Self-Secure Inverters Against Malicious Setpoints

Tareq Hossen, *Student Member, IEEE*, Fahmid Sadeque, *Student Member*, IEEE, Mehmetcan Gursoy, *Student Member*, IEEE, and Behrooz Mirafzal, *Senior Member, IEEE*

***Abstract*— The next generation of grid-interactive inverters brings a communication feature that allows data sharing from utility supervisory controllers and smart devices that are connected to the same network. This feature enhances the control capabilities of grid-interactive inverters to provide services beyond active power injection. However, communication networks entail more vulnerable surfaces to malicious attacks that may result in modifying active and reactive power setpoints and causing weak-grid conditions or abnormal inverter operation. In this paper, steady-state and the dynamic behavior of the inverter for the incoming setpoints are analyzed to detect false data injection attacks and provide device-level security. The steady-state behavior of the inverter in the operating region is determined from the grid parameters such as the grid voltage and the grid impedance. These estimations are accomplished by the proposed self-security technique through a low-frequency signal injection-based approach combined with the recursive least square method. Moreover, a reduced fourth-order inverter model is used as the dynamic reference model, and grid parameters as well as the incoming setpoints are implemented to the reference model to verify whether the dynamic behavior of the inverter is inside the permissible region of operation. The validity and performance of the proposed method are verified experimentally through Allen-Bradley Powerflex 755 three-phase inverter and a 12 kW NHR 9410 regenerative power grid emulator. The results show that the self-secure smart-inverter is able to accept or reject the incoming commands and thus is protected from malicious cyber-physical attacks.**

***Index Terms*—Smart inverter, cyber-physical attack, self-security, inverter operational region, grid parameter estimation, recursive least square.**

I. INTRODUCTION

Conventional electromechanical energy conversion-based power systems are evolving to next-generation power electronics-based smart power systems due to environmental concerns. Nowadays, inverters are being implemented in the modern power infrastructure to minimize the release of greenhouse gasses and support renewable power generation. The goal was to deliver the maximum active power generated by solar and wind turbines to the grid in former applications. Then, capabilities of the conventional inverters are improved by controlling reactive power to achieve unity power factor and reduce power losses in the system. Moreover, controlling the active and reactive power of the grid-interactive inverters enlightened the researchers to address the stability and efficiency issues at the grid side. To fill this gap, grid supporting, also called ancillary services, such as voltage regulation and harmonic compensations, and grid forming features such as power-sharing, voltage, and frequency control are developed. These advances in inverter control techniques improve the inverter dynamics, form the fundamentals of smart inverters, and allow high penetration of smart inverters and renewable energy sources to the grid.

Device communication protocols and improvements in internet technologies allow interaction between devices connected to the same network in a power system. Thus, supervisory commands, system information, or measurement data can be shared among each smart device to enhance the stability of the inverters as well as the stability of the grid. However, increasing the number of communication channels by implementing more smart devices in the system can provide hackers alternative ways to perform cyberattacks on the smart inverters that can cause undesired inverter operating conditions, damage the power system, and lead to high economic problems. For instance, an attacker can alter essential parameters used by the inverter's controller, the measurement data, or active (P) and reactive power (Q) setpoints of the inverter to jeopardize inverter's operation. Thinking of high penetration of renewables in a large-scale power application, jeopardized inverter operation can bring new challenges regarding to the secure, reliable, and stable operation of the power network [1], [2].

Anomaly detection is an essential feature for smart inverters to prevent malicious activities and protect the power system. For instance, police forces can provide security to protect residents and their properties. However, some residents own surveillance systems to prevent any illegal activities that police cannot detect at the time instant. Nonetheless, detecting cyberattacks would become more challenging if bad data received by the inverters are intentionally sent from a person through a trusted device such as a utility supervisory control and data acquisition (SCADA) unit. Modified data sent by secure channels can bypass system-level security protocols and demand the inverter to inject excessive active power or reduce the power quality. Both cases can cause voltage fluctuations at the grid side. Moreover, according to the IEEE 1547-2018 standards provided by [3], voltage ride-through function is required for inverters during under and overvoltage conditions for a specific period. Therefore, device-level security for inverters is necessary and yet needs attention to verify the data integrity, identify tempered power setpoints, and ensure secure and reliable operation of smart inverters in a specified period [4].

Many research works are conducted to ensure the safe and stable operation of the power electronics converters under cyber-physical attacks. Active synchronous detection method (ASDM) is proposed in the literature [5] and [6], to overcome the cyberattacks in microgrid networks. In these methods, the microgrid control center generates low magnitudes probing signal and send it to the controller to identify cyberattacks. The

This material is based upon work supported by the Department of Energy, Office of Energy Efficiency and Renewable Energy (EERE), Solar Energy Technologies Office, under Award Number DE-EE0008767.

impact of cyberattacks on the reactive power capability of an inverter-based distributed generation system is discussed in [7]. Moreover, a data-driven approach for grid-interactive inverters to detect cyberattacks has been presented in [8] and [9], and sensor malfunction detection and mitigation strategy have been proposed in [10]. Also, an event-driven attack-resilient controller is developed in [11] to eliminate the stealth-attack in AC microgrid. These researches have presented different approaches that provide protection for different types of cyberattacks at the system level. However, no device-level security measures have been presented by these authors.

Although the impact of a device-level cyberattack may appear to be insignificant to the power grid, malfunction in a single inverter unit can result in sequential failure of the cluster of smart inverters in large-scale power systems. For instance, in August 2016, inaccurate frequency measurement due to a phase-locked-loop malfunction tripped a single inverter resulting in sequential failure that caused a 1200 MW power loss on the transmission lines connected to the southern California PV firm [12]. Therefore, device-level security is necessary to ensure reliable operation.

Self-security is a state-of-the-art device-level anomaly detection feature that can be used to identify cyberattacks. In this manuscript, the proposed self-security feature analyzes the incoming command and detects device level cyber-physical attacks targeting inverter PQ setpoints by checking the steady-state and the dynamic behaviors of the inverter. The steady-state behavior is examined to identify the operating region by utilizing the estimated grid impedance and voltage. The estimation is performed in real-time by adopting a low-frequency signal injection-based method combined with the recursive least square (RLS) method. Moreover, the dynamic behavior is observed through a reduced fourth-order model of the inverter.

The paper is organized as follows. Section II presents a description of the system. Section III elaborately illustrates the proposed self-security approach of the smart inverter. Experiment results are provided in section IV. Finally, section V discusses the contribution and future aspects of the research presented in this paper.

II. System Description and Modeling

In this section, the self-security functionality of the grid-interactive smart-inverters is discussed. In Fig. 1, a cyber-physical power system is represented where a channel between a cyber network and a physical network is provided through the communication link. In a power system, utility supervisory controllers, aggregator controllers, solar leaser controllers, data processors, etc. can form a cyber network. On the other hand, smart meters, smart inverters, battery chargers, smart loads, etc. can form a physical network. The purpose of device-level and system-level communication is to advance the capabilities in system monitoring and control under normal and abnormal operation.

In this paper, unauthorized external data that request a change in smart inverter PQ setpoints are considered as cyberattacks. Notice that each smart inverter equips a local controller to inject the desired power into the utility grid. The inverter utilizes the proposed self-security technique to analyze the received commands and decide to accept or reject the received data. As a grid-interactive inverter, a three-phase PQ controlled two-level voltage source inverter (2L-VSI) developed in [13] and [14] is utilized, and the block diagram is also provided in Fig.1. the inverter output terminals are connected to the point-of-common-coupling (PCC) through an LCL filter. Herein, L_1, L_2, and C_f denote the inverter-side inductance, the grid-side inductance, and the capacitance of the filter connected in delta, respectively. In addition, Z_g represents the Thevenin equivalent impedance between the PCC and the grid that consists of a resistance R_g, and inductance L_g.

III. Self-Secure Smart Inverter Design For Cyber Attack Prevention

The proposed self-security feature evaluates the PQ setpoints based on the grid and smart inverter parameters. This feature determines the operating region of the inverter in real-time to identify manipulated setpoints. This allows the inverter to accept or reject the incoming setpoints. The proposed algorithm can be explained in four sections: (i) operating region evaluation, (ii) online grid parameter estimation, (iii) attack detection, and (iv) dynamic performance estimation.

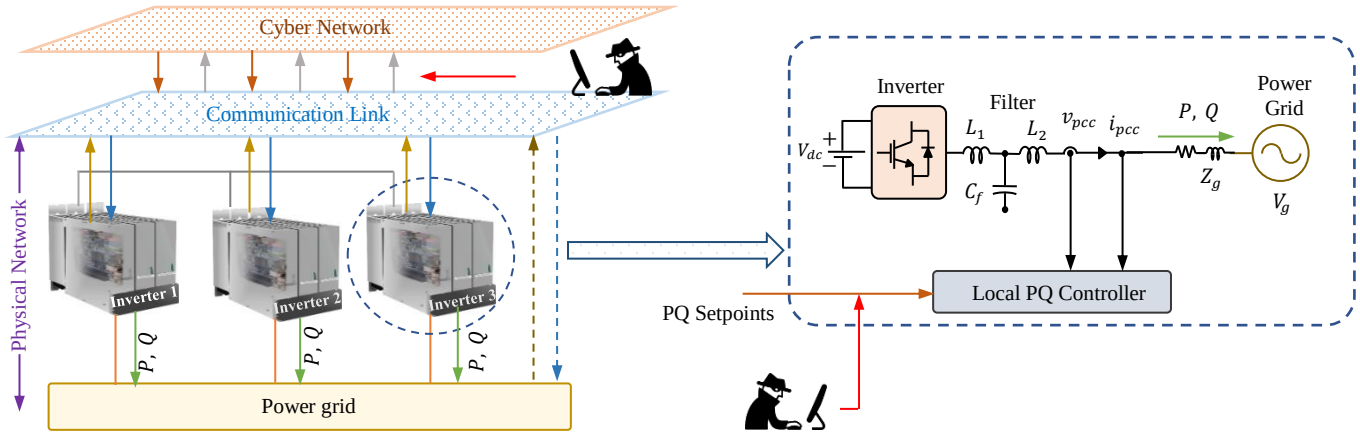

Fig. 1. Smart inverters connected to the power grid and possible cyberattack scenarios.

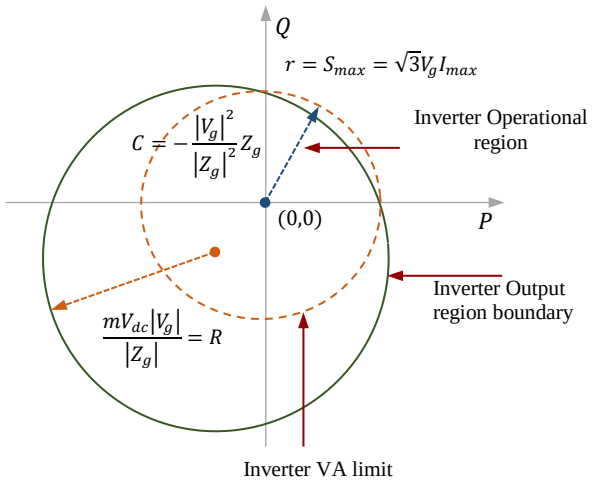

Fig. 2. Normal operating region of a grid-interactive inverter in a distribution grid

A. *Operating Region Evaluation*

In [1] and [15], safe operation region for grid-interactive smart inverters are discussed. The inverter operation region for power injection to the grid is provided in Fig. 2. Herein, $|V_g|$, δ, k_m, and m denote line-line RMS grid voltages, the phase-angle between the grid and inverter voltages, the linear modulation index, and the modulation index, respectively. Assuming, m is in the linear modulation region, i.e., $0 \leq m \leq 1$, and V_g, Z_g, and V_{dc} are constants, the operation region corresponds to a disk in the PQ- plane with a radius R centered at C. Notice, R decreases inversely proportional to Z_g, and directly proportional to dc-bus voltage V_{dc}. On the other hand, the rated capacity of the inverter is illustrated as a circle with a radius r, centered at the origin. To achieve stable operation, the smart inverter should operate inside the region where these circles intersect with each other because this region contains all the valid PQ setpoints [16]. Any points that fall outside of the intersected region causes abnormal behavior. Since m and V_{dc} are known, it is required to estimate the grid impedance and the voltage to determine the operating region. Thus, the smart inverter decides the validity of the incoming PQ setpoints to confirm device-level security.

B. *Online Grid Parameter Estimation*

An estimation technique needs to be incorporated to determine the grid parameters. One phase of a three-phase grid-interactive inverter is shown in Fig. 3. In literature, there are many active and passive methods [17] for grid parameter estimation such as adaptive identification techniques, voltage transients, signal injections, etc. where adaptive identification techniques include adaptive model reference [18] and recursive least square method [19]. However, these methods cannot be directly implemented for Z_g and V_g estimation because V_g is unknown. Applying KVL at the PCC, one can obtain the following equation.

$$V_{pcc} = R_g i_g + L_g \frac{di_g}{dt} + V_g \tag{1}$$

In this paper, a signal injection technique is combined with the RLS method to estimate the grid parameters. The signal injection technique injects external perturbation for a short

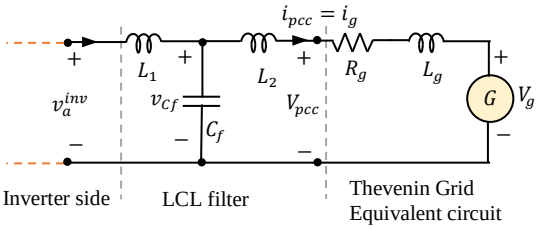

Fig.3. Simplified phase-a circuit of a three-phase grid-interactive VSI.

period to monitor the response of the system as soon as new setpoints are received. There are two techniques for signal injection: i) low-frequency signal injection ii) high-frequency signal injection [18]. Nevertheless, there are significant disadvantages to the high-frequency signal injection method. One of the problems is that the high-frequency injection should be performed precisely, so the active LCL filter connected to the inverter output does not attenuate the high-frequency components of current or voltages [17]. On the other hand, the low-frequency signal is not attenuated by the LCL filter [20]. In this work, a low-frequency signal with a small magnitude is momentarily injected to estimate the grid impedance. Applying KVL at the PCC, one can calculate

$$\hat{V}_{pcc} = R_g \hat{\imath}_g + L_g \frac{d\hat{\imath}_g}{dt} \tag{2}$$

where, $\hat{\imath}_g$ is the current injected into the grid at $f_{in} \neq 60\ Hz$ and $\hat{V}_{pcc}$ is the voltage measured at the point of common coupling at f_{in}. Notice, f_{in} has to be chosen such that the grid voltage does not have any component at that frequency, i.e $\hat{V}_g = 0$. This part describes the RLS formulation for the Z_g estimation. The output measurement for the RLS, $y(t)$ at the time instant t_1 can be represented as

$$y(t_1) = \hat{\imath}_g(t_1), \tag{3}$$

and $u(t)$ is the input measurement for the RLS

$$u(t_1) = \hat{V}_{pcc}(t_1), \tag{4}$$

Consider, T is the sampling time of the measurement and matrix $A = [a_1 \quad a_2]^{\mathrm{T}}$ which includes unknown parameters and measurement matrix $W = [-y(t_1) \quad u(t_1)]^{\mathrm{T}}$. The parameters can be expressed as $a_1 = (L_g T/R_g - 1)$ and $a_2 = T/L_g$. Therefore, the grid inductance can be represented as $L_g = T/a_2$ and grid resistance can be represented as $R_g = L_g T/(1 + a_1)$. In the recursive form, the least square problem is formulated using (5) and (6). Here, M is the number of measurements, R_M is the covariance matrix, where it is initialized as is 2×2 identity matrix, μ is the forgetting factor bounded as $\mu = [0\ 1]$ where μ is selected between 0.85 and 0.95. In addition, unknown parameter vector A can be estimated for M measurements as,

$$A_M = A_{M-1} - R_M^{-1} W(t_M)\big(W^T(t_M)A_{M-1} - y(t_M)\big), \tag{5}$$

where, the covariance matrix R_M is defined as

$$R_M = \mu \sum_{i=1}^{M-1} \mu^{M-i-1} W(t_i)W^T(t_i) + W(t_M)W^T(t_M), \tag{6}$$

Estimated R_g and L_g can be used to calculate the grid voltage using (1).

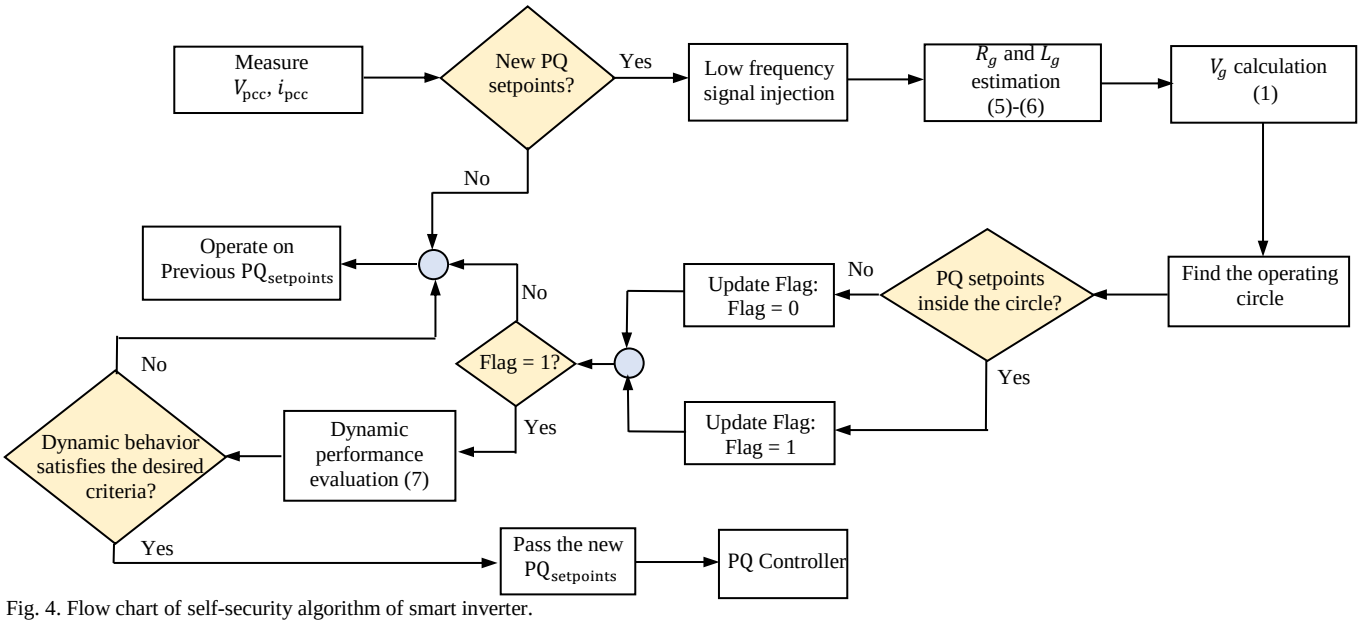

Fig. 4. Flow chart of self-security algorithm of smart inverter.

C. Attack Detection

In Fig. 4, the proposed cyberattack detection algorithm first measures the voltage and current at the PCC. The algorithm then verifies whether the incoming PQ setpoints are valid or manipulated. After a new setpoint is received, the algorithm will inject a low-frequency signal momentarily and estimate R_g and L_g in real-time using (5) and (6). An eighth order Butterworth lowpass filter is used to extract the low-frequency components for the parameter estimation. Next, the grid voltage is estimated using (1). After that, the validity of incoming PQ setpoints is verified. If the PQ setpoints are outside of the desired inverter operating region, the self-security algorithm rejects the incoming PQ setpoints and set the PQ points to previously defined PQ setpoints for safety. Nevertheless, if the incoming PQ setpoints are inside the desired region, the algorithm accepts the incoming PQ setpoints, and the inverter injects demanded power to the grid.

D. Dynamic Performance Estimation

As soon as a new setpoint is applied, the response of the inverter can temporarily fall outside of the desired region due to its transient behavior and return to its normal operation. This behavior may jeopardize the normal operation of the inverter in practice. Hence, evaluating the dynamic behavior of a smart inverter for new PQ setpoints is required to prevent the inverter from falling into the abnormal region. The full-order state-space model has been developed to depict the impacts of the control scheme, filter parameters, and the effects of the grid impedance on inverter stability [21]. It is also verified that the full-order grid-connected VSI model can be reduced to a fourth-order model to represent the dynamic characteristics [22]. Thus, the dynamic characteristics of a smart inverter can be modeled using the reduced fourth-order model that includes high and low-frequency dynamics, as shown in (7).

$$H_{VP}(s) = \frac{K(\omega_L^2\omega_H^2)(s+z)}{(s^2+2\sigma_L s+\omega_L^2)(s^2+2\sigma_H s+\omega_H^2)}, \qquad (7)$$

where, the high-frequency dynamics ω_H is a function of circuit parameters L_1, L_2, L_g, and C_f, and low-frequency dynamics ω_L is a function of the bandwidth of the inner current controller loop. Herein, σ_L, σ_H, z, and K represent low-frequency damping co-efficient, high-frequency damping co-efficient, zeros, and gain of the fourth-order model, respectively. Depending on the system parameters, the dynamic behavior of a grid-tied inverter can fall in an over-damped, critically-damped, or under-damped response, neglecting high-frequency phenomena. The dynamic performance of the smart inverter was assessed from (7) using the reduced fourth-order model in MATLAB/Simulink. For a step change in active power, $\Delta P = 1.5$ kW at 1.0 s, the RMS voltage at the inverter's output terminals was recorded for full-order circuit simulation and reduced fourth-order model. For the reduced-order model low-frequency dynamics ω_L was selected according to inner-current controller bandwidth, which is a function of the controller gain parameters K_p and K_i. Also, the high-frequency dynamics ω_H was selected based on inverter circuit parameters $L_1 = 1\ mH$, $L_2 = 0.5\ mH$, $L_g = 1\ mH$, and $C_f = 30\ \mu F$. In Fig. 5(a), reduced-order model response closely

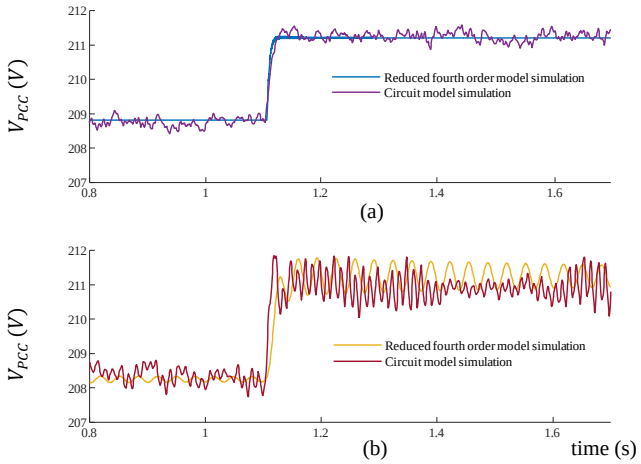

Fig. 5. Dynamic response for given step of ΔP for circuit model and reduced fourth order model.

TABLE IV
PARAMETERS FOR EXPERIMENTAL SET-UP

Parameters	Values
Fundamental frequency	60 Hz
PWM carrier frequency	10 kHz
$V_{LL,rms}$	208
V_{dc}	360 V
L_1 (Inverter-side of LCL)	1.0 mH
C_f (Δ)	30 µF
L_2 (Grid-side of LCL)	0.5 mH

matches the response of the full-order circuit model. Similarly, in Fig. 5(b), the reduced-order model response follows the oscillatory (under-damped) response of the full-order circuit when L_g was changed from 1 mH to 3.5 mH. Therefore, the results estimated by the fourth-order model were in good agreement with the outcomes of the full-order circuit simulations.

IV. EXPERIMENTAL RESULTS

This section describes the performance of the proposed self-security algorithm of a three-phase grid-interactive inverter setup. In Fig. 6, the experiment was performed at 208 V RMS grid voltage using a 12 kW NHR 9410 regenerative power grid emulator. Allen-Bradley Powerflex 755 was employed as the three-phase VSI operating at 1 kW, and the dc input voltage was set to 360V. The details of the system parameters are shown in Table I. The closed-loop control was implemented using dSpace 1103 platform. CP030 current probes and ADP300 differential probes were used to measure current and voltage waveforms, respectively.

Fig. 7 shows that a sudden variation in dc-bus voltage from 360 V to 300 V changes the line-current operational condition from normal to abnormal. Similarly, Fig. 8 shows that at (t = 3.20 s) a sudden change in grid impedance from 1 mH to 3.5 mH also caused abnormal line-current. The change in both dc-bus voltage and grid impedance shrinks the size of the operating region shown in Fig. 2.

Fig. 9 shows the grid parameter estimation. At (t = 0.35 s), grid resistance and grid inductance have changed using a circuit breaker, and one can conclude that the RLS method can accurately estimate the actual quantity in real-time.

In Fig. 10, the efficacy of the self-security algorithm was checked for two different incoming PQ setpoints, where O_1 denotes the first setpoints ($P_1 = 1\ kW, Q_1 = 2.1\ kVAR$), and

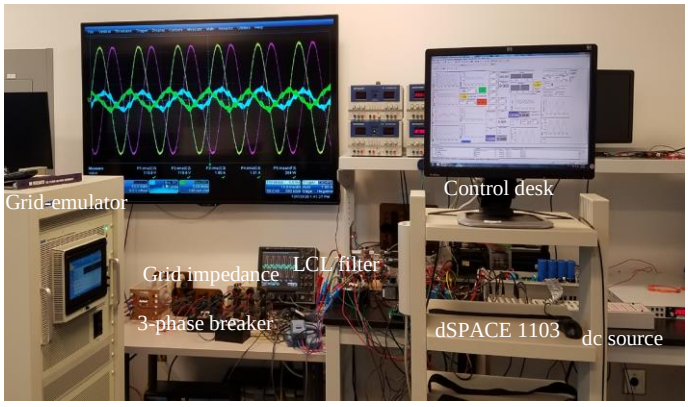

Fig. 6. Hardware setup for self-security algorithm implementation

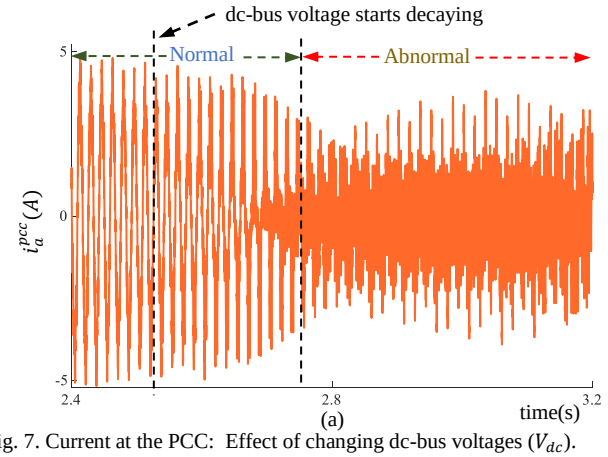

Fig. 7. Current at the PCC: Effect of changing dc-bus voltages (V_{dc}).

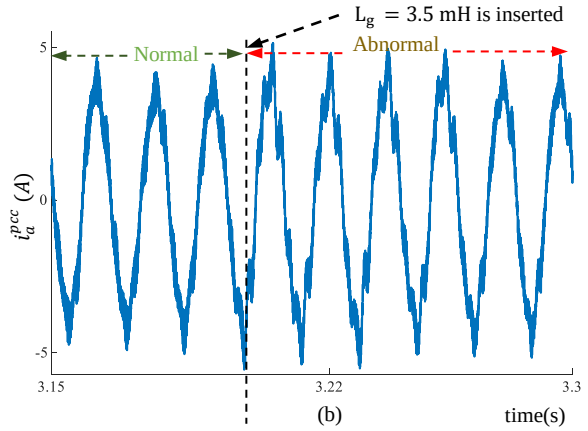

Fig. 8. Current at the PCC: Effect of changing grid impedance (Z_g).

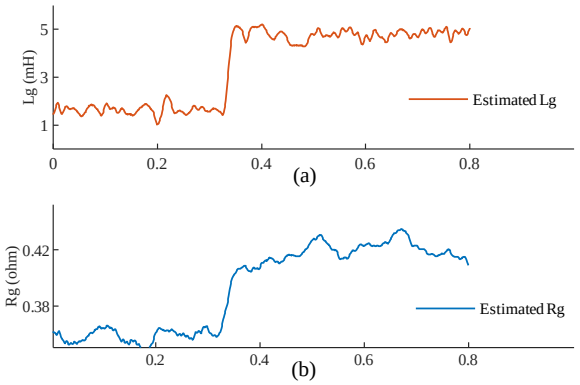

Fig. 9. Estimation result from control desk (a) grid inductance (L_g) and (b) grid resistance (R_g) estimation using RLS.

O_2 denotes the other setpoints ($P_2 = 1.5\ kW, Q_2 = 3\ kVAR$). The green circle represents the accepted points, while the red circle represents the rejected values.

V. CONCLUSION

In this paper, a device-level self-security feature of the smart inverter has been developed to identify the cyber-physical attacks to the smart inverters. With the developed method, the inverter could identify malicious setpoints that could bypass the system-level security and decide whether to accept or reject the new setpoints. With a low-frequency injection-based recursive least square approximation technique, the inverter first estimated the grid voltage and impedance value. Then, a safe

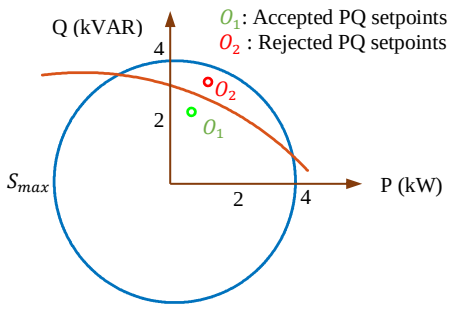

Fig. 10. Checking the authenticity of incoming setpoints by self-secure algorithm.

region of operation is identified. The PQ setpoints coming from the supervisory controller are then checked through a steady-state model and fourth-order dynamic model by estimating whether the system lies within the safe region of operation. The proposed method is tested experimentally, and the results verified that the method could be an effective device-level security measure for cyber-physical attacks.

VI. References

[1] B. Mirafzal and A. Adib, "On grid-interactive smart inverters: Features and advancements," *IEEE Access*, vol. 8, pp. 160526-160536, 2020.

[2] J. C. Balda, A. Mantooth, R. Blum, and P. Tenti, "Cybersecurity and power electronics: Addressing the security vulnerabilities of the internet of things," *IEEE Power Electron. Mag.*, vol. 4, no. 4, pp. 37-43, Dec. 2017.

[3] B. Arbab-Zavar, E. Palacios-Garcia, J. Vasquez, and J. Guerrero, "Smart inverters for microgrid applications: A review," *Energies*, vol. 12, no. 5, Mar. 2019.

[4] C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, "Microgrid cyber security reference architecture," Sandia Nat. Lab., Albuquerque, NM, Tech. Rep. SAND2013-5472, 2013.

[5] Y. Li, P. Zhang, L. Zhang, and B. Wang, "Active synchronous detection of deception attacks in microgrid control systems," *IEEE Trans. Smart Grid*, vol. 8, no. 1, pp. 373-375, Jan. 2017.

[6] Y. Li, Y. Qin, P. Zhang, and A. Herzberg, "SDN-enabled cyber-physical security in networked microgrids," *IEEE Trans. Sustain. Energy*, vol. 10, no. 3, pp. 1613-1622, July 2019.

[7] A. Majumdar, Y. P. Agalgaonkar, B. C. Pal, and R. Gottschalg, "Centralized volt–var optimization strategy considering malicious attack on distributed energy resources control," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 148-156, Jan. 2018.

[8] F. Li et al., "Detection and identification of cyber and physical attacks on distribution power grids with PVS: An online high-dimensional data-driven approach," *IEEE J. Emerg. Sel. Topics Power Electron*, Sep. 2019.

[9] K. Abdollah, W. Su, and T. Jin, "A machine learning based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Trans. Ind. Informat.*, Jan. 2020.

[10] A. Teymouri and A. Mehrizi-Sani, "Sensor malfunction detection and mitigation strategy for a multilevel photovoltaic converter," *IEEE Trans. Energy Convers.*, vol. 35, no. 2, pp. 886-895, June 2020.

[11] S. Sahoo, Y. Yang, and F. Blaabjerg, "Resilient synchronization strategy for AC microgrids under cyber attacks," *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 73-77, Jan. 2021.

[12] North American Electric Reliability Corporation, "1200 MW fault induced solar photovoltaic resource interruption disturbance report," NERC, Jun. 2017.

[13] D. S. Ochs, B. Mirafzal, and P. Sotoodeh, "A method of seamless transitions between grid-tied and stand-alone modes of operation for utility-interactive three-phase inverters," *IEEE Trans. Ind. Appl.*, vol. 26, no. 3, pp. 1934-1941, May 2014.

[14] A. Adib, J. Lamb, and B. Mirafzal, "Ancillary services via VSIs in microgrids with maximum DC-bus voltage utilization," *IEEE Trans. Ind. Appl.*, vol. 55, no. 1, pp. 648-658, Jan.-Feb. 2019.

[15] J. Lamb and B. Mirafzal, "Grid-interactive cascaded H-bridge multilevel converter PQ plane operating region analysis," *IEEE Trans. Ind. Appl.*, vol. 53, no. 6, pp. 5744-5752, Nov.-Dec. 2017.

[16] J. Lamb and B. Mirafzal, "Active and reactive power operational region for grid-interactive cascaded H-bridge multilevel converters," *2016 IEEE Energy Conversion Congress and Exposition (ECCE)*, Milwaukee, WI, 2016, pp. 1-6.

[17] P. García, M. Sumner, Á. Navarro-Rodríguez, J. M. Guerrero, and J. García, "Observer-based pulsed signal injection for grid impedance estimation in three-phase systems," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 7888-7899, Oct. 2018.

[18] L. Asiminoaei, R. Teodorescu, F. Blaabjerg, and U. Borup, "Implementation and test of an online embedded grid impedance estimation technique for PV inverters," *IEEE Trans. Ind. Electron.*, vol. 52, no. 4, pp. 1136-1144, Aug. 2005.

[19] J. Benzaquen, F. Fateh, and B. Mirafzal, "On the dynamic performance of variable-frequency AC–DC converters," *IEEE Trans. Transport. Electrific.*, vol. 6, no. 2, pp. 530-539, June 2020.

[20] D. Reigosa, F. Briz, C. B. Charro, P. Garcia, and J. M. Guerrero, "Active islanding detection using high-frequency signal injection," *IEEE Trans. Ind. Appl.*, vol. 48, no. 5, pp. 1588-1597, Sep.-Oct. 2012.

[21] A. Adib, B. Mirafzal, X. Wang, and F. Blaabjerg, "On stability of voltage source inverters in weak grids," *IEEE Access*, vol. 6, pp. 4427-4439, 2018.

[22] A. Adib, F. Fateh, M. B. Shadmand, and B. Mirafzal, "A reduced-order technique for stability investigation of voltage source inverters," *2018 IEEE Energy Conversion Congress and Exposition (ECCE)*, Portland, OR, 2018, pp. 5351-5356.