Electrical Power and Energy Systems 141 (2022) 108039

Contents lists available at ScienceDirect

International Journal of Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Edge security in smart inverters: Physical invariants based approach

Anusha Kumaresan [a,*,1,2], Nandha Kumar Kandasamy [b,2], Robert E. Kooij [c,d]

[a] Energy Research Institute at NTU (ERI@N), Interdisciplinary Graduate Programme, Nanyang Technological University, 639798, Singapore
[b] Lite-On Singapore Pte. Ltd., 556741, Singapore
[c] Delft University of Technology, Faculty of Electrical Engineering, Mathematics and Computer Science, Mekelweg 4, 2628 CD Delft, The Netherlands
[d] TNO, Unit ICT, Anna van Buerenplein 1, 2595 DA, Den Haag, The Netherlands

ARTICLE INFO

Keywords:
Cyber security
Edge security
Physical invariant
Smart photovoltaic inverter
Volt/VAR control

ABSTRACT

The endeavour towards making power distribution systems (PDSs) smarter has made the interdependence on communication network indispensable. Further, prospective high penetration of intermittent renewable energy sources in the form of distributed energy resources (DERs) has resulted in the necessity for smart controllers on such DERs. Inverters are employed for the purpose of DC to AC power conversion in the distribution network where the present standards require these inverters to be smart. In general, distributed energy resource management systems (DERMS) calculate and send set points/operating points to these smart inverters using protocols such as smart energy profile (SEP) 2.0. Given the nature of sites at which such DERs are installed i.e., home area networks with a pool of IoT(Internet-of-Things) devices, the opportunity for a malicious actor to sabotage the operation is typically higher than that for a transmission system. National Electric Sector Cyber-security Organization Resource (NESCOR) has described several failure scenarios and impact analyses in case of cyber attacks on DERs. One such failure scenario concerns attacks on real/reactive power control commands. In this paper, it is demonstrated that physical invariant based security on the edge devices, i.e. smart controllers deployed in DER inverters, is an effective approach to minimize the impact of cyber attacks targeting reactive power control in DER inverters. The proposed defense is generic and can also be extended to attacks on real-power control. The proposed defense is validated on a co-simulation platform (OpenDSS and MATLAB/SIMULINK).

1. Introduction

While traditional power systems were centralized, the need for improved reliability and power/energy security initiated [1] the increase in deployment of distributed energy resources (DERs) [2]. Factors such as increasing energy demand, economic and environmental issues in using fossil fuel, and decreasing cost of renewable energy sources (RES) led to the growing attention towards their deployment [3]. Hence, RESs are extensively employed for DER applications, usually as a combination (hybrid) of two or more variants to tackle their inherent intermittent behaviour [4]. Solar energy is a promising source among the RESs owing to its pollution free nature, availability of unlimited energy from the sun, and above all, the drastically decreasing cost of solar photovoltaic (PV) panels [5,6], and hence, it is widely adopted. Irrespective of the advantages, solar PV power also depends on the intermittent solar irradiance level and module temperature [7,8].

As a result, high penetration of solar PV results in grid stabilization issues such as voltage sag/swell [9], voltage flickers and power quality issues [10]. This in turn, might damage the electrical equipment present in the network. Hence, under these conditions, DERs are forced to disconnect from the system. The above process is called islanding [11] and is not preferable due to constraints such as restarting time and manual effort involved in restarting the DERs [12]. Further, islanding might lead to cascaded islanding of other DERs.

Many plausible solutions that can be used to mitigate these grid connection complications such as Volt/VAR control [13,14], frequency/watt control [15,16], Volt/watt [17], ramp rate control [18], etc., are available in the literature. DER inverters with such capabilities are usually referred to as smart inverters [19] and IEEE 1547 is a standard that provides regulatory limits for smooth integration and coordination of such smart inverters in power distribution systems (PDSs) [20]. The coordination of DERs is usually handled by a distributed energy resource management system (DERMS). DERMS calculates the optimal values of the parameters for the smooth operation of the system based on historic data and status of all the equipment in the system [21]. The

* Corresponding author.
E-mail addresses: anusha010@e.ntu.edu.sg (A. Kumaresan), nandha001@e.ntu.edu.sg (N.K. Kandasamy), r.e.kooij@tudelft.nl (R.E. Kooij).
[1] Department of Electrical and Electronics Engineering, National Institute of Technology Puducherry, Karaikal, UT of Puducherry, India 609609.
[2] Singapore University of Technology and Design, 8 Somapah Rd, Singapore 487372.

https://doi.org/10.1016/j.ijepes.2022.108039
Received 28 May 2021; Received in revised form 24 December 2021; Accepted 5 February 2022
Available online 15 March 2022

smart inverter receives the set points for real/reactive power injection from DERMS through protocols such as smart energy profile (SEP) 2.0. There will be more cyber-security concern when a large set of inverters (distributed actuators) at geographically dispersed consumer sites are controlled, rather than using dedicated energy sources that are professionally managed. The main attribute owing to this is the usage of information and communication technologies (ICT) for coordinating the smart inverters. Moreover, non-professionals run the inverters in locations that are not physically protected [22,23] and are hence vulnerable to compromise [24]. Further, there will be an increase in the cyber threat space when internet-of-things (IoT) devices are used for energy management functions such as home energy management system (HEMS). Indeed, there are reports on large-scale attacks exploiting an expansive installation of IoT devices such as Mirai malware-based attacks on webcams [25]. Attacks such as false data injection (FDI), can severely affect the performance of power system equipment, domestic/industrial appliances, or even cause local blackouts, which can cascade further.

While the network and communication community continuously updates the network threat vectors for implementing the cyber-security measures at various network layers, organizations such as '*National Electric Sector Cyber-security Organization Resource (NESCOR)*'- a U.S based organization, focuses on electric sector failure scenarios and impact analyses [23]. State-of-the art for generic cyber security for power grids is presented in articles such as [26] but has little focus on NESCOR related failure scenarios. NESCOR serves as a focal point to bring together domestic and international experts; and test security of novel technology, architectures, and their applications to the electric sector. Such failure scenarios can be conveniently used to develop cyber security on the edge devices i.e., smart controllers in inverters. *Orthogonal security especially at the physical layer/at the edge device which has access to direct physical measurements can significantly improve the overall security [27,28].* Orthogonal security is defined as the idea in which at every layer, at least two security systems are deployed that are complementary to each other and it is usually categorized under defense-in-depth strategies [29]. The effectiveness of orthogonal security has been demonstrated convincingly for other critical infrastructure such as water treatment plants [30]. It is critical to include multi-layer security as it can be observed from [31,32] that even consensus based algorithms are not immune to cyber attacks.

The need for adhoc security features is a usual concern on such defense mechanism. It is to be noted that the proposed defense is not a conventional network intrusion detection/avoidance system, but rather follows the paradigm of '*security by design*' [33], which needs to be fundamentally incorporated in DER inverters. In the power domain, such features are referred to as interlocks which prevent obvious failures, in this case, anomalies in the sensed physical parameter values. The proposed defense can also be used as a trigger to deploy remedial actions such as reconfigurable control to overcome the harmful impacts of cyber attacks on real/reactive power control. The proposed defense relies on physical layer security (PLS) [34] by leveraging on the local measurements and control commands received to identify the anomalies. The proposed defense assists the inverter to switch to a fail-safe control mode by relying only on the local measurements when an anomalous condition is detected. Hence, an orthogonal defense is achieved, a detailed explanation is provided in Section 4.2. In this context, the contributions of the paper are,

1. Unlike traditional physical impact analysis, failure scenarios are selected from NESCOR, then FDI attacks are curated for the corresponding failure scenarios and their physical space impacts are studied,
2. A defense mechanism based on local voltage measurements is proposed. The proposed voltage based defense has different goal and application compared to the current based defense [35]. *The current based defense only protects the prosumer from power supply interruption but ignores the impact on PDS, whereas the voltage based defense considers the impact on PDS as well,*
3. Validation of the proposed defense using a co-simulation platform (OpenDSS and SIMULINK tool-box from MATLAB). Though co-simulation is a well known technique [36], to the best of authors' knowledge, it has not been used for security validation of DERs with the complete physical process included.

2. Literature survey

The state-of-the-art with respect to the DER control is presented in this section. The power flows may get reversed frequently and bus voltage magnitudes could fluctuate considerably in a PDS with high penetration of RESs and significant elastic (e.g., deferrable) loads. For instance, there could be 15% variation in power generated by a solar PV system in one-minute intervals [37]. The bus voltage in a PDS is affected by active power variations as well unlike transmission systems. It should be noted that the PV power generation could easily exceed the local power demand during sunny sky periods causing over-voltage conditions [38]. Similarly, the PV generation could be weak which can cause under-voltage conditions.

The U.S. Department of Energy [39], has recommended DER participation in ancillary services for power system operation and control. There is a requirement of a smart or integrated grid when there is a high penetration of DERs such as more than 10%. This is to ensure that the grid management services can be provided by the RESs, DERs and loads [40]. The aggregation of inverters is required at various levels with such an integrated grid structure. This aggregation might be required for groups of inverters in one region or from the same manufacturer [40]. Such aggregations are not only required for the communication of control signals but also, for other services such as firmware update [40]. To cope up with the issues that come with the aggregation of DER inverters, several approaches have been proposed in literature including hierarchical distributed control [41]. Stochastic reactive power management is proposed by [42] for voltage related issues and a two-stage voltage control is proposed by [43], whereas [44] proposed an active power based voltage regulation, authors in [45] suggested a secured co-ordination for voltage support using authentication from the DERs. Utilizing DERs for reactive power control has been reported by many authors, and voltage rise mitigation using reactive power control has been reported as early as 2008 [38]. To enable distributed reactive power control, the inverters should provide such features and a typical design for an inverter with reactive power control is presented in [46]. The different options for reactive power control in DERS is presented in [37]. It has also been demonstrated in [42] that over-sizing of inverters enhances the robustness of voltage control for PDS. Various modes of operation were examined in [14], by changing the reactive power in accordance with the voltage at the point of common coupling (PCC) of the PV.

Digital signatures and time-stamping is presented to authenticate commands in distributed voltage control [45]. However, in cases where the utility head-end system is compromised, command authentication fails and thus, it will fail to protect from the attacks targeting the prosumer end. A prosumer is an electricity consumer who has at least one DER installed at his/her premises and is able to support the grid with the produced electricity. Further, the increase of IoT devices in energy management implies that the control network for active/reactive power control no longer operates in an isolated environment. Hence, risk of cyber-attacks and threats would be higher than usual for the reactive power control of RES inverters which are part of the aggregator [47], where several DERs are operated simultaneously to provide ancillary services to the grid. Further, even well defended core mission-critical infrastructures have been subjected to severe cyber-attacks such as the Stuxnet attack [48] and the Ukraine power system attack [49]. Real-world attacks such as malicious control attack on critical infrastructure — Maroochy Water Service in Australia [50], attack on Western energy sector targeted by sophisticated attack group [51] and demos such as aurora vulnerability by Idaho National Laboratory [52] have motivated

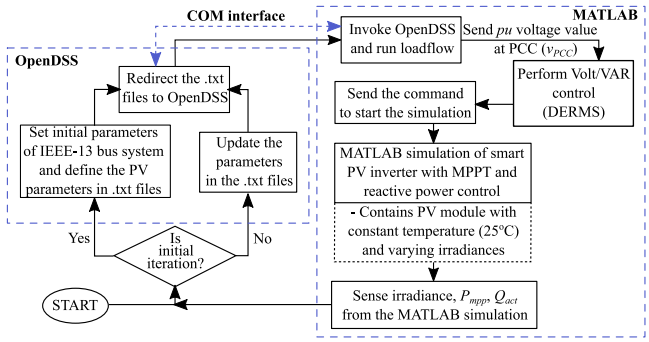

Fig. 1. Flow chart depicting data transfer between MATLAB and OpenDSS.

many research efforts on how cyber-attacks may impact power systems such as false data injection (FDI) attacks against automatic gain control [53], load redistribution attacks [54], and general networked control [55]. FDI attacks can go beyond automatic generation controls (AGCs) and general network control. A survey on FDI attacks, impacts and defense for state-estimation in power system is presented in [56]. Cyber threat evaluation and defense technologies are also proposed for distributed DC microgrids [57]. Data integrity attacks can have impact on the overall operation cost as well. The authors in [58] have outlined such impacts on a DC optimal power flow algorithm. Many authors have proposed defenses against FDI attacks, such as reactance perturbation [59].

Many government agencies such as the Department of Homeland security in the United States (U.S.) [60] have reported multiple attacks against power systems. In the report [23], which was jointly published by NESCOR and the Electric Power Research Institute (EPRI) from the U.S., a total of 26 failure scenarios for DERs are reported. In particular, the failure scenarios DER.6-9, DER.14, DER.16, DER.18, describe possible failures where the adversaries attempt to create an imbalance by affecting the availability of the DERs. As mentioned earlier, the network and communication community continuously updates the network threat vectors for implementing the cyber-security measures at various network layers. For example, Digital signatures and time-stamping based authentication commands in distributed voltage control [45], reactance perturbation [59], and other methods [56] are available in literature. However, orthogonal security or defense-in-depth has not been addressed for DERs in the methods available in the state-of-the-art. The defense proposed in [35] is one such orthogonal defense focusing on avoiding the power supply interruption at prosumer site. However, the impact on PDS is not considered in the above defense. Though the authors in [61] used co-simulation for assessing DER security defenses, the authors neither used NESCOR failure scenarios or simulated the inverter level functions; only the controller and network functions were simulated for security assessment. It can be observed that there is gap in the literature for methods on edge security on smart inverters to alleviate or at least minimize the impact of cyber attacks on DERs with respect to overall PDS . In this paper, the authors propose a defense method based on local voltage measurement that has the potential to bridge this gap.

3. Background and simulation setup

A co-simulation environment to realize DERMS functionalities in a distribution grid with smart inverters was created using OpenDSS and MATLAB/SIMULINK. This enables us to test the proposed defense mechanism, as it could be directly implemented on the detailed model of the inverter run on the MATLAB/SIMULINK platform. The IEEE-13 node test feeder[3] is taken as the distribution network. It is assumed that 10 RES inverters, each of rating 62.5 kVA, are connected to bus 634 of the radial feeder. The flow chart depicting the control flow is depicted in Fig. 1.

A MATLAB script invokes the OpenDSS to run loadflow analysis. The snapshot mode is opted as the feeder is solved for the values available only at that instant. With the voltage per unit (pu) value available at the PCC (v_{PCC}) obtained from the solver, Volt/VAR control is executed. The reference reactive power, Q_{ref} corresponding to v_{PCC}, is sent to the MATLAB/SIMULINK model of the DER inverter. To maintain v_{PCC} within permissible limits, Q_{ref} will be inversely proportional to the obtained voltage at the PCC.

The simulation of the smart DER inverter connected to the grid consists of a PV panel, three phase voltage source inverters (VSI) with decoupled control for active and reactive power injection to the grid as depicted in Fig. 2. The actual reactive power, Q_{act}, sensed from the simulation, might vary from the Q_{ref} command given. Hence, Q_{act}, irradiance (irr) and the maximum power for the present irradiance, P_{mpp} are obtained from the simulation and sent back to update the parameters in OpenDSS. This process takes place in a continuous manner, as in real-time operation. Each process or control block of the system considered is explained in detail below.

3.1. Loadflow analysis in opendss

For achieving fast and accurate loadflow analysis for PDSs, an open source electric power distribution system simulator (DSS), OpenDSS from EPRI is predominantly used [62]. The quasi-static time series simulation (QSTS) feature of OpenDSS enables precise calculation on large data [63]. However, the RES[4] system behaviour and the inverter behaviour cannot be simulated with OpenDSS.

3.2. Interfacing MATLAB and OpenDSS

MATLAB/SIMULINK is the widely used platform for simulating the behaviour of RES and smart inverter behaviour. OpenDSS and MATLAB/SIMULINK are interfaced using the common object model (COM) interface feature available in OpenDSS. Hence, control action (say, commands received from DERMS) can be executed in MATLAB/SIMULINK and the load flow analysis can be executed in OpenDSS.

3.3. Maximum power point tracking (MPPT) control

The MPPT control is used to extract the maximum power from the PV system. Many MPPT control techniques are present in the literature [64–66], and the perturb and observe (P&O)-based MPPT algorithm [67,68] is the conventional and widely employed algorithm in industry, owing to its simple structure and ease in implementation. Moreover, uniform irradiance condition is assumed in this paper with constant cell temperature, as the objective lies in demonstrating the physical invariant based security on the edge devices, rather than optimizing the smart controllers. Therefore, P&O-based MPPT algorithm suits the best, as only the initial convergence takes time, and when the irradiance changes, fast convergence can be achieved. This is not possible in advanced optimization-based techniques, which requires resetting of the search boundary or reinitialization of the search point.

The flowchart depicting the P&O-based MMPT control, which is opted in the modelling of the single-stage grid-connected PV system in this paper is shown in Fig. 3. After sensing the required parameters, such as the PV panel current, i_{pv}, PV panel voltage, v_{pv}, the algorithm is delayed by one instant. A comparison is made if the current instant PV power, $p_{pv}(k)$ is more than the previous instant PV power, $p_{pv}(k-1)$. If

[3] https://site.ieee.org/pes-testfeeders/resources/

[4] In this paper, solar PV is chosen as the example RES, however, the analysis holds for any other type of RES or storage devices with smart inverters.

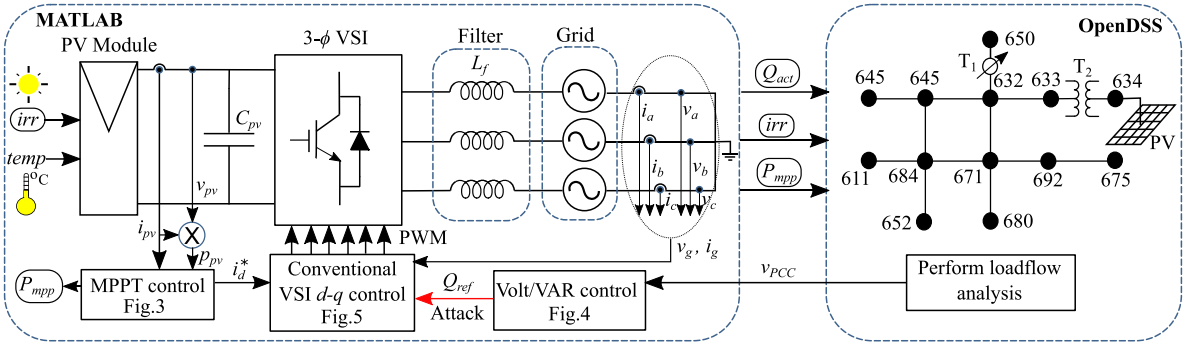

Fig. 2. Block diagram for the model of grid-connected smart PV inverter.

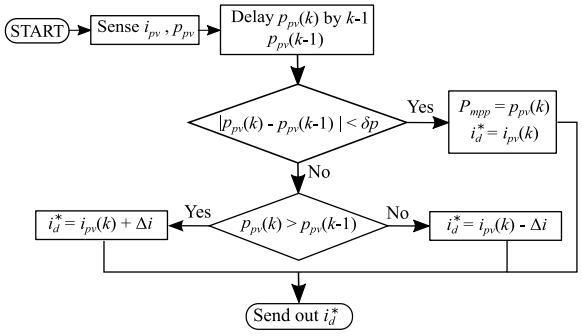

Fig. 3. MPPT control.

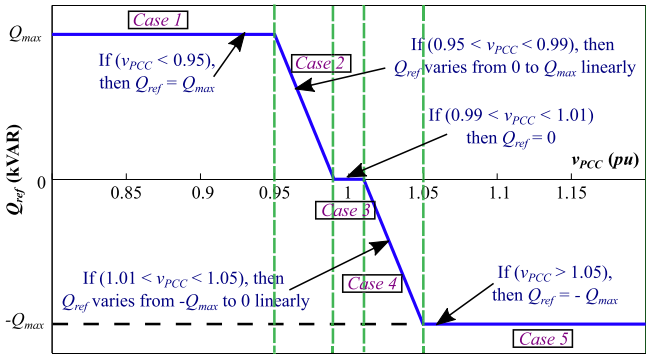

Fig. 4. Volt/VAR curve used.

so, the peak is not yet attained, and the current reference is increased by Δi, which can be regarded as 1% of the short circuit current, i_{sc} at standard test conditions (STC). Else, Δi is subtracted from $p_{pv}(k)$ to avoid diverging away from the maximum power point (MPP) power. A stopping condition, $|p_{pv}(k) - p_{pv}(k-1)|$ is checked to be less than δ_p to determine the MPP power, P_{mpp}, where δ_p can be regarded as 10% of the MPP power at STC. If the condition is met, the PV power at the current instant, $i_{pv}(k-1)$ is sent out as the current reference to the d–q controller.

3.4. Volt/VAR characteristics and control

The Volt/VAR control is used in order to operate the DER inverter at the required power factor, by absorbing or delivering reactive power to the grid. With such a control, v_{PCC} can be maintained within the permissible limits. The Volt/VAR curve specifies the amount of reactive power the smart inverter needs to provide with respect to v_{PCC}. The maximum possible reactive power the PV inverter could supply is given by Q_{max}, and the smallest possible value is given by $-Q_{max}$ as depicted in Fig. 4. Q_{max} value can be calculated as

$$Q_{max} = \sqrt{S^2 - P_{mpp}^2}, \tag{1}$$

where S denotes the kVA capacity of the inverter.

The value of P_{mpp} will vary based on the changes in the RES source, say irradiance changes in case of solar PV. Hence, Q_{max} will also vary with the changes in the real power. The following characteristics is selected for the Volt/VAR control with regard to the recommendations provided in [69].

$$Q_{ref} = \begin{cases} Q_{max}, & \text{if } v_{PCC} < 0.95 \\ (-25v_{PCC} + 24.75)Q_{max}, & \text{if } 0.95 \le v_{PCC} \le 0.99 \\ 0, & \text{if } 0.99 < v_{PCC} < 1.01 \\ (-25v_{PCC} + 25.25)Q_{max}, & \text{if } 1.01 \le v_{PCC} \le 1.05 \\ -Q_{max}, & \text{if } v_{PCC} > 1.05. \end{cases} \tag{2}$$

The following are the different cases in the Volt/VAR characteristics:

Case 1 - $v_{PCC} < 0.95$

The Q_{ref} value is set as Q_{max} as seen from Fig. 4 and Eq. (2). It can be observed that when v_{PCC} is below 0.95 pu, the inverter injects reactive power into the grid, which is analogous to capacitor action, in order to boost up the voltage at the PCC.

Case 2 - $0.95 \le v_{PCC} \le 0.99$

The Q_{ref} value is varied linearly from Q_{max} to 0 as seen from Fig. 4. The end points of this line are given by (0.95, Q_{max}) and (0.99, 0). Consequently, using the line equation, the expression for Q_{ref} is represented as in Eq. (2).

Case 3 - $0.99 < v_{PCC} < 1.01$

The Q_{ref} value is set as 0, as the v_{PCC} value is well within the required limits. Hence, injection/absorption of reactive power is not required, and the inverter operates in the unity power factor mode.

Case 4 - $1.01 \le v_{PCC} \le 0.99$

The Q_{ref} value is varied linearly from 0 to $-Q_{max}$ as seen from Fig. 4. The end points of this line are given by (1.05, $-Q_{max}$) and (1.01, 0). Consequently, using the line equation, the expression for Q_{ref} is represented as in Eq. (2).

Case 5 - $v_{PCC} > 1.05$

The Q_{ref} value is set as $-Q_{max}$ as seen from Fig. 4 and Eq. (2). When v_{PCC} goes beyond 1.05 pu, the inverter acts in an inductive manner, absorbing the reactive power from the grid. By doing so, it will reduce the v_{PCC} value and maintain it within the permissible limits.

The Q_{max} described above can be kept constant, which eliminates the calculation of Q_{max} at every instant. The above is elaborated in [37,42] and is achieved by assigning to S a value higher than P_{mpp}^{max},

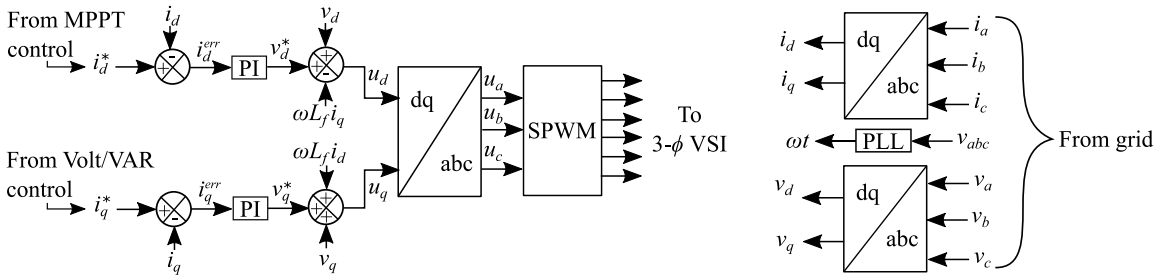

Fig. 5. Conventional VSI *d–q* control.

where P_{mpp}^{max} denotes the maximum of all P_{mpp} in the power–voltage (P–V) characteristic curves for any environmental condition:

$$S^{max} = \alpha P_{mpp}^{max}, \text{ where } \alpha > 1. \tag{3}$$

For the purpose of Volt/VAR control, Q_{max} is to be fixed to denote the maximum reactive power absorption/delivery capability of the inverter present in the system. When $\alpha = 1$, the reactive power becomes 0, and the inverter operates at the unity power factor mode when the environmental conditions produce the maximum MPP power for the given location ($S^{max} = P_{mpp}^{max} \implies Q_{max} = 0$).

However, while doing so, the smart functionality of the inverter such as the Volt/VAR control cannot be achieved, where the reactive power reference, Q_{ref} is altered in order to maintain voltage at the point of common coupling, v_{PCC}, within the permissible limits, such as in the case mentioned when the active power is P_{mpp}^{max}.

Hence, in order to guarantee the reactive power absorption/delivery capability of the inverter at all times, the power factor and safety factor are considered to determine the value of α. This process is oversizing of inverters and it ensures that, even if the inverter happens to handle real power at full capacity, there will be remaining reactive power left for voltage control. Hence, $\alpha > 1$ rather than being $\alpha \geq 1$.

The over-sizing ensures that, even if the inverter happens to handling real power at full capacity, there will be remaining reactive power left for voltage control. For example, if $\alpha = 1.2$[5] (i.e., 20% oversize), the guaranteed remaining reactive power capacity will be $0.63 \times P_{mpp}$, over-sizing not only makes Q_{max} time-invariant, but also allows reactive power injection into the grid when $P_{mpp} = P_{mpp}^{max}$. Hence, Q_{max} can be fixed as $\sqrt{S^{max^2} - P_{mpp}^{max^2}}$ for varying irradiance and cell temperature values.

3.5. Conventional VSI d–q control

The modelling of a grid-connected smart PV inverter is executed using the methods presented in [70–72].

The control structure is represented in Fig. 5. As depicted from Fig. 2, the three-phase grid voltage, v_g (v_a, v_b, v_c) and the three-phase grid current, i_g (i_a, i_b, i_c) are sensed. These three-phase time varying quantities are converted to a constant dc quantity in direct and quadrature frame (*d–q*), as v_d, i_d and v_q, i_q respectively.

With respect to the *d–q* frame, the active power (P) and reactive power (Q) are given by:

$$P = \frac{3}{2}(v_d i_d + v_q i_q) \text{ , and} \tag{4}$$

$$Q = \frac{3}{2}(v_q i_d - v_d i_q). \tag{5}$$

It is clearly visible that both P and Q depend on the parameters in the *d–q* frame. Major smart inverter functionalities that can address high RES penetration include dynamic Volt/VAR control, active power control/curtailment and Volt/Watt control. It is important to have decoupled control for achieving the above functionalities. Decoupled control aids in controlling the active and reactive power independently. When either one of the commands is varied, the other parameter remains undisturbed. Moreover, v_q is made 0 by aligning v_d with the voltage space vector for vital decoupling. This is done if the reference for the d–q transformation is considered as the voltage at the phase locked loop's (PLL) connection point. Consequently, when $v_q = 0$, P and Q are reduced as:

$$P = \frac{3}{2} v_d i_d \text{ , and} \tag{6}$$

$$Q = -\frac{3}{2} v_d i_q. \tag{7}$$

Hence, P and Q are indirectly controlled by i_d and i_q, for a set value of v_d. The current reference for the d-axis, i_d^*, is obtained from the MPPT controller, and the current reference for the q-axis, i_q^* is obtained from the Volt/VAR control and from (7). A proportional integral (PI) controller is used to align the actual values with the reference values. Furthermore, the control equations [70] are given by:

$$u_d = v_d^* + v_d - \omega L_f i_q \text{ , and} \tag{8}$$

$$u_q = v_q^* + v_q + \omega L_f i_d. \tag{9}$$

These *d–q* components obtained are then changed to three-phase time varying quantities namely, u_a, u_b, u_c. Finally, sinusoidal pulse width modulation (SPWM) is employed to generate firing pulses for the VSI to operate.

3.6. ICT threat model

ICT threat model gives a picture of 'how the attacker can execute the attack' with the vulnerabilities in computing devices or network. FDI attacks originating either at computing devices such as DERMS or originating in communication channels working on protocols such as SEP 2.0 is considered as the threat model. The FDI attacks are designed using 'Bias Attacks' principle, however, the inferences are general and are not affected by this choice. Since, only whether a real value such as commands and measurements is tampered or not and how much the tampered value deviate from the actual values affect the operation; not the type of attack. The bias attacks are created by adding constant offset to the true value of a control parameter or measurement values.

Bias attacks could be launched by using numerous attack surfaces. Especially, inherent features such as wireless communications, consumer grade devices, non professional management, etc. at residential DERs site make them most vulnerable. There are multiple possibilities such as compromising the HEMS to tamper the actuation parameters values of the RES inverter or the packets could be modified by the attacker over the home wireless network etc. There are various examples where home Wifi network in spite of encryption was compromised by brute force or due to weak passwords or careless management [51].

As an example of a bias attack, the following representation of the inverters and DERMS in discrete-time state space is considered.

$$\mathcal{P}: \begin{cases} x_{k+1} = Ax_k + Bu_k \\ y_k = Cx_k \end{cases} \tag{10}$$

[5] $\alpha = 1.2$ is considered in this paper.

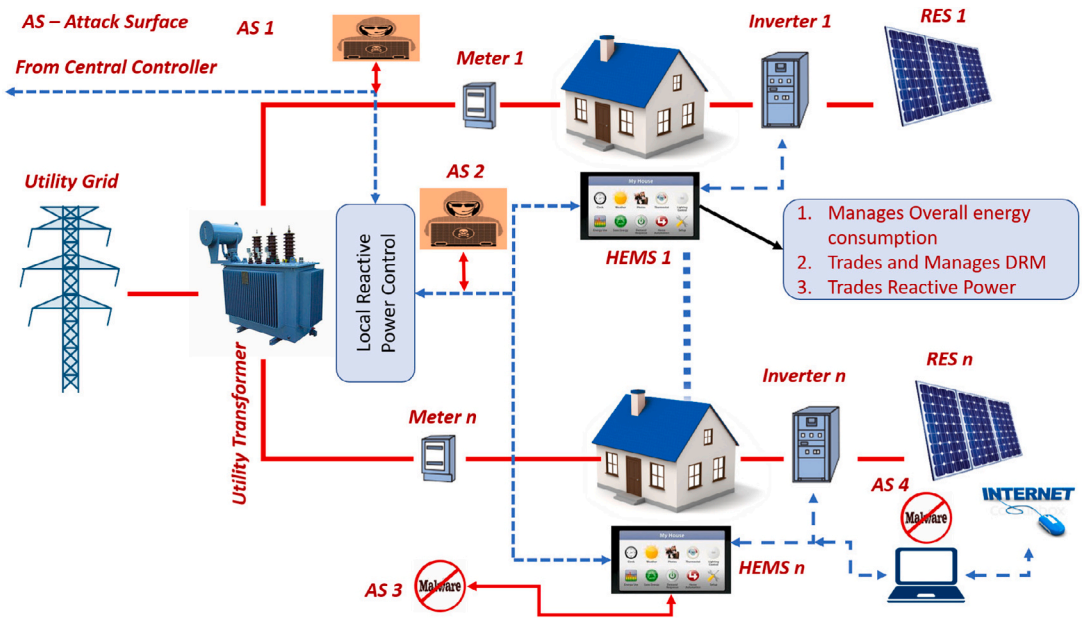

Fig. 6. Power distribution system with distributed RES generation. AS indicates a possible attack surface.

where $x_k = [V_i]^T$ denotes the state of the distribution system and V_i represents the voltage at ith PCC, $i = 1 \dots n$ where n is the number of PCCs; $u_k = [Q_j^C \ 0]^T$ is the control action vector required for voltage control, where Q_j^C is the reactive power reference to the jth inverter, $j = 1 \dots m$; and $y_k = [v_i]^T$ is the measurement vector from voltage sensors at a given sampling instant k. A, B and C are proportionality matrices. For a bias attack on the measurement data, at each sampling instant the measured voltage vector is modified by a static bias δ to reflect the new measurement vector $\overline{y}_k$ would be represented as $\overline{y}_k = [(v_i \pm \delta_i)]^T$. The bias δ will have an impact on the control action u_k in the next state.

Infrastructure-side ICT components, such as programmable logic controllers (PLCs) or industrial PCs that act as bridge between the utility-operated control centres and interconnected PDSs are not immune to cyber attacks. Owing to professional management such as use of firewalls and other security protocols, the infrastructure-side ICT is harder to compromise in reference to the residential DER sites. However, the feasibility to attack such sites are not impossible and is evident from novel attacks reported in literature such as [48,73], and the real-world attacks [55].

When an attack on infrastructure-side ICT is successful, it will result in large-scale and immediate impact. Whereas, when individual DER sites are compromised the impact that an attacker could cause is relatively lower. For example, if the attacker compromises the industrial computer used for implementing DERMS functionalities, the attacker has higher capabilities such as modifying the control logic of DERMS itself. Apart from such attacks eavesdropping could also be carried out by the attacker on control and measurement data in the PDS. Such eavesdropping is essential for gaining the knowledge for creating the attack actions. The modified Volt/VAR characteristics described in the next section, will be used to impose an attack on the Volt/VAR curve. Various attack surfaces from the ICT perspective are shown in Fig. 6.

3.7. Physical process threat model/attack goal

Physical process threat model or attack goal is the actual physical impact that the attacker intends to achieve employing the ICT threat model. Physical process threat model gives a picture of 'what the attacker intends to achieve with the attack'. The attack goal considered for analysis is voltage drop/rise in the selected PDS. The condition that can enable such an attack is high load demand and weak RES generation (e.g. low irradiance in case of solar PV). As a result, the corresponding DER site can potentially provide higher proportion of the remaining apparent power capacity for reactive power control. The above condition becomes always true when the RES inverter is oversized. The attacker's aim is to use the available reactive power capacity to create a voltage rise or voltage drop beyond the allowed limits. It is assumed that the actuation command sent to the RES inverter is compromised to achieve a maliciously high reactive power consumption or injection. The reduction or increase in the PDS's voltage from the nominal value will be created by the excessive consumption or injection of reactive power respectively from multiple inverters is coordinated. Though over-sizing provides guaranteed reactive power capacity for robustness it can be turned into a destructive weapon by a skilled attacker.

4. Attack execution and proposed defense

4.1. Attack execution by modifying volt/VAR curve

In order to mitigate the stability issues imparted by the intermittent nature of the PV, the Volt/VAR control has been opted, which was elaborated in Section 3.4. It could be viewed in Fig. 4 that, when v_{PCC} increases, Q_{ref} should decrease and vice versa. For demonstration of the attack, it is assumed that the adversary is interested in deteriorating the grid function by inducing an attack to modify the standard Volt/VAR characteristics as shown in Figs. 7(a) and (b). The attack is executed by forcing Q_{ref} to be proportional to v_{PCC}, or as a step change, which will make the grid collapse at a faster rate. The characteristics of a sudden proportional step change which will create an adverse effect is represented by:

$$Q_{ref} = \begin{cases} -Q_{max}, & \text{if } v_{PCC} < 1 \\ 0, & \text{if } v_{PCC} = 1 \\ Q_{max}, & \text{if } v_{PCC} > 1. \end{cases} \tag{11}$$

This attack can lead to sudden over-voltage or under-voltage which can result in the disconnection of the PV from the grid. Such disconnection could cascade and result in local blackouts within the PDS. Further, with such disconnections, restarting the DERs requires more time and can create great complications i.e., resulting in extended restoration time. Complications include, but are not limited to, change in the

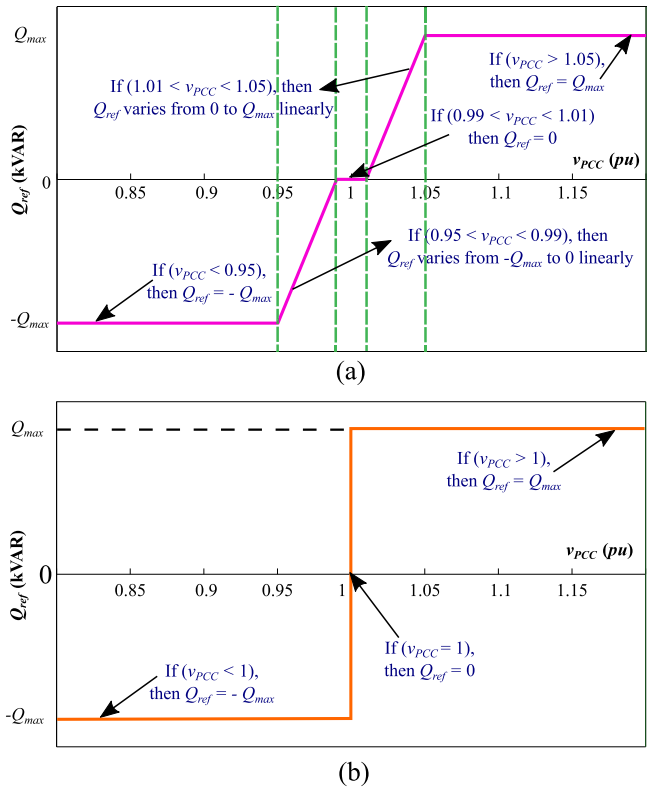

Fig. 7. Modified Volt/VAR curve due to cyber attack: (a) Proportional change, and (b) step change.

references (master for the grid), and out-of-sync operations of rotating machines such as motors. Master in a grid refers to the generator providing the voltage, frequency and phase angle reference to the other generators to enable synchronous operation that is essential for stable grid.

4.2. Proposed defense

Our proposed defense is based upon the physical invariant approach. The approach could be used for components that exhibit continuous states. The states of interest for the proposed application is the present voltage at the PCC and the reactive power command received. The state variables used for the defense are those that can be measured directly from the sensors to which the smart inverters have direct access. A discrepancy between the expected state and the received Q_{ref} command is used for activating the defense.

In DER inverters, the proposed defense is implemented as an interlock that could be employed as a PLS [34]. It should be noted that the PLS mentioned in this paper is not a conventional PLS in network security, rather with respect to electrical components in the system. The proposed scheme leverages on the local measurements. Hence, it can be implemented as an interlock in the existing controllers of the inverters or in low cost field programmable (FPGA) chips. The method is also generic and can be applied for other failure scenarios such as to the cases described by NESCOR.

The cost of FPGA chips will have very little impact on the unit cost of the inverters. For example, a 'Spartan-7, 938 Blocks, 6000 Macrocells, 180 Kbit RAM FPGA' from XILINX retails (the actual price would be significantly lower for bulk orders) for less than 20 USD. Whereas a 5 kVA inverter from GOODWEE is priced at 1700 USD in Alibaba (wholesale price). It is to be noted that Spartan-7 is one of the latest FPGAs from XILINX and there are cheaper versions available in the market.

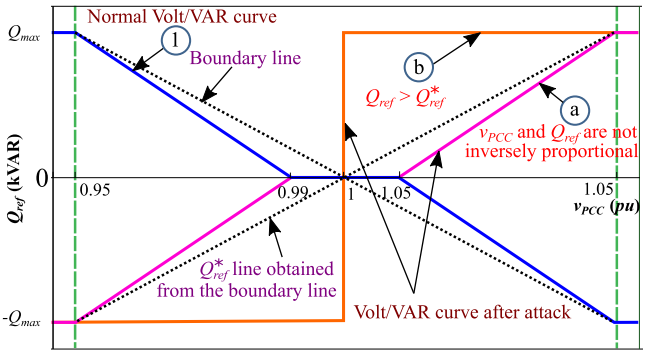

Fig. 8. Detection of cyber attack.

Since the controller in the inverter has access to the local voltage measurement and is also responsible for executing the commands, the inverter controller is directed to continuously check the Q_{ref} command with reference to the v_{PCC} value. The proposed block checks if the command received has the following described anomalies:

1. Presence of directly proportional relation between Q_{ref} and v_{PCC}: It can be seen from Fig. 8, curve (1), that in a normal Volt/VAR curve, there exists an inversely proportional relationship between Q_{ref} command and the v_{PCC}. However, the curve under attack (a) (as in Fig. 7(a)) showcases a directly proportional relationship, which will further drive the v_{PCC} to go out of the limits, rather than bounding it to be within the IEEE 1547 standards. This check can be done in the range of v_{PCC} ϵ $(-Q_{max}, Q_{max})$-(0.99, 1.01). The region of (0.99, 1.01) is removed from the checking range, as a tolerance of 1% of the nominal v_{PCC} value of 1 pu is chosen. Hence, within that removed region, Q_{ref} can be 0, or even a directly proportional relationship would not have an impact to drive v_{PCC} out of the limits.
2. High reactive power injection/absorption command when v_{PCC} is within the limits: This case can be realized with the curve under attack (b) (as in Fig. 7(b)). Since a step change of Q_{ref} is provided, it is difficult to detect the attack from the first sanity check mentioned. Exactly at v_{PCC} = 1, the Q_{ref} changes in a directly proportional manner, with a high difference of $2Q_{max}$ from the previous instant. At the other points, there is a constant value, and following sanity check 1, this characteristic should not be a problem. Hence, in order to detect such an attack, a boundary line is set, which connects the end points of the normal Volt/VAR curve as shown in Fig. 8, having a slope of $-20Q_{max}$. The same boundary line is reflected as a Q^*_{ref} line, with $Q_{ref}(k)^* = 20v_{PCC}(k)Q_{max}$, where $k = 0, 1, 2, \ldots$. Hence, if $Q_{ref}(k) > Q^*_{ref}(k)$, then, it can be confirmed that an attack has occurred.

The flowchart depicting the sanity checks is shown in Fig. 9. From the Volt/VAR control, $v_{PCC}(k)$ and $Q_{ref}(k)$ are obtained. Then, there is a check to ensure the received $Q_{ref}(k)$ is within the maximum reactive power capacity of the inverter. If not, the values are appropriately fixed as Q_{max}, if $Q_{ref}(k) > Q_{max}$ or $-Q_{max}$ if $Q_{ref}(k) < -Q_{max}$. Next, $v_{PCC}(k)$ is examined to ensure if it is within the IEEE 1547 limits $(0.95 < v_{PCC}(k) < 1.05)$. If not, the inverter trips. Then, a comparison on the input commands from the current instant with the previous instant is done in order to sense if there is a change in the inputs. If there are no changes, the operation continues, or else, the first sanity check is applied. This is done by inspecting the sign of the difference of the input commands. For an inversely proportional relationship, the signs should be opposite. If so, the second sanity check is done to check if $Q_{ref}(k) < Q^*_{ref}(k)$. If this sanity check is also passed, then the Q_{ref}

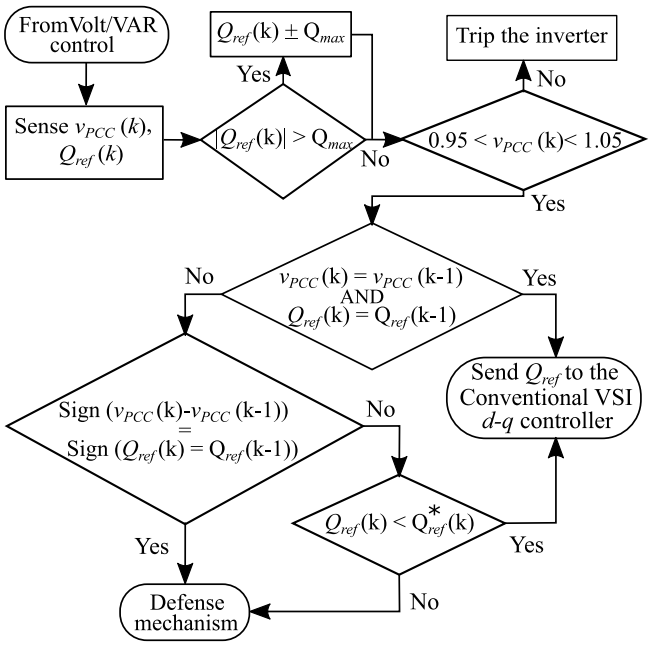

Fig. 9. Flowchart depicting sanity checks.

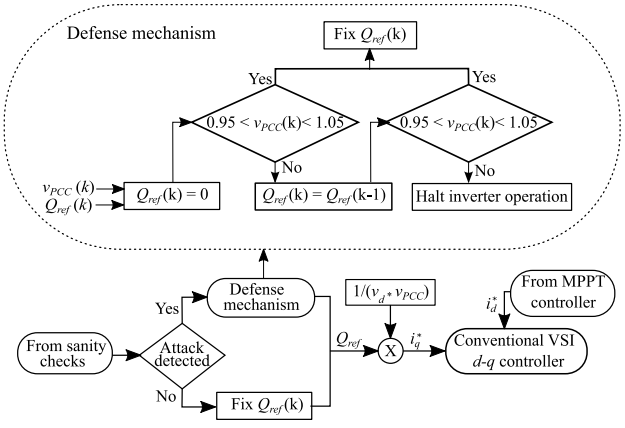

Fig. 10. Proposed defense mechanism.

command is send to the conventional VSI d–q controller. If either one of the checks is not satisfied, the defense mechanism is applied.

If any of the above cases are detected, the inverter is forced to operate in any of the following modes:

1. Operate at unity power factor mode: It is discussed in Section 3.4 that the Volt/VAR control is used to extend the operation of the VSI to a wider range of v_{PCC} by controlling the reactive power injection to the grid. Hence, with the unity power factor operation, v_{PCC} will be reflected as the same value obtained from the loadflow analysis.
2. Operate at the Q_{ref} command received from the previous instant: If the first remedial measure does not limit the v_{PCC} within the permissible limits, the next action is to operate the inverter at $Q_{ref}(k-1)$, rather than at $Q_{ref}(k)$, where the attack is made. Drastic change in v_{PCC} is infrequent, and hence, $Q_{ref}(k)$ can be set as $Q_{ref}(k-1)$, to limit v_{PCC} within the limits.
3. Halt the operation of the inverter: If both the remedial actions are not sufficient to curb v_{PCC} within the limits, the inverter operation is halted.

A block diagram for the proposed defense is presented in Fig. 10. It can be seen that in the proposed defense, before the Q_{ref} command is passed to the controllers, the relevance of the command is verified using an interlock. A central controller is used to control all the RES for reactive power injection/absorption. However, when an attacker compromise the measurement values or the control commands, the defense is executed at DER site (security is implemented on the edge device). The local controller in the RES implements the proposed defense based on the measurements at the PCC and the central controller does not take any control action. Hence, if the PCC measurements and the control actions contradict each other, the edge security implements the control actions irrespective of the state of other inverters.

Currently two types of solutions are followed in the market,

1. *TYPE 1:* The inverter controller shown in Fig. 2 is an Industrial IoT (IIoT) device and is capable of communicating with the cloud using relevant APIs,
2. *TYPE 2:* The inverter controller is a standard controller with local communication interfaces such as Modbus over RS485 or CAN bus. An IoT Gateway either connects a single inverter controller or multiple inverter controller to the cloud using relevant APIs. The architecture from a system currently available in the market is shown in the figure below (Fig. 11),

The system configuration is from our industry partner that is being deployed in multiple countries such as New Zealand, Indonesia etc. Though the PCS is a *TYPE 1* inverter, the *TYPE 2* configuration is followed but it is capable of working in *TYPE 1* mode as well. Please note that this practical system is capable of handling both PV and energy storage system (ESS) whereas the system considered in this paper considers only PV systems. Our industry partner is the OEM for ESS and system integrator for the power pillar shown in Fig. 11.

The IIoT device of *TYPE 1* has access to all the measurement data as it directly handles the sensor data and has connectivity to internet. Hence, the invariants could be implemented directly on the IIoT controller, e.g., EH series Goodwe inverters. In case of *TYPE 2*, the controller market as EMU (Energy Monitoring Unit) collects the measurement data from the PCS and BMS controllers using either Modbus RS485 or CAN bus and links it to the cloud energy management system (EMS). The cloud EMS could be a DERMS. There are two options either the implementation could be done on the PCS or EMU. Implementation on PCS would be a layer 0/PLS as described in the paper, whereas implementation on EMU has one layer of non-networked communication involved but the computation burden would be removed from the PCS.

In general, process based intrusion detection systems (PIDS) are effectively anomaly detectors that can detect failures along with cyber-attacks. Hence the answer to the question - 'how to differentiate an attack from failure?' is critical. A good example of such a case is that, say the voltage sensor at the PCC has failed and though the PCC voltage is normal, it is reflecting only 80% of the measured value. Now even if there is no attack and if the DERMS sends a legitimate command for reactive power consumption, the algorithm might tag it as a cyber attack (hypothetically). The complete failure of sensors can be ignored as the inverters are grid-tied inverters and hence will automatically disconnect if there is no signal from the sensors at PCC. The cases where $x\%$ of the measured value is reflected are to be differentiated from the cyber-attacks. The proposed method utilizes physical invariants and the same could be used for identifying sudden failures, any significant change in voltage would have an equivalent impact on the current and vice-versa. The above method cannot be used to differentiate progressive failures of sensor and failure of both sensors i.e., both sensors having failure in such a manner that $x\%$ of the measured value is reflected is highly unlikely. Hence, physical invariants i.e., correlation of current and voltage sensors could be used to differentiate the attacks from failures. The authors are currently working on correlation to differentiate attacks from failures. Authors

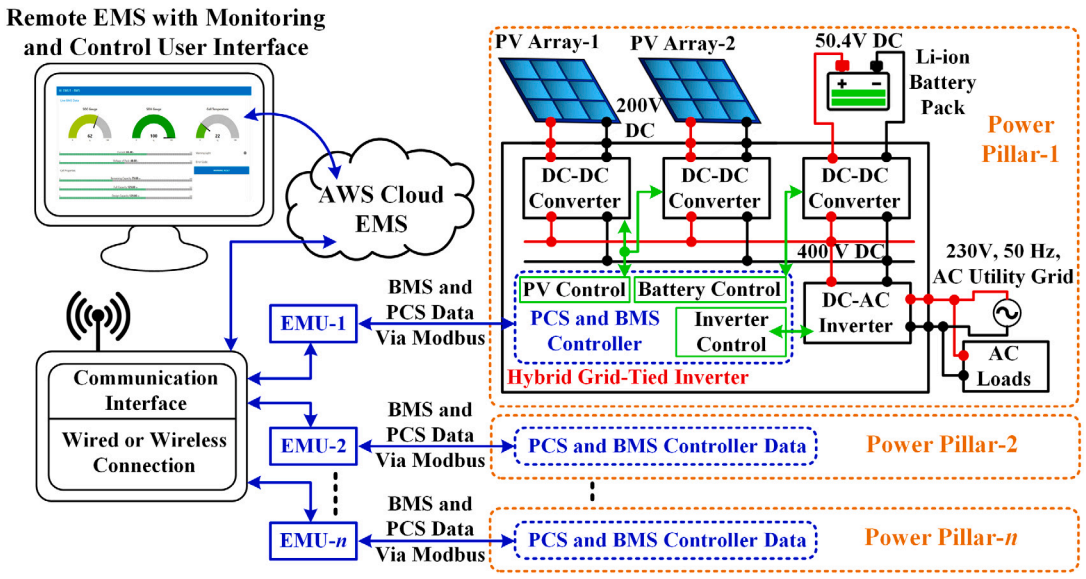

Fig. 11. Architecture for *TYPE 2* system, EMU — Energy Monitoring Unit, PCS — Power conversion System, BMS — Battery Management System, EMS — Energy Management System, AWS — Amazon Web Services.

Table 1
Simulation setup parameters.

Parameter	Value
Open circuit voltage, v_{oc}	1504 V
PV panel maximum power, P_{mpp}^{max}	40 kW
Voltage at maximum power point, v_m	1240 V
Capacitance at the PV side, C_{pv}	2 mF
RMS value of line voltage of grid, v_g	480 V
Grid frequency, f_g	60 Hz
Switching frequency, f_s	10 kHz
kp, ki value for current controller in d, q frame	75, 450

are planning to use techniques such as the one proposed in [74] for Fault tolerant operation.

The results are described in detail in the following section. It is to be noted that the proposed defense is a physical layer defense (layer 0) and should function even in the absence/failure of communication. Hence, it is designed in such way that the state of the system is not required. It relies only on the measurements that are locally available and categorizes the commands based on the value of v_{PCC} and rationality, for example when the v_{PCC} is lower than the allowed limits i.e., $0.95v_{PCC}$ any additional reactive power consumption would result in further decrease of v_{PCC}. The algorithm will tag this as an attack and switch to a locally controlled setting that is similar to MPPT. This implies that the DERMS can no longer control the inverters.

5. Results and discussions

5.1. MATLAB modelling of grid-connected smart PV inverter

An overall block diagram of the MATLAB/SIMULINK model is shown in Fig. 2. The model contains a PV panel with MPPT controller, three phase VSI, decoupled active and reactive power controller and SPWM technique for triggering the insulated gate bipolar transistors (IGBTs) present in the VSI. The PV parameters and values for the MATLAB/SIMULINK set-up are described in Table 1. Irradiance is made to vary every 0.5 s, with the cell temperature kept constant at 25 °C. The PI controllers are appropriately tuned and their values are included in Table 1.

The MPPT controller is based on the P&O method, which sends the current reference in the d-frame, i_d^*. The current reference in the q-frame, $i_{q\text{-}ref}$ is provided by inspecting the Q_{ref} command. The inverter receives the Q_{ref} command during the following modes of operation: (1) where the inverter operates at unity power factor, and (2) when Q_{ref} is received after the Volt/VAR control. The irradiance (irr), actual values of the reactive power (Q_{act}), and the MPP power (P_{mpp}) are sensed and are output of the simulation model.

5.2. Simulation results

In this section we present simulation results for four scenarios: a base case (i.e., no Volt/VAR control), normal scenario where there is Volt/VAR control but no cyber attacks, cyber attack without and with the proposed defense are presented. Following the simulation results discussions are presented as inference of this study.

The proposed defense is validated using the co-simulation setup consisting of connected PV systems, with the PV and inverter implemented on MATLAB/SIMULINK, DERMS implemented on MATLAB code and distribution network (IEEE 13 bus system) implement on OpenDSS. From MATLAB/SIMULINK, the pu value of parameters such as P_{mpp}, irr, Q_{act} and v_{PCC} are sensed and are plotted for 100 iterations as shown in Fig. 12. It can be noted that the graph of P_{mpp} follows the same pattern as irr, as the module temperature is fixed as constant.

For the base case, the Volt/VAR control is not used. Hence, it can be viewed from Fig. 12(a) that the PV inverter is operated at unity power factor mode, which is evident from the graph of Q_{act}, which stays close to 0. In this case, it is observed that v_{PCC} is within the limits specified by IEEE 1547 standards. For the normal scenario i.e. when there are no cyber attacks, while the Volt/VAR control curve is applied as specified in Eq. (2). Fig. 12(b) shows that v_{PCC} has been controlled to be well within the limits by proper Volt/VAR control. Q_{act} is observed to be varied so as to make v_{PCC} between 0.95 pu and 1.05 pu.

Following the base case and normal scenario, a case with cyber attack and without the proposed defense is presented. The cyber attack is implemented in such a way that it causes modification of the Volt/VAR curve. The characteristics of the modified curve used in this case is as described in Eq. (11). Fig. 12(c) shows that v_{PCC} varies between 0.894 pu and 0.906 pu, which is well below the minimum permissible limit of 0.95 pu. Hence, an attack has been induced that has resulted in a reduced voltage below the permissible operating range.

Finally, Fig. 12(d) shows that v_{PCC} can be controlled within the required limits, by implementing the proposed defense mechanism. The same control curve as during cyber-attack is used, however, by employing the defense, v_{PCC} is controlled to be within the permissible limits.

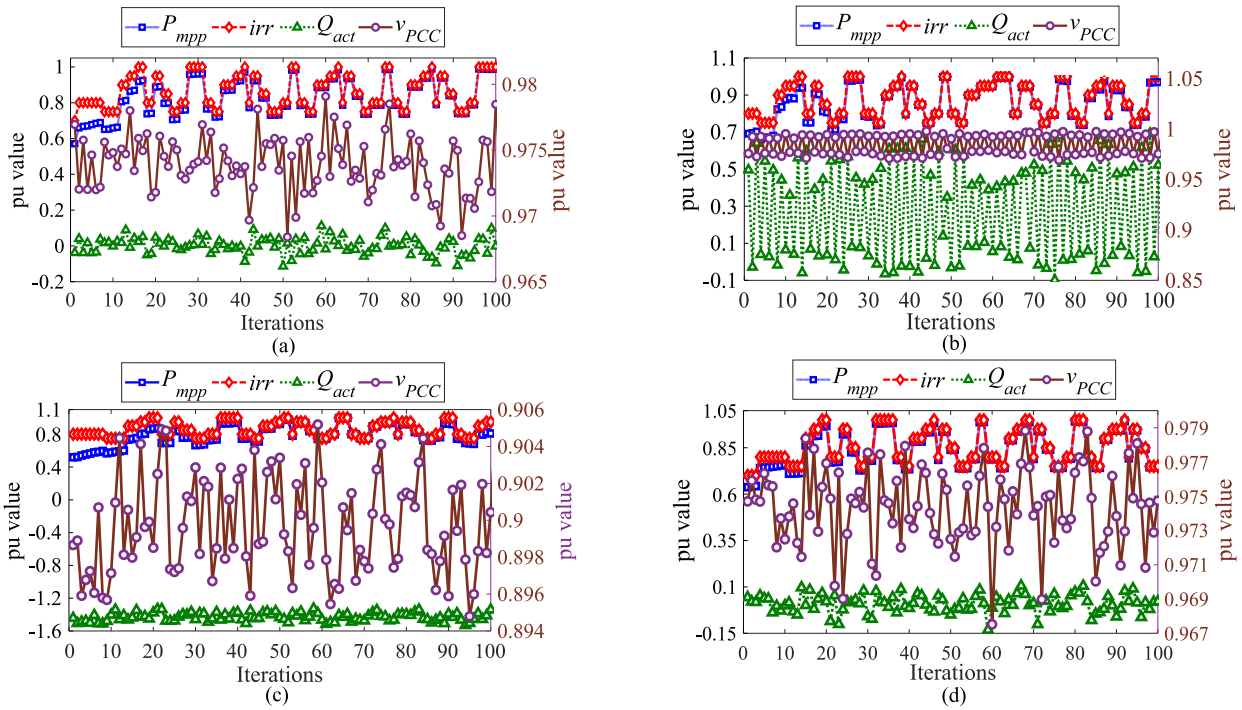

Fig. 12. Simulation results for the sensed parameters: (a) Unity power factor operation — base case, (b) Volt/VAR control without cyber attack — normal Scenario, (c) cyber attack without the proposed defense, and (d) cyber attack with the proposed defense.

When the defense mechanism is active, as discussed in Section 4.2, the commands will be monitored by the range checker. If the commands are rational with respect to the interlock rules, the Q_{ref} obtained from the DERMS will be directed to the inverter control. Else, the command is categorized as an anomalous command and the inverter is made to operate in unity power factor mode. The results corresponding to the above is presented in Fig. 10(b).

5.3. Discussion

The inference from the results is that a simple interlock based on an invariant at the physical layer, helps to evade obviously anomalous commands, due to a cyber-attack or even a communication failure. As the proposed security does not depend on any other communication infrastructure, the reliability of the system could be ensured. However, sub-optimal performance of the grid cannot be avoided as the proposed defense triggers the inverter to operate in non-coordinated mode and defeats the purpose of Volt/VAR control availability. In fact the attacker could use the defense against the system by sending anomalous commands and making sure that Volt/VAR control is unavailable.

As an alternative, instead of switching to unity power factor mode, the inverter can be operated in such a manner that the Q_{ref} is modified to ensure that the v_{PCC} range is within the permissible limits of 0.95 pu and 1.05 pu using a reconfigurable control. The authors are currently working on reconfigurable control for the same defense. However, the intention of avoiding obvious malicious commands is still possible with the proposed method. For the NESCOR failure scenarios, it is feasible to reduce the attack surface (from physical process standpoint) and make it harder for attackers to achieve their intention of affecting the performance of the distribution system. The same principle can also be extended to applications such as demand response management. When such PLS along with reconfigurable control is combined with traditional network security, it is relatively easy to avoid most of the cyber attacks against smart distribution system. A limitations of the proposed method is that unlike traditional security it is not comprehensive and it is not goal agnostic. Further, since it is based on local measurements, the rest of the system state is not taken into consideration when the remedial actions are carried out.

6. Conclusion

In this paper, we presented a physical invariant based security mechanism for edge devices i.e., smart controllers deployed in DER inverters. It was demonstrated that it is an effective approach to minimize the impact of cyber attacks targeting reactive power control in DER inverters. The proposed defense was validated using a co-simulation platform (OpenDSS and MATLAB/SIMULINK). To ensure that fidelity is not compromised the system of grid-connected smart PV inverter was modelled with the aid of MATLAB/SIMU-LINK and OpenDSS. The Volt/VAR control was implemented to achieve a smart inverter. A base case was simulated to showcase the voltage control at PCC using Volt/VAR control. Cyber attacks were launched to modify the Volt/VAR curve characteristics and hence affect the normal operation.

Simulation results without the proposed defense demonstrated inability of the smart inverters to maintain the safe operating range prescribed by the IEEE 1547 standards during cyber attacks. The proposed defense mechanism was implemented using a controller that continuously monitors for an anomaly, and executes the remedial action. Simulation results provided evidence that with the proposed defense mechanism the voltage at PCC can be maintained within the prescribed operating range, even during cyber attacks. The authors are working on a reconfigurable control that can avoid the failure of the proposed defense in cases when the attackers deliberately target the proposed defense to affect the operations of DERs.

CRediT authorship contribution statement

Anusha Kumaresan: Conceptualization, Methodology, Software, Validation, Writing – original draft. **Nandha Kumar Kandasamy:** Conceptualization, Data curation, Writing – original draft, Supervision. **Robert E. Kooij:** Conceptualization, Supervision, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported in part by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2018NCR-NSOE005-0001) and administered by the National Cybersecurity R&D Directorate.

References

[1] Galvan E, Mandal P, Sang Y. Networked microgrids with roof-top solar PV and battery energy storage to improve distribution grids resilience to natural disasters. Int J Electr Power Energy Syst 2020;123:106239.
[2] Pepermans G, Driesen J, Haeseldonckx D, Belmans R, D'haeseleer W. Distributed generation: Definition, benefits and issues. Energy policy 2005;33:787–98.
[3] Panwar NL, Kaushik SC, Kothari S. Role of renewable energy sources in environmental protection: A review. Renew Sustain Energy Rev Apr. 2011;15:1513–24.
[4] Krishna KS, Kumar KS. A review on hybrid renewable energy systems. Renew Sustain Energy Rev 2015;52:907–16.
[5] Kabir E, Kumar P, Kumar S, Adelodun AA, Kim K-H. Sol energy : Potential and future prospects. Renew Sustain Energy Rev 2018;82:894–900.
[6] Kannan N, Vakeesan D. Sol energy for future world:-A review. Renew Sustain Energy Rev 2016;62:1092–105.
[7] Ibrahim H, Anani N. Variations of PV module parameters with irradiance and temperature. Energy Procedia 2017;134:276–85.
[8] Skoplaki E, Palyvos JA. On the temperature dependence of photovoltaic module electrical performance: A review of efficiency/power correlations. Sol Energy 2009;83:614–24.
[9] Tran Q-T, Pham MC, Parent L, Sousa K. Integration of PV systems into grid: From impact analysis to solutions. In: 2018 IEEE inter. conf. on environment and electrical engineering and 2018 IEEE industrial and commercial power systems Europe. IEEE; 2018, p. 1–6.
[10] Liang X. Emerging power quality challenges due to integration of renewable energy sources. IEEE Trans Ind App 2017;53:855–66.
[11] Jouybari-Moghaddam H, Hosseinian SH, Vahidi B. An introduction to active distribution networks islanding issues. In: 2012 Proceedings of 17th conference on electrical power distribution. 2012. p. 1–6.
[12] Khamis A, Shareef H, Bizkevelci E, Khatib T. A review of islanding detection techniques for renewable distributed generation systems. Renew Sustain Energy Rev 2013;28:483–93.
[13] Liang R-H, Chen Y-K, Chen Y-T. Volt/Var control in a distribution system by a fuzzy optimization approach. Int J Electr Power Energy Syst 2011;33:278–87.
[14] Smith JW, Sunderman W, Dugan R, Seal B. Smart inverter volt/var control functions for high penetration of PV on distribution systems. In: 2011 IEEE/PES power systems conference and exposition. IEEE; 2011, p. 1–6.
[15] Neely J, Johnson J, Delhotal J, Gonzalez S, Lave M. Evaluation of PV frequency-watt function for fast frequency reserves. In: 2016 IEEE applied power electronics conference and exposition. IEEE; 2016, p. 1926–33.
[16] Johnson J, Neely JC, Delhotal JJ, Lave M. Photovoltaic frequency–Watt curve design for frequency regulation and fast contingency reserves. IEEE J Photovolt 2016;6:1611–8.
[17] Kashani MG, Mobarrez M, Bhattacharya S. Smart inverter volt-watt control design in high PV-penetrated distribution systems. IEEE Trans Ind Appl 2019;55:1147–56.
[18] Sukumar S, Mokhlis H, Mekhilef S, Karimi M, Raza S. Ramp-rate control approach based on dynamic smoothing parameter to mitigate solar PV output fluctuations. Int J Electr Power Energy Syst 2018;96:296–305.
[19] Klapp D, Vollkommer HT. Application of an intelligent static switch to the point of common coupling to satisfy IEEE 1547 compliance. In: 2007 IEEE power engineering society general meeting. IEEE; 2007, p. 1–4.
[20] Schauder C. Impact of FERC 661-A and IEEE 1547 on photovoltaic inverter design. In: 2011 IEEE power and energy society general meeting. IEEE; 2011, p. 1–6.
[21] Byun J, Hong I, Kang B, Park S. A smart energy distribution and management system for renewable energy distribution and context-aware services based on user patterns and load forecasting. IEEE Trans Consum Electron 2011;57:436–44.
[22] Qi J. Cybersecurity for distributed energy resources and smart inverters. IET Cyber-Phys Syst Theory Appl 2016;1:28–39.
[23] Lee A. Electric sector failure scenarios and impact analyses, 1. National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group; 2013.
[24] Sebastian DJ, Hahn A. Exploring emerging cybersecurity risks from network-connected DER devices. In: 2017 North American power symposium. IEEE; 2017, p. 1–6.
[25] Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, et al. Understanding the mirai botnet. In: USENIX security symposium. 2017. p. 1092–110.
[26] Sun C-C, Hahn A, Liu C-C. Cyber security of a power grid: State-of-the-art. Int J Electr Power Energy Syst 2018;99:45–56.
[27] Shrivastava S, Adepu S, Mathur A. Design and assessment of an orthogonal defense mechanism for a water treatment facility. Robot Auton Syst 2018;101:114–25.
[28] Adepu S, Shrivastava S, Mathur A. Argus: An orthogonal defense framework to protect public infrastructure against cyber-physical attacks. IEEE Internet Comput 2016;20:38–45.
[29] Mackintosh M, Epiphaniou G, Al-Khateeb H, Burnham K, Pillai P, Hammoudeh M. Preliminaries of orthogonal layered defence using functional and assurance controls in industrial control systems. J Sens Actuator Netw 2019;8:14.
[30] Mathur A. SecWater: A multi-layer security framework for water treatment plants. In: Proceedings of the 3rd international workshop on cyber-physical systems for smart water networks. 2017. p. 29–32.
[31] Duan J, Chow M-Y. A novel data integrity attack on consensus-based distributed energy management algorithm using local information. IEEE Trans Ind Inf 2019;15:1544–53. http://dx.doi.org/10.1109/TII.2018.2851248.
[32] Duan J, Chow M-Y. Data integrity attack on consensus-based distributed energy management algorithm. In: 2017 IEEE power energy society general meeting. 2017, p. 1–5. http://dx.doi.org/10.1109/PESGM.2017.8274544.
[33] Adepu S, Mathur A. From design to invariants: Detecting attacks on cyber physical systems. In: 2017 IEEE international conference on software quality, reliability and security companion. IEEE; 2017, p. 533–40.
[34] Kandasamy NK. An investigation on feasibility and security for cyberattacks on generator synchronization process. IEEE Trans Ind Inf 2020;16:5825–34. http://dx.doi.org/10.1109/TII.2019.2957828.
[35] Kandasamy NK. Prosumer site power interruption attacks: Exploiting the reactive power control feature in smart inverters. IET Gener Transm Distrib 2020;14:5372–80.
[36] Hammad E, Ezeme M, Farraj A. Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification. Int J Electr Power Energy Syst 2019;104:817–26.
[37] Turitsyn K, Sulc P, Backhaus S, Chertkov M. Options for control of reactive power by distributed photovoltaic generators. Proc IEEE 2011;99:1063–73.
[38] Carvalho PMS, Correia PF, Ferreira LA. Distributed reactive power generation control for voltage rise mitigation in distribution networks. IEEE Trans Power Syst May 2008;23:766–72.
[39] Boston T, Interconnection P. DOE workshop: Load participation in capacity and ancillary services markets. Technical report, Audubon, PA (United States): PJM Interconnection; 2011.
[40] Basso T, Chakraborty S, Hoke A, Coddington M. IEEE 1547 Standards advancing grid modernization. In: Photovoltaic specialist conference, 2015 IEEE 42nd. IEEE; 2015, p. 1–5.
[41] Lu X, Xia S, Sun G, Hu J, Zou W, Zhou Q, et al. Hierarchical distributed control approach for multiple on-site ders coordinated operation in microgrid. Int J Electr Power Energy Syst 2021;129:106864.
[42] Kekatos V, Wang G, Conejo AJ, Giannakis GB. Stochastic reactive power management in microgrids with renewables. IEEE Trans Power Syst 2014;30:3386–95.
[43] Robbins BA, Hadjicostis CN, Domínguez-García AD. A two-stage distributed architecture for voltage control in power distribution systems. IEEE Trans Power Syst 2013;28:1470–82.
[44] Samadi A, Eriksson R, Söder L, Rawn BG, Boemer JC. Coordinated active power-dependent voltage regulation in distribution grids with PV systems. IEEE Trans power delivery 2014;29:1454–64.
[45] Rogers KM, Klump R, Khurana H, Aquino-Lugo AA, Overbye TJ. An authenticated control framework for distributed voltage support on the smart grid. IEEE Trans Smart Grid 2010;1:40–7.
[46] Kutkut N. An AC PV module with reactive power capability: Need and benefit. Technical report, Petra Solar, Inc..
[47] Gunduz H, Jayaweera D. Reliability assessment of a power system with cyber-physical interactive operation of photovoltaic systems. Int J Electr Power Energy Syst 2018;101:371–84.
[48] Kushner D. The real story of stuxnet. IEEE Spectr 2013;3:48–53.
[49] Defense Case Use. Analysis of the cyber attack on the Ukrainian power grid. 388. Electricity Information Sharing and Analysis Center (E-ISAC); 2016.
[50] Abrams M, Weiss J. Malicious control system cyber security attack case study–Maroochy water services, Australia. McLean, VA: The MITRE Corporation; 2008.
[51] Langill JT. Defending against the dragonfly cyber security attacks. 2014, Retrieved 11, 2015.
[52] Zeller M. Myth or reality—Does the aurora vulnerability pose a risk to my generator? In: 2011 64th Annual conference for protective relay engineers. IEEE; 2011, p. 130–6.
[53] Sridhar S, Govindarasu M. Model-based attack detection and mitigation for automatic generation control. IEEE Trans Smart Grid 2014;5:580–91.
[54] Yuan Y, Li Z, Ren K. Modeling load redistribution attacks in power systems. IEEE Trans Smart Grid 2011;2:382–90.
[55] Teixeira A, Sandberg H, Johansson KH. Networked control systems under cyber attacks with applications to power networks. In: American control conference, 2010. IEEE; 2010, p. 3690–6.

[56] Deng R, Xiao G, Lu R, Liang H, Vasilakos AV. False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey. IEEE Trans Ind Inf 2017;13:411–23.
[57] Poudel BP, Mustafa A, Bidram A, Modares H. Detection and mitigation of cyber-threats in the DC microgrid distributed control system. Int J Electr Power Energy Syst 2020;120:105968.
[58] Duan J, Zeng W, Chow M-Y. Economic impact of data integrity attacks on distributed DC optimal power flow algorithm. In: 2015 North American power symposium. 2015, p. 1–7. http://dx.doi.org/10.1109/NAPS.2015.7335167.
[59] Liu C, Zhou M, Wu J, Long C, Farraj A, Hammad E, et al. Reactance perturbation for enhancing detection of FDI attacks in power system state estimation. In: 2017 IEEE global conference on signal and information processing. IEEE; 2017, p. 523–7.
[60] John F, Marty E. NCCIC/ICS-CERT Industrial control systems assessment summary report. Home Land Security; 2015, Available online.
[61] Johnson J, Onunkwo I, Cordeiro P, Wright BJ, Jacobs N, Lai C. Assessing DER network cybersecurity defences in a power-communication co-simulation environment. IET Cyber-Phys Syst Theory Appl 2020;5:274–82.
[62] Tzartzev R, Grady WM, Patel J. Impact of high-penetration PV on distribution feeders. In: 2012 3rd IEEE PES innovative smart grid technologies Europe. IEEE; 2012, p. 1–6.
[63] Monger S, Vega R, Krishnaswami H, et al. Simulation of smart functionalities of photovoltaic inverters by interfacing OpenDSS and MATLAB. In: 2015 IEEE 16th workshop on control and modeling for power electronics. IEEE; 2015, p. 1–6.
[64] Podder AK, Roy NK, Pota HR. MPPT methods for solar PV systems: A critical review based on tracking nature. IET Renew Power Gener 2019;13:1615–32.
[65] Dhimish M. Assessing MPPT techniques on hot-spotted and partially shaded photovoltaic modules: Comprehensive review based on experimental data. IEEE Trans Elect Dev 2019;66:1132–44.
[66] Zhou T, Sun W. Study on maximum power point tracking of photovoltaic array in irregular shadow. Int J Electr Power Energy Syst 2015;66:227–34.
[67] Kollimalla SK, Mishra MK. Variable perturbation size adaptive P&O MPPT algorithm for sudden changes in irradiance. IEEE Trans Sustain Energy 2014;5:718–28.
[68] Ali AIM, Mohamed HRA. Improved P&O MPPT algorithm with efficient open-circuit voltage estimation for two-stage grid-integrated PV system under realistic solar radiation. Int J Electr Power Energy Syst 2022;137:107805.
[69] Seal B, Cleveland F, Allen Hefner A. Distributed energy management (DER): Advanced power system management functions and information exchanges for inverter-based DER devices, modelled in IEC 61850-90-7. In: Advanced functions of DER inverters. Electric Power Research Institute; 2012, URL: http://xanthus-consulting.com/Publications/documents/Advanced_Functions_for_DER_Inverters_Modeled_in_IEC_61850-90-7.pdf.
[70] Yazdani A, Iravani R. Voltage-sourced converters in power systems: Modeling, control, and applications. John Wiley & Sons; 2010.
[71] Jenisha CM, Ammasaigounden N, Kumaresan N, BhagyaSri K. Power electronic interface with de-coupled control for wind-driven PMSG feeding utility grid and DC load. IET Power Electron 2017;11:329–38.
[72] Lakshmi M, Hemamalini S. Decoupled control of grid connected photovoltaic system using fractional order controller. Ain Shams Eng J 2018;9:927–37.
[73] Garcia L, Brasser F, Cintuglu MH, Sadeghi A-R, Mohammed OA, Zonouz SA. Hey, my malware knows physics! Attacking PLCs with physical model aware Rootkit. In: NDSS. 2017.
[74] Sardashti A, Ramezani A. Fault tolerant control of islanded AC microgrids under sensor and communication link faults using online recursive reduced-order estimation. Int J Electr Power Energy Syst 2021;126:106578.