Journal of Electrical Systems and Information Technology

REVIEW Open Access

A narrative perspective of island detection methods under the lens of cyber-attack in data-driven smart grid

Apoorva Shukla[1], Soham Dutta[2*], Sourav Kumar Sahu[3] and Pradip Kumar Sadhu[1]

*Correspondence:
soham.dutta@manipal.edu

[1] Department of Electrical Engineering, Indian Institute of Technology (Indian School of Mines), Dhanbad, Jharkhand 826004, India
[2] Department of Electrical and Electronics Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka 576104, India
[3] Department of Electrical and Electronics Engineering, Birla Institute of Technology, Mesra, Ranchi, Jharkhand 835215, India

Abstract

As criminals and hackers are developing new methods to interfere with the operation of the power grid, the nature of grid vulnerabilities and threats is continuously evolving. The growing interest in transitioning the unidirectional power system to a bidirectional data-driven modern grid will further escalate these issues. The question of cyber security becomes essential in particular critical decisions such as island detection. The incorrect decision of island occurrence may completely disrupt the operation of a portion of the grid, causing substantial damage to electrical equipment and grid maintenance workers. Fast monitoring and accurate control of unplanned islanding detection are essential for distributed generation-based active networks for providing continuous power supply to critical loads. Considering the above aspects, this paper serves on the perspective of different island detection methods and various aspects of cyber security. The type of cyber-attacks is categorized in terms of their behavior. Key points are discussed about how, when, and in what fashion and degree it can harm all the sectors of the grid, i.e., generation, transmission, and distribution system. Finally, the impact of cyber-physical attacks on the islanding decision system is presented. The research remedies for such measures are also presented. Moreover, a comparison is being made among various island detection methods based on the extent of impact of different cyber-attacks on the operation of these methods. Some promising future solutions for cyber-secure island detection methods are also suggested.

Keywords: Cyber-physical systems, Cyber-attack, Distributed generation, Island detection, Data-driven smart grid

Introduction

The sharp increase in power consumption has led to an increase in distribution generation (DG) requirements to meet the grid demand requirements and the local loads. Smart grid and DG integration are promising approaches for solving the power system demand problem. There has been a considerable increase in the installation of DG near utility distribution system over the past decade [1, 2]. The DG resources such as PV (photovoltaic) cells, wind energy conversion system or fuel cells offer several potential benefits to utility and customers in terms of economic, technical, and environmental aspects. As DG integration is unavoidable due to expanding power demand, the biggest

challenge due to incorporating DG into the power system network is unintentional islanding operation. Islanding operation occurs when a part of an active distribution system, which includes DG, is separated from the rest of the network, while still being energized by a single DG or multiple DGs. Unintentional islanding impacts the personal safety of the maintenance workforce and may result in an unsynchronized reclosing action, which can also harm the DGs. Owing to the unplanned nature, it may cause damage to loads due to inadequate voltage and frequency control services provided by DG [1–3]. Such undesirable events could be due to tripping of circuit breakers, manual errors, interruption for maintenance services, equipment failure or network reconfiguration [4, 5]. Therefore, the IEEE std. 2003 states clearly that the disconnection of DG from utility should happen within 2 s of islanding inception [6]. Similarly, the IEC 61727 standard also states that islanding detection and DG disconnection should happen at a maximum time span of 2 s [7]. Therefore, the efficient protection and detection of these undesirable conditions are of prime importance in smart grids.

To regulate and efficiently control the electric power grids, digital measurement devices are getting the upper hand in the present time. A smart grid incorporates several computing and communication devices, control and intelligent monitoring, smart meter, and real-time communication that facilitates real-time control between various components in the power system [8]. This digitization of the power grid has led to the growth of voluminous data that are needed to be transferred to various locations of the grid. The protection of these data becoming very crucial in the data-driven intelligent power system. The amalgamation of the cyber system (communication, info-tech (IT)), security, and automated control infrastructure) and physical system in the smart grid leads to the progress of cyber-physical system, and each of system is been handled by its own regulations, protocols, and standards [9, 10]. The digital measurements reflect the accuracy and construction of improvised power system operation and control of the installed sensors, which are vulnerable to unknown events such as device malfunction and cyber-physical attacks [11]. The attacker can fabricate figures, initialize denial of services, or disrupt the communication channel of the measurement device and control center.

History clearly illustrates the exposure of industrial communication and control systems to cyber-attacks. The power outage of 9th January that left nearly all of Pakistan, i.e., approx. 200 million people without electricity [12] is a significant example. Similarly, Mumbai, on 12th October, 2020, suffered due to a small technical glitch that caused its power-transmission a blackout. In March 2019, Venezuela was left lurching in the dark without electric power for more than a week [13]. The blackout left the country with 32 million people in complete disarray [14]. At least 43 deaths were attributed to the blackout [15]. On December 23, 2015, the cyber-attack on Ukraine power grid clearly demonstrated that attackers can easily manipulate internal devices and abuse them as per their needs [16]. The Ukraine power grid cyber-attack left the country with no power for hours [17, 18]. In 2010, a cyber-attack targeted both the hardware and software of Siemens industrial control scheme and exploited its Windows operating system [19, 20]. As a result, 60% of Iran's Bushehr Nuclear Power Plant (BNPP) remains under threat leading to a constant fear of cyber warfare [21]. Cyber spies entered the US electrical grid on 8th April 2009 that disturbed

the complete software programs and power system [22]. On September 26–27, 2007, and in January 2005 a cyber-attack led to major interferences in the electric supply in the city of Rio de Janeiro, affecting more than three million people in Brazil [23]. On September 28, 2003 Italy went into a country-wide blackout except Sardinia resulted from a power failure while interconnection between power and communication network, hindering services of more than 56 million customers [16]. In the same year, between August 14–28, a power failure for 4 days was experienced in central Canada, and the North- Eastern US. This impacted over fifty million citizens, which sums up to 62,000 MW of power, and it took almost 14 days to restore from the entire event [24].

The smart grid has some potential vulnerabilities because of the enormous dependence on communication networks [25]. Steps were taken by DOE (Department of Energy's) Cyber security Road Map for Energy Delivery System (EDS) [26], North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection (CIP) standard [27], National Institute of Standard & Technology Interagency Report (NISTIR)7628 [28, 29] and National Electric Sector Cybersecurity Organization Resources (NESCOR) report [30] have discussed future grid's safety and pliability to cyber-attacks. In these circumstances, diverse efforts are being considered as the light shed moment for the digital and the physical world.

The false trigging of the islanding detection signal, if executed by the cyber attacker can lead the smart grid to disrupt power leading to a blackout in major portion of the grid. This will result in severe fluctuation in the islanded grid's frequency and voltage, which may further reduce the power quality and hence reliability of the grid. The reverse of this condition, i.e., sending of non-occurrence of island signal by the cyber attacker even though islanding has occurred can also cause extensive damages. Therefore, it is important to analyze the impact of the cyberattack on various island detection algorithms to develop effective countermeasures for enhancing cyber-physical safety. In continuation with the discussion, this study presents a review of various island detection methods, the elements of cyber-physical systems in a smart grid, various methods of cyber-attacks, and their impact on the normal operation of island detection methods. The contributions of this narrative perspective are as per the following:

1. Although there are many papers on island detection methods and cyber security methods in power systems, there are no papers connecting these two. Thus, the author(s) establishes the connection between island detection methods and cyber threats in this work.
2. The list of objectives and requirements for cyber-physical security of island detection methods is identified for the first time.
3. The analysis on wide aspects of cyber threats on the functioning of different island detection methods are discussed in detail, which is not present in available literature as per the best knowledge of the author(s).
4. The probable methods of eliminating the fear of cyber threats for various island detection methods are also dealt with for the first time.
5. Finally, a research gap is identified which can motivate the researchers and engineers to think about future cyber-attack proof island detection methods.

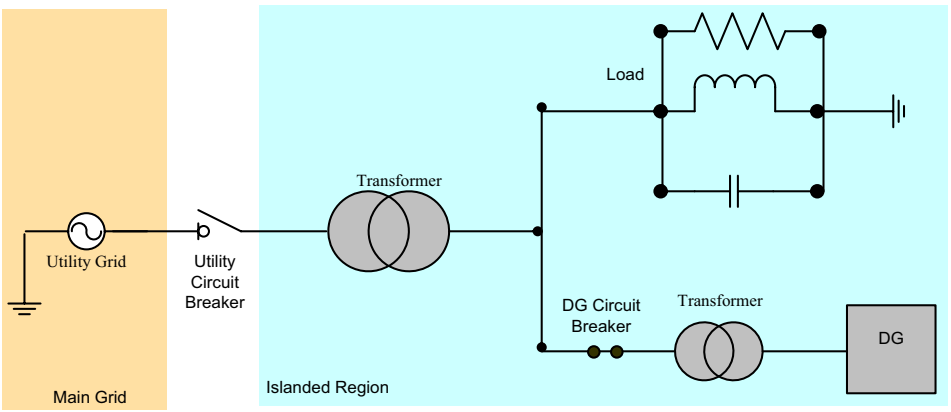

Fig. 1 Concept of islanding condition in power system

The rest of the paper is structured in eight sections. The concept of islanding is explained in "Concept of islanding" section. Various island detection methods, with their advantages and disadvantages, are described in "Islanding detection methods" section. In "Cyber-physical security of smart grids" section, the cyber-physical security aspects of smart grids are dealt. The requirements of the cyber-physical structure of smart-grid are laid down in "Requirements of cyber-physical structure of smart grid" section. The various types of cyber-physical attack in smart grid and general defense measure is mentioned in "Types of cyber-physical-attack in smart grid and general defense measure" section. The effect of cyber threats on different island detection methods is discussed in "Effect of cyber-attack on island detection" section. "Conclusion" section concludes this paper. The future research directions are also elaborated in this section.

Concept of islanding

The islanding happens when the circuit breaker between the utility and a section of the power system containing DG and loads, opens as in Fig. 1. In this condition, the DG continues to feed the local loads. Thus, in islanding situation, a section of the grid is entirely energized by one or more DGs, while electrically detached from the main grid. This condition of islanding operation normally arises due to the following causes:

a. Fault on the line linking the DG and the utility.
b. In the absence of precise frequency control.
c. Failure of the stability between generation and load in the islanded circuit.
d. Chance opening of the electrical supply subsequently after a system let-down.
e. The rapid change in the loads in the network distribution system.
f. Planned downtime for maintenance activities on the grid.
g. Physical intervention or manual errors.
h. Natural phenomena, e.g., thunderstorms, earth quakes, volcanic eruptions, etc.

There are two basic types of islanding conditions—intentional and unintentional islanding. Intentional islanding is the process of purposely splitting the DG into

self-sufficient controllable island regions, to power the local grid [31, 32]. It is performed to plan maintenance activities needed for the main utility grid. Unintentional islanding is an unexpected operation that may occur at any time due to fault or different uncertainties in the electric system [33]. This type of islanding is a risk for system security, as it may create instability to the system network like voltage and frequency unbalance, harmonics occurrence, equipment damage, electric shock, etc. [34, 35].

Islanding detection methods

The islanding detection method is broadly divided into four main sets: local scheme, remote scheme, signal processing-based technique, and intelligence-based method, as shown in Fig. 2 [4, 36, 37]. The techniques are characterized by several factors, like non-detection zone (NDZ), power quality, speed of detection in error, rate of detection of error, and its efficiency with multiple inverter cases [38]. A detailed discussion of these techniques is explained in the following sections.

Remote islanding detection method

Remote islanding detection method utilizes the principle of communication infrastructure between utility grid and the DGs. As soon as islanding occurs, immediately a trip signal is shared with DG source, and it deliberately forces a section of the grid into a condition that will guarantee to isolate the DG systems. The remote scheme has negligible NDZ, i.e., it can work even during zero power flow (before islanding) between the main grid and the islanded grid. Additionally, it does not impact the power quality of the system, and it has high reliability and faster response time. Moreover, it works effectively with multiple DG systems. On the other side, owing to its high-priced and complex problem, its implementation on a small-scale system is not preferred [39, 40]. Power line carrier communication (PLCC) scheme, supervisory control, and data acquisition (SCADA) process, transfer-trip method, and phasor measurement unit (PMU) are the variety of schemes that falls under this detection method. A schematic of the remote islanding detection method is shown in Fig. 3, where the main utility grid and DG unit share the information using a communication channel. The summary of various remote island detection techniques is given in Table 1.

Local islanding detection method

This method measures variation in some system parameter, for e.g. voltage, current, impedance, frequency, phase angle, active and reactive power and harmonic distortion on DG side for detecting islanding. The measurement may be direct or indirect or both. On this basis, the local methods are further classified as, passive technique, active technique and hybrid technique. The different types of these techniques have increased rapidly over the last few years [41, 42].

Passive islanding detection technique

The passive islanding detection technique basically identifies islanding by observing passive parameters at the point of common coupling (PCC), such as current, voltage, impedance, frequency, active power, total harmonic distortion (THD), phase angle and

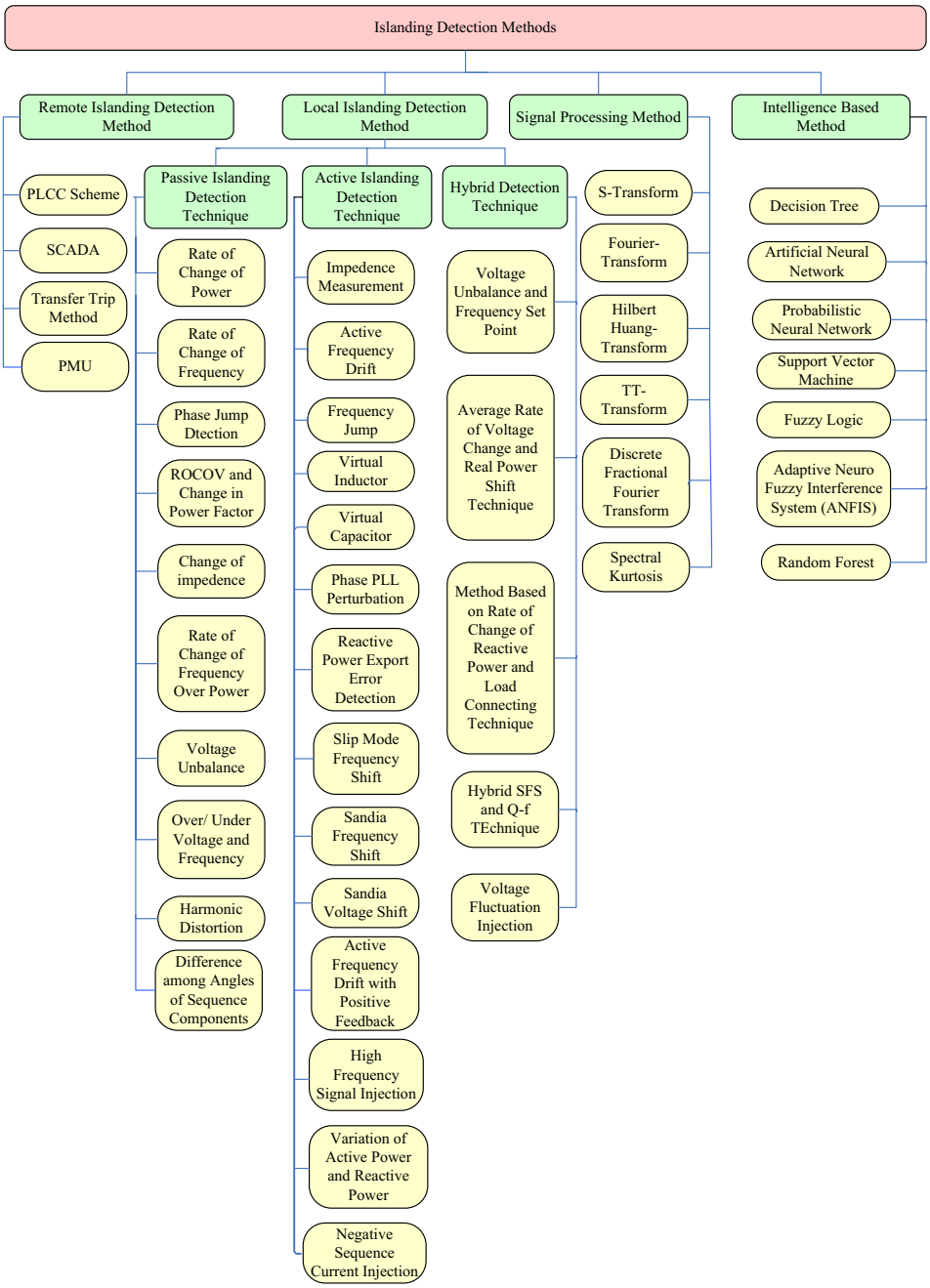

Fig. 2 Classification of various islanding detection methods [4, 36, 37]

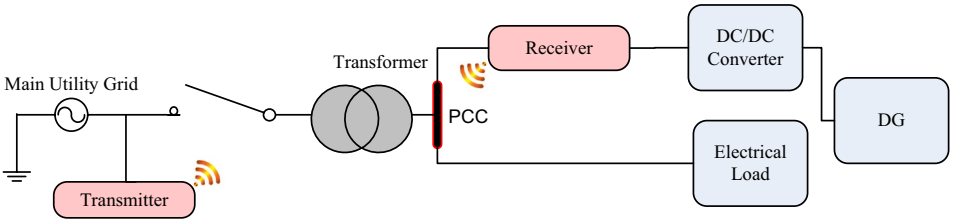

Fig. 3 A schematic of remote islanding detection scenario

Table 1 Summary of various remote island detection techniques

Technique	Advantage	Drawback	Speed	DG network type	DG system	Detection time	References
PLCC	Zero NDZ, reliable, low detection time and no false tripping	High cost and highly complex	Fast	NA	PV	Depend on communication latency	[39]
SCADA	Zero NDZ, and no false tripping	High cost	Fast	Radial	PV and wind	Depend on method	[40]
Transfer-trip	Zero NDZ and no false tripping	High cost	Very Fast	NA	PV	Depend on the equipment used	[39]

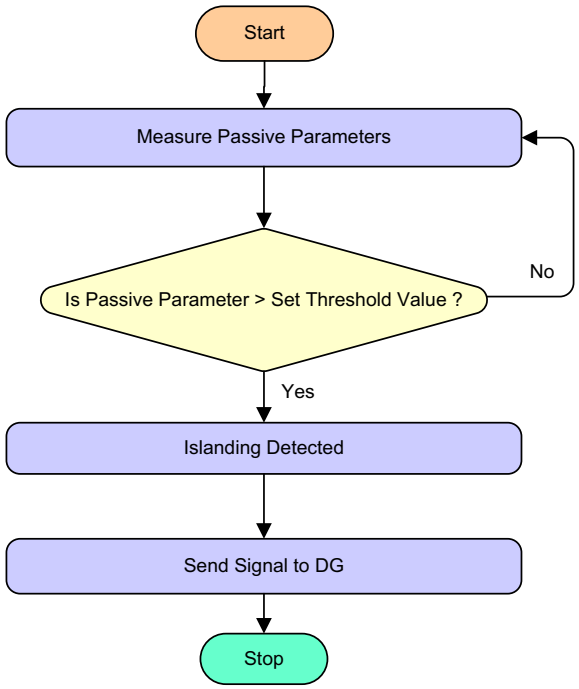

Fig. 4 Algorithm for passive islanding detection method [43]

other parameters [43]. The flow chart of the passive islanding detection process is presented in Fig. 4. It relies on a pre-set threshold to detect islanding, i.e., when the rate of alteration of a passive parameter exceeds that of a maximum limit, it indicates that the system has become islanded. Some of conventional passive detection schemes are rate of change of power (ROCOP) [44], rate of change of frequency (ROCOF) [45–47], phase jump detection [48, 49], rate of change of frequency over power [50, 51], (ROCOV) rate of change of voltage and change in power factor [52], change in impedance [53] voltage unbalance, over/under voltage (OV/UV), over/under frequency (OF/UF), harmonic distortion [38, 49, 54, 55] and sequence component angles [52]. Some modified, passive detection schemes are Kalman filter-based technique, auto-correlation function-based scheme, s-transform-based scheme and Fourier transform-based technique. The setting

Table 2 Summary of various passive island detection technique

Technique	Advantage	Drawback	Speed	DG network type	DG system	Detection time	References
ROCOP	Short detection time	Very high NDZ	Faster than OV/UV and OF/UF	Radial	NA	26 µs	[44]
ROCOF	Short detection time, able to differentiate between islanding and non-islanding scenario effectively	Very high NDZ	Faster than OF/UF	Radial	Synchronous	0.5–0.7 µs	[45–47]
Phase Jump Detection	Short detection time	High NDZ	Low	Radial	Inverter-based	0.1 s	[48]
Rate of Change of Frequency over Power	Detect island quickly and can differentiate between islanding and non-islanding scenario accurately	Moderate NDZ	Faster than OV/UV and OF/UF	Small-scale radial	Synchronous	0.2–0.3 s	[50, 51]
Rate of change in voltage and change in power factor	Low NDZ	High cost	Fast	Radial	Two synchronous distributed generation	0.5 s	[52]
Change in impedance	Detect island quickly	High NDZ	Faster than ROCOF	Small-scale radial	Synchronous	0.5 s	[53]
Over/under voltage, over/under frequency	Moderate NDZ	High NDZ	low	Radial	Synchronous	0.2–0.4 s	[49, 54, 55]

of the thresholds requires special consideration. Setting a lesser limit can cause trouble with tripping and false islanding detection. However, if the limit is too high, it will result in islanding conditions being undetected. This method cannot sense islanding if both active, as well as reactive power, are balanced in between the pre-islanded grid and the main grid. Therefore, the method suffers from large NDZ. The passive detection method has some major advantages, such as not impacting the power quality or grid operation, being cost-effective and having fast detection speed [48, 56]. A summary of various passive island detection techniques is given in Table 2.

Active islanding detection technique

The active islanding detection technique deals with the grid by injecting perturbation into the system variables directly. The active islanding method involves a feedback method to find islanding through parameter changes. An external fabricated signal such as voltage, current and harmonic signal participate with power system operation

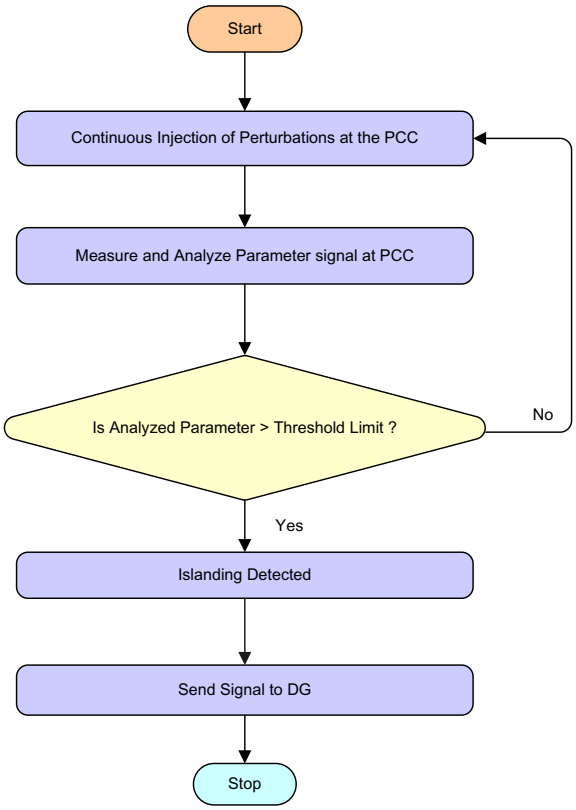

Fig. 5 Algorithm for active islanding detection method

and brings significant changes in system parameters during islanding, triggering the island detection signal. The effect of these injected signals is not noteworthy if the DG is not islanded from the utility grid [57, 58]. Figure 5 depicts the basic flowchart of the active islanding detection. Impedance measurement (IM) [53, 59], active frequency drift (AFD) [54, 60], frequency jump (FJ) [38], virtual inductor [61], virtual capacitor [62], (phase locked loop) PLL perturbation method, reactive power export error detection (RPEED) [5], slip mode frequency shift (SMFS) [63–65], Sandia frequency shift (SFS) [42, 66, 67], Sandia voltage shift (SVS) [37, 68, 69], active frequency drift with positive feedback (AFDPF) [70], high frequency signal injection [71, 72], fluctuations in active and reactive power [37, 38, 54] and negative sequence current injection [73, 74] are examples of active islanding detection. This method is more effective and accurate in comparison to the passive method of islanding detection. The active method has relatively small NDZ, but has a slow response toward error detection rate. Moreover, it requires additional electronic equipment in the system in order to inject perturbation. Furthermore, this method increases the system complexity and requires additional detection time to observe perturbation response on the power system. Since it interferes with an additional signal during the entire operation of the grid, it significantly lowers the power quality of the system and its stability. A summary of various active island detection techniques is given in Table 3.

Table 3 Summary of various active island detection technique

Technique	Advantage	Drawback	Speed	DG network type	DG system	Detection time	References
SFS	Low NDZ	Power quality degradation	Fast	Radial	VSC (voltage source converters)	0.9–0.10 s	[42, 66, 67]
High frequency signal injection	Low NDZ	Power quality degradation	Very fast	Radial	VSC	60 µs	[71]
SVS	Low NDZ	Power quality degradation	Fast	Small-scale radial	Inverter-based	0.2–0.231 s	[37, 68, 69]
SMFS	Low NDZ	Power quality degradation	Fast	Radial	VSC	0.2–0.37 s	[63, 64]
AFDPF	Very low NDZ	High cost, power quality degradation	Fast	Radial	Inverter based	928 µs	[70]

Hybrid islanding detection technique

The hybrid islanding detection technique runs on the principle of active and passive islanding detection methods to remove the problem with both techniques. For example, large NDZ is the main problem in the passive detection method and power quality issue in the active method due to perturbation. Such problems can be overcome by a hybrid technique [75]. During hybrid detection of islanding, the passive technique works as the primary method, whereas the active function works as the ancillary method, as depicted in Fig. 6. It can be effectively applied to complex systems [76, 77]. The hybrid methods can improve multiple performance indices. However, the aforementioned technique escalates the system cost, along with large islanding detection time. Voltage unbalanced and frequency set point-based method [78], the average rate of voltage change and real power shift technique [79], a method based on the rate of change of reactive power and load connecting technique [80], hybrid SFS and Q-F method [81], voltage fluctuation injection [82] are some example of the hybrid islanding detection technique. Each islanding detection technique has its own pros and cons. The choice of the islanding detection method depends on the DG technology used and the complexity of the grid. The hybrid detection method with the mixture of both agile passive and a precise active technique seems to be the answer. However, this hybrid method has some unresolved issues that include accuracy, high detection time, and compatibility with multiple DGs. These restrictions can be overpowered by signal processing techniques and intelligence-based methods. A summary of various hybrid island detection techniques is given in Table 4.

Signal processing-based method

Signal processing-based methods are used to further improvise the results of passive as well as an active detection method. The signal processing method has helped many researchers in understanding the islanded mode of operation regardless of its location of control. Such methods have the properties such as conformability, cost-effectiveness,

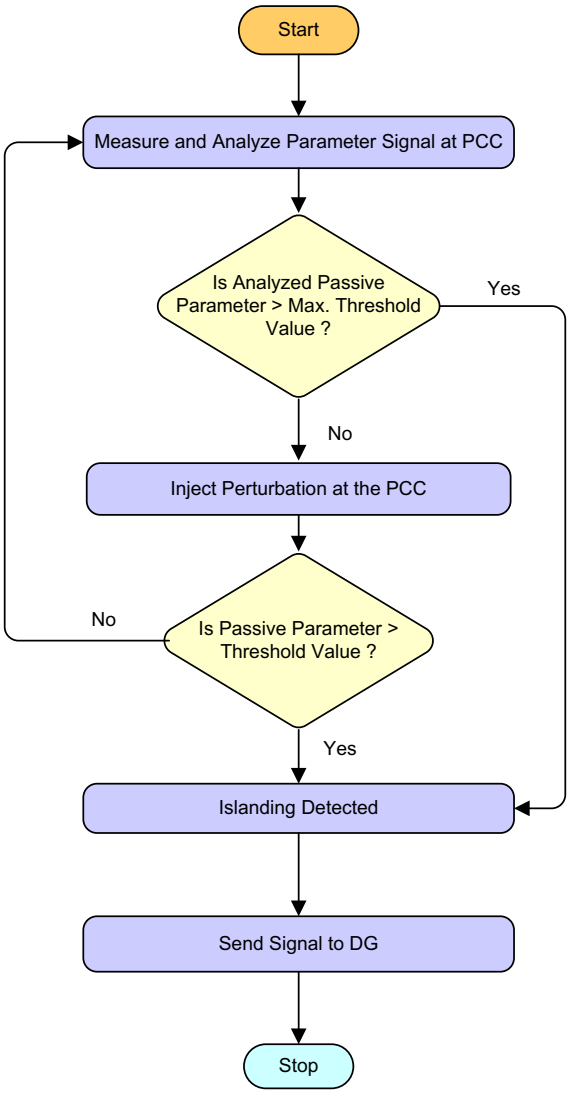

Fig. 6 Algorithm for hybrid islanding detection method

stability, and ease of alteration, which has helped the researcher in the extraction of the hidden characteristics of the measured signal to detect the islanding. Figure 7 shows the step involved in carrying out islanding detection. The signals such as voltage or current are taken from the PCC, and features are extracted with signal processing tools. The features obtained are then compared with a threshold to identify island conditions. Common signal processing classifier used in islanding detection are wavelet transform (WT) [83, 84], s-transform [85–87], discrete fractional Fourier transform (FT) [88], Hilbert Huang transform (HHT) [89, 90] and spectral kurtosis [91]. Over the last decade, the signal processing methods have received huge attention from researchers owing to their flexibility. A summary of various signal processing method is given in Table 5.

Table 4 Summary of various hybrid island detection technique

Technique	Advantage	Drawback	Speed	DG network type	DG system	Detection time	References
Voltage unbalance and frequency set-point	Multiple islanding condition can be detected and has small NDZ	Power quality is degraded	Fast	Mesh	Inverter based	< 2 s	[78]
Average rate of voltage change and real power shift technique	Small NDZ	Degradation of power quality	Low	Radial	Inverter based	0.51 s	[79]
Hybrid SFS and QF method	Low NDZ and decrease the effect of active method	Slightly degrade power quality	High	Radial	Inverter-based	$\leq$ 0.4 s	[81]
Voltage fluctuation injection	Accuracy in island detection and has small NDZ	Power quality get affected and degraded	High	Radial	Inverter based	0.3 s	[82]

Intelligence-based method

Intelligence-based islanding methods are similar to that of the signal processing-based method. In the signal processing method, the input parameter signal is compared with a fixed value. The range of this fixed value is hard to determine. To obtain this threshold value automatically, an intelligence-based method is used with the signal processing method for islanding detection. Figure 8 shows an elementary flow chart diagram of the intelligence-based method with a signal processing technique. The classifier is trained from numerous simulations done beforehand. After it is properly trained, the extracted features obtained from the signal processing technique is fed to the classifier for classification of island conditions [92]. The commonly used intelligence-based method associated with signal processing-based islanding detection method includes decision tree (DT) [93–95], artificial neural network (ANN) [96–98], probabilistic neural network (PNN) [76, 99], support vector machine (SVM) [100, 101], fuzzy logic control (FL) [102–104], adaptive neuro-fuzzy interference system (ANFIS) [105] and random forest (RF) [106]. A summary of various intelligence-based method is given in Table 6 and the comparison between different island detection methods is made in Table 7.

From the above discussions, it can be observed that the island detection methods depends on the components of smart grid, especially its communication structure. Thus, the components of the smart grid must be in a healthy state for the island detection methods to work perfectly. An attack on any of these structures may cause maloperation of the islanding algorithm. Thus, it is necessary to have a knowledge of the cyber-physical security of the smart grids in order to assess the island detection algorithms in terms of cyber security.

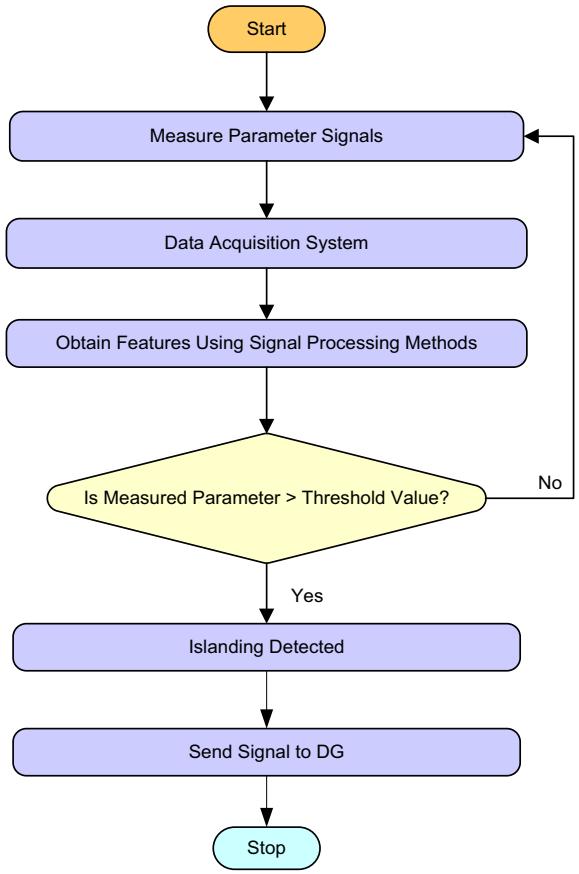

Fig. 7 Algorithm for signal processing-based islanding detection method

Table 5 Summary of various signal processing-based island detection technique

Technique	Advantage	Drawback	Speed	DG network type	DG system	Detection time	References
WT	Less complex and fast computation	Sensitive to noise	Fast	Mesh	PV and diesel	Less than 2 s (45 μs)	[83, 84]
ST	Immune to noise	Unable to detect low frequencies	Faster than WT	Mesh	Wind and PV	≤ 20 μs	[86]
FT	No information is lost during transformation	Sensitive to noise	Low	Radial	Wind and PV	0.01 s	[88]
HHT	Highly efficient	Localization problem	Fast	Both rail and mesh	Wind, PV and fuel	–	[90]

Cyber-physical security of smart grids

Implementation of electricity transfer over grids with cyber integration has an extensive impact on power system organization. During the last few years, several researchers have comprehensively studied the smart grid, its cyber-physical system structure, security

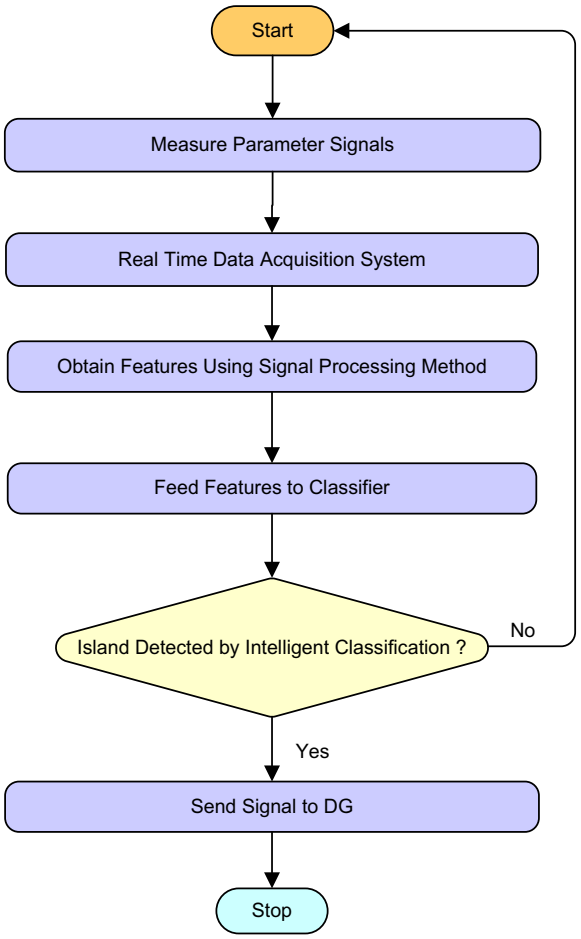

Fig. 8 Algorithm for intelligence-based method islanding detection method

Table 6 Summary of various intelligence-based island detection technique

Technique	Advantage	Drawback	Speed	DG network type	DG system	Detection time	References
DT	Scaling of data is not required	Calculation can become more complex	Moderate	Radial	Synchronous	< 2 s	[93]
ANN	Robust to noise	Not reliable	Fast	Radial	Synchronous	–	[97]
SVM	Efficiently manages memory	Not suitable for large dataset	Fast	Mesh	Wind, PV and synchronous	–	[99]
FL	Simple	Need experts knowledge	Fast	Both radial and mesh	synchronous	20 µs	[100]

and infrastructure. Figure 9 illustrates the typical type of cyber-physical structure of a smart grid. Smart grid infrastructure of electric power system is generally categorized into generation, transmission, and distribution system [107]. Smart grid infrastructure advancement has made cyber-physical security a serious challenge for power system

Table 7 Comparison between different island detection methods

Technique	Fundamental principle	NDZ	Run-on-time	False tripping %	Relevance in DG system	Operation-al cost
Remote	Communication between main grid and DG	Zero NDZ	High	Negligible	Highly desired	Very high
Active	Injecting disturbance and further analysing the impact on system	Small NDZ	Short	Minimal	Not-preferred	Low
Passive	Monitoring smart grid system parameter for comparing them with pre-defined threshold value	Large NDZ	Very-short	High	Highly preferred	Low
Hybrid	Amalgamation of passive and active islanding detection method as primary and secondary detection section respectively	Very small NDZ	Short	Minimal	Not-preferred	Low
Signal- processing	Evaluation of received signal by signal processing tool after stabilization of operation	Minimal	Short	Minimal	Highly desired	Low
Intelligence	Real-time data accusation system and obtain features using signal processing method	Minimal	Short	Minutest	Preferred	Low

operation. The infrastructure generates extra issues for warranting its security. Availability, integrity and confidentiality of available data are priorities of a cyber-physical system. Cyber attackers aim and threaten these elements so as to influence the data being transferred for operation and control [108]. Cyber threat on these can affect the system component and its infrastructure. Thus, cyber security mechanism in data-driven grids is needed to prevent a rise in physical and cyber-attack.

Physical security

Integration of power system smart devices and cyber systems in physical structure introduces new challenges, as most of the devices and systems are insufficient to security features against vulnerability. Lack of sufficient protection against cyber-attack can result in equipment damage, personal safety hazards, and grid protection device. Thus, this

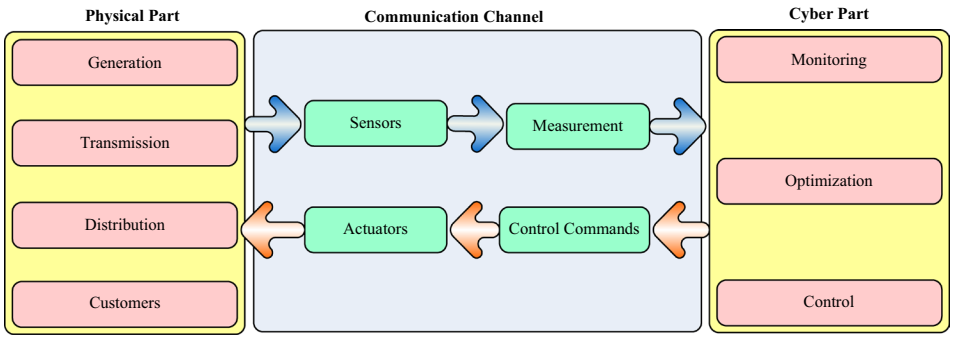

Fig. 9 Cyber-physical structure of smart grid [107]

allows the attacker to produce high impact on the physical system. Therefore, in order to spot the attacker at physical device layering, various control devices should be installed and monitored. Energy buffer is also used to detect errors and cyber-attack at points of common coupling and buses. Further, the smart inverter can also detect cyberattacks, system anomalies and other events.

Cyber-security

Similar to physical security, cyber security of the grid needs to incorporate physical aspects. Cyber security is a component in the expansion of the smart grid [109]. The attacker may lead the system to disastrous consequences by utilizing the mechanism of the control system to lock the operator out of the system. Therefore, an extensive range of cyber security is required to prevent the attacker from acquiring access over the cyber grid network. A secured wired and wireless network must be provided for reliable connection between the control center, substation& actuator. Numerous approaches are developed to check both network communication and control devices within the system. Smart inverters, SCADA system measurement, smart meters, and WAN networks (Wide area network) are the basic databases that can be trusted to identify malicious threats.

Generation system attack

The power system is a complex enterprise and is managed by its analogous control devices; generating station is one of them. Electrical power generated is step-up so that the load generation balance can be maintained to meet the dynamic load demand. In order to maintain balance frequency and power, load–frequency control should be monitored. Load–frequency control manages turbine speed and generator output by using a primary controller while the secondary controller manages system frequency. An attacker can manipulate data in these controllers by opening and closing the circuit breaker of the generator. This instability in generating system desynchronizes the generator and ultimately hampers the stability. In addition to this, the attacker can mislead the frequency controller into performing fake frequency determination for load shedding in the generation system, which exerts significant loss and delays in the generation of power [110–112].

Transmission system attack

The electric power system is the bulk movement of generated electric power across a long distance through a transmission network to an electrical substation. Long distance transmission network requires reliable communication for control of the power grid, while voltage regulation is operated in the transmission system. Fault-sensing protective relays and circuit breakers are equipped at each end of the line to cut-off faulted conductors and overloaded lines. Protection of the transmission line from cyber-physical attack is usually so critical that it has inspired researchers to investigate the potential of attack targeting the monitoring, communication, and control of power transmission. In the meantime, vulnerabilities in transmission networks are continuously evolving. Some of the important known area of threats where a malicious attack can bypass or access control of the system are transmission line protection breaker control, substation automation mainframe, digital relay computers, communication network, etc. Manipulated control commands or false measurement injected by attacker leads to load shedding, multiple tripping and finally resulting in the massive blackout of transmission grid [113]. Interconnected power transmission grid modeled as multiple substations, where multiple measurements and complex control algorithm control are there. A minimal disturbance in operation, results in sequential loss of substation and its transmission line. An informed attacker can penetrate malicious attacks and gain full control of the substation and transmission network. False data from the attacker's end can manipulate the voltage controller configuration, which results in voltage oscillation and voltage violation in the system [114]. The switching system subsequently steered to an unstable operation state, which can lead to frequency instabilities and cascading failure in the system [115, 116], which results in tripping of lines and circuit breakers. Communication with the help of GPS (global positioning system) satellite in a smart grid transmission system are more accurate and provides time stamp to all PMU data so that measurement can be synchronized to enhance the interconnected power system. However, the attacker can spoof the GPS signal to provide a fake time stamp, which induces error in the transmission line, resulting in miscalculation. Spoofing also changes the clock offset of PMU, which increases false alarms in the voltage stability control system, leading to a shutdown of transmission services.

Distribution system attack

The power distribution system is the stage in the delivery of electric power. The distribution substation is connected to the transmission system to manage the transmitted voltage at the distribution transformer located near customer's premises. Smart meters have been installed in the distribution system of the smart grid for two-way communication between grid and customer for advance metering infrastructure (AMI). Advanced metering infrastructure is composed of a controller, energy display, and communication network. Communication from the grid to smart meter to the customer may occur via signaling and GPS. Bringing functionality like this to a power distribution system without incorporating security increases the probability of attack in large-scale areas like reasons of countries and cities [117]. The victims may face network blockade or blackout for an extended period of time [118].

Requirements of cyber-physical structure of smart grid

Cyber-attack prevention includes communication security, protecting sensor data, system architecture control security, access to system security control, machine learning-based algorithms to detect irregularity, cloud-based information security, communication system security, cybersecurity based on game theory approach, encryption, data privacy/integrity, filtering of bad-data, pre-estimation of bad-data, cryptographic algorithm and encryption mechanism [119]. Smart grids need to define their section of security control deriving from a standard, such as ISA (Industry Standard Architecture) [120], (National Institute of Standard and Technology) NIST SP800-53 [121], ISO 27002 (International organisation of Standardization) [122], NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) [123]. Figure 10 presents an overview of NIST updated smart grid infrastructure model with a composite high-level view of seven different areas of generation, operation, market, transmission, distribution, service provider, and customer [29, 29]. Each area and its sub-domain initiate technical roles and assistance for the smart grid. The generation unit produces electric energy with innovative systems and technologies in the smart grid, which involves nuclear fossil fuels, tidal force, hydroelectric, wind, and solar [124–126]. The deepening amalgamation of the renewable energy system is helping to improve the sustainability of these generation systems.

Transmission and distribution systems use smart substations, which can be remotely handled with a sensor and smart electrical devices. The PMU utilizes GPS to provide high resolution and reliable measurement in the transmission system, aiding the execution of wide-area monitoring, protection and control over high-speed communication [127]. The AMI is implemented with an intelligent meter, sensor, and sensor network in the distributed system that provides innovative two-way, real-time communication in the smart grid which monitors demand response, consumer engagement, energy management, and power quality deficiencies. The energy storage, electric vehicles, industrial area and other emerging technology on customer side continuously demands up-gradation to the generation, transmission, and distribution of electricity.

The smart power system (smart generation network, smart transmission network, smart sub-station and smart control center) depends on a communication system for stable and dynamic control as the system requirement is based on the information and IT security. Therefore, the communication system in smart grid has inducted numerous cyber infrastructures with the power system. Computation and information are continuously initiated and transmitted between power system and cyber systems. On the basis of this computation and measurement, optimal control policies are determined in order to handle the situation and command to coordinate actuator in the smart grid power system. Communication in these intelligent grid mainly requires SCADA system and network, or PLCC system. The fact that SCADA system work for remote site and network, therefore, are being unified with external system, creates new possibilities in power systems. This is because, SCADA system and network are more reliable, accurate, provide information in real-time, can give trend-analysis report, allow system to perform dynamic maintenance without any operation hindrance, which increases life-span of the system equipment. But on the other hand, they are extremely vulnerable to threat. As a consequence, ground of cyber-physical structure of smart grid is to conceptualize

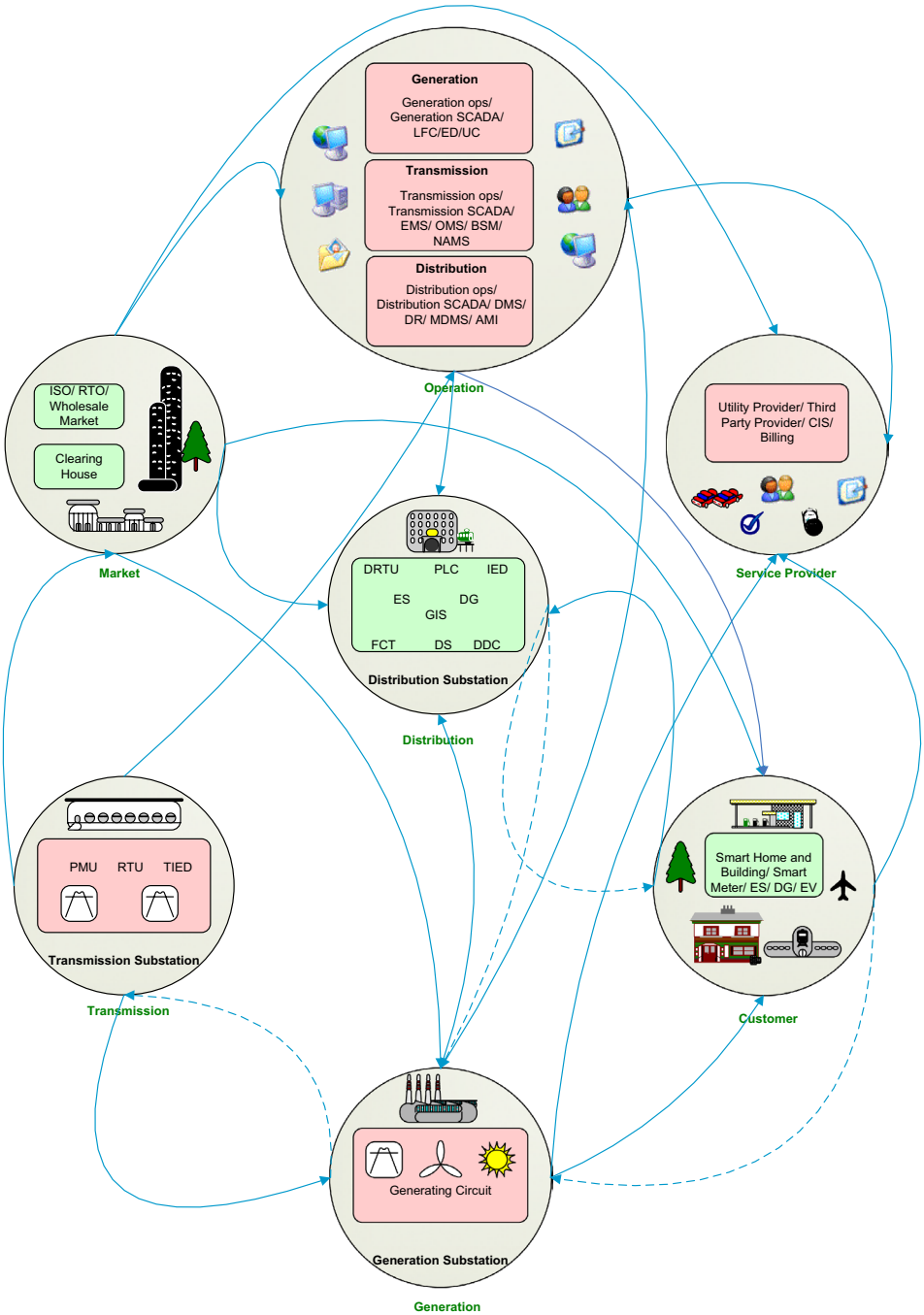

Fig. 10 Revised smart grid conceptual model by National Institute of Standard and Technology [29]. PMU, Phasor Measurement Unit; T-RTU, Transmission Remote Terminal Unit; TIED, Transmission Intelligent Electronic Device; ISO, Independent System Operator; RTO, Regional Transmission Organization; LFC, Load Frequency Control; ED, Economic Dispatch; UC, Unit Commitment; EMS, Energy Management Systems; OMS, Outage Management Systems; BSM, Bulk Storage Management; WAMS, Wide-Area Management System; DMS, Distributed Management System; DR, Demand Response; MDMS, Meter Data Management System; AMI, Advance Metering Infrastructure; CIS, Customer Information System; ES, Energy Storage; DG, Distributed Generation; EV, Electric Vehicle; D-RTU, Distributed Remote Terminal Unit; PLC, Programmable Logic Circuit; IED, Intelligent Electronic Device; GIS, Geographic Information System; FCT, Field Crew Tool; DS, Distributed Sensor; DDC, Distributed Data Collector

for every specific domain (generation substation, transmission substation, distribution substation, operation unit, market, service provider and consumer). Therefore, new communication standard and protocol such as DNP-3 (Distributed Network protocol) and IEC-61850 (International Electro-technical commissions) have been developed and introduced for communication in smart grid, substation and control centers in order to accommodate the integration of PMU, renewable energy and energy storage. This provides an atmosphere that involves possible digital entrance and its exposures.

Types of cyber-physical-attack in smart grid and general defense measure

This section of work offers a synopsis of various possible cyber-attacks in accordance with the cyber and the physical systems. Cyber-attack refers to a scheme to manipulate or introduce the potential vulnerabilities in the cyber system assembly of data-driven smart power grids [128, 129]. The devices such as smart inverters, battery controllers, and cloud data storage introduce vulnerabilities as the communication network connects them to a central monitoring and control station. The communication network generally has remote access to the control center for operators via a communication channel. The attacker may attack the communication system and accomplish a malicious cyber-attack on the communication protection relay. Eventually, it trips the circuit breaker, resulting in blackouts [130, 131]. Another critical threat in the smart grid is measurement-based attacks [132]. In this, the attacker manipulates the measured data and weakens the situational awareness by misleading control action, i.e., by reporting false contingencies. Further, a malicious act in the smart grid known as volumetric attack, in this kind of attack the attacker transmit a substantial amount of network-traffic to the recipient, thereby debilitating the smart grid system or cramping the network infrastructure [133]. The most common outcome of these attacks on the smart grid can be an operational failure, synchronization loss, interruption in power supply, severe financial damage, complete blackout, social welfare damage, data theft, and cascading failure [134]. It may impact the overall power system supply at all levels, including power system control, generation, transmission, and distribution.

Another method of cyber-attack includes barring the communication for data transfer. Barring the communication is accomplished by overflowing the communication channel with massive data traffic or by introducing a mechanism that triggers a communication crash. This phenomenon eventually leads to the deprivation of data to legitimate users. Another cyber-attack includes replaying/resending the same data over a long time to misdirect the legitimate users to do a particular action as per the hacker's desire [135]. Another practice of cyber threat is a malware attack, where an attacker injects malicious software to control systems to disrupt and destroy the conventional operation of the digital network by manipulating the threshold value. Another type of program attack is a web threat, where the attacker intrudes and keeps track of routing information in the web application. In this type of attack, the attacker's inclination is toward peculiar information, for example- a password or initiating a command. In a cross-site-scripting attack, multiple malicious data content is communicated in the transmission channel toward target browser; when the target network operation is set-forth, malicious data is broadcasted and exposed to vulnerabilities. Covert attack, in this type of attack the attackers uses systems specific information in order to monitor and control the transmit

signal, accordingly the attacker construct a concealed and secure attack substructure with the help of systems' precise information, which further injected in channel of measurement and actuation [136–138]. Thus, the following attacks are repeatedly followed by cyber-intruder for malfunctioning the communication links of data-driven smart grids.

1. False data injection attack
2. Denial-of-services attack
3. Replay attack
4. Malware-virus attack
5. Web-attack
6. XXs-attack

Since monitoring of generator unit, transmission system, substation system, smart inverter, smart meter, communication between the control center and actuator produces a huge amount of data. These data are to be kept in the cloud-based system or any remote high-security data centers; these data are more vulnerable to launch attacks. Extensive investigation on cyber threat schemes has announced grid operators establishing various defense mechanisms, divided into two stages- protection and detection.

Protection

A cyber-physical structure like a smart grid contributes a large volume of data. Protection of these data is very critical. Protection against cyber threats generally relies on the building of secured communication, conserving critical information, monitoring intrusion, use of secure software, controlling access to system and data, smart inverter, SCADA system measurement, smart meter, WAN network, physical security, cyber security, encryption, meter safety, data privacy, data integrity and mitigation of exposed vulnerabilities. Along with this, the direction of approach with technical execution (network, and physical security, encryption, meter safety, data privacy, and data integrity) instigate the system security. Mixed integer liner program optimization, game-theoretic approach, graph-based approach, state estimation approach and meter measurement approach etc. [139–144] have been proposed for false data injection type attack. Method for determining load-distribution attack is developed in [145]. Data accumulation in AMI of a smart meter is one of the primary targets for attackers [146]. Therefore, a secure distribution mechanism and key management have been proposed as the best protection against unauthorized access to smart meters [147]. Cloud-based information and communication technology is one more target for attackers. Therefore, a secure and flexible information management structure with cloud computing configuration is developed in [148]. The architecture of cloud computing consists of two parts—(a) Front-end and (b) back-end. Front-end is comprised of web servers and contains user side interface to access the computing platform, while the back-end is owned by a service provider, which includes an enormous amount of virtual machines, data storage, security-mechanism, traffic-control-mechanism server, and deploying models. For secure communication, cloud computing has four major components—(a) infrastructure services, (b) software services, (c) platform services and (d) data services. And have

four main clusters for configuration—(a) general user service, (b) control and management services, (c) information service, and (d) electricity distribution service [149].

Detection

Despite efficient threat protection for the smart grid, an attacker still have control over the exposed or vulnerable component. In case of such protection failure, machine learning-based bad-data detection algorithm [150], sensor-based bad-data detection [151], filtering of bad-data detection [152], pre-estimation-based bad-data detection [153], model-based approach [154], game-theoretic approach [155], hypothesis testing detection method [156], improved Kalman filtering method [157], and federated learning-based detection mechanism [158] have been an obvious choice to provide effective security and countering against cyber threat. These methods, as mentioned above, identifies five significant types of intrusion in the system—(a) detect an attack from their signature, (b) detect the attack by deviating from the normal system behavior, (c) combination of anomaly and misused base method [159], (d) detect the attack at event management security of information system, (e) detects an attack from there communication pattern on transmission traffic. Furthermore, these methods are capable of identifying attacks that are unnoticeable.

Effect of cyber-attack on island detection

This section of the paper investigates the effect of the cyber- attack on island detection algorithms. Cyber-attack can manipulate and restrict data flowing through communication channels, which endangers island detection methods' success. Thus, a proper analysis is required, and possible solutions must be found.

False data injection attack

False data injection attack, a classification of integrity attack is the major category of cyber-attack in island detection. In this, the attacker target and modify the measurement vector and sabotage the real-time data [160]. The attacker induces false data to unstabilize the operation to disrupt the islanding detection technique. When the attacker induces false data to manipulate the threshold value of the relay setting to a different value, a false triggering happens. Even if there is no fault in the system, the attacker can inject false data, which leads to false islanding detection that could lead to load shedding and unnecessary generation rescheduling.

In the remote islanding detection method, the basic principle is communication between the main utility grid and distribution generation via the SCADA system, PLCC scheme, and the transfer trip method. As discussed in "Remote islanding detection method" section of this paper, these methods use computers, servers, and various electronic devices, which are very prone to false data injection attacks. Attackers can induce false data in any server or device to disrupt the operation, which may lead to a failure of the island detection method. Therefore, the remote island detection method requires physical security as it uses various electronic equipment and cyber security, as the communication and transmission are via server or modem, as discussed in "Cyber-physical security of smart grids" section. Various

methods discussed in [152, 153, 161] can be introduced in remote techniques to detect island conditions and protect the system from cyber-attack.

Furthermore, in the case of local island detection method (passive island detection technique, active island detection technique, and hybrid island detection technique), frequency, voltage, and harmonics are monitored and injected respectively against a pre-defined threshold limit for detection. The attacker can inject false data to manipulate threshold values which could affect analyzing the parameters. This false data injection attack can be in generation, transmission, or distribution systems, which may lead to a fake island or no island detection. This leads to the failure of the local island detection method. Therefore, a graph-based approach [142], linear program operation [139], and protection method by machine learning-based bad-data detection algorithm [150] are required in local techniques. Further in-case of the signal processing island detection method and in the intelligence-based island detection method, a false data injection attack may work if the signal processing unit rapidly adapts new data format.

Denial-of-services attack

A denial-of-service attack is a data intrusion type attack, i.e., the attacker does not allow any information to pass through the transmission to receiving side. In this, a blockage mechanism is introduced so that a communication channel is obstructed between the remote and the main grid. In a smart grid distribution system, energy and information flow are bi-directional via communication links like modem, wireless point, server, and monitor control. Therefore, cyber-attack is always possible. Attacker target devices like PMU, μPMU, USB (Universal Serial Bus), Intelligent electronic devices, smart meter, main computer server, smart inverter and communication network which are connected to GPS system. Thus, when island condition occurs, the information is not transferred, leading to communication failure, and hence the DG remains unaware of the island situation. Significantly it affects the performance of the power system in the islanded grid.

As the above-mentioned attack is a data-driven type of attack and remote island detection is based on communication infrastructure, an attacker can easily obstruct the communication channel leading to the failure of the method. Therefore, a secure and flexible structure with cloud computing configuration [148] and filtering of bad data [152] protection and detection can be developed in remote techniques. Similarly, in case of local island detection methods (passive island detection technique, active island detection technique, and hybrid island detection technique), an attacker cannot affect passive and hybrid methods if they work on the traditional ROCOF method on not receiving any signal, but active methods fail to detect this denial-of-service attack as the technique deal by injecting perturbation into the grid system variable. Therefore, secure configuration [149] and pre-estimation-based bad-data detection [153] can be introduced to make it cyber-proof. For the signal processing island detection method and intelligence-based island detection method, the denial-of-service attack may be avoided if the island detection method uses the traditional ROCOF method on not receiving any signal.

Replay attack

Due to the interdependence of all islanding detection methods on wireless sensor communication channels, the attacker may use multiple identities and attack the traffic flow of the signal. As the attacker in replay attack has previous snap short of legitimate data, which can mislead the system for a longer time leading to fake or no island detection. Also, in a replay attack, the attacker gets access to the control system of the smart meter or inverter and injects a fake or modified signal into the system, causing false triggering.

The remote island detection method uses PLCC scheme, SCADA network system and control devices etc., for secure cyber communication between generation-transmission-distribution systems. Thus, replay attackers can get easy access to the control system of SCADA, PLCC, and smart inverter etc. Therefore, the remote island detection method fails to detect replay attack disturbance. Thus, a new approach for protection, such as methods used in [140, 141, 152, 155] can be used against replay attacks. In the case of local island detection method (passive island detection technique, active island detection technique, and hybrid island detection technique) replay attackers may get detected as they use a time-shifted version of the original data, but the detection totally depends on the nature of GOOSE method. Further, signal processing island detection method and intelligence-based island detection method may work against replay attacks with the use of cloud-based information and communication technology [148], machine learning-based bad-data detection algorithm [150], sensor-based bad-data detection algorithm [151], filtering of bad-data detection [152], and pre-estimation based bad data detection [153].

A similar explanation and remedial measures follow for the malware-virus attack, web attack and XXs-attack. The remote methods fail under malware-virus attacks and web-attack. However, XXS-attack may not work on SCADA and transfer tripping. The active methods fail under malware-virus attacks and web-attack. However, XXs-attack may be avoided by using the proper disturbance injection method. The case is reversed for passive methods where it is able to handle malware-virus attacks and web-attack but not XXs-attack. Also, the signal processing and intelligence methods are unable to check XXs-attack. Hybrid methods are somewhat able to handle malware-virus attack, web-attack, and XXs-attack.

Thus, in case of false triggering of islanding, achieved through an attack, that particular islanded grid gets compromised and loses power leading to a blackout in the region. Further, if there is a real islanding situation, but the attacker formulates the outcome, and no signal is received, then the islanded portion will encounter severe fluctuation in voltage and frequency, which damages the load to an intense degree. This false islanding detection during the normal condition and also the other way round results in frequency and voltage differences between islanded grid and the main grid. For reconnecting with the main grid, frequency and voltage in this islanded grid must be synchronized accordingly with the main grid. If this synchronization is not done as per the main grid, then a huge circulating current can flow in the grid, causing extensive damage. Thus, under the real undesirable islanding scenario and false islanding scenario, the reliability and resiliency of the grid get reduced due to the cyber-attacks. Another major consequence of cyber-attack is to the maintenance

Table 8 Comparison of effect of cyber-attacks on various island detection methods

Island detection methods	Type of cyber attack					
	Denial-of-services attack	**False data injection**	**Replay attack**	**Malware-virus attack**	**Web-attack**	**Cross-site-scripting attack**
Remote	Fail	Fail	Fail	Fail	Fail	May work on SCADA and transfer tripping
Active	Fail	May fail (depends on the nature of VPN)	May fail (depends on the nature of GOOSE message)	Fail	Fail	May work (depend on nature of phase perturbation injection)
Passive	May work if it works on traditional ROCOF on not receiving any signal	May fail (depends on the nature of VPN)	May fail (depends on the nature of GOOSE message)	May work if it works on traditional ROCOF on not receiving any signal	May work if it works on modified Kalman filter based technique	Fail
Hybrid	May work if it works on traditional ROCOF on not receiving any signal	May fail (depends on the nature of VPN)	May fail (depends on the nature of GOOSE message)	May work if it works on traditional ROCOF on not receiving any signal	May work if it works on modified Kalman filter based technique	May work (depend on nature of fluctuation injection)
Signal Processing	May work if it works on traditional ROCOF on not receiving any signal	May work if the signal processor rapidly adapts to new data formats	May work if the signal processor detects bad data	May work if the signal communication is through cloud based information and communication technology	May work with Deep learning techniques and cloud computing	Fail
Intelligence	May work if it works on traditional ROCOF on not receiving any signal	May work if the classifier is also trained for false data detection	May work with Deep learning techniques	May work if the signal communication is through cloud based information and communication technology	May work with Deep learning techniques and cloud computing	Fail

team of the islanded grid, who are ignorant of the actual scenario of the islanded condition of the grid and are still in action. Thus, developing a cyber-secured island detection algorithm must be of prime importance.

The comparison of the effect of cyber-attacks on various island detection methods is given in Table 8. It can be seen from the table that the remote methods are most affected by the cyber-attacks as their principle of working is based mainly on the communication network. For active methods, a denial of services attack disrupts its functioning since the effect of introducing the disturbance injection is required for its functioning, which depends on the communication system. For false data injection, active, passive as well as hybrid methods may overcome the threat if it uses a proper virtual portable network (VPN). Application of a proper generic object-oriented substation event (GOOSE) message can obstruct replay attack to some extent for all the local island detection methods. If the passive, hybrid, signal processing, and intelligence methods works on traditional ROCOF on not receiving any signal, then it can avoid denial of services attacks to a limited extent. The signal processing techniques may rapidly adapt to new data formats and detect bad data to counter false data injection and replay attacks. The intelligence technique may use deep learning techniques to detect false data and replaying if data. Thus, as signal processing and intelligence technique are advanced in handling cyber threats, these island detection methods are least affected by cyber threats.

Conclusion

The objective of the paper is to motivate the researchers to develop an island detection method that is capable of handling cyber threats. The interval span of the survey is considered from 1990s to the present time. However, to stress on the recent methods, the majority of the research papers considered in this survey is taken after 2010. Although there are many papers on island detection methods and cyber security methods in power systems, no papers connect these two according to the authors' best knowledge. Thus, this paper tries to establish the connection between island detection methods and cyber threats. The paper analyses the island detection methods in terms of cyber security rather than reviewing any papers which deal with cyber-proof island detection methods (as there are no papers available). The objective is achieved by reviewing the prevailing islanding detection techniques and the theory, mechanism as well as control techniques of cyber-attack. After that, the effect of cyber-attack on island detection methods is further investigated. Moreover, probable measures to counter these issues in island detection methods by using machine learning techniques, computational techniques, filtering techniques, model-based approaches, etc., have also been discussed. Hence, the paper provides a narrative perspective of island detection methods under the lens of cyber-attack in a data-driven smart grid. This narrative perspective hints at opening new research gates for building cyber-secured IT-based island detection methods in the future. Some of them are mentioned as per the following:

1. Designing of a universal standard required for secured data communication in island detection methods.
2. Modifications of old protocols or introduction of new protocols for threat-free data transmission.

3. Utilizing advanced machine learning techniques, blockchain technology, and statistical-based new island detection methods capable of mitigating cyber-attack efficiently.
4. Analyzing cloud-based island detection approach possessing the ability to dynamically learn from past attacks and capable of self-healing after errors.
5. Revisiting smart inverters and smart meters in a smarter way to provide a tailored solution to cyber-attacks.

Acknowledgements
Not applicable.

Author contributions
AS developed the methodology. SD and SKS handled the writing process. PKS obtained the tabular data. All authors read and approved the final manuscript.

Funding
Not applicable.

Availability of data and materials
No dataset generated as it is a review paper.

Declarations

Competing interests
The authors declare that they have no competing interests.

Received: 2 September 2022 Accepted: 25 February 2023
Published online: 14 March 2023

References

1. Saleh SA, Aljankawey AS, Meng R, Meng J, Chang L, Diduch CP (2015) Apparent power-based anti-islanding protection for distributed cogeneration systems. IEEE Trans Ind Appl 52(1):83–98
2. Dey B, Dutta S, Garcia Marquez FP (2023) Intelligent demand side management for exhaustive techno-economic analysis of microgrid system. Sustainability 15(3):1795
3. Cao Q, Liu F, Zhu G, Chen W (2015) PMU based islanding detection method for large photovoltaic power station. In: 2015 IEEE 11th international conference on power electronics and drive systems. IEEE, pp 126–131
4. Yu B, Matsui M, Yu G (2010) A review of current anti-islanding methods for photovoltaic power system. Sol Energy 84(5):745–754
5. Chowdhury SP, Chowdhury S, Crossley PA (2009) Islanding protection of active distribution networks with renewable distributed generators: a comprehensive survey. Electr Power Syst Res 79(6):984–992
6. Photovoltaics DG, Storage E (2009) IEEE application guide for IEEE Std 1547™. IEEE standard for interconnecting distributed resources with electric power systems
7. IEC, S (2004) Photovoltaic (PV) systems characteristics of the utility interface. IEC Std 61:727
8. Xue Y, Yu X (2017) Beyond smart grid—cyber–physical–social system in energy future [point of view]. Proc IEEE 105(12):2290–2292
9. Adamiak MG, Apostolov AP, Begovic MM, Henville CF, Martin KE, Michel GL, Phadke AG, Thorp JS (2006) Wide area protection—technology and infrastructures. IEEE Trans Power Deliv 21(2):601–609
10. Hashemi-Dezaki H, Askarian-Abyaneh H, Haeri-Khiavi H (2016) Impacts of direct cyber-power interdependencies on smart grid reliability under various penetration levels of microturbine/wind/solar distributed generations. IET Gener Transm Distrib 10(4):928–937
11. Musleh AS, Khalid HM, Muyeen SM, Al-Durra A (2017) A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications. IEEE Syst J 13(1):710–719
12. Masood S (2021) Much of Pakistan loses power in massive blackout. The New York Times. ISSN 0362-4331. Retrieved 10 Jan 2022
13. Venezuela sufre el tercer apagón en solo tres semanas., March 29, 2019.Telemundo 51 (**in Spanish**)
14. Huge power outage leaves most of Venezuela in darkness., Retrieved 9 Mar 2019
15. Arroyo L (2019) Denuncian ONGs: apagón deja al menos 43 pacientes muertos en Venezuela [NGOs denounce: blackout leaves at least 43 patients dead in Venezuela]
16. Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S (2010) Catastrophic cascade of failures in interdependent networks. Nature 464(7291):1025–1028
17. Soltan S, Yannakakis M, Zussman G (2016) Power grid state estimation following a joint cyber and physical attack. IEEE Trans Control Netw Syst 5(1):499–512
18. Fairley P (2016) Cybersecurity at us utilities due for an upgrade: tech to detect intrusions into industrial control systems will be mandatory [news]. IEEE Spectr 53(5):11–13

19. Falliere N, Murchu LO, Chien E (2011) Symantec security response: W32. stuxnet dossier. Symantec Corporation, Tempe
20. Min B, Varadharajan V (2014) Design and analysis of security attacks against critical smart grid infrastructures. In: 2014 19th international conference on engineering of complex computer systems. IEEE, pp 59–68
21. Bou-Harb E, Fachkha C, Pourzandi M, Debbabi M, Assi C (2013) Communication security for smart grid distribution networks. IEEE Commun Mag 51(1):42–49
22. (2009) US electrical grid compromised. Network Security 2009(4):20. ISSN 1353-4858. https://doi.org/10.1016/S1353-4858(09)70044-3
23. Sabotaging the system. CBS News. August 29, 2010. Archived from the original on November 10, 2009
24. Wu YK, Chang SM, Hu YL (2017) Literature review of power system blackouts. Energy Procedia 141:428–431
25. Wang W, Lu Z (2013) Cyber security in the smart grid: survey and challenges. Comput Netw 57(5):1344–1371
26. Sissine F (2016) DOE's office of electricity delivery and energy reliability (OE): a primer, with appropriations for FY2016. Library of Congress, Congressional Research Service
27. Assessment LTR (2009) North American Electric Reliability Corporation (Nerc). Atlanta, GA
28. NIST I (2014) 7628 Revision 1:"guidelines for smart grid cyber security"
29. Greer C, Wollman DA, Prochaska D, Boynton PA, Mazer JA, Nguyen C, FitzPatrick G, Nelson TL, Koepke GH, Hefner Jr, AR, Pillitteri VY (2014) Nist framework and roadmap for smart grid interoperability standards, release 3.0
30. National Electric Sector Cybersecurity Organization Resource (NESCOR): 'wide area monitoring, protection, and control systems (WAMPAC)—standards for cyber security requirements', 2012. http://www.smartgrid.epri.com/doc/ESRFSD.pdf
31. Verma S, Dutta S, Sadhu PK, Reddy MJB, Mohanta DK (2019) Islanding detection using bi-directional energy meter in a DFIG based active distribution network. In: 2019 international conference on computer, electrical & communication engineering (ICCECE). IEEE, pp 1–4
32. Dutta S, Verma S, Sadhu PK, Reddy MJB, Mohanta DK (2019) Islanding detection in a distribution system: a pattern assessment based approach using Concordia analysis. In: 2019 20th international conference on intelligent system application to power systems (ISAP). IEEE, pp 1–5
33. Abokhalil AG, Awan AB, Al-Qawasmi AR (2018) Comparative study of passive and active islanding detection methods for PV grid-connected systems. Sustainability 10(6):1798
34. Noor F, Arumugam R, Vaziri MY (2005) Unintentional islanding and comparison of prevention techniques. In: Proceedings of the 37th annual North American power symposium, 2005. IEEE, pp 90–96
35. Jiayi H, Chuanwen J, Rong X (2008) A review on distributed energy resources and MicroGrid. Renew Sustain Energy Rev 12(9):2472–2483
36. Teoh WY, Tan CW (2011) An overview of islanding detection methods in photovoltaic systems. World Acad Sci Eng Technol 5:1341–1349
37. Velasco D, Trujillo CL, Garcerá G, Figueres E (2010) Review of anti-islanding techniques in distributed generators. Renew Sustain Energy Rev 14(6):1608–1614
38. Li C, Cao C, Cao Y, Kuang Y, Zeng L, Fang B (2014) A review of islanding detection methods for microgrid. Renew Sustain Energy Rev 35:211–220
39. Do HT, Zhang X, Nguyen NV, Li SS, Chu TTT (2015) Passive-islanding detection method using the wavelet packet transform in grid-connected photovoltaic systems. IEEE Trans Power Electron 31(10):6955–6967
40. Barsali S, Ceraolo M, Pelacchi P, Poli D (2002) Control techniques of dispersed generators to improve the continuity of electricity supply. In: 2002 IEEE power engineering society winter meeting. Conference proceedings (Cat. No. 02CH37309), vol 2. IEEE, pp 789–794
41. Trujillo C, Velasco D, Figueres E, Garcerá G (2010) Local and remote techniques for islanding detection in distributed generators. Distrib Gener 119-140
42. Khamis A, Shareef H, Bizkevelci E, Khatib T (2013) A review of islanding detection techniques for renewable distributed generation systems. Renew Sustain Energy Rev 28:483–493
43. Reddy C, Reddy KH (2019) A new passive islanding detection technique for integrated distributed generation system using rate of change of regulator voltage over reactive power at balanced islanding. J Electr Eng Technol 14(2):527–534
44. Ahmad KNEK, Selvaraj J, Abd Rahim N (2013) A review of the islanding detection methods in grid-connected PV inverters. Renew Sustain Energy Rev 21:756–766
45. Ding X, Crossley PA (2005) Islanding detection for distributed generation. In: 2005 IEEE Russia power tech. IEEE, pp 1–4
46. Freitas W, Xu W, Affonso CM, Huang Z (2005) Comparative analysis between ROCOF and vector surge relays for distributed generation applications. IEEE Trans Power Deliv 20(2):1315–1324
47. Jia K, Bi T, Liu B, Thomas D, Goodman A (2014) Advanced islanding detection utilized in distribution systems with DFIG. Int J Electr Power Energy Syst 63:113–123
48. Haider R, Kim CH, Ghanbari T, Bukhari SBA, uz Zaman MS, Baloch S, Oh YS (2018) Passive islanding detection scheme based on autocorrelation function of modal current envelope for photovoltaic units. IET Gener Transm Distrib 12(3):726–736
49. Singam B, Hui LY (2006) Assessing SMS and PJD schemes of anti-islanding with varying quality factor. In: 2006 IEEE international power and energy conference. IEEE, pp 196–201
50. Pai FS, Huang SJ (2001) A detection algorithm for islanding-prevention of dispersed consumer-owned storage and generating units. IEEE Trans Energy Convers 16(4):346–351
51. Salles D, Freitas W, Vieira JC, Venkatesh B (2014) A practical method for nondetection zone estimation of passive anti-islanding schemes applied to synchronous distributed generators. IEEE Trans Power Deliv 30(5):2066–2076

52. Salman SK, King DJ, Weller G (2001) New loss of mains detection algorithm for embedded generation using rate of change of voltage and changes in power factors. In: 2001 Seventh international conference on developments in power system protection (IEE). IET, pp 82–85
53. O'kane P, Fox B (1997) Loss of mains detection for embedded generation by system impedance monitoring. In: Sixth international conference on developments in power system protection (Conf. Publ. No. 434). IET, pp 95–98
54. De Mango F, Liserre M, Dell'Aquila A (2006) Overview of anti-islanding algorithms for PV systems. Part II: active methods. In:2006 12th international power electronics and motion control conference. IEEE, pp 1884–1889
55. Jang SI, Kim KH (2004) An islanding detection method for distributed generations using voltage unbalance and total harmonic distortion of current. IEEE Trans Power Deliv 19(2):745–752
56. Laghari JA, Mokhlis H, Karimi M, Bakar AHA, Mohamad H (2014) Computational intelligence based techniques for islanding detection of distributed generation in distribution network: a review. Energy Convers Manag 88:139–152
57. Skocil T, Gomis-Bellmunt O, Montesinos-Miracle D, Galceran-Arellano S, Rull-Duran J (2009) Passive and active methods of islanding for PV systems. In: 2009 13th European conference on power electronics and applications. IEEE, pp 1–10
58. Reddy CR, Reddy KH (2019) Ndz analysis of various passive islanding detection methods for integrated dg system over balanced islanding. Int J Integr Eng 11(8):206–220
59. Hamzeh M, Farhangi S, Farhangi B (2008) A new control method in PV grid connected inverters for anti-islanding protection by impedance monitoring. In: 2008 11th workshop on control and modeling for power electronics. IEEE, pp 1–5
60. Bei TZ (2017) Accurate active islanding detection method for grid-tied inverters in distributed generation. IET Renew Power Gener 11(13):1633–1639
61. Jou HL, Chiang WJ, Wu JC (2007) Virtual inductor-based islanding detection method for grid-connected power inverter of distributed power generation system. IET Renew Power Gener 1(3):175–181
62. Chiang WJ, Jou HL, Wu JC (2012) Active islanding detection method for inverter-based distribution generation power system. Int J Electr Power Energy Syst 42(1):158–166
63. Akhlaghi S, Akhlaghi A, Ghadimi AA (2016) Performance analysis of the slip mode frequency shift islanding detection method under different inverter interface control strategies. In: 2016 IEEE power and energy conference at Illinois (PECI). IEEE, pp 1–7
64. Lopes LA, Sun H (2006) Performance assessment of active frequency drifting islanding detection methods. IEEE Trans Energy Convers 21(1):171–180
65. Liu F, Kang Y, Zhang Y, Duan S, Lin X (2010) Improved SMS islanding detection method for grid-connected converters. IET Renew Power Gener 4(1):36–42
66. Zeineldin HH, Kennedy S (2008) Sandia frequency-shift parameter selection to eliminate nondetection zones. IEEE Trans Power Deliv 24(1):486–487
67. Zeineldin HH, Conti S (2011) Sandia frequency shift parameter selection for multi-inverter systems to eliminate nondetection zone. IET Renew Power Gener 5(2):175–183
68. Bahrani B, Karimi H, Iravani R (2009) Nondetection zone assessment of an active islanding detection method and its experimental evaluation. IEEE Trans Power Deliv 26(2):517–525
69. Trujillo CL, Velasco D, Figueres E, Garcerá G (2010) Analysis of active islanding detection methods for grid-connected microinverters for renewable energy processing. Appl Energy 87(11):3591–3605
70. Ropp ME, Begovic M, Rohatgi A (1999) Analysis and performance assessment of the active frequency drift method of islanding prevention. IEEE Trans Energy Convers 14(3):810–816
71. Reigosa D, Briz F, Blanco C, García P, Guerrero JM (2013) Active islanding detection for multiple parallel-connected inverter-based distributed generators using high-frequency signal injection. IEEE Trans Power Electron 29(3):1192–1199
72. Reigosa D, Briz F, Charro CB, García P, Guerrero JM (2012) Active islanding detection using high-frequency signal injection. IEEE Trans Ind Appl 48(5):1588–1597
73. Karimi H, Yazdani A, Iravani R (2008) Negative-sequence current injection for fast islanding detection of a distributed resource unit. IEEE Trans Power Electron 23(1):298–307
74. Tuyen ND, Fujita G (2011) Negative-sequence current injection of dispersed generation for islanding detection and unbalanced fault ride-through. In: 2011 46th international universities' power engineering conference (UPEC). VDE, pp 1–6
75. Pal D, Panigrahi BK (2020) Analysis and mitigation of the impact of ancillary services on anti-islanding protection of distributed generators. IEEE Trans Sustain Energy 11(4):2950–2961
76. Khamis A, Shareef H, Mohamed A, Bizkevelci E (2015) Islanding detection in a distributed generation integrated power system using phase space technique and probabilistic neural network. Neurocomputing 148:587–599
77. Bower WI, Ropp M (2002) Evaluation of islanding detection methods for utility-interactive inverters in photovoltaic systems (No. SAND2002-3591). Sandia National Lab. (SNL-NM), Albuquerque, NM (United States); Sandia National Lab. (SNL-CA), Livermore, CA (United States)
78. Menon V, Nehrir MH (2007) A hybrid islanding detection technique using voltage unbalance and frequency set point. IEEE Trans Power Syst 22(1):442–448
79. Mahat P, Chen Z, Bak-Jensen B (2009) A hybrid islanding detection technique using average rate of voltage change and real power shift. IEEE Trans Power Deliv 24(2):764–771
80. Laghari JA, Mokhlis H, Bakar AHA, Karimi M (2013) A new islanding detection technique for multiple mini hydro based on rate of change of reactive power and load connecting strategy. Energy Convers Manag 76:215–224
81. Vahedi H, Noroozian R, Jalilvand A, Gharehpetian GB (2010) Hybrid SFS and Qf islanding detection method for inverter-based DG. In: 2010 IEEE international conference on power and energy. IEEE, pp 672–676
82. Chang WY (2010) A hybrid islanding detection method for distributed synchronous generators. In: The 2010 international power electronics conference-ECCE ASIA. IEEE, pp 1326–1330
83. Polikar R (1999) The story of wavelets. Physics and modern topics in mechanical and electrical engineering, pp 192–197

84. Chen S (2005) Feature selection for identification and classification of power quality disturbances. In: IEEE power engineering society general meeting, 2005. IEEE, pp 2301–2306
85. Ray PK, Mohanty SR, Kishor N, Dubey HC (2010) Coherency determination in grid-connected distributed generation based hybrid system under islanding scenarios. In: 2010 IEEE international conference on power and energy. IEEE, pp 85–88
86. Ray PK, Kishor N, Mohanty SR (2010) S-transform based islanding detection in grid-connected distributed generation based power system. In: 2010 IEEE international energy conference. IEEE, pp 612–617
87. Ray PK, Mohanty SR, Kishor N (2011) Disturbance detection in grid-connected distributed generation system using wavelet and S-transform. Electr Power Syst Res 81(3):805–819
88. Karimi M, Mokhtari H, Iravani MR (2000) Wavelet based on-line disturbance detection for power quality applications. IEEE Trans Power Deliv 15(4):1212–1220
89. Afroni MJ, Sutanto D, Stirling D (2013) Analysis of nonstationary power-quality waveforms using iterative Hilbert Huang transform and SAX algorithm. IEEE Trans Power Deliv 28(4):2134–2144
90. Drummond CF, Sutanto D (2010) Classification of power quality disturbances using the iterative Hilbert Huang transform. In: Proceedings of 14th international conference on harmonics and quality of power-ICHQP 2010. IEEE, pp 1–7
91. Singh S, Dutta S, Sahu SK, Sadhu PK (2021) Spectral kurtosis-based island detection technique. In: Advances in smart grid automation and Industry 4.0: select proceedings of ICETSGAI4, vol 0. Springer, Singapore, pp 699–706
92. Sahu SK, Roy M, Dutta S, Ghosh D, Mohanta DK (2023) Machine learning based adaptive fault diagnosis considering hosting capacity amendment in active distribution network. Electr Power Syst Res 216:109025
93. Heidari M, Seifossadat G, Razaz M (2013) Application of decision tree and discrete wavelet transform for an optimized intelligent-based islanding detection method in distributed systems with distributed generations. Renew Sustain Energy Rev 27:525–532
94. Senroy N, Heydt GT, Vittal V (2006) Decision tree assisted controlled islanding. IEEE Trans Power Syst 21(4):1790–1797
95. El-Arroudi K, Joos G, Kamwa I, McGillis DT (2007) Intelligent-based approach to islanding detection in distributed generation. IEEE Trans Power Deliv 22(2):828–835
96. Fukuda T, Shibata T (1992) Theory and applications of neural networks for industrial control systems. IEEE Trans Ind Electron 39(6):472–489
97. Hartmann NB, dos Santos RC, Grilo AP, Vieira JCM (2017) Hardware implementation and real-time evaluation of an ANN-based algorithm for anti-islanding protection of distributed generators. IEEE Trans Ind Electron 65(6):5051–5059
98. Merlin VL, Santos RC, Grilo AP, Vieira JCM, Coury DV, Oleskovicz M (2016) A new artificial neural network based method for islanding detection of distributed generators. Int J Electr Power Energy Syst 75:139–151
99. Goh AT (2002) Probabilistic neural network for evaluating seismic liquefaction potential. Can Geotech J 39(1):219–232
100. Alshareef S, Talwar S, Morsi WG (2014) A new approach based on wavelet design and machine learning for islanding detection of distributed generation. IEEE Trans Smart Grid 5(4):1575–1583
101. Matic-Cuka B, Kezunovic M (2014) Islanding detection for inverter-based distributed generation using support vector machine method. IEEE Trans Smart Grid 5(6):2676–2686
102. Rosolowski E, Burek A, Jedut L (2007) A new method for islanding detection in distributed generation. Wroclaw University of Technology, Wrocław
103. Dash PK, Padhee M, Panigrahi TK (2012) A hybrid time–frequency approach based fuzzy logic system for power island detection in grid connected distributed generation. Int J Electr Power Energy Syst 42(1):453–464
104. Hashemi F, Ghadimi N, Sobhani B (2013) Islanding detection for inverter-based DG coupled with using an adaptive neuro-fuzzy inference system. Int J Electr Power Energy Syst 45(1):443–455
105. Shayeghi H, Sobhani B (2014) Zero NDZ assessment for anti-islanding protection using wavelet analysis and neuro-fuzzy system in inverter based distributed generation. Energy Convers Manag 79:616–625
106. Dutta S, Reddy MJB, Mohanta DK, Kushwah MS, Sadhu PK (2020) μPMU-based intelligent island detection–the first crucial step toward enhancing grid resilience with MG. IET Smart Grid 3(2):162–173
107. Wood AJ, Wollenberg BF, Sheblé GB (2013) Power generation, operation, and control. Wiley
108. Vellaithurai C, Srivastava A, Zonouz S, Berthier R (2014) CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures. IEEE Trans Smart Grid 6(2):566–575
109. Pillitteri VY, Brewer TL (2014) Guidelines for smart grid cybersecurity
110. Liu S, Liu XP, El Saddik A (2013) Denial-of-service (DoS) attacks on load frequency control in smart grids. In: 2013 IEEE PES innovative smart grid technologies conference (ISGT). IEEE, pp 1–6
111. Sargolzaei A, Yen K, Abdelghani MN (2014) Delayed inputs attack on load frequency control in smart grid. In: ISGT 2014. IEEE, pp 1–5
112. Srikantha P, Kundur D (2015) Denial of service attacks and mitigation for stability in cyber-enabled power grid. In: 2015 IEEE power & energy society innovative smart grid technologies conference (ISGT). IEEE, pp 1–5
113. Tweed K (2014) Attack on nine substations could take down US grid. IEEE Spectrum. https://spectrum.ieee.org/attack-on-nine-substations-could-take-down-us-grid. Accessed 29 Sep 2022
114. Sridhar S, Manimaran G (2011) Data integrity attack and its impacts on voltage control loop in power grid. In: 2011 IEEE power and energy society general meeting. IEEE, pp 1–6
115. Liu S, Mashayekh S, Kundur D, Zourntos T, Butler-Purry K (2013) A framework for modeling cyber-physical switching attacks in smart grid. IEEE Trans Emerg Top Comput 1(2):273–285
116. Liu S, Chen B, Zourntos T, Kundur D, Butler-Purry K (2014) A coordinated multi-switch attack for cascading failures in smart grid. IEEE Trans Smart Grid 5(3):1183–1195
117. Díaz Redondo RP, Fernández-Vilas A, Fernández dos Reis G (2020) Security aspects in smart meters: analysis and prevention. Sensors 20(14):3977

118. Diovu RC, Agee JT (2017) A cloud-based openflow firewall for mitigation against DDoS attacks in smart grid AMI networks. In: 2017 IEEE PES PowerAfrica. IEEE, pp 28–33
119. Suo H, Wan J, Zou C, Liu J (2012) Security in the internet of things: a review. In: 2012 international conference on computer science and electronics engineering, vol 3. IEEE, pp 648–651
120. ANSI/ISA-99.02.01-2009 standard, security for industrial automation and control systems part 2: establishing an industrial automation and control systems security program (2009). http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821
121. Mell P, Grance T (2011) NIST Computer Security Division & Computer Security Resource Center, vol 12(2012), pp 800–145. Retrieved January
122. Information technology—security techniques—information security management systems—code of practice for information security management, ISO/IEC 27002:2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297
123. NERC CIP standards as approved by the NERC Board of Trustees (2006). ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf
124. Gungor VC, Sahin D, Kocak T, Ergut S, Buccella C, Cecati C, Hancke GP (2011) Smart grid technologies: communication technologies and standards. IEEE Trans Ind Inf 7(4):529–539
125. Fang X, Misra S, Xue G, Yang D (2011) Smart grid—the new and improved power grid: a survey. IEEE Commun Surv Tutor 14(4):944–980
126. Yan Y, Qian Y, Sharif H, Tipper D (2012) A survey on smart grid communication infrastructures: motivations, requirements and challenges. IEEE Commun Surv Tutor 15(1):5–20
127. Dutta S, Sadhu PK, Reddy MJB, Mohanta DK (2020) Role of microphasor measurement unit for decision making based on enhanced situational awareness of a modern distribution system. In: Decision making applications in modern power systems. Academic Press, pp 181–199
128. Sridhar S, Hahn A, Govindarasu M (2011) Cyber–physical system security for the electric power grid. Proc IEEE 100(1):210–224
129. Liu S, Liu PX, Wang X (2016) Effects of cyber attacks on islanded microgrid frequency control. In: 2016 IEEE 20th international conference on computer supported cooperative work in design (CSCWD). IEEE, pp 461–464
130. Tan S, De D, Song WZ, Yang J, Das SK (2016) Survey of security advances in smart grid: a data driven approach. IEEE Commun Surv Tutor 19(1):397–422
131. Fan Z, Kulkarni P, Gormus S, Efthymiou C, Kalogridis G, Sooriyabandara M, Zhu Z, Lambotharan S, Chin WH (2012) Smart grid communications: overview of research challenges, solutions, and standardization activities. IEEE Commun Surv Tutor 15(1):21–38
132. Abhinav S, Modares H, Lewis FL, Ferrese F, Davoudi A (2017) Synchrony in networked microgrids under attacks. IEEE Trans Smart Grid 9(6):6731–6741
133. Cai T, Jia T, Adepu S, Li Y, Yang Z (2023) ADAM: an adaptive DDoS attack mitigation scheme in software-defined cyber-physical system. IEEE Trans Ind Inform, Early Access
134. Grid NS (2010) Introduction to NISTIR 7628 guidelines for smart grid cyber security. Guideline, Sep
135. Tran TT, Shin OS, Lee JH (2013) Detection of replay attacks in smart grid systems. In: 2013 international conference on computing, management and telecommunications (ComManTel). IEEE, pp 298–302
136. Fritz R, Zhang P (2018) Modeling and detection of cyber attacks on discrete event systems. IFAC-PapersOnLine 51(7):285–290
137. Hoehn A, Zhang P (2016) Detection of covert attacks and zero dynamics attacks in cyber-physical systems. In: 2016 American control conference (ACC). IEEE, pp 302–307
138. Li W, Xie L, Wang Z (2018) A novel covert agent for stealthy attacks on industrial control systems using least squares support vector regression. J Electr Comput Eng 2018:1–14
139. Bompard E, Napoli R, Xue F (2009) Analysis of structural vulnerabilities in power transmission grids. Int J Crit Infrastruct Prot 2(1–2):5–12
140. Bompard E, Napoli R, Xue F (2010) Extended topological approach for the assessment of structural vulnerability in transmission networks. IET Gener Transm Distrib 4(6):716–724
141. Bompard E, Pons E, Wu D (2012) Extended topological metrics for the analysis of power grid vulnerability. IEEE Syst J 6(3):481–487
142. Bompard E, Wu D, Xue F (2011) Structural vulnerability of power systems: a topological approach. Electr Power Syst Res 81(7):1334–1340
143. Habibi MR, Baghaee HR, Dragičević T, Blaabjerg F (2020) False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks. IEEE Trans Circuits Syst II Express Briefs 68(2):717–721
144. Habibi MR, Baghaee HR, Dragičević T, Blaabjerg F (2020) Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. IEEE J Emerg Sel Top Power Electron 9(5):5294–5310
145. Zhao P, Xia J, Dai Y, He J (2010) Wind speed prediction using support vector regression. In: 2010 5th IEEE conference on industrial electronics and applications. IEEE, pp 882–886
146. Mustafa MA, Zhang N, Kalogridis G, Fan Z (2015) DEP2SA: A decentralized efficient privacy-preserving and selective aggregation scheme in advanced metering infrastructure. IEEE Access 3:2828–2846
147. Tsai JL, Lo NW (2015) Secure anonymous key distribution scheme for smart grid. IEEE Trans Smart Grid 7(2):906–914
148. Baek J, Vu QH, Liu JK, Huang X, Xiang Y (2014) A secure cloud computing based framework for big data information management of smart grid. IEEE Trans Cloud Comput 3(2):233–244
149. Kinney S (2016) The smart grid and its key role in the Industrial IoT. https://www.rti.com/industries/energy/smart-grid#:~:text=RTI%20Connext%20DDS%20helps%20build,delivery%20from%20generator%20to%20outlet. Accessed 25 July 2022
150. Esmalifalak M, Liu L, Nguyen N, Zhenge R, Han Z (2017) Detecting stealthy false data injection using machine learning in smart grid. IEEE Syst J 11(3):1644–1652. https://doi.org/10.1109/JSYST.2014.2341597

151. Shukla V, Qiao D (2007) Distinguishing data transience from false injection in sensor networks. In: 2007 4th annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks. IEEE, pp 41–50
152. Yu Z, Guan Y (2005) A dynamic en-route scheme for filtering false data injection in wireless sensor networks. In: Proceedings of the 3rd international conference on embedded networked sensor systems, pp 294–295
153. Kosut O, Jia L, Thomas RJ, Tong L (2010) Limiting false data attacks on power system state estimation. In: 2010 44th annual conference on information sciences and systems (CISS). IEEE, pp 1–6
154. Mo Y, Chabukswar R, Sinopoli B (2013) Detecting integrity attacks on SCADA systems. IEEE Trans Control Syst Technol 22(4):1396–1407
155. Vamvoudakis KG, Hespanha JP, Sinopoli B, Mo Y (2014) Detection in adversarial environments. IEEE Trans Autom Control 59(12):3209–3223
156. Zhang H, Qi Y, Zhou H, Zhang J, Sun J (2017) Testing and defending methods against DoS attack in state estimation. Asian J Control 19(4):1295–1305
157. Yang C, Zheng J, Ren X, Yang W, Shi H, Shi L (2017) Multi-sensor Kalman filtering with intermittent measurements. IEEE Trans Autom Control 63(3):797–804
158. Li Y, Wei X, Li Y, Dong Z, Shahidehpour M (2022) Detection of false data injection attacks in smart grid: a secure federated deep learning approach. IEEE Trans Smart Grid 13(6):4862–4872
159. Bhuyan MH, Bhattacharyya DK, Kalita JK (2013) Network anomaly detection: methods, systems and tools. IEEE Commun Surv Tutor 16(1):303–336
160. Ghiasi M, Niknam T, Wang Z, Mehrandezh M, Dehghani M, Ghadimi N (2023) A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: past, present and future. Electr Power Syst Res 215:108975
161. Bitirgen K, Filik ÜB (2023) A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid. Int J Crit Infrastruct Prot 40:100582

Publisher's Note