEEE Region 10 Conference TENCON 2008. IEEE. 2008.
63. Depuru SSSR, Wang L, Devabhaktuni V. Support vector machine based data classification for detection of electricity theft. In IEEE/PES Power Systems Conference and Exposition (PSCE). IEEE. 2011.
64. Depuru SSSR, Wang L, Devabhaktuni V, Nelapati P. A hybrid neural network model and encoding technique for enhanced classification of energy consumption data. In IEEE Power and Energy Society General Meeting. IEEE. 2011.
65. Jindal A, Dua A, Kaur K. Decision tree and svm-based data analytics for theft detection in smart grid. IEEE Transactions on Industrial Informatics. 2016;12(3):1005–16. https://doi.org/10.1109/TII.2016.2543145.
66. Glauner P, Boechat A, Dolberg L, State R, Bettinger F, Rangoni Y, Duarte D. Large-scale detection of non-technical losses in imbalanced data sets. In IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE. 2016.
67. Ghanbari M, Kinsner W, Ferens K. Anomaly detection in a smart grid using wavelet transform, variance fractal dimension and an artificial neural network. In IEEE Electrical Power and Energy Conference (EPEC). IEEE. 2016.
68. Sargolzaei A, Yen K, Abdelghani M. Delayed inputs attack on load frequency control in smart grid. In IEEE PES Innovative Smart Grid Technologies Conference (ISGT). 2014.
69. Sargolzaei A, Yen KK, Abdelghani MN. Preventing time-delay switch attack on load frequency control in distributed power systems. IEEE Transactions on Smart Grid. 2016;7:1176–85.
70. Shafique M, Iqbal N. Load frequency resilient control of power system against delayed input cyber attack. In Symposium on Recent Advances in Electrical Engineering (RAEE). IEEE. 2015.
71. Sargolzaei A, Yen KK, Abdelghani M, Sargolzaei S, Car-bunar B. Resilient design of networked control systems under time delay switch attacks, application in smart grid. IEEE Access, vol. PP. 2017; 1–1.
72. Piro C, Shields C, Levine BN. Detecting the sybil attack in mobile ad hoc networks. In Securecomm and Workshops. IEEE. 2006.
73. Lv S, Wang X, Zhao X, Zhou X. Detecting the sybil attack cooperatively in wireless sensor networks. In International Conference on Computational Intelligence and Security, 2008. CIS '08. IEEE. 2008.
74. Rabieh K, Mahmoud MMEA, Guo TN, Younis M. Cross-layer scheme for detecting large-scale colluding sybil attack in vanets. In IEEE International Conference on Communications (ICC). IEEE. 2015.
75. Sharma AK, Saroj SK, Chauhan SK, Saini SK. Sybil attack prevention and detection in vehicular ad hoc network. In International Conference on Computing, Communication and Automation (ICCCA). IEEE. 2016.
76. Sarigiannidis P, Karapistoli E, Economides AA. Detecting sybil attacks in wireless sensor networks using uwb ranging-based information. Expert Syst Appl. Nov. 2015;42(21):7560–72. https://doi.org/10.1016/j.eswa.2015.05.057.
77. Hoehn A, Zhang P. Detection of replay attacks in cyberphysical systems. In American Control Conference (ACC). IEEE. 2016.
78. Misra S, Tayeen ASM, Xu W. Sybilexposer: an effective scheme to detect sybil communities in online social networks. In IEEE International Conference on Communications (ICC). IEEE. 2016.
79. Gu P, Khatoun R, Begriche Y, Serhrouchni A. Vehicle driving pattern based sybil attack detection. In IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS). IEEE. 2016.
80. Irita T, Namerikawa T. Detection of replay attack on smart grid with code signal and bargaining game. In 2017 American Control Conference (ACC). IEEE. 2017.
81.•• Mohsenian-Rad A-H, Leon-Garcia A. Distributed internet-based load altering attacks against smart power grids. IEEE Transactions on Smart Grid. 2011. **The article introduces indirect cyber attacks to power systems taking advantage of the mutual dependency of smart grids and IoT**;2(4):667–74. https://doi.org/10.1109/TSG.2011.2160297.
82. Dvorkin Y, Garg S. Iot-enabled distributed cyber-attacks on transmission and distribution grids. In Proceedings of the 49th North American Power Symposium (NAPS). 2017.
83. Amini S, Mohsenian-Rad H, Pasqualetti F. Dynamic load altering attacks in smart grid. In 2015 I.E. Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE. 2015.
84. Amini S, Pasqualetti F, Mohsenian-Rad H. Dynamic load altering attacks against power system stability: attack models and protection schemes. IEEE Trans Smart Grid. 2016;99:1. https://doi.org/10.1109/TSG.2016.2622686.
85. Amini S, Pasqualetti F, Mohsenian-Rad H. Detecting dynamic load altering attacks: a data-driven time- frequency analysis. In 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL; 2015. p 503-8. https://doi.org/10.1109/SmartGridComm.2015.7436350.
86. Baer WS, Hassell S, Vollaar BA. Electricity requirements for a digital society. Santa Monica, Tech. Rep.: RAND Corporation; 2002.
87. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I, Zaharia M. Above the clouds: a berkeley view of cloud computing. University of California, Berkeley, Tech. Rep. 2009.