Decentralized Anomaly Characterization Certificates in Cyber-Physical Power Electronics Based Power Systems

Gupta, Kirti; Sahoo, Subham; Mohanty, Rabindra; Panigrahi, Bijaya Ketan; Blaabjerg, Frede

Published in:
2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)

DOI (link to publication from Publisher):
10.1109/COMPEL52922.2021.9645984

Publication date:
2021

Document Version
Accepted author manuscript, peer reviewed version

Decentralized Anomaly Characterization Certificates in Cyber-Physical Power Electronics Based Power Systems

Kirti Gupta
Department of Electrical Engineering
Indian Institute of Technology, Delhi
Delhi, 110016, India
Email: Kirti.Gupta@ee.iitd.ac.in

Subham Sahoo
Department of Energy
Aalborg University
Aalborg, 9220, Denmark
Email: sssa@energy.aau.dk

Rabindra Mohanty
EEE Department
BITS Pilani, Hyderabad Campus
Telangana, 500078, India
Email: rabindra.m@hyderabad.bits-pilani.ac.in

Bijaya Ketan Panigrahi
Department of Electrical Engineering
Indian Institute of Technology, Delhi
Delhi, 110016, India
Email: Bijaya.Ketan.Panigrahi@ee.iitd.ac.in

Frede Blaabjerg
Department of Energy
Aalborg University
Aalborg, 9220 , Denmark
Email: fbl@energy.aau.dk

***Abstract*—Modern power electronics based power systems with inclusion of information and communication technologies (ICT) have emerged to be cyber-physical systems, making it vulnerable to both cyber and physical anomalies. These systems on one hand are susceptible to grid/system faults, whereas on the other hand, ICT can easily be the potential target of the third-party adversaries. On top, the transient response of cyber-physical power electronics based power systems (PEPS) to the said critical disturbances is very fast, which becomes another challenge to distinguish them accurately within a short time frame. To address this challenge, this paper certifies cyber-physical anomalies using physics-informed empirical laws governed by mapping X-Y plane between locally measured frequency (f) and d-axis voltage (V_d) only, forming a decentralized approach. The anomaly characterization between physical and cyber faults is carried out by tracing the trajectory movement online in the aforementioned X-Y plane. Basically, the physics-informed laws determine the boundaries in this plane to segregate between grid faults and cyber attacks. This decentralized method is effective in classifying the anomalies only within 5 ms (with 20 samples/cycle in a 50 Hz system), which has been validated on modified CIGRE LV benchmark distribution network with real-time (RT) simulations in OPAL-RT environment with HYPERSIM software.**

***Index Terms*—Decentralized anomaly characterization, cyber-physical systems, cyber attacks, faults.**

I. Introduction

Modern power systems with power electronic devices, sensors, loads etc. in physical domain and communication links in cyber domain transforms it into a cyber-physical system [1]. The cooperative control provides a scalable and reliable information exchange platform, as compared to the centralized control, which are susceptible to single point failure and high bandwidth requirements [2]. The cooperative framework relies on the information exchanged between the local and the neighbouring distributed generators (DGs), making it a mild prospect for cyber-physical anomalies [3]. An anomaly can be termed as any abnormal behaviour, which can be an outcome of either fault, device/sensor failure or a cyber attack [4]. Physical faults can occur from grid faults such as, LG, LLG, LLLG, LL (where 'L' represents line and 'G' represents ground), damaging the equipments; affecting the reliability of a section or the whole system based on its type and location. The physical devices such as sensors are also vulnerable to faults and failures, which can affect the operation of the system. Cyber attack such as denial of service (DoS) or physical communication link failure, compromises availability ; whereas confidentiality and integrity are affected by false data injection attacks (FDIA), data packet loss [1]–[4]. The paper discusses the FDIA, where the adversary may initiate such attacks either on sensors, controllers or communication links disrupting the control action. These physical and cyber intrusions can propagate throughout the entire network through information exchanges and impact the performance and stability of the system. These anomalies mandate quick countermeasures in cyber-physical PEPS, which may affect the system performance, if not removed at the right instant. The schemes to detect such intrusions can be broadly classified into model-based and data-driven approaches. Although recent literature separately discusses the detection of physical [5], [6] and cyber [7], [8] anomalies, a convenient scheme to differentiate between these anomalies still need to be explored. This is because cyber attacks can be deliberately designed having characteristics similar to a physical fault, which might lead to operational failure if not detected correctly.

A few works in the field of cyber-physical anomaly

978-1-6654-3635-9/21/$31.00 ©2021 IEEE

detection have also been addressed by the researchers. An intelligent data-driven anomaly identification technique to classify faults, detect cyber attacks and localize them has been proposed in [9]. Although it eliminates complex mathematical modeling but may suffer from over-fitting and requires qualitative training data pertaining to several scenarios. In [10], a parametric time frequency logic framework has been presented, which does not require model information. It extracts the time-frequency content from training data to detect traces of anomaly in testing data. In [4], authors utilize the locally available frequency and average voltage trajectories of the inverters for a window of 100 ms to differentiate the cyber-physical anomalies. This could be a long time margin, since the faults need to be isolated in a much shorter time-frame. The typical operation time of a overcurrent relay (OCR) is 1 cycle [11] with coordination time interval (CTI) of 200 ms (includes circuit breaker opening time, safety factor for current transformer saturation and relay setting errors) to comply with IEEE Standard 242-2001 [12]. This necessitates stringent requirement in the characterization process in power electronic systems on faster detection of these anomalies, such that the decision can be quickly routed to the protection systems. To bridge this gap, this paper is focused on certifying the characterization of these anomalies with the help of empirical physics informed laws for each distributed generation (DG). These laws are then used to define certain regions on a X-Y plane, where Y-axis represent locally measured d-axis voltage and X-axis represent locally measured frequency. Hence, anomaly characterization is validated in an online manner if the trajectory in the aforementioned plane moves out of the defined regions within a time margin of 5 ms. This effort can be quite elementary in taking a coordinated decision with the protection system for grid faults. Moreover in case of other anomalies, the diagnosis can be directed towards the existing cyber security tool. Finally, the proposed technique successfully differentiates between the cyber and physical anomalies by classifying cyber attacks on voltage and frequency; bus/line faults and voltage sensor faults accurately.

The key advantages of this work can be summarized as:

- We design an online anomaly characterization with regions defined in f-V_d plane using local measurements, which makes the process decentralized. To the best of authors' knowledge, physics-informed decentralized anomaly characterization has never been proposed in the realm of power electronics security.
- The proposed scheme efficiently detects the anomaly in 5 ms (20 samples/cycle in a 50 Hz system), which can direct the decision either towards the protection systems (for faults) or the cybersecurity mitigation tool (for cyber attacks).
- We do not require deployment of additional sensors to characterize between anomalies. It is simple and scalable to different networked power electronic systems with the available sensors.

The remainder of the paper is organized as: a brief description of the problem is presented in the Section II. The proposed scheme is discussed in the Section III with the performance validation of the developed scheme is presented in the Section IV. Finally, the work is concluded in Section V .

II. Problem Formulation

We consider the modified CIGRE LV benchmark distribution system in islanded mode to validate our approach. The system with five inverter-interfaced DGs, apparent power 'S', power factor 'pf' of the loads and buses 'B' are shown in the Fig. 1. The physical layer of each DG comprises of power-electronic components (e.g, inverter), LC filter and output impedance. These DGs are connected to each other via line impedances and resistances. Further, for regulating power (active/reactive), voltage and frequency; more details for each DG with their corresponding control loops has been shown in Fig. 2.

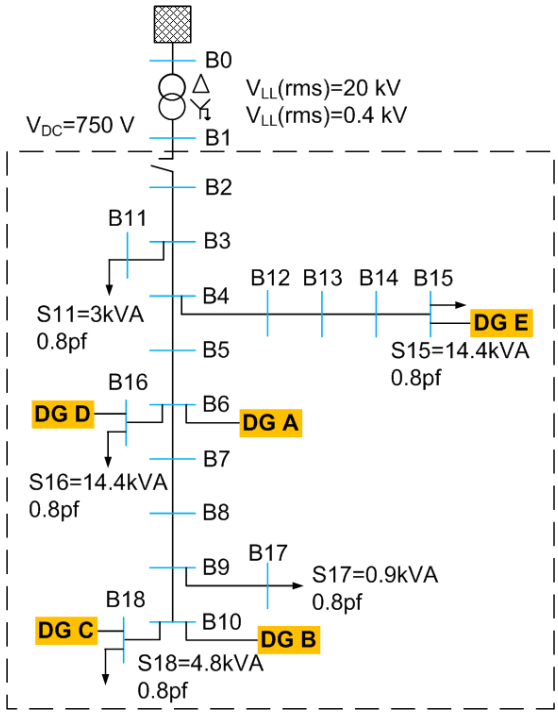


Fig. 1: Modified CIGRE LV distribution islanded network (in dashed section).

The primary controller is the part of physical domain which includes droop controller and faster inner control loops (voltage and current) [13]. Each primary controller receives the voltage (V^{abc}) and current (I^{abc}, I^{abc}_{inv}) information from its respective sensors to generate power, voltage and frequency accordingly. As primary controller itself is not sufficient to drive the system to zero steady state error, so in addition to primary controllers, each DG has secondary controllers (SC) which communicate to each other in cyber layer. These SCs on receiving power (active; P^i or reactive; Q^i), frequency f^i, voltage information locally; share them to their neighbouring SCs (j $\in$ N_i) as specified by the

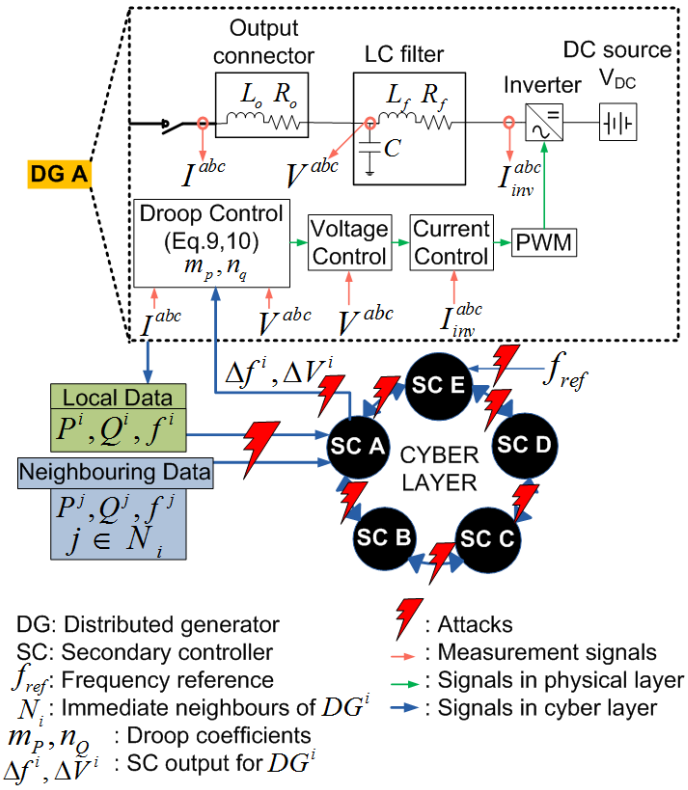


Fig. 2: Control loops for DG A.

communication graph in the cyber domain [3]. These SCs generate the frequency (and voltage) correction terms (Δf^i, ΔV^i) corresponding to each DG. In this work, we are considering a ring communication graph with unity edge weights (a_{ij}). The SCs (local controllers; LC) are responsible only for proportional active (and reactive) power sharing and frequency restoration. Further, the pinned DG (DG E) receives the reference signal (f_{ref}) from the master controller (MC).

The physical layer on one hand, may suffer from faults (buses or lines) and sensor (voltage or current) failure. The faults on buses (or lines) degrades the reliability of supply affecting the customers. Similarly, sensor faults will make the corresponding measurements unavailable to the changes in the system and would not be able to inform to the controllers to take the required control action. The sensor faults therefore would also lead to the unreliable operation of the system and may also lead to unstable operating conditions. The cyber layer on the other hand, comprising of the communication infrastructure are highly susceptible to attacks by the third-party adversaries. The consequences of various attack points shown in Fig. 2, are elaborated further.

- Master Controller (MC): Modification of reference values given by (1) will tend to drive the system to unstable operating points.

$$f^C_{ref} = f_{ref} + f^A_{ref} \tag{1}$$

- Local Controller (LC): These can have false data injection at any of the ends such as:
  - while receiving information: Assuming information vector received locally be $x^i(t)$=[$P^i(t)$, $Q^i(t)$, $f^i(t)$]. The attacker can modify these signals as:

$$x^{iC}(t) = x^i(t) + x^{iA}(t) \tag{2}$$

    These modified signals presented in (2) will tend to generate incorrect correction terms leading to unreliable voltage and frequency set points.
  - while sending correction signals: Assuming correction signals sent to the primary controller from its respective SC be expressed as, $y^i(t)$=[$\Delta f^i(t)$, $\Delta V^i(t)$]. The false data can be injected as:

$$y^{iC}(t) = y^i(t) + y^{iA}(t) \tag{3}$$

    These attacks will deliberately modify the correction terms, driving the system to undesired set points.
- Communication link (CL): Similar to assumption of information being shared for the secondary control objectives, the data communicated between the SCs can be expressed as x^j(t)=[$P^j(t)$, Q^j(t), f^j(t)]. The modified data by the attacker can be given as:

$$x^{jC}(t) = x^j(t) + x^{jA}(t) \tag{4}$$

These attacks will also generate the undesired correction terms to the primary controllers, which may lead to unstable operating conditions.

For simplicity, the time dependency is not explicitly shown in rest of the paper.

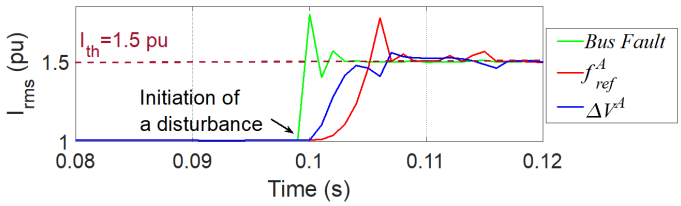


Fig. 3: Time-domain simulations at DG A for various disturbances.

This paper considers attack on MC with manipulated f_{ref} and attack on the voltage correction signals ΔV sent by LC. It is worth mentioning here that the attack surface for each DG is not limited to the above-mentioned scenarios. During faults, the relays with its corresponding protection schemes are responsible for isolating the faulted section from the healthy section to maintain the reliability of supply. On the contrary, for cyber attacks, the embedded mitigation algorithms on the controllers come into play. Also the third-party adversaries can deliberately design cyber attacks to have characteristics like that of a physical fault which will lead to operational failure if not detected correctly [14], [15]. As shown in Fig. 3, the rms value of output current reaches the threshold value of 1.5 pu for each disturbance i.e, bus faults, cyber attacks on f_{ref} and ΔV occurring at t = 0.1 s. This will cause the maloperation

of OCR. Therefore, to counteract the effect of such physical and cyber anomalies; as the actions taking by their respective devices are different making it crucial to identify the type of anomaly. The next section discusses the novel decentralized anomaly detection approach using local data of f and V_d.

III. Proposed Method

The following section elaborates the equations involved in the droop [13] and secondary controllers [3] as shown in Fig. 2. The instantaneous reactive and active power components q and p from the measured output voltage (V^{abc}) and current (I^{abc}) are expressed as (5), (6) respectively.

$$q = -v_d i_q + v_q i_d \tag{5}$$

$$p = v_d i_d + v_q i_q \tag{6}$$

These instantaneous power components when passed through low-pass filters (ω_c as the cut-off frequency), the reactive and real powers Q and P corresponding to the fundamental component is obtained as shown in (7) and (8) respectively.

$$Q = \left(\frac{\omega_c}{s+\omega_c}\right) q \tag{7}$$

$$P = \left(\frac{\omega_c}{s+\omega_c}\right) p \tag{8}$$

To share the reactive (or active) power droop is introduced in the voltage (or frequency) equation as expressed by (9) and (10) respectively. Here, superscript 'i' denotes the equations corresponding to DG^i. V^*, ω_{ref} are the nominal set point d-axis output voltage and reference frequency respectively. n_q and m_p stands for reactive and active power droop coefficients.

$$V^i_{dref} = V^* - n^i_q Q^i \tag{9}$$

$$\omega^i = \omega_{ref} - m^i_p . P^i \tag{10}$$

Further, the secondary correction terms corresponding to voltage (ΔV^i) and frequency ($\Delta\omega^i$) is added to above droop equations (9) and (10) to include the effect of both the droop and secondary controllers (SC) and obtain the final equations shown in (11) and (12).

$$V^i_{dref} = V^* - n^i_q Q^i + \Delta V^i \tag{11}$$

$$\omega^i = \omega_{ref} - m^i_p . P^i + \Delta\omega^i \tag{12}$$

The cooperative controller equations for voltage and frequency are defined by (13) and (14) respectively. The local data are represented by superscript 'i' and the neighbouring data to DG^i are represented by superscript 'j'. The edge weights (a_{ij}) are considered to be unity.

$$\dot{e}^i_v = -\sum_{j\in N_i} a_{ij}\left(n^i_q . Q^i - n^j_q . Q^j\right) \tag{13}$$

$$\dot{e}^i_\omega = -\sum_{j\in N_i} a_{ij}\left(m^i_p . P^i - m^j_p . P^j\right) - \sum_{j\in N_i} a_{ij}\left(\omega^i - \omega^j\right) - \sum_{j\in N_i} g_i\left(\omega^i - \omega_{ref}\right) \tag{14}$$

Further, $\dot{e}^i_v$ is fed into a PI controller defined as, G_v=$K^i_{pv} + K^i_{iv}/s$ in which s is the laplace operator to generate the voltage correction term (ΔV^i) as shown in (15).

$$\Delta V^i = K^i_{pv}\dot{e}^i_v + K^i_{iv} e^i_v \tag{15}$$

Similar analysis can be performed to obtain frequency correction term ($\Delta\omega^i$) as shown in (16).

$$\Delta\omega^i = K^i_{p\omega}\dot{e}^i_\omega + K^i_{i\omega} e^i_\omega \tag{16}$$

Neglecting inner control loop dynamics and substituting the above-mentioned equations in (11), (12), we get (17) for a system of n DGs. The equation for deviation in frequency ($\dot{\omega}$) is computed in a similar way and relation $f = \omega/(2.\pi)$ is used to obtain the equation for $\dot{f}$. This frequency deviation ($\dot{f}$) is divided by (17), to get (18) for i^{th} DG.

$$\begin{aligned}\left[\dot{\mathbf{V}}_d\right]_{nx1} = &-[\boldsymbol{\omega}_c]_{nxn}[\mathbf{V}_d]_{nx1} + \left[\dot{\mathbf{V}}^*\right]_{nx1} + [\boldsymbol{\omega}_c]_{nxn}[\mathbf{V}^*]_{nx1} - \\ &\left([\mathbf{I}]_{nxn} + [\mathbf{K}_{pv}]_{nxn}[\mathbf{L}_v]_{nxn}\right)[\mathbf{n}_q]_{nxn}[\boldsymbol{\omega}_c]_{nxn}[\mathbf{q}]_{nx1} + \\ &[\mathbf{K}_{iv}]_{nxn}[\dot{\mathbf{e}}_v]_{nx1} + [\mathbf{K}_{iv}]_{nxn}[\boldsymbol{\omega}_c]_{nxn}[\mathbf{e}_v]_{nx1}\end{aligned} \tag{17}$$

$$\frac{\dot{V}^i_d}{\dot{f}^i} = \frac{[2\Pi]\left[1 + K^i_{p\omega}\sum_{j\in N_i} a_{ij} + K^i_{p\omega}\sum_{j\in N_i} g_i\right]\begin{bmatrix}\dot{V}^* + \omega_c V^* - \omega_c n^i_q . q^i - \omega_c K^i_{pv}\left(\sum_{j\in N_i} a_{ij}\left(n^i_q . q^i - n^j_q . q^j\right)\right) + \\ K^i_{iv}\dot{e}^i_v + \omega_c K^i_{iv} e^i_v - \omega_c V^i_d\end{bmatrix}}{\begin{bmatrix}\left(1 + K^i_{p\omega}\sum_{j\in N_i} g_i\right)\dot{\omega}_{ref} + \omega_c\left(1 + K^i_{p\omega}\sum_{j\in N_i} g_i\right)\omega_{ref} - \omega_c\left(1 + K^i_{p\omega}\sum_{j\in N_i} a_{ij}\right)m^i_p . p^i + \\ \omega_c K^i_{p\omega}\sum_{j\in N_i} a_{ij}\left(m^j_p . p^j\right) + K^i_{i\omega}\dot{e}^i_\omega + \omega_c K^i_{i\omega} e^i_\omega + K^i_{p\omega}\sum_{j\in N_i} a_{ij}\left(\dot{\omega}^j\right) - \\ \omega_c\left(1 + K^i_{p\omega}\sum_{j\in N_i} a_{ij} + K^i_{p\omega}\sum_{j\in N_i} g_i\right)\omega^i + \omega_c K^i_{p\omega}\sum_{j\in N_i} a_{ij}\left(\omega^j\right)\end{bmatrix}} \tag{18}$$

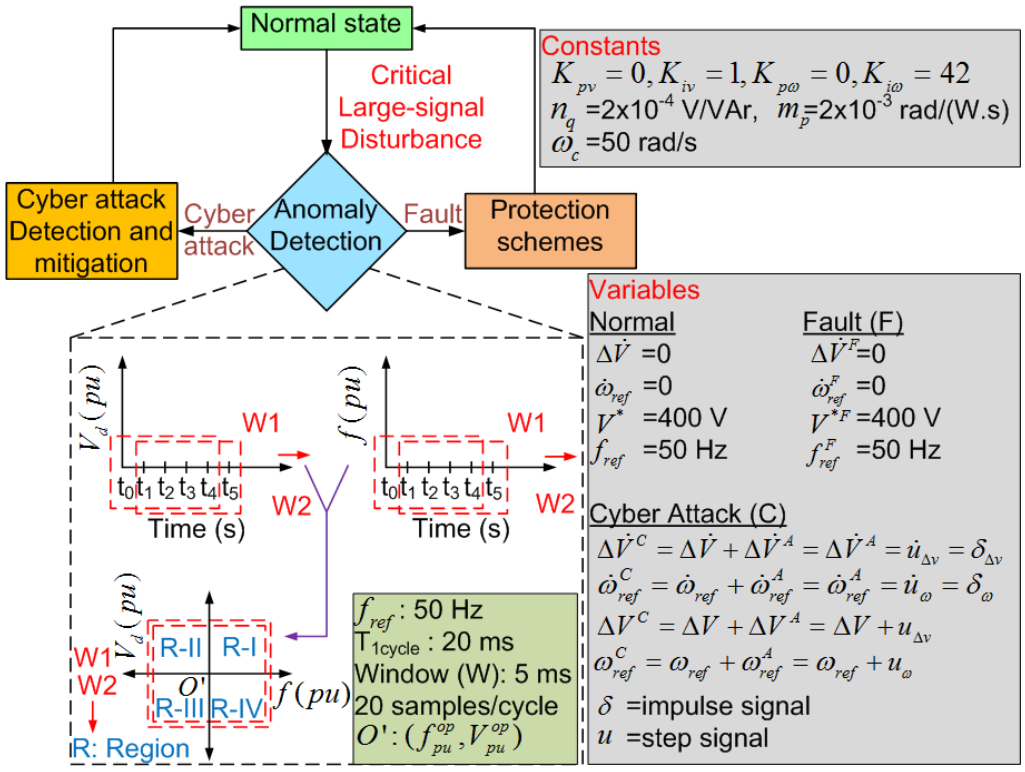


Fig. 4: Proposed decentralized anomaly characterization scheme.

The voltage and frequency parameters being controlled from secondary control layer (prone to cyber attack due the integration of information and communication framework), hence their deviations with respect to each other expressed by (18) forms the basis to analyze the prevailing cyber-physical situation. The significance of anomaly detection is presented in Fig. 4, where on arrival of any critical large-signal disturbance, it distinguishes the anomalies to follow the corresponding mitigation strategy [16], [17], restoring the system back to its normal state. Figure 4 shows for a given DG (f_{ref}=50 Hz), the detection scheme investigates the trajectory of f(pu) versus V_d(pu) with a moving window of 5 ms (20 samples/cycle) to have a selective and fast decision such that the protection system remains unaltered. The origin (O') is at (f^{op}_{pu}, V^{op}_{pu}), representing the operating frequency (pu) and voltage (pu) of a DG. The frequency being the global parameter, holds the relation f^{op}=f_{ref} (=1 pu) in normal state, whereas voltages at the buses being a local parameter does not exactly coincides with V^*. From (18) and conditions as mentioned in Fig. 4 for different cases, the trajectories would move in different regions aiding to recognize the event. In case of faults (buses/lines/voltage sensors), the trajectory would traverse in regions R-III and R-IV. In case of voltage sensor faults, the trajectory would settle down to zero voltage value. Similarly, with the cyber event, the initial traversal would be in the regions R-I and R-II due to the secondary control action. This trajectory plot therefore would analyze the present situation of the system and act accordingly to maintain the reliability and stability of the system.

IV. Result and Discussion

To evaluate the performance of the proposed scheme, modified CIGRE LV distribution benchmark system with fixed DC source (V_{DC} = 700 V) (Fig. 1) is simulated in real-time in OP-5700 with HYPERSIM software. The system is operating at a nominal voltage (V^*) of 400 V and reference frequency (f_{ref}) of 50 Hz. The details of the testbed [3] as shown in Fig. 5 with the parameters of the system, DG are mentioned in [12], [18].

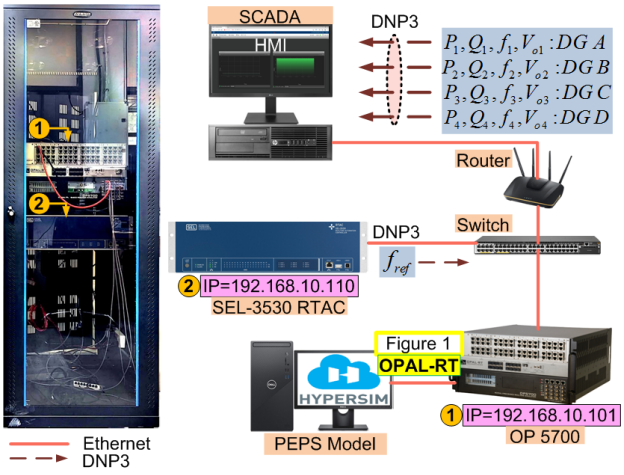
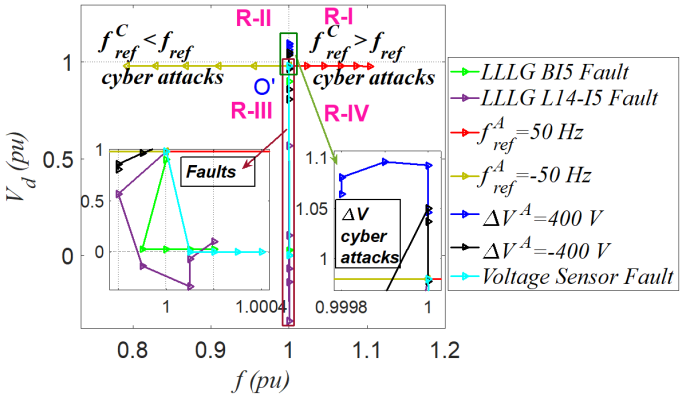
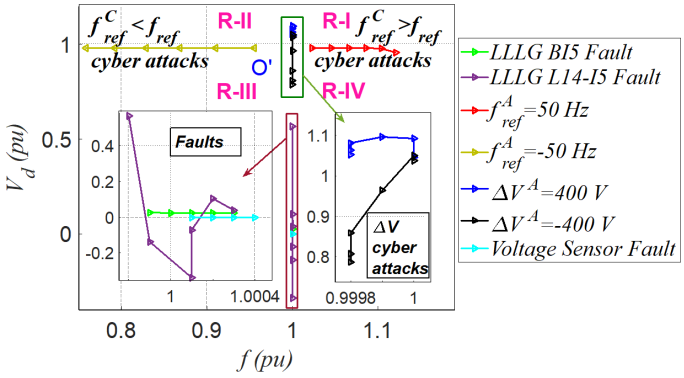


Fig. 5: Testbed setup [3].

The response of this cyber-physical PEPS is illustrated in Fig. 6 for a 5 ms window. The origin is represented by O'



(a)



(b)

Fig. 6: Trajectory in CIGRE LV distribution system for **(a)** first window (W1) and **(b)** second window (W2).

denoting the operating frequency and voltage as (1 pu, 0.9 pu) respectively. Using (18) with the variables as mentioned in Fig. 4 for various scenarios of fault and cyber attacks different trajectories can be obtained. The RT simulation in Fig. 6 shows that positive and negative frequency-based cyber attacks cause the movement of trajectories along right and left sides of f-axis respectively. The unique feature observed is that the transient voltage initially moves into the regions (R-I) or (R-II) under cyber attacks on voltage signals, (ascribed to the response of distributed secondary control algorithm) whereas they traverse along R-III and R-IV in case of physical faults (attributed to the response of primary control resulting in decrease in voltage). The time-scale separation between the primary and secondary controllers differs by considerably large values (say 10 times or more) hence can aid in differentiating the cyber-physical anomalies to prevent the false tripping of relays. Moreover, a remarkable observation is that for phase faults on bus or in between lines, the movement trajectories are observed in R-III and R-IV whereas for voltage sensor faults, the trajectory settles down to a voltage of 0 pu and continues to be there with the passage of time.

V. Conclusions and Future Work

The real-time simulation results verify the effectiveness of the proposed scheme, identifying the cyber and physical anomalies separately within 5 ms (considering a practical case of 20 samples/cycle) assisted by local f and V_d measurements making it simple and scalable to different networked power electronic systems without any additional resource. The future work would be to incorporate detection of the stealthy attacks.

References

[1] S. K. Mazumder et al., "A Review of Current Research Trends in Power-Electronic Innovations in Cyber-Physical Systems," in *IEEE Journal of Emerging and Selected Topics in Power Electronics*, doi: 10.1109/JESTPE.2021.3051876.

[2] Q. Shafiee, J. M. Guerrero and J. C. Vasquez, "Distributed Secondary Control for Islanded Microgrids—A Novel Approach," in *IEEE Transactions on Power Electronics*, vol. 29, no. 2, pp. 1018-1031, Feb. 2014, doi: 10.1109/TPEL.2013.2259506.

[3] K. Gupta, S. Sahoo, B. K. Panigrahi, F. Blaabjerg, and P. Popovski, "On the Assessment of Cyber Risks and Attack Surfaces in a Real-Time Co-Simulation Cybersecurity Testbed for Inverter-Based Microgrids," *Energies*, vol. 14, no. 16, p. 4941, 2021. [Online]. Available: https://www.mdpi.com/1996-1073/14/16/4941.

[4] S. Sahoo, Y. Yang and F. Blaabjerg, "Resilient Synchronization Strategy for AC Microgrids Under Cyber Attacks," in *IEEE Transactions on Power Electronics*, vol. 36, no. 1, pp. 73-77, Jan. 2021, doi: 10.1109/TPEL.2020.3005208.

[5] E. Casagrande, W. L. Woon, H. H. Zeineldin and D. Svetinovic, "A Differential Sequence Component Protection Scheme for Microgrids With Inverter-Based Distributed Generators," in *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 29-37, Jan. 2014, doi: 10.1109/TSG.2013.2251017.

[6] S. C. Paiva, R. L. de Araujo Ribeiro, D. K. Alves, F. B. Costa, and T. d. O. A. Rocha, "A wavelet-based hybrid islanding detection system applied for distributed generators interconnected to AC microgrids," *International Journal of Electrical Power & Energy Systems*, vol. 121, p. 106032, 2020.

[7] W. Ao, Y. Song, and C. Wen, "Adaptive cyber-physical system attack detection and reconstruction with application to power systems," *IET Control Theory & Applications*, vol. 10, no. 12, pp. 1458-1468, 2016.

[8] Z. Pang, G. Liu, D. Zhou, F. Hou and D. Sun, "Two-Channel False Data Injection Attacks Against Output Tracking Control of Networked Systems," in *IEEE Transactions on Industrial Electronics*, vol. 63, no. 5, pp. 3242-3251, May 2016, doi: 10.1109/TIE.2016.2535119.

[9] A. A. Khan, O. A. Beg, M. Alamaniotis, and S. Ahmed, "Intelligent anomaly identification in cyber-physical inverter-based systems," *Electric Power Systems Research*, vol. 193, p. 107024, 2021.

[10] O. A. Beg, L. V. Nguyen, T. T. Johnson and A. Davoudi, "Cyber-Physical Anomaly Detection in Microgrids Using Time-Frequency Logic Formalism," in *IEEE Access*, vol. 9, pp. 20012-20021, 2021, doi: 10.1109/ACCESS.2021.3055229.

[11] J. L. Blackburn and T. J. Domin, Protective relaying: principles and applications. CRC press, 2006.

[12] I. 242-2001, "IEEE recommended practice for protection and coordination of industrial and commercial power systems," 2001.

[13] N. Pogaku, M. Prodanovic and T. C. Green, "Modeling, Analysis and Testing of Autonomous Operation of an Inverter-Based Microgrid," in *IEEE Transactions on Power Electronics*, vol. 22, no. 2, pp. 613-625, March 2007, doi: 10.1109/TPEL.2006.890003.

[14] A. Afshari, M. Karrari, H. R. Baghaee and G. B. Gharehpetian, "Resilient Synchronization of Voltage/Frequency in AC Microgrids Under Deception Attacks," in *IEEE Systems Journal*, vol. 15, no. 2, pp. 2125-2136, June 2021, doi: 10.1109/JSYST.2020.2992309.

[15] S. Sahoo, J. C. Peng, A. Devakumar, S. Mishra and T. Dragičević, "On Detection of False Data in Cooperative DC Microgrids—A Discordant Element Approach," in *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562-6571, Aug. 2020, doi: 10.1109/TIE.2019.2938497.

[16] R. Mohanty, S. Sahoo, A. K. Pradhan and F. Blaabjerg, "A Cosine Similarity Based Centralized Protection Scheme for DC Microgrids," in *IEEE Journal of Emerging and Selected Topics in Power Electronics*, doi: 10.1109/JESTPE.2021.3060587.

[17] S. Sahoo, T. Dragičević and F. Blaabjerg, "An Event-Driven Resilient Control Strategy for DC Microgrids," in *IEEE Transactions on Power Electronics*, vol. 35, no. 12, pp. 13714-13724, Dec. 2020, doi: 10.1109/TPEL.2020.2995584.

[18] S. Barsali, Benchmark systems for network integration of renewable and distributed energy resources, 2014.