IET Cyber-Physical Systems: Theory & Applications

Review Article

Cyber-physical attacks and defences in the smart grid: a survey

ISSN 2398-3396
Received on 20th October 2016
Revised on 8th November 2016
Accepted on 8th November 2016
doi: 10.1049/iet-cps.2016.0019
www.ietdl.org

Haibo He ✉, *Jun Yan*

Department of Electrical, Computer, and Biomedical Engineering, University of Rhode Island, Kingston, RI 02881, USA
✉ *E-mail: he@ele.uri.edu*

Abstract: The smart grid is arguably one of the most complex cyber-physical systems (CPS). Complex security challenges have been revealed in both the physical and the cyber parts of the smart grid, and an integrative analysis on the cyber-physical (CP) security is emerging. This paper provides a comprehensive and systematic review of the critical attack threats and defence strategies in the smart grid. We start this survey with an overview of the smart grid security from the CP perspective, and then focuses on prominent CP attack schemes with significant impact on the smart grid operation and corresponding defense solutions. With an in-depth review of the attacks and defences, we then discuss the opportunities and challenges along the smart grid CP security. We hope this paper raises awareness of the CP attack threats and defence strategies in complex CPS-based infrastructures such as the smart grid and inspires research effort toward the development of secure and resilient CP infrastructures.

1 Introduction

Cyber-physical systems (CPSs) are inducing profound changes in the modern society. Composed of computation, communication, and physical systems and processes, CPS integrate, and coordinate heterogeneous components with increasing intelligent, interactive, and distributed operations in the modern critical infrastructures. The emerging smart grid, being one of the most complex CPS ever built in history, witnesses such transformations during the ongoing integration of power and energy systems with information and communication technologies (ICTs) [1]. The fundamental changes in this critical infrastructure are leading toward far-reaching impacts on not only the energy, but also a number of critical interdependent sectors.

The smart grid encompasses complex systems of power, energy, control, sensory, computing, and communication. The complexity and heterogeneity in this architecture have underscored the potential challenges to its security and resilience. On one hand, the interconnection of bulk power systems is complicating the protection against inherent physical vulnerabilities therein. On the other hand, the cyber-integration requires substantial investments on security designs and upgrades against unforeseen patterns and threats from the cyberspace. The collective research effort on cybersecurity and physical security have been striding fast and fostering a new area of CP security for the smart grid [2].

An essential and primary focus of CP security is the investigation of complex attack schemes. Powered by the information and computation resources in the cyberspace, malicious attackers can conceive intrigue schemes to exploit both known and zero-day vulnerabilities in the smart grid. Compared with traditional power system and communication network security, CP security is still in an 'infancy' period. However, existing investigations have already revealed some catastrophic consequences that are largely unprepared by the government, industry, and public. The assessments of vulnerability and resilience against the CP attacks are providing the cornerstones for comprehensive defensive plans and emergency responses for the critical electrical power infrastructure.

In the meantime, the investigations of attack threats and the developments of defence strategies remain far from comprehensive. Inspections of cyber and physical security are essential for the security of smart grid, but neither direction alone is able to provide inclusive understandings and solutions without incorporating the other. Although many of the revealed attack threats are accompanied with protection, detection, or mitigation strategies, a large portion of the uncovered threats still remain to be addressed. Furthermore, the ongoing developments and deployments of CPS and technologies in the smart grid are continuously unveiling new vulnerabilities and schemes; the known threats also merit prompt re-evaluation in line with the new progresses. It has thereby become a task of paramount importance to keep up with the latest advances along this research frontier.

To this end, this paper aims to provide a review on the state-of-the-art of CP attack schemes and defence strategies in the smart grid. Instead of enumerating all potential attack schemes, this paper will focus on the most critical schemes, where attackers have the potential to significantly disrupt or damage power system operations. The victims emerge from the critical assets in generation and transmission systems as well as the field devices of distribution systems and customers. As shown in this paper, the attack threats are substantial and prevalent, yet they may still just be the tip of the iceberg. We hope to facilitate the understanding of existing and emerging vulnerabilities and to inspire innovations and solutions for the security and resilience of the smart grid as well as other critical CPS infrastructures.

In the rest of this paper, we first provide an overview of the CP security problems in the smart grid in Section 2, which will introduce the smart grid as a CPS infrastructure and the need for an integrative perspective of CP security. In Section 3, we will review the critical CP attack schemes revealed by extensive investigations. Section 4 reviews the defence strategies developed against these revealed attack threats. Section 5 discusses the challenges and opportunities to address the security of smart grid based on the existing attack schemes and defence strategies. The conclusions are provided in Section 6.

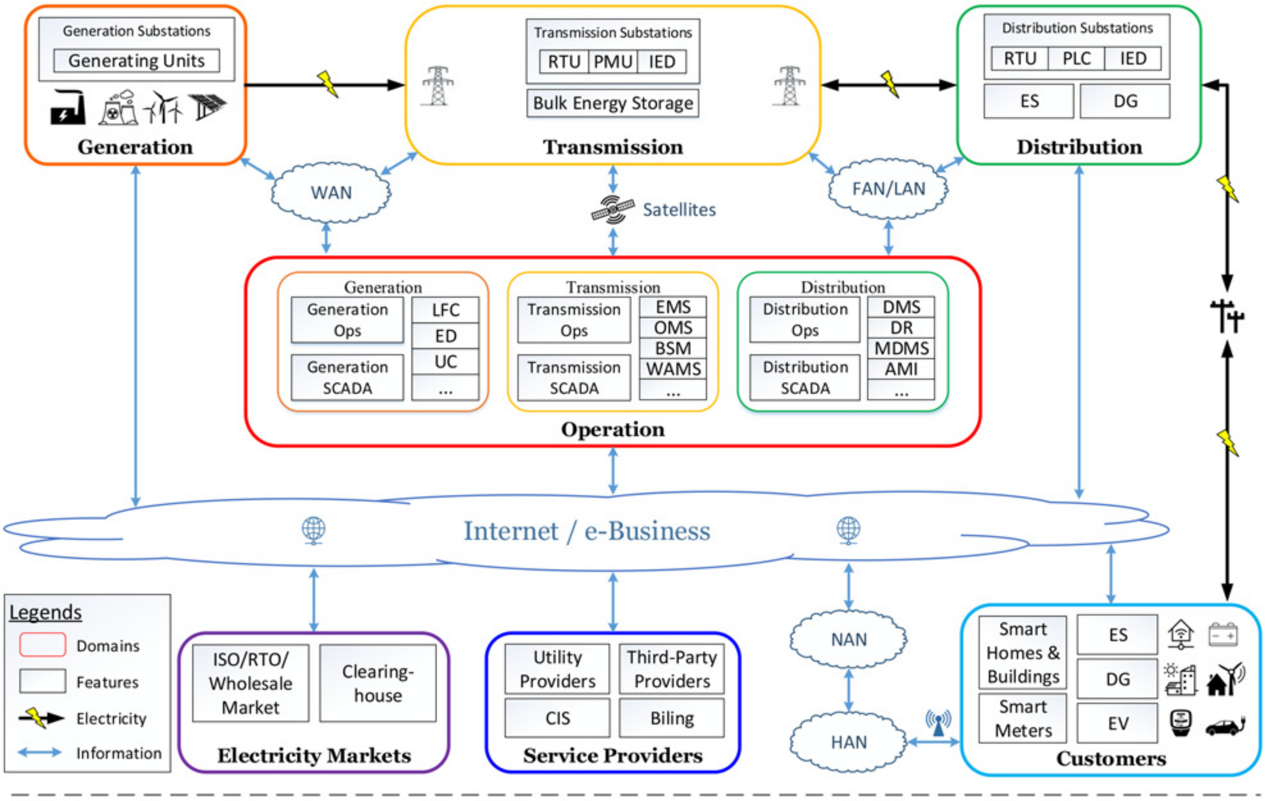
2 CP perspective of smart grid security

2.1 Smart grid as a CPS

The smart grid is built on a monolithic physical infrastructure of electrical power systems which have been generally categorised into generation, transmission, and distribution systems [3]. In the traditional paradigm of power system operations, the electricity is generated in power plants and delivered along the transmission systems to customers in the distribution systems. Energy management systems (EMSs) located in control centres monitor and control this unidirectional process through supervisory control and data acquisition (SCADA) systems. The SCADA systems are usually hosted on dedicated communication infrastructures comprising wide-area networks, field area networks, and local area networks. Networked sensors in the system collect measurements, e.g. voltage and currents, and transmit the data to the control systems through remote terminal units (RTU) in the SCADA system. The RTU are also responsible for the operation of actuators to adjust topology and parameters of the dynamic system. The physical systems of generation, transmission, and distribution are interconnected through transmission lines and substations deployed in the field. On top of these infrastructures, regional transmission organisations and independent system operators coordinate the system operations among service providers and consumers in the electricity market. An overview of the entire smart grid infrastructure has been shown in Fig. 1, which contains seven domains of generation, transmission, distribution, operation, electricity markets, service providers, and customers, as defined by the National Institute of Standards and Technologies (NIST) [4].

Innovative systems and technologies in the smart grid have been transforming the traditional power systems in numerous areas [5–7]. The growing integration of renewable energy systems (RESs) improves the sustainability and economics of generation systems. Distributed energy resources (DERs) allow customer-side power generation and management with more flexibility and reliability, reshaping the existing patterns of power flows from unidirectional into bidirectional. The phasor measurement unit (PMU) utilises global positioning system (GPS) to provide more frequent, accurate, and reliable synchronised measurements in the transmission systems, enabling the implementation of wide-area monitoring, protection, and control (WAMPAC) over high-speed communication networks [8]. The advanced metering infrastructure (AMI) systems with millions of smart meters in the distribution systems provide innovative two-way, real-time (RT) communications in the smart grid, which promote numerous benefits from demand response, energy management, and consumer engagement. In addition, the increasing presence of energy storage, electrical vehicles, and other emerging techniques are consistently introducing new changes to the generation, transmission, and distribution of electricity.

The information, computation, and communication systems in smart grid have instituted a ubiquitous cyber infrastructure interwoven with the PSs. Measurements and commands are constantly generated and transmitted between cyber and PSs. The measurements from the PSs are primarily composed of status data and analogue data: the status data contain the topological connectivity of power grid components; the analogue data are measurements of the system dynamics. On the basis of the measurements, operators determine the optimal control policies and issue the control commands to coordinate actuators in the PSs.



AMI: Advanced Metering Infrastructure
BSM: Bulk Storage Management
CIS: Customer Information System
DG: Distributed Generation
DMS: Distributed Management Systems
DR: Demand Response
ED: Economic Dispatch
EMS: Energy Management Systems
ES: Energy Storage
FAN: Field Area Networks
HAN: Home Area Networks
IED: Intelligent Electronic Devices
ISO: Independent System Operator
LAN: Local Area Networks
LFC: Load Frequency Control
MDMS: Meter Data Management Systems
NAN: Neighbourhood Area Networks
OMS: Outage Management Systems
PLC: Programmable Logic Circuits
PMU: Phasor Measurement Units
RTO: Regional Transmission Organization
RTU: Remote Terminal Units
SCADA: Supervisory Control And Data Acquisition
UC: Unit Commitment
WAMS: Wide-Area Monitoring Systems
WAN: Wide Area Networks

Fig. 1 *Overview of the smart grid architecture based on the NIST framework*

In the presence of a fault or disturbance, diagnostic logs are recorded by supplementary recording devices to support the location, evaluation, mitigation, and restorations during emergencies.

Sensor measurements are processed by centralised and distributed computation devices deployed at different levels and locations in the smart grid. In the traditional centralised operations, critical computations in EMS, including the state estimation (SE), optimal power flow (OPF), economic dispatch (ED), and automatic generation control (AGC), among others, are hosted in the control centres. In pursuit of better efficiency, resiliency, and flexibility, latest developments in intelligent electronic devices and programmable logic circuits have increased the utilisation of distributed and localised computations in the smart grid.

Communications in the smart grid have been primarily hosted on proprietary SCADA systems and networks. Industrial protocols such as IEC 61850 and DNP3 have been developed for communications between and within control centres and substations. New communication standards are being introduced in the smart grid to accommodate the integration of renewable energies, energy storage, and PMUs. Meanwhile, with the increasing efficiency requirements and cost pressures, the smart grid also increasingly relies on public communication infrastructures. Industrial control systems are accessing the Internet via ICT interfaces. Two-way communications between service providers and customers are also widely established through the AMI system, allowing flexible demand response for reliability and economic benefits.

2.2 CP security of the smart grid

Security challenges in the smart grid have been on the rise in both physical and cyber spaces [9, 10]. The power systems have inherent physical vulnerabilities that could result in massive blackouts from a small number of contingencies [11]. The integration of RES introduces non-linearity, uncertainty, time-variance to existing power systems, and the new patterns from DER are inducing significant impacts on the stability [12]. The cyber-integration has imposed significant security challenges, as tremendous threats arise from the attacker's ability to launch intrigue, remote, simultaneous, and/or coordinated attacks from the cyberspace. An informed attack scheme can exert disruptions and damages ranging from service interruptions, power blackouts, economic losses, to life-threatening threats, where personal, societal, and national securities may all be affected.

The research on cyber-physical security of the smart grid advances on a frontier of CPS, striving at the intersection of physical security of power and energy systems and the cybersecurity of information, computation, and communication systems [2]. Incorporation of the strengths of physical and cybersecurity is an essential requirement for the security and resilience of this critical infrastructure. In what follows, we will briefly discuss the strengths and weaknesses of physical and cybersecurity for the smart grid and highlight the importance of CP security.

2.2.1 Physical security: The physical security of power systems has been protected through the screening and assessment of contingencies. The contingency analysis (CA) evaluates the power system security after credible inadvertent contingencies on a selection of operating points [11]. Typically, the CA covers faults, disturbances, and planned outages, among others. Contingency-related security constraints are subsequently established by the CA to ensure the survivability of power systems with minimal interruptions to the delivery of electricity. Both the steady-state and transient security analysis of power systems serve as the foundation of CP security for the smart grid.

However, the interconnected power systems and the emerging CPS have presented challenges to the physical security analysis. The complexity and cost of the CA increase dramatically when the system scales, rendering it difficult to conduct multi-CA or implement $N-k$ security in bulk power systems. The heterogeneity and complexity of hardware, software, and operations in power systems also limit accurate and timely evaluation of remotely located contingencies whose impact could propagate through long distance at the speed of electromagnetic waveform. Without sufficient wide-area coordination, multiple local remedial actions may compete, instead of collaborate, with each other, resulting in deteriorate impacts such as cascading failures or blackouts [13].

Moreover, the cyber-integration introduces new challenges. Most field devices and systems are not designed with sufficient security features against malignant events, particularly from the cyberspace. As the cyber-integration exposes the system to access points and resources in the cyberspace, investigations have been revealing vulnerabilities, both unknown and zero-day, in the emerging smart grid. The lack of sufficient protection against coordinated cyber-attacks could be catastrophic, as illustrated in the cyber-attack on a Ukraine regional grid [14]. Intelligent and automated systems, which have been designed to enhance the system security and reliability, maybe turned as weapons against the smart grid itself. With all these emerging threats, the traditional power system security merits an in-depth overhaul in the era of smart grid.

2.2.2 Cybersecurity: The cybersecurity has been identified as a major component in the development of smart grid [15]. Principles of confidentiality, integrity, and availability (the CIA triad) have been established for the information security in the system. Intrusion detection systems (IDSs) and firewalls have been deployed to defend control centres and field devices against external intrusions. Secure protocols have also protected the SCADA communications within and between control centres, substations, and actuators. Secured wired and wireless networks have also provided trustworthy communications for the emerging PMU and AMI systems.

Meanwhile, the cybersecurity for the smart grid also needs to further accommodate physical properties, requirements, and dependencies of power systems. For instance, though it is common to deny access to an account after a number of failed log-in attempts, it is mostly unacceptable in power system control systems. Attackers may utilise the mechanism to lock operators out of the system that will result in disastrous consequences. Moreover, anomaly and signature-based IDSs also need to adapt to emerging and diversifying patterns in the smart grid to effectively identify the malicious attempts. Last but not least, the RT data streams in the smart grid also pose big data challenges to the cybersecurity analysis. Similar to the physical security, there is an urgent need to incorporate physical aspects into the cybersecurity of the smart grid.

2.2.3 CP security: A secure smart grid is contingent on the integrative security that combines the strength in both physical and cybersecurity analysis against both inadvertent and malignant events. Vulnerabilities and contingencies shall be investigated on a broader spectrum. The causes, processes, and consequences across the CP spaces shall be comprehensively analysed with consideration of the interdependence and interoperability therein. Smart grid operators should be aware of the risks of measurements and commands corrupted by attackers externally and internally. Mitigation and restoration effort need to be guided with adequate security awareness to avoid secondary damages in the post-attack systems.

In security analysis, critical vulnerabilities are often revealed through scenarios where attackers are characterised with feasible resources, knowledge, and objectives. The investigation of attack schemes often serves as the first step to establish security in a vulnerable system. While it is impractical to exhaust all potential attack schemes, the worst-case analysis is of practical meaning to understand the feasibility and impact of a potential attack threat. The extensive investigations into the smart grid security have revealed a significant number of attack schemes that could exploit critical vulnerabilities with severe disruptions and damages. The understanding of these schemes is critical to establish and enhance the CP security of the existing systems and technologies in the smart grid; it will also help direct the effort to discover new vulnerabilities and solutions for the emerging CPS in this critical infrastructure.

3 CP attacks on the smart grid

3.1 Overview

In this paper, we refer to CP attack as the intrigue schemes exploiting the vulnerabilities in the CP structure of the smart grid. Although dedicated attacks on either cyber or PSs also pose threats to the system, investigation on the integrative CP attacks is an emerging yet critical topic that remains largely unclear. The interconnection of millions of field devices has created a huge attack surface while associated vulnerabilities be remotely located across the CP domains; moreover, the interfaces in-between the CP structures are also vulnerable to attacks launched from both domains.

Fig. 2 illustrates a typical CP structure of smart grid. The CP loop of information and operations can be compromised at the control centres and systems, two-way communication channels, and the physical power systems. The vulnerability of this structure has been illustrated in the recent incidence of Ukraine power grid attack in 2016 [14]: malware injected from the communication channels allowed the attacker to obtain illegal access to the control centres. The information was collected subsequently to determine the critical lines in the regional grid. Malicious commands were then sent to trip these lines that led to a widespread power blackout. The control system was further hacked to delay the restoration process.

Knowledgeable attackers can directly exploit vulnerabilities of control systems to exert immediate and significant impacts in the smart grid. Depending on the target systems or policy, the impact of control-based attacks ranges from transient voltage and frequency instability, steady-state line overloading and load shedding, to massive blackouts resulting from cascading failures. An introduction to the control systems in smart grid and their attack-resilience can be found in [16], and a generalised control-attack model has been developed in [17]. Measurement-based attacks pose another critical threat in the smart grid. Instead of directly manipulate control signals, attackers can compromise the measurements to weaken situation awareness by concealing the occurrence of disturbances or mislead control actions by reporting non-existing contingencies. Both types of attacks are within the scope of CP attacks discussed in this paper.

Two types of factors are commonly considered in the design of a critical attack scheme: the cost of the attacker and the cost of the defender. For the attacker, the costs typically include the resources and knowledge required to launch the attack; in many cases, the risk of being detected is also included. For the defender or operator, the costs typically comprise from equipment damages, power outages, and economic losses. The rest of this section will unfold the attack schemes on generation, transmission, distribution, and electricity markets, respectively.

3.2 Generation system attacks

Interconnected power systems are managed by corresponding control areas, among which redundant power generated in one area flow along the tie-lines into another. The power generation in each control area is required to meet the dynamic load demand and the net interchanges so the load-generation balance can be maintained. To this end, the AGC has been widely implemented in modern generation systems. A functional diagram of the AGC is illustrated in Fig. 3.

An AGC system consists of two major functions: (i) the load-frequency control (LFC) that maintains the load-generation power balance and system frequency; (ii) the ED that distributes the generation among generators with minimal operating costs subject to stability and security constraints. Since ED does not directly issue control commands to the system, we will focus on the LFC-related attack schemes herein.

The LFC uses a primary controller to govern turbine speeds and adjust the generator outputs. In addition, a supplementary/secondary controller is employed to maintain system frequency based on the area control error (ACE). The ACE is obtained as a function of inter-area power interchanges ΔP_{TL} and system frequency deviations Δf

$$\mathrm{ACE} = \Delta P_{\mathrm{TL}} - \beta\Delta f \qquad (1)$$

where β is a scale factor. In normal operations, the value of ACE in each control area should be minimised toward zero.

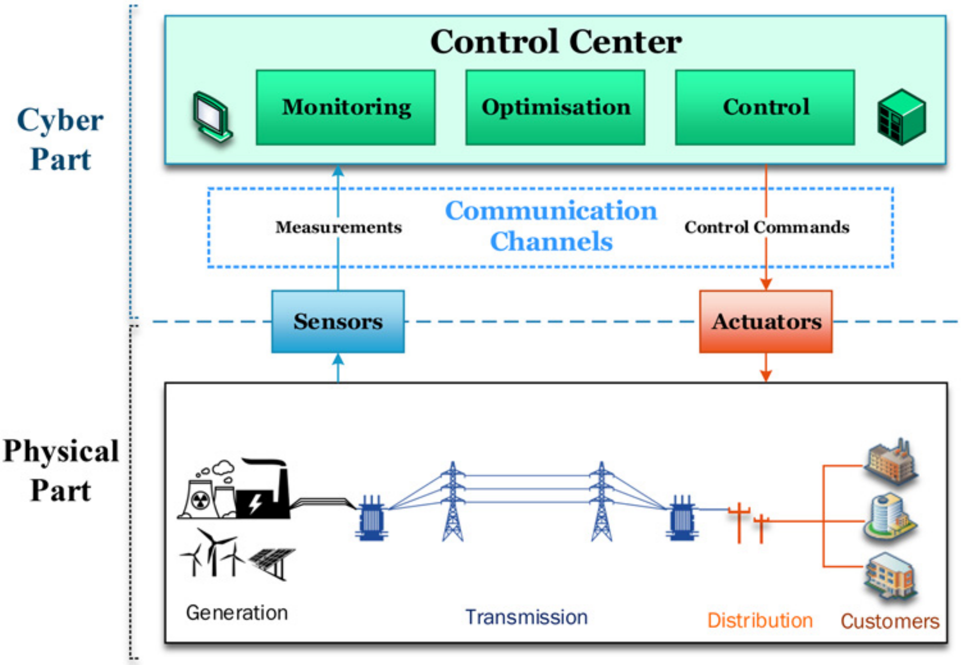


Fig. 2 *Typical CP structure in the smart grid: an integrative system with cyber and physical parts*

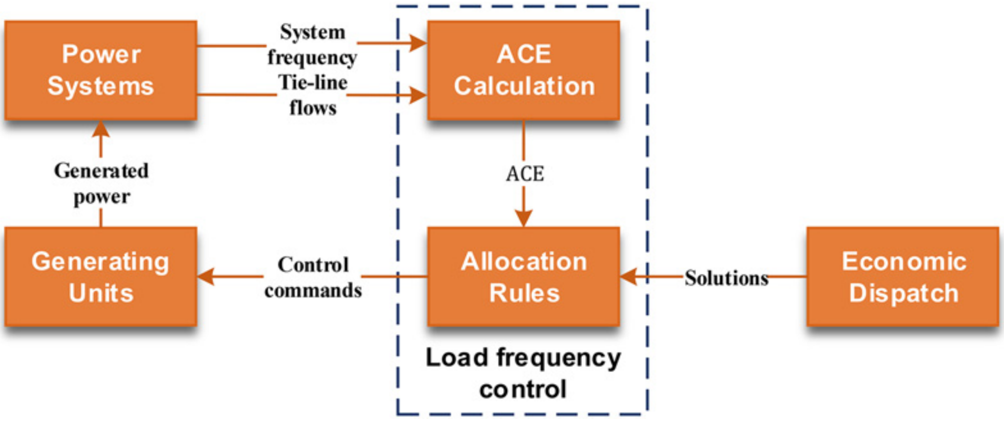


Fig. 3 *Functional modules in the AGC control loop based on [18]*

The Aurora attack is a test scheme that exploits the vulnerability in the primary controller of AGC [19]. In the original test conducted by the Idaho National Lab, an assumed cyber-attacker applies fast opening and closure of the circuit breakers of a generator. When the actions are conducted within a critical time window, the generator became desynchronised and was ultimately destroyed. The impacts of the Aurora attack range from a short-term power outage to a long-term generation deficiency. An Aurora-like CP attack with incomplete information of the power system has been subsequently developed [20].

CP attacks on the input of secondary controller have also demonstrated feasible impacts on power system frequency stability. Four typical manipulations on the AGC input, i.e. scaling, ramping, pulse, and random attack, have been investigated in [21]. The investigation has demonstrated that the attacked inputs have effectively misled the LFC to incorrectly perform under-frequency load shedding in response to a fake frequency deviation. In addition, a malicious attacker can also induce substantial instability in the generation system by exerting significant loss [22] or delay [23, 24] of the measurement packets sent to the AGC.

A reachability analysis has revealed that malicious control signals sent by the LFC will cause inter-area power swinging in the system [25]. The swinging will mislead protective relays to trip generation units from the grid, leading to power shortages and/or outages as in the Aurora attack. Further investigation has proposed a malicious control policy that is robust against incomplete information and model uncertainty [26]: the incomplete information can be addressed by Markov chain Monte Carlo simulations and the model uncertainty is addressed by the feedback linearisation.

3.3 Transmission system attacks

Transmission systems are responsible for the delivery of generated power across long distance through transmission lines and substations. In the meantime, voltage regulations are also operated in transmission systems. Protective relays and circuit breakers are deployed to cut off overloaded lines, generators, and load demands in emergent situations. The multitude and criticality of the transmission systems have inspired a large number of investigations on the potential CP attack schemes targeting the control and monitoring systems for power transmission.

3.3.1 Interdiction attacks: The interdiction analysis is among the earliest investigations of power transmission system vulnerability under large-scale malicious attacks [27]. An interdiction refers to the tripping of lines, transformers, generators, buses, and/or substations in the transmission grid. In practise, the interdiction can be conducted directly by manipulated control commands or indirectly by false measurements. On the basis of a steady-state model, a bi-level max–min optimisation problem for the interdiction analysis has been formulated as

$$\begin{aligned} &\max_{\boldsymbol{\delta}\in\Delta}\min_{\boldsymbol{P}} \quad \boldsymbol{c}^{\mathrm{T}}\boldsymbol{P} \\ &\quad \text{s.t.} \quad g(\boldsymbol{P},\ \boldsymbol{\delta}) \le \boldsymbol{b} \\ &\boldsymbol{P} \ge \boldsymbol{0}. \end{aligned} \tag{2}$$

where an attacker leverages the interdiction to maximise the system operator's minimal costs of operation and load shedding. $g(\boldsymbol{P},\ \boldsymbol{\delta})$ are the OPF constraint functions with an upper-bound vector $\boldsymbol{b}$, $\boldsymbol{c}$ is a vector of linearised cost factors, and $\boldsymbol{P}$ are the power system dynamics subjected to physical constraints. The inner minimisation solves an OPF problem in normal operations, and the outer maximisation solves the optimal interdiction as a binary vector $\boldsymbol{\delta}$ in the complete interdiction set Δ. The solutions can be obtained by mixed-integer bi-level programming [28, 29], greedy search [30], game theory [31], and generalised Benders decomposition [32]. An interdiction scheme targeting wind farms in the smart grid through vulnerabilities the SCADA/EMS system has been recently proposed [33].

While interdiction has been modelled as multiple concurrent tripping in the above investigations, sequential attack schemes have revealed the risks of blackout resulting from multi-line interdiction [34, 35]. As the timing and order of interdiction are non-trivial challenges to the formulation of an optimisation problem [34, 35], data-driven approach based on reinforcement learning [36] and heuristic approach based on risk graph [37] have been proposed to search for the critical attack sequence. Both sequential schemes have identified effective schemes to exploit the cascading failure vulnerability that leads to massive blackouts.

3.3.2 Complex network (CN)-based attacks: A notable number of investigations have been developed based on CN theories [38]. In general, the CN-based attacks have employed the interdiction as the means of attack; however, it is commonly assumed that the attacker does not possess the knowledge of the RT operational information (the analogue measurements); instead, the attacker can only access the information of system topology (the status measurements). Interconnected power grids are modelled as graphs of nodes (substations) and edges (lines) with designated physical properties. Topological and structural information are then utilised to identify the most-vulnerable components in the transmission system, which can be further visualised intuitively [39, 40]. A comparison has been summarised in Table 1 and illustrated examples on the IEEE 39-Bus New England Test System have been provided in Fig. 4.

The merit of investigations on CN-based attacks is two-fold: (i) the information required to launch a fully informed attack maybe inaccessible or incomplete; the obtained information may also become obsolete; (ii) a devastating attack does not necessarily rely on the full knowledge of the system dynamics; publicly and

Table 1 Comparison of attacker's knowledge in different CN-based models

Categories	System models	Basic information	Vulnerability metrics
topological	undirected graphs	connectivity	degree, centrality betweenness
structural	hybrid/CNs	capacity of lines impedance	electrical and extended betweenness
operational	power grids	voltage/frequency power flow	stability margin load shedding

commercially available data can be used to construct effective schemes that cause catastrophic blackouts.

Among the CN-based attacks, topological models have been proposed to analyse the risk of cascaded attacks [42–46]. On top of the topological models, hybrid models have integrated topological and electrical properties to integrate structural vulnerabilities in the transmission system [47–51]. Cascaded attack schemes on substations and transmission lines based on the hybrid models have been proposed [52, 53].

3.3.3 Substation attacks: Transmission substations host multiple measurement, control, and communication facilities. A compromised or damaged substation often results in the simultaneous loss of the victim substation as well as its transmission lines. A report from the Federal Energy Regulatory Commission has suggested that, while there were over 55,000 substations in operation across the USA, the entire interconnected transmission system could suffer a major blackout when coordinated attacks had been launched on as few as nine transmission substations [54].

An early investigation on substation network security has demonstrated that an attacker is capable of penetrating multi-layers of firewalls and password protections to gain full control of a substation [55]. Credible impacts of multi-substation intrusions have been subsequently evaluated in [56], and the potential risks given consideration of cascading failures under multi-substation attacks have been demonstrated in [57]. As shown in Fig. 5, the clustering-based vulnerability analysis can effectively identify the most-vulnerable victims in a bulk power grid.

Within a compromised substation, the voltage control loop of flexible alternating current (AC) transmission system becomes vulnerable to malicious attacks [58]. Malicious messages can be injected to manipulate the configuration of the voltage controllers that results in voltage violations and oscillations in the system [59]. Detailed simulations of typical substation attacks have been conducted in [60], and the cybersecurity issues of substation automation systems have been comprehensively analysed [61, 62].

3.3.4 CP switching attacks: The switching attack is another family of CP attacks developed against the power transmission systems [63–66]. Circuit breakers can switch the transmission

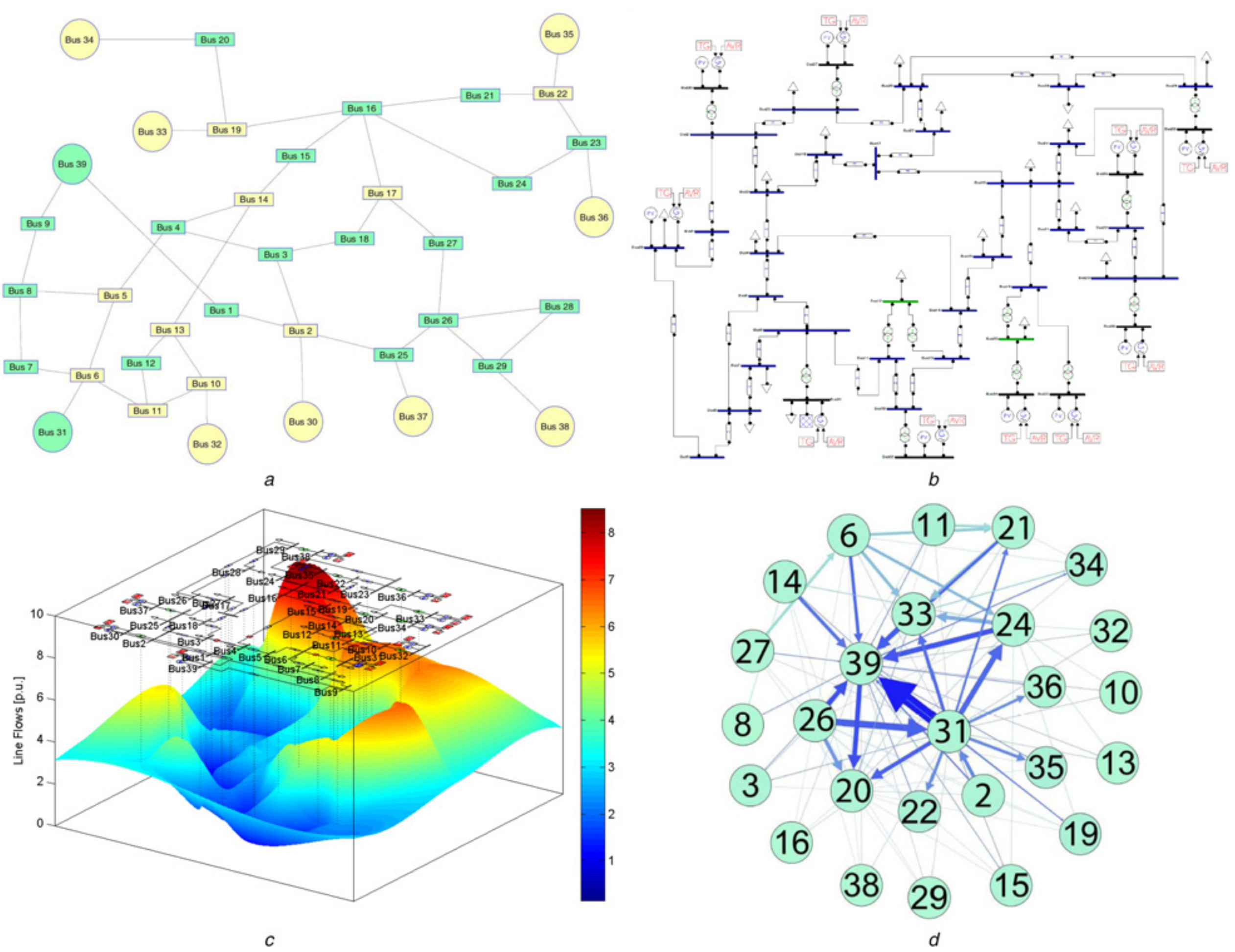


Fig. 4 *Knowledge of the transmission grid: from topological information to vulnerability analysis*

a Topological information: Connectivity of the system is shown by its topology, where generation substations are highlighted as circles and distribution substations are shown in green, respectively

b Structural information: Static generation and transmission parameters are included into the one-line diagram [41]

c Operational information: The per unit active power flows are included and shown in the three-dimensional contour map [41]

d Vulnerability visualisation: A risk graph is constructed to conduct sequential substation attacks [39]

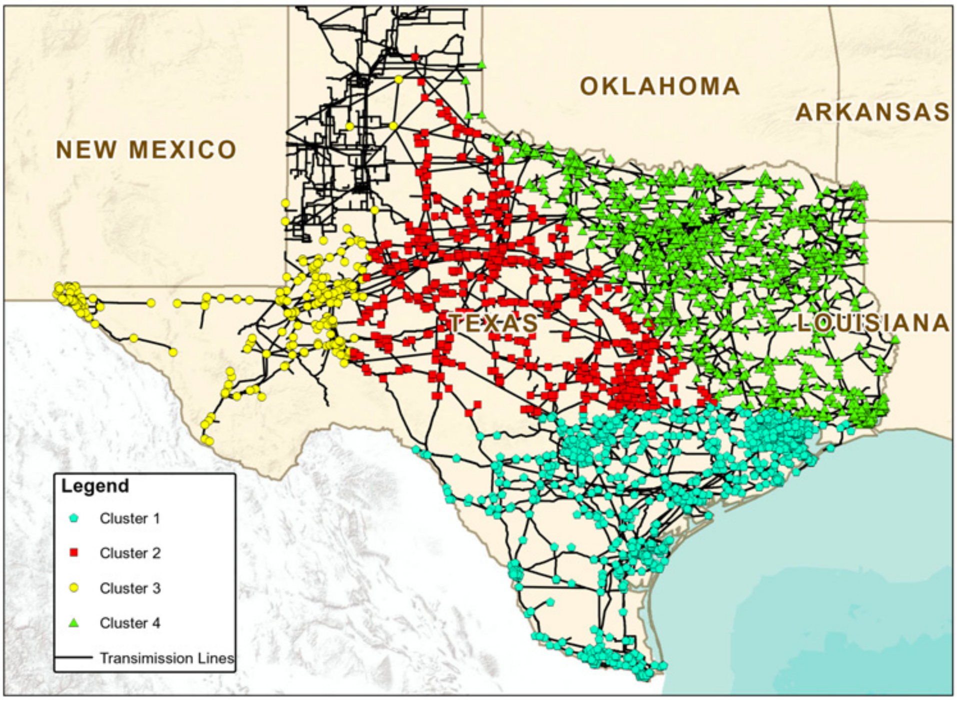


Fig. 5 *Self-organising map (SOM) based analysis of multi-substation attacks [57]. Distant substations from each of the coloured self-organised regions form a critical victim set that could result in massive blackouts in the system*

systems between complex discontinuous dynamics. Given the system state x, the switching signal $s(x,\ t)$, and two distinctive system dynamics f_1 and f_2, the non-linear power system can be presented by the following variable structure system [67, 68]

$$\dot{x} = \begin{cases} f_1(x,\ t) & s(x,\ t) \geq 0 \\ f_2(x,\ t) & s(x,\ t) < 0 \end{cases} \tag{3}$$

An informed attacker can issue malicious switching signals to re-configure the power transmissions based on local structure information, and the switched system is subsequently steered to a degraded or unstable operation states. With consideration of model errors and incomplete information, the investigation has shown that single switching attack will cause frequency and voltage instabilities in the system [67]. In addition, multi-switching attacks on distributed circuit breakers are able to initiate a series of cascading failures [68]. Recently, it has been shown that the switching attacks can also exploit the energy storage systems to destabilise the transmission systems [69]. Some discussion regarding the practical limitations of the switching attack have been provided in terms of sampling, quantification, and signal-to-noise ratio [70].

3.3.5 State estimation attacks: The SE is a core function in the smart grid that has been shown to be vulnerable to a large number of CP attack schemes. As shown in Fig. 6, SE is the entry function that processes the raw measurements of system topology and dynamics to obtain accurate estimation of the state variables for various subsequent EMS applications [71]. In a linear direct-current (DC) model, the fundamental SE problem can be written as

$$\boldsymbol{z} = \boldsymbol{Hx} + \boldsymbol{n} \tag{4}$$

where $\boldsymbol{z}$ is the measurement vector, $\boldsymbol{x}$ is the state vector, $\boldsymbol{n}$ is a white Gaussian measurement noise, and $\boldsymbol{H}$ is the Jacobian matrix built on system topology. The estimation problem is commonly solved by the weighted least square (WLS) method. In practise, bad data from faulty sensor and missing data will degrade the estimation accuracy. Residual-based χ^2-test and largest normalised residual test have been employed in the bad data detection and elimination (BDDE) process to remove such bad data from the measurements.

The false data injection attack (FDIA) is a notorious family of CP attacks targeting a vulnerability in the residual-based BDDE system. Assume that a malicious attacker has the ability to inject a false data vector $\boldsymbol{a}$ into the measurements, which in the form of $\boldsymbol{z}_a = \boldsymbol{z} + \boldsymbol{a}$.

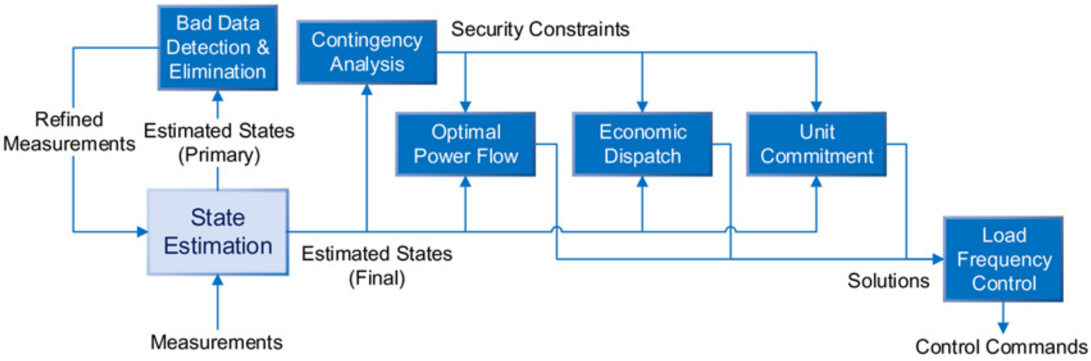


Fig. 6 *SE and subsequent functions in the EMS*

The FDIA scheme has revealed that, given the full knowledge of the Jacobian $\boldsymbol{H}$, an attack vector $\boldsymbol{a}$ undetectable by BDDE can be generated [72]. The stealth attack vector is given in the form of $\boldsymbol{a} = \boldsymbol{Hc}$, where $\boldsymbol{c}$ is the false state vector. The sufficient and necessary condition of the existence of an undetectable attack vector has been proved in [73]. While the scheme was originally proposed based on the DC model of SE, it has also subsequently extended to the AC-based SE [74]. A recent survey [75] has provided a summary of the state-of-the-art in FDIA, while this paper would like to highlight three major objectives in the existing FDIA schemes:

Objective 1: Least-effort attacks: Find the sparsest attack vector with the least number of measurements to be compromised.
Objective 2: Least-information attacks: Find the attack vector with the least required information of system topology.
Objective 3: Target-specific attacks: Find the attack vector toward a specific post-attack effect.

For Objective 1, finding the least-effort attack is NP-hard problem [76], and the solution is dependent on the system topology. To effectively identify the minimal stealth attack, schemes have been developed based on heuristic [72], greedy [77, 78], graph theoretic [79], and sparse optimisation [80, 81].

For Objective 2, investigations have revealed that an undetectable attack vector can be constructed without the complete information of $\boldsymbol{H}$. Stealth FDIA schemes with incomplete information have been developed based on graph method [82] and data-driven approaches [83, 84]. Even without the knowledge of $\boldsymbol{H}$, investigations have shown that historic measurements can still be used to construct an undetectable FDIA [85, 86].

For Objective 3, FDIA has been utilised to exert specific damages. The maximal SE error can be obtained by solving a potential game with a minimal detection rate [87]. Errors can be propagated into the OPF solutions through customised FDIA schemes [88, 89]. Line overloading can be further induced the erroneous OPF solution [90]. Target-specific FDIA schemes have also been developed systematically to induce load redistribution (LR) in the transmission systems and transmission congestion in the electricity markets to induce operational costs and obtain financial arbitrages, respectively. Detail introductions on both families of FDIA schemes will be provided later in this section.

Other than the FDIA schemes, it is notable that (4) also reveals other SE vulnerabilities. Instead of the measurement vector, the Jacobian matrix $\boldsymbol{H}$ can also be compromised to forge a false data [91]. Attacking the line impedance alone will also induce misinformed voltage deviations and load shedding [92]. A two-stage optimisation for undetectable state-and-topology attack has been developed in [93], which has effectively increased the risk of line outages.

In contrast to the construction of undetectable attack vectors, malicious attackers can also intentionally create detectable false data to reduce the availability of measurements. As the BDDE consistently removes bad data from the measurements, an attacker can manipulate the measurements to frame good data so they would be incorrectly removed [94]. In contrast to the FDIA schemes, framing requires no information on the topology or parameters of the system; a subset of the measurements provides sufficient information to manipulate the normal data into bad data. The scheme effectively increases the SE error by an arbitrary degree while the number of measurements to be corrupted has been significantly reduced.

An advanced jamming strategy has been proposed to obtain an optimal scheme in the presence of protected measurements based on recursive min-cut [95]. Further investigation has indicated that the jamming attack is effective unless all measurements have been secured [96]. In addition, the availability of status data can also be reduced by the jamming attack, in which attacking a single circuit breaker on a transmission line could effectively perturb the SE without corrupting any measurements [97].

3.3.6 Load redistribution attacks: LR attack is a variant of target-specific FDIA schemes [98, 99]. With the knowledge of system topology and dynamics, the injected false data can be crafted intentionally to redistribute individual bus load in the system without changing the overall load demands. Both the location and the quantity of the stealth injection can be solved precisely by the proposed schemes to induce immediate and delayed operational costs from the redistributed load demand. A concept of attacking region has been proposed to construct an LR attack with incomplete information [100]. The attacking region can be effectively localised into the vicinity of a target transmission line [101]. The concept has also been utilised to identify attack vectors in the AC SE with incomplete information [102]. A recent investigation has validated the non-negligible impact on the power system reliability from the LR attacks [103].

Investigations have demonstrated that the LR attacks can be utilised to construct coordinated multi-stage schemes [104–106]. First, a designated scheme has been proposed to mask the occurrence of line outages to the system operator [104]. The masking attack has been further utilised to conceal line outages created by the LR attack. A bi-level optimisation problem has been formulated for this combined scheme with consideration of the defender's responses [105]. The scheme has been further developed into a tri-level optimisation problem against the security constrained ED in the EMS [106]. It has been revealed that an attacker is capable of identifying an effective scheme to create line overloading in the system, even if the operator implements a dedicated multi-solution strategy against the LR attacks. These serial LR schemes have illustrated that CP attacks can be orchestrated to compose sophisticated multi-stage schemes with severe impacts.

3.3.7 PMU attacks: Compared with the SCADA system, the PMUs are collecting more frequent and accurate measurements for the WAMPAC system [107]. Communications with GPS satellites provide time stamps to all PMUs, so that their measurements can be synchronised for significantly enhanced situation awareness in interconnected power systems. However, recent investigations have revealed that the dependence of GPS signals for synchronised measurements can render PMUs vulnerable under spoofing attacks [108, 109].

Spoofing is the malicious impersonation of a trusted device in the system, which has been used to provide fake time stamps to the PMUs [108]. Two types of errors induced by corrupted time stamps have been identified: the phase angle error and the time of arrival (TOA) error. The phase angle error will mislead fault detection and location of transmission lines with an amplitude modulation and create false stability margins with incorrect Thevenin equivalents; the TOA error will result in miscalculation of disturbance event locations that delays or misleads mitigation and restoration effort. The spoofing can also alter the clock offset of a receiving PMU to increase both false alarms and false negatives in voltage stability monitoring systems [109].

3.4 Distribution system/customer-side attacks

Millions of smart meters have been installed in the AMI systems across the USA and more are on the way. These smart meters provide RT two-way communication between customers and the utility. In general, the AMI system is composed of smart meters, data concentrators/aggregators, and AMI head-ends, which has been hierarchically deployed from customers to the distribution systems [110]. Owing to budget and hardware limitations, smart meters only carry limited or light-weight security mechanisms against malicious attacks [111, 112]. This makes them vulnerable and frequent targets of CP attacks. Although each meter has limited impacts on the system stability when compromised, the CP threat of AMI attacks is not negligible, particularly when a cluster of smart meters has been attacked [113].

To date, energy thefts [114, 115] and information/privacy leakages [116–119] have been identified as the most prominent threats to the AMI system. The former will result in economic losses at various scales, while the latter maybe exploited to infer customer behaviours and personal information. In addition, the threat of denial-of-service attacks is also a critical issue in the smart grid, as it limits the availability of reliable and available measurements [120]. By compromising any smart meters, an attacker can exploit the ubiquitous two-way communication to flood the AMI system with malicious packets, which may effectively paralyse the metering networks [121, 122].

3.5 Electricity market attacks

In the smart grid, the price of electricity is determined by the locational marginal prices (LMPs) from the day-ahead and RT markets, which are both obtained by solving respective OPF problems. Recall that in Fig. 6, the solution of OPF is dependent on the network topology and estimated system states; as a result, the LMP is also vulnerable to SE attacks [123].

CP attack schemes exploit the RT LMP vulnerability in the transmission congestion management. A transmission congestion occurs when the power flow on transmission lines reach the line capacity (i.e. the thermal rating limit). To meet the electricity request under congested conditions, generators in the vicinity will be temporarily dispatched, which are often considerably more costly. As a result, the price of electricity is affected dramatically on an imminent congestion. An attacker can leverage this mechanism to gain illegal profit from the price margin before and after the attack or induce frequent transmission congestion to impose expensive operations to the system.

Investigations have identified several feasible schemes targeting the RT markets. Attacks schemes have been developed based on vulnerabilities in virtual bidding mechanism [124], system topology information [73], generation ramping limits [125], and distributed energy management [126]. The sensitivity of LMP to the corrupted sensor data has been investigated in [127], and an index to quantify the impacts of electricity market attacks has been proposed [128]. Instead of manipulating the line flow in the measurements, the line ratings can also be attacked to induce transmission congestion [129]. The RT pricing system is also vulnerable under data integrity attacks, e.g. scaling and delay attacks, which will cause demand/price fluctuations as well as increase system operating costs [130]. A stealth scheme to generate arbitrary pricing signals has been further proposed in [131]. In addition to the impacts on the control and management side, the hijacked pricing information can alter the load demand of customers, which will retroactively create overloading and instabilities in the system [132].

4 Defence against CP attacks

The extensive investigations on potential CP attack schemes have allowed grid operators to establish various defence mechanisms, which have been commonly orchestrated in three stages: protection, detection, and mitigation. In this section, we will review the generic and attack-specified defence strategies against the CP attacks as follows.

4.1 Protection

Generic protection against CP attacks relies on the establishment of secured communication, the preservation of critical information, and the alleviation of exposed vulnerabilities. Since the early discussion on the challenges of cybersecurity in power systems [133], innovative systems, protocols, and technologies have been developed for the protection of smart grid security. These effort have been reiterated in a number of comprehensive reviews [134–137]. The secure communication in smart grid can effectively dissolve a majority of the CP attack threats. While it is difficult to conduct field tests on the operating power systems, dedicated security testbeds have been developed to validate the attack schemes and facilitate the development of security enhancements [138–144]. A framework has also been developed to evaluate the exposure of physical components in the cyberspace [145].

Meanwhile, a number of attack-specific protections can be implemented strategically to reduce or erase certain CP attack threats. The threat of FDIA schemes can be effectively reduced or eliminated by the protection of a few critical measurements, as the stealthiness is dependent on the number of measurements being compromised. The protection can be achieved by the installation of secured or encrypted devices on critical locations so the protected measurements are immune to the injections. To identify these locations, greedy algorithms have been proposed to heuristically search for the critical subsets of measurements [77, 146]. Mixed-integer linear programming optimisation [147, 148] and game-theoretic approach [149] have been proposed with consideration of the costs of attackers and defenders, respectively. The optimal locations can also be obtained by graph-based approaches, which also provide suboptimal solutions for situations where the complexity is a major concern [150]. Protection strategies for critical measurements against the FDIA-based LR attacks have also been proposed in [98, 99].

Alternatively, protection against FDIA can be achieved through the preservation or rearrangement of crucial information in the system. Covert power network topological information can effectively enhance the security of SE when a subset of the line reactance has been preserved from the attacker's knowledge [151]. Re-configuration of the topological information in the cyberspace can also eliminate the risk of FDIA in large-scale distribution systems [152]. Recent development of distributed SE systems has also exhibited promising attack-resilience for the protection of SE measurements [153].

For the AMI systems, secure key management and distribution mechanisms have been developed as the most effective protection against unauthorised accesses to smart meters [154–156]. In addition, game-theoretic approach for the optimal deployment of encrypted smart meters with limited budget [157] and Markov decision process (MDP)-based preventative maintenance strategy [158] have both been developed for the protection of smart meters.

4.2 Detection

Despite the protection effort, an attacker will still have the advantage to initiate attacks on poorly protected components. In case of such protection failures, IDSs are employed as the major defence mechanisms at the second stage. Signature- and anomaly based IDSs have been developed against known and unknown attack threats, respectively, which are deployed at various layers and locations to detect the traces of imminent attacks. These early warnings allow system operators to react with proper countermeasures and/or emergency plans so the attack impacts can be minimised.

At the control centres, generic detection mechanisms have been developed and integrated into CPS control systems. Both model-based [159] and game-theoretic [160] approaches have been developed to provide effective security enhancement against the CP attacks. Physical watermarking of control inputs is a promising technique to authenticate the integrity of control systems [161]. With the physical watermarking, an artificial control noise known only by the operator is injected to produce predictable measurement outputs from the controlled systems. Since the noise is unknown to the attacker, the pattern between the noisy-input and predicted output will be altered and subsequently detected in the presence of an attack. A run-time semantic analysis has also been developed to provide early warnings on altered control commands in the SCADA system [162]. With an efficient look-ahead power flow analysis, the semantic analysis simulates the execution consequence of control packets to issue alerts if the execution would result in unfavourable impacts such as line outages.

A model-based IDS has been developed against the input attacks on the AGC system [21]. The IDS utilises RT load forecast to predict the ACEs over time, and their performances are compared with that of the actual ACEs obtained. With statistical and temporal characterisations of these performance, anomaly detection in the IDS is able to detect scaled and ramped inputs before they are sent into the AGC system.

Interdiction in the transmission system maybe observed by effective online contingency screening [163]. The nature of these tripping can be further examined by IDSs deployed at substations. A standard-specific IDS for automated substations has been proposed in [164]. A dedicated IDS has been developed to identify temporal anomalies induced by multi-substation attacks [56]. Host-based and network-based IDSs have been integrated in an innovative strategy against simultaneous multi-substation intrusions [165].

While the threat of PMU attacks has only been revealed recently, detection mechanisms have been developed against both manipulation and spoofing attacks on PMU. Innovative IDSs have been proposed against generic manipulations of PMU data based on whitelist/behaviour [166], network topology [167, 168], and data mining [169]. A comprehensive IDS across both physical and cyber layers has been developed to identify the PMU data attacked by the GPS spoofing [170].

Hierarchical IDSs have been developed against CP attacks on the AMI systems based on behaviour rules [171] and data stream mining [172]. A distributed multi-layer IDS has been proposed in [173], and an early warning system has been developed in [174]. Active inspections by the service providers and mutual inspections between the providers and the customers have been developed to effectively detect attacked smart meters [175, 176]. To hold a malicious meter accountable in home area networks and neighbourhood area networks, an effective peer-review strategy has been developed in [177]. To detect energy thefts, an evaluation of IDSs has been conducted in [178], while machine learning-based IDSs have been recently developed in [179, 180].

Detection mechanisms against the FDIA schemes have been developed along multiple directions. An integrative Kalman filter-based detector against both bad data and false data has been developed in [181]. Instead of a WLS estimator, a Kalman estimator has been implemented in this innovative mechanism. A χ^2-detector is then used to detect the bad data and an Euclidean detector is used to detect the false data. High-performance FDIA detectors have been proposed based on adaptive cumulative sum detection [182] and quickest detection [183]. An online anomaly detection considering load forecasts, generation schedules, and synchrophasors has also been developed in [184]. Furthermore, machine learning approaches have been proposed to identify the false data based on statistic information. Both supervised distributed support vector machine based on alternating direction method of multipliers and semi-supervised anomaly detection based on principal component analysis have been developed recently to classify the false data from the normal data even with incomplete measurements [185]. A variety of supervised and semi-supervised classifiers have also been evaluated in [186], which have displayed robust performances in both online and offline scenarios. Using historic data, generalised likelihood ratio detector can provide the optimal detection against weak FDIA schemes when the attacker could not compromise the minimal required number of measurement to construct undetectable FDIA schemes [79, 187].

4.3 Mitigation

When signs of an attack have been confirmed, mitigation efforts are made by the system operator to minimise the potential disruptions and damages. If the attack has been cleared from the system, existing mitigation and restoration mechanisms can effectively resume the secure and reliable power system operations. However, if the attack threat has not been resolved, the operator needs to consider persisting malicious attempts in the system. In such interactive scenarios, mitigation strategies are commonly modelled and solved by bi-level optimisation or game-theoretic approaches.

An attacker–defender game has been developed against generic attacks on power system components [188], and a zero-sum game between an informed cyber-attacker and a system operator has been proposed under different network configurations [189]. To deceive an attacker with misinformation so the attack damage can be reduced, a zero-sum Markov game has been proposed in [190], based on which a scalable solution has been further developed [191].

For mitigation against interdiction, a tri-level optimisation has been developed, which introduces countermeasures of the defender in a third-level minimisation into the problem [192]. Alternatively, line switching has been proposed as an effective strategy to mitigate the interdiction, which is introduced directly in the lower/inner-level of the bi-level optimisation. The solutions with the minimal cost of the operator can be obtained by genetic algorithm [193], Benders decomposition [194], and single-level reformulation [195]. In addition, MDP has also been integrated to model the attack-defence interaction in a substation intrusion [196]. By modelling a successful intrusion as a probabilistic event, the investigation has formulated a competition to gain access of multiple substations between the attacker and the operator. The optimal solution is obtained with consideration of system parameters, the attacker's resources, and the operator's budgets.

A coordinated mitigation framework for the mitigation against FDIA has been developed in [197]. Security metrics have been proposed within the framework to evaluate the importance of substations and measurements. Strategies in both the network layer and the application layer have been developed to mitigate the threat of attacks. Game-theoretic approach has also been applied to achieve an optimal equilibrium given the resources and costs of attackers and defenders [149], where a notable strategy has been identified for the multi-attacker scenario: the defender can use the game-theoretic approach to achieve a critical equilibrium, at which the impacts from multiple attackers can be cancelled even when the operator has no knowledge of the attacker's intentions. The zero-sum game approach has also been applied for the mitigation of attacks on electricity market where the attacker is given limited resources [198].

5 Opportunities and challenges

The smart grid encompasses a vast diversity of devices and facilities that are vulnerable under CP attacks. Despite the extensive research effort reviewed in this paper, the vulnerability and security of a large portion of components in the smart grid remain to be carefully examined in the presence of a potential attacker. Critical mechanisms such as the unit commitment, demand response, and distributed intelligence may also become targets of malicious attacks, for which the potential damages remain unknown to date. Large-scale integration of DER including energy storage, distributed generations, and electrical vehicles will have strong impacts on the stability that can be exploited. In addition to the expansion of vulnerability screening and assessment, we would also like to highlight four critical opportunities and challenges in the future investigation of CP attacks as follows.

5.1 Influence of interdependence

Interdependence is a driving force behind the development of smart grid security. To date, the majority of CP attack schemes have exploited the interdependence to launch attacks in the cyberspace and induce damages to the PSs. Meanwhile, the physical attacks targeting cybersecurity have been less investigated, but the threats can be nevertheless devastating when the dependence of PSs is exploited. Most cybersecurity mechanisms have assumed the availability and reliability of electrical power to operate designated electronic devices. Under physical attacks, these devices can be damaged or disabled by intentional surges and outages of electricity. Such vulnerabilities should also be integrated into the investigation of the CP security in the smart grid.

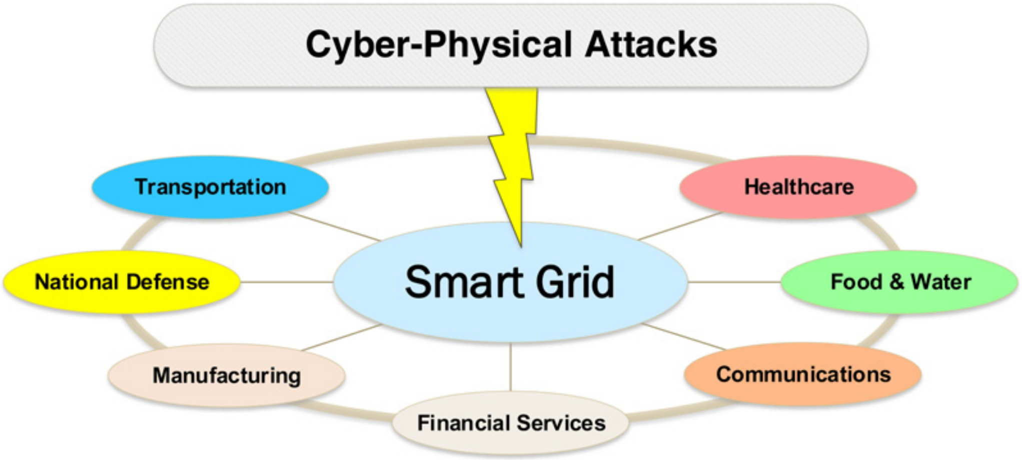


Fig. 7 *Example of interdependent sectors vulnerable under CP attacks on the smart grid*

It should also be noted that vulnerability of CP interdependence maybe exploited frequently and interactively by complex intrigue schemes. Assume that an attacker has launched an attack and successfully induced a power outage: during this outage, the security mechanism on some critical field devices can be compromised, and the parameters and data stored therein maybe manipulated. Once the power has been restored, the attacker can either utilise the compromised device to access more information from the cyberspace or induce further damages into the physical system. To date, there are still limited investigations into this kind of schemes that repeatedly exploit the vulnerability of the CP interdependence.

On a broader sense, the interdependence does not only exist between the cyber and physical spaces within the smart grid. Through cyber and physical interconnections, other critical infrastructures are also vulnerable under CP attacks on the smart grid, as illustrated in Fig. 7. Investigations on the cross-infrastructure interdependence have largely remained to be conducted.

5.2 Temporal vulnerability

CP attacks are largely equipped with the ability to launch multiple remote and coordinated intrusions. While most of the multi-target schemes reviewed in this paper have constructed the attacks in a simultaneous manner, time has been less frequently considered as a relevant factor mostly due to the complexity of time-domain analysis. However, the timing of multiple attacks, particularly for those launched in a sequential manner, is critical to the potential impacts of CP attacks in a realistic scenario.

For instance, attacks launched during the peak load and the normal load will most likely result in different impacts on system stability, which shall be responded with different levels of attack awareness. In addition, when an attack vector is successfully injected into the system, the duration it remains undetected and uncleaned will also have a substantial influence of the damage it can exert in the system, as discussed in the feasibility of Aurora attack [19]. In addition, as revealed in the sequential interdiction on transmission lines and automated substations [35–37], the timing and ordering of coordinated sequential attacks will also play an important role in the eventual blackouts. With a proper timing, not only will concurrence be removed as a stringent condition of attack feasibility, but the early warnings of an imminent large-scale attack can be diluted. Nevertheless, informed sequential attacks have still demonstrated the ability to cause greater damages than the concurrent counterparts.

5.3 Imperfect attacks

Investigations of CP attacks are often conducted in the worst-case scenario to fully evaluate their impacts on the system. Assumptions of the worst-case scenario usually include the full access of resource, knowledge, and/or control of the system as well as a well-defined intention of the attack objective. These ‘perfect attacks’ are crucial to reveal the maximal damages an attacker may induce in the system.

However, in terms of practical and usable security, a perfect attack is usually infeasible. The attacks that an operator may face more frequently are the imperfect attacks, some of which could be completely uninformed. While incomplete information, hierarchical information, and limited resources have been considered in some of the investigations, the evaluation of system vulnerability under imperfect attacks need to be incorporated as a standard feature to investigate and grade the threats of all feasible attack attempts. More specifically, the level of security should be evaluated with respect to the level of resource, knowledge, and control compromised by the attackers, so that corresponding level of warnings and responses can be effectively developed.

5.4 Attack-resilient designs

As it is impossible to enumerate or eliminate every potential attack threats for a perfectly secured smart grid, the concept of attack-resilience should be integrated against the permanent presence and evolution of threats. Additional security features and mechanisms against the most common attacks should be incorporated into the design of measurement and control systems. The costs of attack-resilient designs should be balanced with that of emergent situations, so that a proper trade-off between economic concerns and broader impacts can be achieved. Meanwhile, security analysis should be aware that the development and deployment of advanced and distributed intelligence are double-edged: the intelligent systems are both targets of CP attacks as well as tools to defend against them. Along with the upgrades being made in generation [199], transmission [200], and distribution systems [201, 202] of the smart grid, security analysis should integrate the impacts of these upgrades, enhance their resilience against potential attacks, and utilise their potentials to improve the security.

6 Conclusions

CP security is at the core of modern CPS. In this paper, we focus specifically on the CP attacks and defences in the smart grid by providing a comprehensive and systematic review of the state-of-the-art in the field, ranging from security foundations, attack schemes, defence strategies, to a wide range of opportunities and challenges. As smart grid has become one of the key technological and economic developments around the globe, this survey provides critical insights into enhancing energy security by maintaining the integrity of smart grid under complex CP attacks.

7 Acknowledgment

We gratefully acknowledge the support from the National Science Foundation through grants CNS 1117314 and ECCS 1053717.

8 References

1 Farhangi, H.: 'The path of the smart grid', *IEEE Power Energy Mag.*, 2010, **8**, (1), pp. 18–28

2 Sridhar, S., Hahn, A., Govindarasu, M.: 'Cyber–physical system security for the electric power grid', *Proc. IEEE*, 2012, **100**, (1), pp. 210–224

3 Wood, A.J., Wollenberg, B.F.: 'Power generation, operation, and control' (John Wiley & Sons, Hoboken, NJ, 2012, 3rd edn.)

4 National Institute of Standards and Technologies (NIST): 'Framework and roadmap for smart grid interoperability standards – release v3.0' (NIST Special Publication, Gaithersburg, MD, 2014)

5 Gungor, V.C., Sahin, D., Kocak, T., *et al.*: 'Smart grid technologies: communication technologies and standards', *IEEE Trans. Ind. Inf.*, 2011, **7**, (4), pp. 529–539

6 Fang, X., Misra, S., Xue, G., *et al.*: 'Smart grid – the new and improved power grid: a survey', *IEEE Commun. Surv. Tutor.*, 2012, **14**, (4), pp. 944–980

7 Yan, Y., Qian, Y., Sharif, H., *et al.*: 'A survey on smart grid communication infrastructures: motivations, requirements and challenges', *IEEE Commun. Surv. Tutor.*, 2013, **15**, (1), pp. 5–20

8 Bertsch, J., Carnal, C., Karlson, D., *et al.*: 'Wide-area protection and power system utilization', *Proc. IEEE*, 2005, **93**, (5), pp. 997–1003

9 Govindarasu, M., Hann, A., Sauer, P.: 'White paper: cyber–physical systems security for smart grid'. 2012

10 Mo, Y., Kim, T.H.J., Brancik, K., *et al.*: 'Cyber–physical security of a smart grid infrastructure', *Proc. IEEE*, 2012, **100**, (1), pp. 195–209

11 Morison, K., Wang, L., Kundur, P.: 'Power system security assessment', *IEEE Power Energy Mag.*, 2004, **2**, (5), pp. 30–39

12 Moslehi, K., Kumar, R.: 'A reliability perspective of the smart grid', *IEEE Trans. Smart Grid*, 2010, **1**, (1), pp. 57–64

13 U.S.-Canada Power System Outage Task Force: 'Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations'. 2004

14 The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): 'Cyber-attack against Ukrainian critical infrastructure'. Alert (IR-ALERT-H-16-056-01), 2016. Available at url: https://www.ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

15 National Institute of Standards and Technologies (NIST): 'Guidelines for smart grid cybersecurity' (NIST Special Publication, Gaithersburg, MD, 2014). Available at url: http://www.dx.doi.org/10.6028/NIST.IR.7628r1

16 Barreto, C., Giraldo, J., Cardenas, A.A., *et al.*: 'Control systems for the power grid and their resiliency to attacks', *IEEE Secur. Priv.*, 2014, **12**, (6), pp. 15–23

17 Mo, Y., Sinopoli, B.: 'On the performance degradation of cyber–physical systems under stealthy integrity attacks', *IEEE Trans. Autom. Control*, 2016, **61**, (9), pp. 2618–2624

18 Kundur, P., Balu, N.J., Lauby, M.G.: 'Power system stability and control' (McGraw-Hill, New York, 1994, 1st edn.)

19 Zeller, M.: 'Common questions and answers addressing the aurora vulnerability'. 2011

20 Srivastava, A., Morris, T., Ernster, T., *et al.*: 'Modeling cyber–physical vulnerability of the smart grid with incomplete information', *IEEE Trans. Smart Grid*, 2013, **4**, (1), pp. 235–244

21 Sridhar, S., Govindarasu, M.: 'Model-based attack detection and mitigation for automatic generation control', *IEEE Trans. Smart Grid*, 2014, **5**, (2), pp. 580–591

22 Liu, S., Liu, X.P., Saddik, A.E.: 'Denial-of-service (DoS) attacks on load frequency control in smart grids'. Proc. Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES, 2013, pp. 1–6

23 Sargolzaei, A., Yen, K., Abdelghani, M.: 'Delayed inputs attack on load frequency control in smart grid'. Proc. Innovative Smart Grid Technologies Conf. (ISGT), 2014 IEEE PES, 2014, pp. 1–5

24 Srikantha, P., Kundur, D.: 'Denial of service attacks and mitigation for stability in cyber-enabled power grid'. Proc. Innovative Smart Grid Technologies Conf. (ISGT), 2015 IEEE Power Energy Society, 2015, pp. 1–5

25 Esfahani, P.M., Vrakopoulou, M., Margellos, K., *et al.*: 'Cyber attack in a two-area power system: impact identification using reachability'. Proc. of the 2010 American Control Conf., 2010, pp. 962–967

26 Esfahani, P.M., Vrakopoulou, M., Margellos, K., *et al.*: 'A robust policy for automatic generation control cyber attack in two area power network'. Proc. 49th IEEE Conf. on Decision and Control (CDC), 2010, pp. 5973–5978

27 Salmeron, J., Wood, K., Baldick, R.: 'Analysis of electric grid security under terrorist threat', *IEEE Trans. Power Syst.*, 2004, **19**, (2), pp. 905–912

28 Motto, A.L., Arroyo, J.M., Galiana, F.D.: 'A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat', *IEEE Trans. Power Syst.*, 2005, **20**, (3), pp. 1357–1365

29 Arroyo, J.M., Galiana, F.D.: 'On the solution of the bilevel programming formulation of the terrorist threat problem', *IEEE Trans. Power Syst.*, 2005, **20**, (2), pp. 789–797

30 Bier, V.M., Gratz, E.R., Haphuriwat, N.J., *et al.*: 'Methodology for identifying near-optimal interdiction strategies for a power transmission system', *Reliab. Eng. Syst. Saf.*, 2007, **92**, (9), pp. 1155–1161

31 Holmgren, A.J., Jenelius, E., Westin, J.: 'Evaluating strategies for defending electric power networks against antagonistic attacks', *IEEE Trans. Power Syst.*, 2007, **22**, (1), pp. 76–84

32 Salmeron, J., Wood, K., Baldick, R.: 'Worst-case interdiction analysis of large-scale electric power grids', *IEEE Trans. Power Syst.*, 2009, **24**, (1), pp. 96–104

33 Zhang, Y., Xiang, Y., Wang, L.: 'Power system reliability assessment incorporating cyber attacks against wind farm energy management systems', *IEEE Trans. Smart Grid*, 2016, **PP**, (99), pp. 1–15 (early access), DOI: 10.1109/TSG.2016.2523515

34 Zhu, Y., Yan, J., Tang, Y., *et al.*: 'The sequential attack against power grid networks'. Proc. 2014 IEEE Int. Conf. on Communications (ICC), 2014, pp. 616–621

35 Yan, J., Tang, Y., Zhu, Y., *et al.*: 'Smart grid vulnerability under cascade-based sequential line-switching attacks'. Proc. 2015 IEEE Global Communications Conf. (GLOBECOM), 2015, pp. 1–7

36 Yan, J., He, H., Zhong, X., *et al.*: 'Q-learning based vulnerability analysis of smart grid against sequential topology attacks', *IEEE Trans. Inf. Forensics Sec.*, 2017, **12**, (1), pp. 200–210

37 Zhu, Y., Yan, J., Tang, Y., *et al.*: 'Resilience analysis of power grids under the sequential attack', *IEEE Trans. Inf. Forensics Sec.*, 2014, **9**, (12), pp. 2340–2354

38 Cuadra, L., Salcedo-Sanz, S., Del Ser, J., *et al.*: 'A critical review of robustness in power grids using complex networks concepts', *Energies*, 2015, **8**, (9), pp. 9211–9265

39 Zhu, Y., Yan, J., Sun, Y., *et al.*: 'Revealing cascading failure vulnerability in power grids using risk-graph', *IEEE Trans. Parallel Distrib. Syst.*, 2014, **25**, (12), pp. 3274–3284

40 Hines, P., Dobson, I., Rezaei, P.: 'Cascading power outages propagate locally in an influence graph that is not the actual grid topology', *IEEE Trans. Power Syst.*, 2016, **PP**, (99), pp. 1–1 (early access), DOI: 10.1109/TPWRS.2016.2578259

41 Yan, J., Tang, Y., He, H., *et al.*: 'Cascading failure analysis with DC power flow model and transient stability analysis', *IEEE Trans. Power Syst.*, 2015, **30**, (1), pp. 285–297

42 Motter, A.E., Lai, Y.-C.: 'Cascade-based attacks on complex networks', *Phys. Rev. E*, 2002, **66**, (6), p. 065102

43 Holme, P., Kim, B.J., Yoon, C.N., *et al.*: 'Attack vulnerability of complex networks', *Phys. Rev. E*, 2002, **65**, (5), p. 056109

44 Rosas-Casals, M., Valverde, S., Solé, R.V.: 'Topological vulnerability of the European power grid under errors and attacks', *Int. J. Bifurcation Chaos*, 2007, **17**, (07), pp. 2465–2475

45 Wang, J.-W., Rong, L.-L.: 'Cascade-based attack vulnerability on the US power grid', *Saf. Sci.*, 2009, **47**, (10), pp. 1332–1336

46 Buldyrev, S.V., Parshani, R., Paul, G., *et al.*: 'Catastrophic cascade of failures in interdependent networks', *Nature*, 2010, **464**, (7291), pp. 1025–1028

47 Bompard, E., Napoli, R., Xue, F.: 'Analysis of structural vulnerabilities in power transmission grids', *Int. J. Crit. Infrastruct. Prot.*, 2009, **2**, (1), pp. 5–12

48 Bompard, E., Napoli, R., Xue, F.: 'Extended topological approach for the assessment of structural vulnerability in transmission networks', *IET Gener. Transm. Distrib.*, 2010, **4**, (6), pp. 716–724

49 Bompard, E., Pons, E., Wu, D.: 'Extended topological metrics for the analysis of power grid vulnerability', *IEEE Syst. J.*, 2012, **6**, (3), pp. 481–487

50 Bompard, E., Wu, D., Xue, F.: 'Structural vulnerability of power systems: a topological approach', *Electr. Power Syst. Res.*, 2011, **81**, (7), pp. 1334–1340

51 Dwivedi, A., Yu, X.: 'A maximum-flow-based complex network approach for power system vulnerability analysis', *IEEE Trans. Ind. Inf.*, 2013, **9**, (1), pp. 81–88

52 Yan, J., He, H., Sun, Y.: 'Integrated security analysis on cascading failure in complex networks', *IEEE Trans. Inf. Forensics Sec.*, 2014, **9**, (3), pp. 451–463

53 Zhu, Y., Yan, J., Tang, Y., *et al.*: 'Joint substation-transmission line vulnerability assessment against the smart grid', *IEEE Trans. Inf. Forensics Sec.*, 2015, **10**, (5), pp. 1010–1024

54 Tweed, K.: 'Attack on nine substations could take down US grid' (IEEE Spectrum, 2014). Available at url: http://www.spectrum.ieee.org/energywise/energy/the-smarter-grid/attack-on-nine-substations-could-take-down-us-grid

55 Ten, C.W., Liu, C.C., Manimaran, G.: 'Vulnerability assessment of cybersecurity for SCADA systems', *IEEE Trans. Power Syst.*, 2008, **23**, (4), pp. 1836–1846

56 Ten, C.W., Hong, J., Liu, C.C.: 'Anomaly detection for cybersecurity of the substations', *IEEE Trans. Smart Grid*, 2011, **2**, (4), pp. 865–873

57 Yan, J., Zhu, Y., He, H., *et al.*: 'Multi-contingency cascading analysis of smart grid based on self-organizing map', *IEEE Trans. Inf. Forensics Sec.*, 2013, **8**, (4), pp. 646–656

58 Phillips, L.R., Tejani, B., Margulies, J., *et al.*: 'Analysis of operations and cybersecurity policies for a system of cooperating flexible alternating current transmission system (facts) devices'. 2005

59 Sridhar, S., Manimaran, G.: 'Data integrity attack and its impacts on voltage control loop in power grid'. Proc. 2011 IEEE Power and Energy Society General Meeting, 2011, pp. 1–6

60 Dondossola, G., Szanto, J., Masera, M., *et al.*: 'Effects of intentional threats to power substation control systems', *Int. J. Crit. Infrastruct.*, 2008, **4**, (1–2), pp. 129–143

61 Hong, J.: 'Cybersecurity of substation automation systems'. PhD thesis, Washington State University, 2014

62 Moreira, N., Molina, E., Lázaro, J., *et al.*: 'Cyber-security in substation automation systems', *Renew. Sustain. Energy Rev.*, 2016, **54**, pp. 1552–1562

63 Liu, S., Feng, X., Kundur, D., *et al.*: 'Switched system models for coordinated cyber–physical attack construction and simulation'. 2011 IEEE First Int.

Workshop on Proc. Smart Grid Modeling and Simulation (SGMS), 2011, pp. 49–54

64 Liu, S., Feng, X., Kundur, D., *et al.*: 'A class of cyber–physical switching attacks for power system disruption'. Proc.of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, 2011, p. 16

65 Liu, S., Mashayekh, S., Kundur, D., *et al.*: 'A smart grid vulnerability analysis framework for coordinated variable structure switching attacks'. Proc. 2012 IEEE Power and Energy Society General Meeting, 2012, pp. 1–6

66 Liu, S., Kundur, D., Zourntos, T., *et al.*: 'Coordinated variable structure switching attack in the presence of model error and state estimation'. 2012 IEEE Third Int. Conf. on Proc. Smart Grid Communications (SmartGridComm), 2012, pp. 318–323

67 Liu, S., Mashayekh, S., Kundur, D., *et al.*: 'A framework for modeling cyber–physical switching attacks in smart grid', *IEEE Trans. Emerging Top. Comput.*, 2013, **1**, (2), pp. 273–285

68 Liu, S., Chen, B., Zourntos, T., *et al.*: 'A coordinated multiswitch attack for cascading failures in smart grid', *IEEE Trans. Smart Grid*, 2014, **5**, (3), pp. 1183–1195

69 Farraj, A.K., Kundur, D.: 'On using energy storage systems in switching attacks that destabilize smart grid systems'. 2015 IEEE Power & Energy Society Proc. Innovative Smart Grid Technologies Conf. (ISGT), IEEE, 2015, pp. 1–5

70 Farraj, A.K., Hammad, E.M., Kundur, D., *et al.*: 'Practical limitations of sliding-mode switching attacks on smart grid systems'. Proc. 2014 IEEE PES General Meeting – Conf. Exposition, 2014, pp. 1–5

71 Abur, A., Exposito, A.G.: 'Power system state estimation: theory and implementation' (CRC Press, Boca Raton, FL, 2004, 1st edn.)

72 Liu, Y., Ning, P., Reiter, M.K.: 'False data injection attacks against state estimation in electric power grids', *ACM Trans. Inf. Syst. Sec. (TISSEC)*, 2011, **14**, (1), p. 13

73 Kim, J., Tong, L.: 'On topology attack of a smart grid: undetectable attacks and countermeasures', *IEEE J. Sel. Areas Commun.*, 2013, **31**, (7), pp. 1294–1305

74 Hug, G., Giampapa, J.A.: 'Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks', *IEEE Trans. Smart Grid*, 2012, **3**, (3), pp. 1362–1370

75 Liang, G., Zhao, J., Luo, F., *et al.*: 'A review of false data injection attacks against modern power systems', *IEEE Trans. Smart Grid*, 2016, **PP**, (99), pp. 1–1 (early access), DOI: 10.1109/TSG.2015.2495133

76 Yang, Q., Yang, J., Yu, W., *et al.*: 'On false data-injection attacks against power system state estimation: modeling and countermeasures', *IEEE Trans. Parallel Distrib. Syst.*, 2014, **25**, (3), pp. 717–729

77 Kim, T.T., Poor, H.V.: 'Strategic protection against data injection attacks on power grids', *IEEE Trans. Smart Grid*, 2011, **2**, (2), pp. 326–333

78 Hao, J., Piechocki, R.J., Kaleshi, D., *et al.*: 'Sparse malicious false data injection attacks and defense mechanisms in smart grids', *IEEE Trans. Ind. Inf.s*, 2015, **11**, (5), pp. 1–12

79 Kosut, O., Jia, L., Thomas, R.J., *et al.*: 'Malicious data attacks on the smart grid', *IEEE Trans. Smart Grid*, 2011, **2**, (4), pp. 645–658

80 Ozay, M., Esnaola, I., Vural, F.T.Y., *et al.*: 'Sparse attack construction and state estimation in the smart grid: centralized and distributed models', *IEEE J. Sel. Areas Commun.*, 2013, **31**, (7), pp. 1306–1318

81 Liu, L., Esmalifalak, M., Ding, Q., *et al.*: 'Detecting false data injection attacks on power grid by sparse optimization', *IEEE Trans. Smart Grid*, 2014, **5**, (2), pp. 612–621

82 Rahman, M.A., Mohsenian-Rad, H.: 'False data injection attacks with incomplete information against smart power grids'. Proc. Global Communications Conf. (GLOBECOM), 2012 IEEE, 2012, pp. 3153–3158

83 Anwar, A., Mahmood, A.N., Pickering, M.: 'Data-driven stealthy injection attacks on smart grid with incomplete measurements'. Proc. Pacific-Asia Workshop on Intelligence and Security Informatics, 2016, pp. 180–192

84 Kim, J., Tong, L., Thomas, R.J.: 'Subspace methods for data attack on state estimation: a data driven approach', *IEEE Trans. Signal Process.*, 2015, **63**, (5), pp. 1102–1114

85 Esmalifalak, M., Nguyen, H., Zheng, R., *et al.*: 'Stealth false data injection using independent component analysis in smart grid'. 2011 IEEE Int. Conf. on Proc. Smart Grid Communications (Smart-GridComm), IEEE, 2011, pp. 244–248

86 Yu, Z.H., Chin, W.L.: 'Blind false data injection attack using PCA approximation method in smart grid', *IEEE Trans. Smart Grid*, 2015, **6**, (3), pp. 1219–1226

87 Esnaola, I., Perlaza, S.M., Poor, H.V., *et al.*: 'Maximum distortion attacks in electricity grids', *IEEE Trans. Smart Grid*, 2016, **7**, (4), pp. 2007–2015

88 Rahman, M.A., Al-Shaer, E., Kavasseri, R.G.: 'A formal model for verifying the impact of stealthy attacks on optimal power flow in power grids'. Proc. ICCPS'14: ACM/IEEE Fifth Int. Conf. on Cyber-Physical Systems (with CPSWeek 2014), 2014, pp. 175–186

89 Rahman, M.A., Al-Shaer, E., Kavasseri, R.: 'Impact analysis of topology poisoning attacks on economic operation of the smart power grid'. 2014 IEEE 34th Int. Conf. on Proc. Distributed Computing Systems (ICDCS), 2014, pp. 649–659

90 Liang, J., Sankar, L., Kosut, O.: 'Vulnerability analysis and consequences of false data injection attack on power system state estimation', *IEEE Trans. Power Syst.*, 2016, **31**, (5), pp. 3864–3872

91 Chakhchoukh, Y., Ishii, H.: 'Coordinated cyber-attacks on the measurement function in hybrid state estimation', *IEEE Trans. Power Syst.*, 2015, **30**, (5), pp. 2487–2497

92 Kim, T., Wright, S.J., Bienstock, D., *et al.*: 'Vulnerability analysis of power systems'. Arxiv preprint arXiv:1503.02360, 2015

93 Zhang, J., Sankar, L.: 'Physical system consequences of unobservable state-and-topology cyber–physical attacks', *IEEE Trans. Smart Grid*, 2016, **7**, (4), pp. 2016–2025

94 Kim, J., Tong, L., Thomas, R.J.: 'Data framing attack on state estimation with unknown network parameters'. Proc. 2013 Asilomar Conf. on Signals, Systems and Computers, 2013, pp. 1388–1392

95 Deka, D., Baldick, R., Vishwanath, S.: 'Optimal data attacks on power grids: leveraging detection & measurement jamming'. Proc. 2015 IEEE Int. Conf. on Smart Grid Communications (SmartGridComm), 2015, pp. 392–397

96 Deka, D., Baldick, R., Vishwanath, S.: 'Jamming aided generalized data attacks: exposing vulnerabilities in secure estimation'. Proc. 2016 49th Hawaii Int. Conf. on System Sciences (HICSS), 2016, pp. 2556–2565

97 Deka, D., Baldick, R., Vishwanath, S.: 'One breaker is enough: hidden topology attacks on power grids'. Proc. 2015 IEEE Power Energy Society General Meeting, 2015, pp. 1–5

98 Yuan, Y., Li, Z., Ren, K.: 'Modeling load redistribution attacks in power systems', *IEEE Trans. Smart Grid*, 2011, **2**, (2), pp. 382–390

99 Yuan, Y., Li, Z., Ren, K.: 'Quantitative analysis of load redistribution attacks in power systems', *IEEE Trans. Parallel Distrib. Syst.*, 2012, **23**, (9), pp. 1731–1738

100 Liu, X., Li, Z.: 'Local load redistribution attacks in power systems with incomplete network information', *IEEE Trans. Smart Grid*, 2014, **5**, (4), pp. 1665–1676

101 Liu, X., Li, Z.: 'Local topology attacks in smart grids', *IEEE Trans. Smart Grid*, 2016, **PP**, (99), pp. 1–10 (early access), DOI: 10.1109/TSG.2016.2532347

102 Liu, X., Li, Z.: 'False data attacks against AC state estimation with incomplete network information', *IEEE Trans. Smart Grid*, 2016, **PP**, (99), pp. 1–10 (early access), DOI: 10.1109/TSG.2016.2521178

103 Xiang, Y., Ding, Z., Zhang, Y., *et al.*: 'Power system reliability evaluation considering load redistribution attacks', *IEEE Trans. Smart Grid*, 2016, **PP**, (99), pp. 1–10 (early access), DOI: 10.1109/TSG.2016.2569589

104 Liu, X., Li, Z., Liu, X., *et al.*: 'Masking transmission line outages via false data injection attacks', *IEEE Trans. Inf. Forensics Sec.*, 2016, **11**, (7), pp. 1592–1602

105 Li, Z., Shahidehpour, M., Alabdulwahab, A., *et al.*: 'Bilevel model for analyzing coordinated cyber–physical attacks on power systems', *IEEE Trans. Smart Grid*, 2016, **7**, (5), pp. 2260–2272

106 Liu, X., Li, Z.: 'Trilevel modeling of cyber attacks on transmission lines', *IEEE Trans. Smart Grid*, 2015, DOI: 0.1109/TSG.2015.2475701

107 Manousakis, N.M., Korres, G.N., Georgilakis, P.S.: 'Taxonomy of PMU placement methodologies', *IEEE Trans. Power Syst.*, 2012, **27**, (2), pp. 1070–1077

108 Zhang, Z., Gong, S., Dimitrovski, A.D., *et al.*: 'Time synchronization attack in smart grid: impact and analysis', *IEEE Trans. Smart Grid*, 2013, **4**, (1), pp. 87–98

109 Jiang, X., Zhang, J., Harding, B.J., *et al.*: 'Spoofing GPS receiver clock offset of phasor measurement units', *IEEE Trans. Power Syst.*, 2013, **28**, (3), pp. 3253–3262

110 Li, H., Gong, S., Lai, L., *et al.*: 'Efficient and secure wireless communications for advanced metering infrastructure in smart grids', *IEEE Trans. Smart Grid*, 2012, **3**, (3), pp. 1540–1551

111 Cleveland, F.M.: 'Cybersecurity issues for advanced metering infrastructure (AMI)'. 2008 IEEE Proc. Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, 2008, pp. 1–5

112 Grochocki, D., Huh, J.H., Berthier, R., *et al.*: 'AMI threats, intrusion detection requirements and deployment recommendations'. 2012 IEEE Third Int. Conf. on Proc. Smart Grid Communications (SmartGridComm), 2012, pp. 395–400

113 Anwar, A., Mahmood, A.N., Tari, Z.: 'Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid', *Inf. Syst.*, 2015, **53**, pp. 201–212. Available at url: http://www.sciencedirect.com/science/article/pii/S0306437914001884

114 McLaughlin, S., Podkuiko, D., McDaniel, P.: 'Energy theft in the advanced metering infrastructure'. Proc. Int. Workshop on Critical Information Infrastructures Security, 2009, pp. 176–187

115 McLaughlin, S., Holbert, B., Fawaz, A., *et al.*: 'A multi-sensor energy theft detection framework for advanced metering infrastructures', *IEEE J. Sel. Areas Commun.*, 2013, **31**, (7), pp. 1319–1330

116 Lisovich, M.A., Mulligan, D.K., Wicker, S.B.: 'Inferring personal information from demand-response systems', *IEEE Sec. Priv.*, 2010, **8**, (1), pp. 11–20

117 Mrmol, F.G., Sorge, C., Ugus, O., *et al.*: 'Do not snoop my habits: preserving privacy in the smart grid', *IEEE Commun. Mag.*, 2012, **50**, (5), pp. 166–172

118 McKenna, E., Richardson, I., Thomson, M.: 'Smart meter data: balancing consumer privacy concerns with legitimate applications', *Energy Policy*, 2012, **41**, pp. 807–814

119 Sankar, L., Rajagopalan, S.R., Mohajer, S., *et al.*: 'Smart meter privacy: a theoretical framework', *IEEE Trans. Smart Grid*, 2013, **4**, (2), pp. 837–846

120 McLaughlin, S., Podkuiko, D., Miadzvezhanka, S., *et al.*: 'Multi-vendor penetration testing in the advanced metering infrastructure'. ACSAC '10 Proc. of the 26th Annual Computer Security Applications Conf., Austin, TX, USA, 2010, pp. 107–116. Available at url: http://www.doi.acm.org/10.1145/1920261.1920277

121 Yi, P., Zhu, T., Zhang, Q., *et al.*: 'A denial of service attack in advanced metering infrastructure network'. Proc. 2014 IEEE Int. Conf. on Communications (ICC), 2014, pp. 1029–1034

122 Yi, P., Zhu, T., Zhang, Q., *et al.*: 'Puppet attack: a denial of service attack in advanced metering infrastructure network', *J. Netw. Comput. Appl.*, 2016, **59**, pp. 325–332

123 Jia, L., Kim, J., Thomas, R.J., *et al.*: 'Impact of data quality on real-time locational marginal price', *IEEE Trans. Power Syst.*, 2014, **29**, (2), pp. 627–636

124 Xie, L., Mo, Y., Sinopoli, B.: 'Integrity data attacks in power market operations', *IEEE Trans. Smart Grid*, 2011, **2**, (4), pp. 659–666

125 Choi, D.H., Xie, L.: 'Ramp-induced data attacks on look-ahead dispatch in real-time power markets', *IEEE Trans. Smart Grid*, 2013, **4**, (3), pp. 1235–1243

126 Duan, J., Zeng, W., Chow, M.Y.: 'Economic impact of data integrity attacks on distributed DC optimal power flow algorithm'. Proc. North American Power Symp. (NAPS), 2015, 2015, pp. 1–7

127 Choi, D.-H., Xie, L.: 'Sensitivity analysis of real-time locational marginal price to SCADA sensor data corruption', *IEEE Trans. Power Syst.*, 2014, **29**, (3), pp. 1110–1120

128 Rangarajan, R.: 'Quantifying the economic impacts of attacks on competitive energy markets'. Proc. North American Power Symp. (NAPS), 2014, 2014, pp. 1–6

129 Ye, H., Ge, Y., Liu, X., *et al.*: 'Transmission line rating attack in two-settlement electricity markets', *IEEE Trans. Smart Grid*, 2016, **7**, (3), pp. 1346–1355

130 Tan, R., Krishna, V.B., Yau, D.K.Y., *et al.*: 'Integrity attacks on real-time pricing in electric power grids', *ACM Trans. Inf. Syst. Sec. (TISSEC)*, 2015, **18**, (2), pp. 5:1–5:33

131 Giraldo, J., Crdenas, A., Quijano, N.: 'Integrity attacks on real-time pricing in smart grids: impact and countermeasures', *IEEE Trans. Smart Grid*, 2016, **PP**, (99), pp. 1–1 (early access) DOI: 10.1109/TSG.2016.2521339

132 Mohsenian-Rad, A.-H., Leon-Garcia, A.: 'Distributed internet-based load altering attacks against smart power grids', *IEEE Trans. Smart Grid*, 2011, **2**, (4), pp. 667–674

133 Wei, D., Lu, Y., Jafari, M., *et al.*: 'Protecting smart grid automation systems against cyber attacks', *IEEE Trans. Smart Grid*, 2011, **2**, (4), pp. 782–795

134 Metke, A.R., Ekl, R.L.: 'Security technology for smart grid networks', *IEEE Trans. Smart Grid*, 2010, **1**, (1), pp. 99–107

135 Yan, Y., Qian, Y., Sharif, H., *et al.*: 'A survey on cybersecurity for smart grid communications', *IEEE Commun. Surv. Tutor.*, 2012, **14**, (4), pp. 998–1010

136 Ma, R., Chen, H.-H., Huang, Y.-R., *et al.*: 'Smart grid communication: its challenges and opportunities', *IEEE Trans. Smart Grid*, 2013, **4**, (1), pp. 36–46

137 Wang, W., Lu, Z.: 'Cybersecurity in the smart grid: survey and challenges', *Comput. Netw.*, 2013, **57**, (5), pp. 1344–1371

138 Qiu, R.C., Hu, Z., Chen, Z., *et al.*: 'Cognitive radio network for the smart grid: experimental system architecture, control algorithms, security, and microgrid testbed', *IEEE Trans. Smart Grid*, 2011, **2**, (4), pp. 724–740

139 Queiroz, C., Mahmood, A., Tari, Z.: 'SCADASim–a framework for building SCADA simulations', *IEEE Trans. Smart Grid*, 2011, **2**, (4), pp. 589–597

140 Mallouhi, M., Al-Nashif, Y., Cox, D., *et al.*: 'A testbed for analyzing security of SCA control systems (TASSCS)'. 2011 IEEE PES Proc. Innovative Smart Grid Technologies (ISGT), 2011, pp. 1–7

141 Hahn, A., Ashok, A., Sridhar, S., *et al.*: 'Cyber–physical security testbeds: architecture, application, and evaluation for smart grid', *IEEE Trans. Smart Grid*, 2013, **4**, (2), pp. 847–855

142 Ashok, A., Wang, P., Brown, M., *et al.*: 'Experimental evaluation of cyber attacks on automatic generation control using a CPS security testbed'. Proc. 2015 IEEE Power Energy Society General Meeting, 2015, pp. 1–5

143 Sun, C.-C., Liu, C.-C., Xie, J.: 'Cyber–physical system security of a power grid: state-of-the-art', *Electronics*, 2016, **5**, (3), p. 40

144 Adhikari, U., Morris, T., Pan, S.: 'WAMS cyber–physical test bed for power system, cybersecurity study, and data mining', *IEEE Trans. Smart Grid*, 2016, **PP**, (99), pp. 1–1 (early access), DOI: 10.1109/TSG.2016.2537210

145 Hahn, A., Govindarasu, M.: 'Cyber attack exposure evaluation framework for the smart grid', *IEEE Trans. Smart Grid*, 2011, **2**, (4), pp. 835–843

146 Deka, D., Baldick, R., Vishwanath, S.: 'Data attack on strategic buses in the power grid: design and protection'. Proc. 2014 IEEE PES General Meeting — Conf. Exposition, 2014, pp. 1–5

147 Deng, R., Xiao, G., Lu, R.: 'Defending against false data injection attacks on power system state estimation', *IEEE Trans. Ind. Inf.*, 2015, **PP**, (99), pp. 1–1 (early access), DOI: 10.1109/TII.2015.2470218

148 Liu, X., Li, Z., Li, Z.: 'Optimal protection strategy against false data injection attacks in power systems', *IEEE Trans. Smart Grid*, 2016, **PP**, (99), pp. 1–1 (early access), DOI: 10.1109/TSG.2015.2508449

149 Sanjab, A., Saad, W.: 'Data injection attacks on smart grids with multiple adversaries: a game-theoretic perspective', *IEEE Trans. Smart Grid*, 2016, **7**, (4), pp. 2038–2049

150 Bi, S., Zhang, Y.J.: 'Graphical methods for defense against false-data injection attacks on power system state estimation', *IEEE Trans. Smart Grid*, 2014, **5**, (3), pp. 1216–1227

151 Bi, S., Zhang, Y.J.: 'Using covert topological information for defense against malicious attacks on DC state estimation', *IEEE J. Sel. Areas Commun.*, 2014, **32**, (7), pp. 1471–1485

152 Talebi, M., Wang, J., Qu, Z.: 'Secure power systems against malicious cyber–physical data attacks: protection and identification'. Proc. Int. Conf. on Power Systems Engineering, 2012, pp. 11–12

153 Etemad, R.H., Lahouti, F.: 'Resilient decentralized consensus-based state estimation for smart grid in presence of false data'. Proc. 2016 IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP), 2016, pp. 3466–3470

154 Liu, N., Chen, J., Zhu, L., *et al.*: 'A key management scheme for secure communications of advanced metering infrastructure in smart grid', *IEEE Trans. Ind. Electron.*, 2013, **60**, (10), pp. 4746–4756

155 Xia, J., Wang, Y.: 'Secure key distribution for the smart grid', *IEEE Trans. Smart Grid*, 2012, **3**, (3), pp. 1437–1443

156 Tsai, J.L., Lo, N.W.: 'Secure anonymous key distribution scheme for smart grid', *IEEE Trans. Smart Grid*, 2016, **7**, (2), pp. 906–914

157 Ismail, Z., Leneutre, J., Bateman, D., *et al.*: 'A game theoretical analysis of data confidentiality attacks on smart-grid AMI', *IEEE J. Sel. Areas Commun.*, 2014, **32**, (7), pp. 1486–1499

158 Guo, Y., Ten, C.W., Hu, S., *et al.*: 'Preventive maintenance for advanced metering infrastructure against malware propagation', *IEEE Trans. Smart Grid*, 2016, **7**, (3), pp. 1314–1328

159 Mo, Y., Chabukswar, R., Sinopoli, B.: 'Detecting integrity attacks on SCADA systems', *IEEE Trans. Control Syst. Technol.*, 2014, **22**, (4), pp. 1396–1407

160 Vamvoudakis, K.G., Hespanha, J.P., Sinopoli, B., *et al.*: 'Detection in adversarial environments', *IEEE Trans. Autom. Control*, 2014, **59**, (12), pp. 3209–3223

161 Mo, Y., Weerakkody, S., Sinopoli, B.: 'Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor outputs', *IEEE Control Syst.*, 2015, **35**, (1), pp. 93–109

162 Lin, H., Slagell, A., Kalbarczyk, Z., *et al.*: 'Runtime semantic security analysis to detect and mitigate control-related attacks in power grids', *IEEE Trans. Smart Grid*, 2016, **PP**, (99), pp. 1–1 (early access), DOI: 10.1109/TSG.2016.2547742

163 Donde, V., Lòpez, V., Lesieutre, B., *et al.*: 'Severe multiple contingency screening in electric power systems', *IEEE Trans. Power Syst.*, 2008, **23**, (2), pp. 406–417

164 Premaratne, U.K., Samarabandu, J., Sidhu, T.S., *et al.*: 'An intrusion detection system for IEC61850 automated substations', *IEEE Trans. Power Deliv.*, 2010, **25**, (4), pp. 2376–2383

165 Hong, J., Liu, C.C., Govindarasu, M.: 'Integrated anomaly detection for cybersecurity of the substations', *IEEE Trans. Smart Grid*, 2014, **5**, (4), pp. 1643–1653

166 Yang, Y., McLaughlin, K., Sezer, S., *et al.*: 'Intrusion detection system for network security in synchrophasor systems'. IET Int. Conf. on Proc. Information and Communications Technologies (IETICT 2013), 2013, pp. 246–252

167 Pal, S., Sikdar, B.: 'A Mechanism for detecting data manipulation attacks on PMU data'. 2014 IEEE Int. Conf. on Proc. Communication Systems (ICCS), 2014, pp. 253–257

168 Pal, S., Sikdar, B., Chow, J.H.: 'Detecting malicious manipulation of synchrophasor data'. Proc. 2015 IEEE Int. Conf. on Smart Grid Communications (Smart-GridComm), 2015, pp. 145–150

169 Morris, T., Pan, S., Adhikari, U., *et al.*: 'Cybersecurity testing and intrusion detection for synchrophasor systems', *Int. J. Netw. Sci.*, 2016, **1**, (1), pp. 28–52

170 Fan, Y., Zhang, Z., Trinkle, M., *et al.*: 'A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids', *IEEE Trans. Smart Grid*, 2015, **6**, (6), pp. 2659–2668

171 Mitchell, R., Chen, I.R.: 'Behavior-rule based intrusion detection systems for safety critical smart grid applications', *IEEE Trans. Smart Grid*, 2013, **4**, (3), pp. 1254–1263

172 Faisal, M.A., Aung, Z., Williams, J.R., *et al.*: 'Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: a feasibility study', *IEEE Syst. J.*, 2015, **9**, (1), pp. 31–44

173 Zhang, Y., Wang, L., Sun, W., *et al.*: 'Distributed intrusion detection system in a multi-layer network architecture of smart grids', *IEEE Trans. Smart Grid*, 2011, **2**, (4), pp. 796–808

174 Fadlullah, Z.M., Fouda, M.M., Kato, N., *et al.*: 'An early warning system against malicious activities for smart grid communications', *IEEE Netw.*, 2011, **25**, (5), pp. 50–55

175 Xiao, Z., Xiao, Y., Du, D.H.C.: 'Exploring malicious meter inspection in neighborhood area smart grids', *IEEE Trans. Smart Grid*, 2013, **4**, (1), pp. 214–226

176 Xiao, Z., Xiao, Y., Du, D.H.C.: 'Non-repudiation in neighborhood area networks for smart grid', *IEEE Commun. Mag.*, 2013, **51**, (1), pp. 18–26

177 Liu, J., Xiao, Y., Gao, J.: 'Achieving accountability in smart grid', *IEEE Syst. J.*, 2014, **8**, (2), pp. 493–508

178 Mashima, D., Cárdenas, A.A.: 'Evaluating electricity theft detectors in smart grid networks'. Proc. Int. Workshop on Recent Advances in Intrusion Detection, 2012, pp. 210–229

179 Jindal, A., Dua, A., Kaur, K., *et al.*: 'Decision tree and SVM based data analytics for theft detection in smart grid', *IEEE Trans. Ind. Inf.*, 2016, **12**, (3), pp. 1005–1016

180 Jokar, P., Arianpoo, N., Leung, V.C.M.: 'Electricity theft detection in AMI using customers's consumption patterns', *IEEE Trans. Smart Grid*, 2016, **7**, (1), pp. 216–226

181 Manandhar, K., Cao, X., Hu, F., *et al.*: 'Detection of faults and attacks including false data injection attack in smart grid using Kalman filter', *IEEE Trans. Control Netw. Syst.*, 2014, **1**, (4), pp. 370–379

182 Huang, Y., Tang, J., Cheng, Y., *et al.*: 'Real-time detection of false data injection in smart grid networks: an adaptive CUSUM method and analysis', *IEEE Syst. J.*, 2016, **10**, (2), pp. 532–543

183 Li, S., Ylmaz, Y., Wang, X.: 'Quickest detection of false data injection attack in wide-area smart grids', *IEEE Trans. Smart Grid*, 2015, **6**, (6), pp. 2725–2735

184 Ashok, A., Govindarasu, M., Ajjarapu, V.: 'Online detection of stealthy false data injection attacks in power system state estimation', *IEEE Trans. Smart Grid*, 2016, **PP**, (99), pp. 1–1 (early access), DOI: 10.1109/TSG.2016.2596298

185 Esmalifalak, M., Liu, L., Nguyen, N., *et al.*: 'Detecting stealthy false data injection using machine learning in smart grid', *IEEE Syst. J.*, 2014, **PP**, (99), pp. 1–1 (early access), DOI: 10.1109/JSYST.2014.2341597

186 Ozay, M., Esnaola, I., Vural, F.T.Y., *et al.*: 'Machine learning methods for attack detection in the smart grid', *IEEE Trans. Neural Netw. Learn. Syst.*, 2016, **27**, (8), pp. 1773–1786

187 Tang, B., Yan, J., Kay, S., *et al.*: 'Detection of false data injection attacks in smart grid under colored Gaussian noise'. Arxiv preprint arXiv:1607.06015, 2016

188 Chen, G., Dong, Z.Y., Hill, D.J., *et al.*: 'Exploring reliable strategies for defending power systems against targeted attacks', *IEEE Trans. Power Syst.*, 2011, **26**, (3), pp. 1000–1009

189 Chen, P.Y., Cheng, S.M., Chen, K.C.: 'Smart attacks in smart grid communication networks', *IEEE Commun. Mag.*, 2012, **50**, (8), pp. 24–29

190 Ma, C.Y.T., Yau, D.K.Y., Lou, X., *et al.*: 'Markov game analysis for attack-defense of power networks under possible misinformation', *IEEE Trans. Power Syst.*, 2013, **28**, (2), pp. 1676–1686

191 Ma, C.Y.T., Yau, D.K.Y., Rao, N.S.V.: 'Scalable solutions of Markov games for smart-grid infrastructure protection', *IEEE Trans. Smart Grid*, 2013, **4**, (1), pp. 47–55

192 Yao, Y., Edmunds, T., Papageorgiou, D., *et al.*: 'Trilevel optimization in power network defense', *IEEE Trans. Syst. Man Cybern. C, Appl. Rev.*, 2007, **37**, (4), pp. 712–718

193 Arroyo, J., Fernández, F.: 'A genetic algorithm approach for the analysis of electric grid interdiction with line switching'. 15th Int. Conf. on Proc. Intelligent System Applications to Power Systems, 2009. ISAP'09, 2009, pp. 1–6

194 Delgadillo, A., Arroyo, J.M., Alguacil, N.: 'Analysis of electric grid interdiction with line switching', *IEEE Trans. Power Syst.*, 2010, **25**, (2), pp. 633–641

195 Zhao, L., Zeng, B.: 'Vulnerability analysis of power grids with line switching', *IEEE Trans. Power Syst.*, 2013, **28**, (3), pp. 2727–2736

196 Chen, Y., Hong, J., Liu, C.C.: 'Modeling of intrusion and defense for assessment of cybersecurity at power substations', *IEEE Trans. Smart Grid*, 2016, **PP**, (99), pp. 1–1 (early access), DOI: 10.1109/TSG.2016.2614603

197 Vukovic, O., Sou, K.C., Dan, G., *et al.*: 'Network-aware mitigation of data integrity attacks on power system state estimation', *IEEE J. Sel. Areas Commun.*, 2012, **30**, (6), pp. 1108–1118

198 Esmalifalak, M., Shi, G., Han, Z., *et al.*: 'Bad data injection attack and defense in electricity market using game theory study', *IEEE Trans. Smart Grid*, 2013, **4**, (1), pp. 160–169

199 Bakken, D.E., Bose, A., Hauser, C.H., *et al.*: 'Smart generation and transmission with coherent, real-time data', *Proc. IEEE*, 2011, **99**, (6), pp. 928–951

200 Li, F., Qiao, W., Sun, H., *et al.*: 'Smart transmission grid: vision and framework', *IEEE Trans. Smart Grid*, 2010, **1**, (2), pp. 168–177

201 Lasseter, R.H.: 'Smart distribution: coupled microgrids', *Proc. IEEE*, 2011, **99**, (6), pp. 1074–1082

202 Arritt, R.F., Dugan, R.C.: 'Distribution system analysis and the future smart grid', *IEEE Trans. Ind. Appl.*, 2011, **47**, (6), pp. 2343–2350