Real-Time Intrusion Detection System for Virtual Power Plants

Journal:	*IEEE Transactions on Smart Grid*
Manuscript ID	TSG-00457-2021
Manuscript Type:	Transactions
Date Submitted by the Author:	24-Mar-2021
Complete List of Authors:	Khan, Ahmad; University of Illinois at Chicago, Department of Electrical & Computer Engineering Shadmand, Mohammad; University of Illinois at Chicago, Department of Electrical & Computer Engineering Mazumder, Sudip; University of Illinois, Chicago, Electrical and Computer Engineering
Technical Topic Area :	Cyber-physical and cybersecurity power grid applications
Key Words:	Inverters, cybersecurity, Photovoltaic systems, Intrusion detection

Real-Time Intrusion Detection System for Virtual Power Plants

Ahmad Khan, *Student Member*, *IEEE*, Mohammad B. Shadmand, *Senior Member*, *IEEE*, Sudip K. Mazumder, *Fellow*, *IEEE*

***Abstract*—This work develops an intrusion detection system (IDS) for virtual power plants (VPP) based on a real-time safe operation regions identification of dispersed energy generators (DEGs). The identified operation regions are utilized as a rapid sanity authentication strategy to spot malicious active and reactive power (PQ) set-points for DEGs at the grid-edge. These malicious PQ set-points are induced by a stealthy cyber intruder manipulating the VPP secondary control layer that generates optimal PQ set-points for DEGs. This is critical, since behind the meter DEGs are unobservable from perspective of the upstream network operators and vice versa, which results in an immense attack surface. The proposed IDS concept is constructed on authenticating a main theorem and its converse theorem. The developed main theorem states that in the safe operation region of the network, all PQ operation set-points are morphismed to unique real valued local PCC bus voltages. While the converse theorem states that all local PCC bus voltages are morphismed to unique real valued operation set-points. Hence, the detection of a nonisomorphism pair of the main theorem and the converse theorem concludes unstable network operation induced by malicious operation set-points breached in the secondary control layer. Once an intrusion is detected, the DEG moves to local primary control mode based on PCC condition and disregards the VPP secondary control layer malicious PQ set-points assignment until further diagnosis by the VPP/utility owner. The theoretical analysis is verified by several case studies for a VPP with multiple DEGs.**

***Index Terms*—virtual power plant, real-time operation regions identifications, intrusion detection system**

I. Introduction

The futuristic energy paradigm will involve high penetration of renewable based generation at the grid edge through embracing dispersed energy generators (DEGs) [1]. At the grid edge, grid-feeding inverters are anticipated to be the prevailing type of DEGs. In such mode, the DEGs are following the inertial response of the network and their capabilities are limited to injecting current into their local point of common coupling (PCC) without considering upstream network constrains and requirements [2]. Thereby, these DEGs are usually unobservable to the upstream network and vice versa. Hence, real-time system level coordination and management is crucial to ensure the optimal utilization of unobservable DEGs that are potentially installed behind the meters [3].

The virtual power plant (VPP) is demonstrating to be an effective paradigm that will facilitate DEGs efficient integration with the power grid. The VPP is defined as a cluster of different scale DEGs that are aggregated into a single consortium. The VPP serve as an interface between transmission and distribution system operators [4]. VPP concept introduction runs superior observability and controllability on DEGs and permits optimal utilization of inverters based generation features. Multiple VPP implementations exist around the world such as the European VPPs reported in [5] and [6]. Moreover, VPPs are classified into two types (i) technical VPP (TVPP) and (ii) commercial VPP (CVPP). The TVPP is considering aggregation of its different DEGs based on technical requirements such as topology, stability, and capacity of both the aggregated DEGs and the network. On the contrary, CVPP is concerned only about profit and active market participation of the aggregated DEGs. Therefore, majority of CVPP studies typically are associated to economic such as bidding methodologies [7, 8], minimum cost operation [9, 10], and optimal day-ahead scheduling [11].

The futuristic power grid is anticipated to be vulnerable to malicious cyber-attacks. This is because more dispersed generation and control devices will operate outside the utility's traditional power-plant administrative domain by employing more DEGs at the grid edge [12]. The attack may be introduced into the VPP infrastructure through the communication medium that enables its harmonious operation. Security breach in the cyber layer of a VPP has a direct influence on its physical layer, which disrupts its nominal operation. A severe cyber-attack typically spreads throughout the grid gradually (i.e., known as the stealthy-attack [13]) to make detection of such an attack extremely difficult at early stages using conventional protection schemes and intrusion-detection mechanisms.

This work is enhancing cybersecurity of the TVPP illustrated in Fig. 1 through preventing malicious operation PQ set-points induced by a stealthy intruder breaching into the slow time scale secondary control layer. The cybersecurity enhancement groundwork is based on a proposed real-time safe operation region identification framework for network of DEGs in TVPP domain. This real-time operation region identification framework is based on the intersection region of all the PCC buses multi-dimensional manifolds' projection on the operational PQ set-points domain. In more details, each local PCC bus is described as multi-dimensional manifold where all the network PQ set-points are considered as the independent domain variables that are constructing the feasible PCC bus voltage range. Additionally, this work exemplifies a correction so the Thévenin analysis obtained with superposition theory is applicable to multi-inverter network. This methodology avoids the necessity of running load flow algorithm multiple times for understanding the TVPP buses safe operational limits. Then, using these multi-dimensional manifold three operation regions are identified for each local PCC bus in the TVPP as the following: (i) safe operation region (SOR), (ii) stable/normal operation region (SNOR), and (iii) unstable operation region (UOR). These operation regions are utilized as a rapid sanity authentication strategy to spot a stealthy intruder that is manipulating the VPP secondary control layer generated PQ

Ahmad Khan, Mohammad B. Shadmand, and Sudip K. Mazumder are with the Department of Electrical and Computer Engineering at University of Illinois at Chicago (e-mail: ahmad20@uic.edu, shadmand@uic.edu, mazumder@uic.edu).

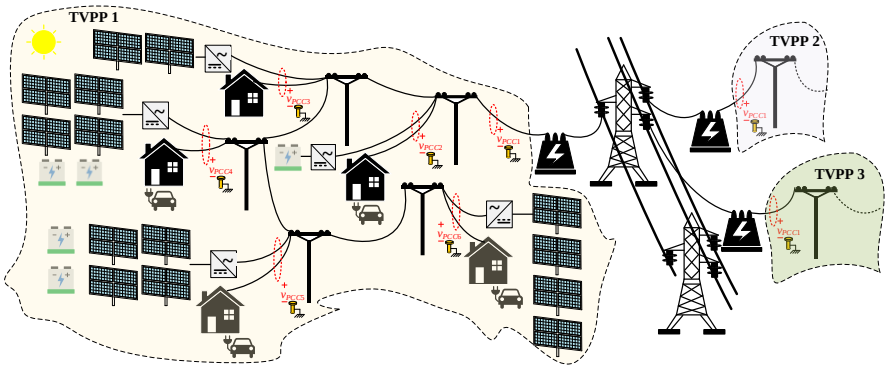
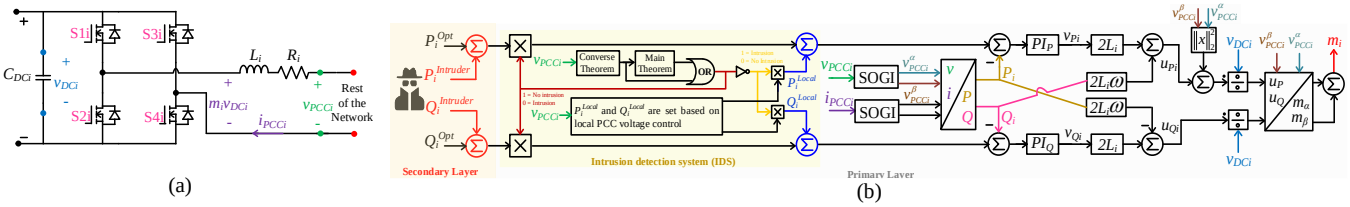


Fig. 1. TVPP concept extended to the grid edge with unobservable single-phase DEGs in grid-feeding mode of operation.



(a) (b)

Fig. 2. Grid-feeding primary control layer considered for DEGs in the TVPP: (a) inverter structure and (b) controller structure with measurements, nonlinear coordinate the transformation illustration, and the intrusion detection system.

set-points for DEGs. Thus, facilitating a real-time linkage between unobservable DEGs and the upstream network. The proposed intrusion detection system (IDS) is initiated after anomalous local PCC bus voltage measurement is detected (i.e., failure to authenticate the converse theorem). Particularly, after the anomaly, the PQ set-points passing from the slow time scale secondary control layer to the primary control layer are authenticated with the proposed real-time operation regions to decide whether the anomalous local PCC bus voltage is a resultant of an stealthy intruder breach or not once a nonisomorphism behavior is detected (i.e., failure to authenticate the developed main theorem).

In the literature, the capability of synchronous generator is estimated through the concept of capability chart. This chart provides the range of dispatchable PQ set-points without jeopardizing the stability of the synchronous generator [14]. The notion of capability chart was first time exploited for TVPP application in [15]. The TVPP capability chart was used as conventional generators capability charts that are employed in scheduling and dispatching optimization. In other words, set-points that belong to the TVPP capability chart are guaranteed to be executable when requested by the upstream network. Though, the capability charts for TVPP are more complex compared to conventional generators. This is because TVPP capability charts are representing aggregation of various DEGs. An example of such capability charts is used to estimate the reactive power injection capability of the TVPP at different active power levels in [16]. Another work is suggesting a methodology for approximating capability chart numerically using repeated time domain simulations in [17]. In general, the capability chart is obtained by repeated load flow solutions for various different scenarios that often are selected randomly. After that, the realistic load flow solutions consequence to points that are constructing the capability chart. Another approaches that are reported in the literature for approximating the capability charts are employing geometrical hypothesis such as polyhedron, ellipse, and so on [18]. Furthermore, capability charts estimation with incorporation of randomness is reported in [19]. Yet, these methods extensively rely on repetitive load flow solutions that needs to be executed in secondary or tertiary control layers, which even turns out to be challenging to utilize fast load flow algorithms due to the dominate resistive nature for the distribution network [20]. Furthermore, the considered potential attack model, in which the intruder is compromising the secondary layer controller and existing load flow algorithms, mandates another sanity checkpoint at the primary layer (i.e. grid edge) for realizing an effective and fast IDS. Hence, to our knowledge, utilizing the existing capability charts for rapid cybersecurity enhancement or intrusion detection against operational PQ set-points manipulation and breaches is not viable in real-time. The major contributions of this paper is summarized in the following bullet points:

- A real-time mechanism for understanding the operation limits/regions of a TVPP with unobservable DEGs without relying on repeated load flow solution at secondary/tertiary control layers for estimating the capability of the TVPP, thus creating a framework for real-time decisions making.
- Proactive intrusion detection for TVPP by utilizing the real-time identified operation regions as a sanity checkpoint for PQ set-points assignments by potentially compromised secondary control layer; thus, detecting and preventing a stealthy cyber intruder that is requesting malicious set-points from the DEGs in a timely manner.

The remainder of the paper is structured as follows: Section II is the illustration of the single-phase TVPP network considered. Section III is real-time operation region identification framework derivation which construct the main theorem. Section IV summarizes steps to utilize the developed main theorem with its converse theorem for intrusion detection.

Section V discusses the results. Finally, section VI concludes the paper.

II. TVPP Network Understudy

The TVPP$_1$ network understudy is portrayed in Fig.1. In this TVPP, the main PCC bus voltage is the potential difference between the low side positive terminal of the distribution pole transformer and the ground conductor (see v_{PCC1} in Fig. 1). Similarly, the internal local PCC buses are considered as each node that consumers at the grid edge are feeding their local loads (see v_{PCC2}, v_{PCC3}, …, v_{PCC_n} in Fig. 1). In addition, DEGs are installed at internal local PCC buses. The grid-feeding inverter primary control layer considered in this work for DEGs is depicted in Fig. 2. The open loop system is represented by the multiple input multiple output (MIMO) linear time invariant (LTI) state space in (1).

$$\begin{bmatrix} \frac{dP_i}{dt} \\ \frac{dQ_i}{dt} \end{bmatrix} = \begin{bmatrix} -R_i L_i^{-1} & -\omega \\ \omega & -R_i L_i^{-1} \end{bmatrix} \begin{bmatrix} P_i \\ Q_i \end{bmatrix} + \begin{bmatrix} 0.5L_i^{-1} & 0 \\ 0 & 0.5L_i^{-1} \end{bmatrix} \begin{bmatrix} u_{Pi} \\ u_{Qi} \end{bmatrix}$$

$$u_{Pi} = m_{\alpha i} v_{DCi} v_{PCCi}^{\alpha} + m_{\beta i} v_{DCi} v_{PCCi}^{\beta} - \left\| v_{PCCi} \right\|_2^2$$

$$u_{Qi} = m_{\alpha i} v_{DCi} v_{PCCi}^{\beta} - m_{\beta i} v_{DCi} v_{PCCi}^{\alpha}$$

$$\left\| v_{PCCi} \right\|_2 = \sqrt{{v_{PCCi}^{\alpha}}^2 + {v_{PCCi}^{\beta}}^2} \qquad (1)$$

$$e_{Pi} = P_{Refi} - P_i \ , \ v_{Pi} = e_{Pi} K_{Ppi} + K_{Pii} \int e_{Pi}(\tau) d\tau$$

$$e_{Qi} = Q_{Refi} - Q_i \ , \ v_{Qi} = e_{Qi} K_{Qpi} + K_{Qii} \int e_{Qi}(\tau) d\tau$$

$$\frac{d^2 e_{Pi}}{dt^2} = -\left(K_{Ppi} + R_i L_i^{-1}\right) \frac{de_{Pi}}{dt} - K_{Pii} e_{Pi}$$

$$\frac{d^2 e_{Qi}}{dt^2} = -\left(K_{Qpi} + R_i L_i^{-1}\right) \frac{de_{Qi}}{dt} - K_{Qii} e_{Qi}$$

This control is guaranteeing that primary control layer stability in the TVPP$_1$. As this control does not suffer from synchronization associated instabilities, harmonics resonance instability, and avoids interaction instabilities that might originate from improper control bandwidth selections for inner and outer control loops. The proof for the stability of the closed loop primary control layer equilibrium is detailed in Appendix A with linear quadratic Lyapunov stability theorem. Also, Appendix B details potential instabilities that might originate from a cyber-attacker at the VPP secondary control layer manipulating PQ set-points.

III. Real-Time Operation Regions Derivations and Intursion Scenario

A. Stealthy Intrusion and Malicious PQ Set-Points Impact

Consider the circuit exemplification in Fig. 3 of the TVPP$_1$ understudy shown in Fig. 1, if a stealthy cyber intruder is targeting the i^{th} local PCC bus in Fig. 3 and manipulates the operation PQ set-points that are passing from the secondary control layer to the primary control layer of the DEG. This intruder does not have access to the information related to network topology or nearby DEGs. Therefore, from the intruder perspective, he is altering the operation set-points and observing the local measurement to understand the impact of his set-points manipulation. Given this lack of information by the intruder, the intruder could initiate catastrophic effect by

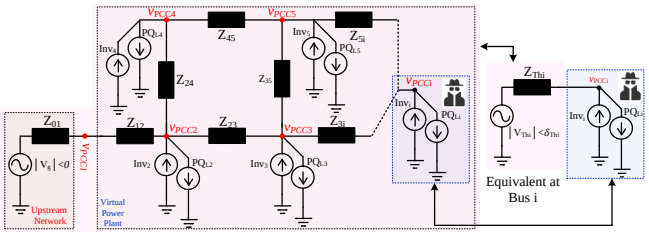


Fig. 3. TVPP general network, illustrating the i^{th} local PCC terminals equivalent circuit.

pushing the targeted PCC bus to operate outside its stable set-points domain by slowly and randomly changing the PQ set-points. Therefore, the hypothesis in this paper is that the primary control layer will be equipped with the operation regions identification in real-time, as a sub-layer in primary. Then, if the DEG is pushed to operate in the UOR by the VPP secondary control layer manipulated PQ set-points, the primary control layer considers that the set-points passing from the VPP secondary control layer are compromised as this will results in nonisomorphism behavior. The basis of the proposed IDS is when anomalous local PCC bus voltage is observed, the converse theorem is authenticated (i.e., the morphism $f: \|\vec{v}_{PCCi}\|_2 \rightarrow \langle P_{PCC1}, Q_{PCC1}, \ldots, P_{PCCN}, Q_{PCCN} \rangle, \mathbb{R} \rightarrow \mathbb{R}^{2N}$). Then, the proposed real-time operation regions are utilized to authenticate the developed main theorem (i.e., the morphism $g: \langle P_{PCC1}, Q_{PCC1}, \ldots, P_{PCCN}, Q_{PCCN} \rangle \rightarrow \|\vec{v}_{PCCi}\|_2, \mathbb{R}^{2N} \rightarrow \mathbb{R}$). If $f \neq g^{-1}$, f and g are nonisomorphism pair and the network is operating in UOR due to inconsistence between the converse theorem and the developed main theorem. After that, the PQ set-points passing from the compromised secondary control layer are disregarded and the grid-feeding inverters are changing their set-points and monitor when the local PCC bus voltage is regaining safe operation.

B. Real-Time Operation Regions Identification and Main Theorem Construction

To understand how the TVPP network stability is impacted by grid-feeding inverters' set-points variations; in this subsection, an illustration of how a single grid-feeding inverter (i.e., representing an unobservable DEG at the grid edge) impacts its local PCC voltage in a general single-phase network is carried out. In this situation, the network is reduced to two buses where the i^{th} targeted grid-feeding inverter sees the rest of the network from its local PCC terminals as a large synchronous impedance (i.e., Thevenin impedance) in series connection with a Thevenin voltage source (see Fig. 3). This Thevenin voltage source ($\vec{v}_{Thi}$) is a function of the rest of the network PQ set-points. Here load flow solutions are not used to estimate the Thevenin voltage. Then, the relation between the Thevenin voltage ($\vec{v}_{Thi}$) and the local PCC voltage for the i^{th} grid-feeding inverter ($\vec{v}_{PCCi}$) is given by,

$$\vec{v}_{PCCi} = \left(R_{Thi} + j\omega L_{Thi}\right) \vec{i}_{PCCi} + \vec{v}_{Thi} \qquad (2)$$

where R_{Thi} is the Thevenin resistance seen by the i^{th} grid-feeding inverter from its local PCC terminals to the main TVPP PCC bus terminal, L_{Thi} is the Thevenin inductance seen by the i^{th} grid-feeding inverter from its local PCC terminals to the main TVPP PCC bus terminals, ω is the nominal angular

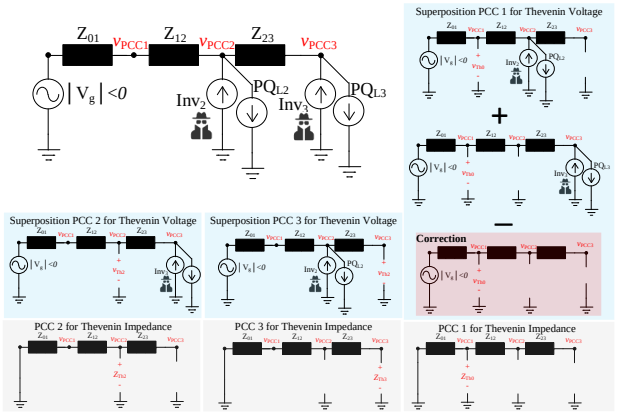


Fig. 4. Four bus single-phase TVPP considered for illustrating the operation regions graphically in scenario I.

frequency of the network, and $\vec{i}_{PCCi}$ is the phasor of the current injected by the i^{th} grid-feeding inverter into its local PCC terminals. Furthermore, in equation (2) the phasor of the local PCC voltage is as (3).

$$\vec{v}_{PCCi} = \|V_{PCCi}\|_2 \angle\delta_{PCCi} = A_i + jB_i \tag{3}$$

Similarly, phasor of the Thevenin voltage is given by,

$$\vec{v}_{Thi} = \|V_{Thi}\|_2 \angle\delta_{Thi} = \|V_{Thi}\|_2 \cos(\delta_{Thi}) + j\|V_{Thi}\|_2 \sin(\delta_{Thi}) \tag{4}$$

To relate the local PCC voltage ($\vec{v}_{PCCi}$) to the commanded PQ set-points of the i^{th} targeted grid-feeding inverter; the local PCC current ($\vec{i}_{PCCi}$) can be written as (5).

$$\begin{aligned}\vec{i}_{PCCi} &= \left(\left(P_i^{Ref} - P_{Li}\right) - j\left(Q_i^{Ref} - Q_{Li}\right)\right)\vec{v}_{PCCi}^{*\,-1} \\ &= \left(P_{PCCi} - jQ_{PCCi}\right)\vec{v}_{PCCi}^{*\,-1}\end{aligned} \tag{5}$$

Where $\vec{v}^*_{PCCi}$ is the complex conjugate of $\vec{v}_{PCCi}$, P_i^{Ref} is the commanded active power reference by the i^{th} targeted grid-feeding inverter, Q_i^{Ref} is the commanded reactive power reference i^{th} targeted grid-feeding inverter, P_{Li} is the active power load at the i^{th} targeted local PCC bus, Q_{Li} is the reactive power load at the i^{th} targeted local PCC bus, P_{PCCi} is the net injected active power at the i^{th} targeted local PCC bus, and Q_{PCCi} is the net injected reactive power at the i^{th} targeted local PCC. Combining the (5) and (2) results in (6).

$$\vec{v}_{PCCi} = \left(R_{Thi} + j\omega L_{Thi}\right)\left(P_{PCCi} - jQ_{PCCi}\right)\vec{v}_{PCCi}^{*\,-1} + \vec{v}_{Thi} \tag{6}$$

Then, multiplying (6) by the complex conjugate of $\vec{v}_{PCCi}$ results in (7).

$$\vec{v}_{PCCi}\vec{v}^*_{PCCi} = \left(R_{Thi} + j\omega L_{Thi}\right)\left(P_{PCCi} - jQ_{PCCi}\right) + \vec{v}_{Thi}\vec{v}^*_{PCCi} \tag{7}$$

The key point from reaching to (7) is that the left hand side (LHS) is all real valued terms. In other words, the imaginary part is zero. This is an obvious resultant form multiplication of the local PCC phasor voltage by its complex conjugate. Thereby, (7) can be rewritten as (8).

$$\begin{aligned}&A_i^2 + B_i^2 = R_{Thi}P_{PCCi} + \omega L_{Thi}Q_{PCCi} + \\ &\|V_{Thi}\|_2\left(A_i\cos(\delta_{Thi}) + B_i\sin(\delta_{Thi})\right) \\ &+ j\left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi} + \|V_{Thi}\|_2\left(A_i\sin(\delta_{Thi}) - B_i\cos(\delta_{Thi})\right)\right)\end{aligned} \tag{8}$$

Then, by equating the real parts of the LHS and right hand side (RHS) of (8); (9) is deduced.

$$\begin{aligned}A_i^2 + B_i^2 &= R_{Thi}P_{PCCi} + \omega L_{Thi}Q_{PCCi} + A_i\|V_{Thi}\|_2\cos(\delta_{Thi}) \\ &+ B_i\|V_{Thi}\|_2\sin(\delta_{Thi})\end{aligned} \tag{9}$$

Similarly, by equating the imaginary parts of the LHS and RHS of (8); (10) is obtained.

$$0 = \omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi} + A_i\|V_{Thi}\|_2\sin(\delta_{Thi}) - B_i\|V_{Thi}\|_2\cos(\delta_{Thi}) \tag{10}$$

Now, from (9) and (10) a solution of A_i and B_i parameters can be determined. Recall that these parameters construct the real and the imaginary component of the i^{th} targeted local PCC voltage given previously by (3). B_i is written in term of A_i from (10) as expressed in (11).

$$B_i = \left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\sec(\delta_{Thi}) + A_i\tan(\delta_{Thi}) \tag{11}$$

For finding a solution for A_i; from combining (11) and (9) this parametric quadratic equation expressed in (12) can be solved.

$$\begin{aligned}&A_i^2 - A_i\left(2\left(R_{Thi}Q_{PCCi} - \omega L_{Thi}P_{PCCi}\right)\|V_{Thi}\|_2^{-1}\sin(\delta_{Thi}) + \|V_{Thi}\|_2\cos(\delta_{Thi})\right) \\ &+\left(\left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\right)^2 - \left(R_{Thi}P_{PCCi} + \omega L_{Thi}Q_{PCCi}\right)\cos^2(\delta_{Thi}) \\ &-\left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi}\right)\cos(\delta_{Thi})\sin(\delta_{Thi}) = 0 \\ &\text{where}\quad a = 1, \\ &b = -\left(2\left(R_{Thi}Q_{PCCi} - \omega L_{Thi}P_{PCCi}\right)\|V_{Thi}\|_2^{-1}\sin(\delta_{Thi}) + \|V_{Thi}\|_2\cos(\delta_{Thi})\right) \\ &, c = \left(\left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\right)^2 \\ &-\left(R_{Thi}P_{PCCi} + \omega L_{Thi}Q_{PCCi}\right)\cos^2(\delta_{Thi}) \\ &-\left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi}\right)\cos(\delta_{Thi})\sin(\delta_{Thi})\end{aligned} \tag{12}$$

Theoretically, equation (12) has two solutions. However, only the solution with a positive sign root is practical. This is because if the grid-feeding inverter is not injecting any current at its local PCC terminals, the local PCC voltage must be equal to the Thevenin voltage. While the impractical solution is giving a contradictory result of $\vec{v}_{PCCi} = 0$. The solution for A_i is given in (13).

$$\begin{aligned}A_i &= 0.5\|V_{Thi}\|_2\cos(\delta_{Thi}) + \left(R_{Thi}Q_{PCCi} - \omega L_{Thi}P_{PCCi}\right)\|V_{Thi}\|_2^{-1}\sin(\delta_{Thi}) \\ &+\sqrt{\begin{aligned}&0.25\|V_{Thi}\|_2^2\cos^2(\delta_{Thi}) + \left(\left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\right)^2\sin^2(\delta_{Thi}) \\ &+\left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi}\right)\cos(\delta_{Thi})\sin(\delta_{Thi}) \\ &-\left(\left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\right)^2 \\ &+\left(R_{Thi}P_{PCCi} + \omega L_{Thi}Q_{PCCi}\right)\cos^2(\delta_{Thi})\end{aligned}}\end{aligned} \tag{13}$$

Additionally, the solution for B_i is given in (14).

$$\begin{aligned}B_i &= \left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\sec(\delta_{Thi}) + 0.5\|V_{Thi}\|_2\sin(\delta_{Thi}) \\ &+\left(R_{Thi}Q_{PCCi} - \omega L_{Thi}P_{PCCi}\right)\|V_{Thi}\|_2^{-1}\sin(\delta_{Thi})\tan(\delta_{Thi}) + \\ &\tan(\delta_{Thi})\sqrt{\begin{aligned}&0.25\|V_{Thi}\|_2^2\cos^2(\delta_{Thi}) + \left(\left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\right)^2\sin^2(\delta_{Thi}) \\ &+\left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi}\right)\cos(\delta_{Thi})\sin(\delta_{Thi}) \\ &-\left(\left(\omega L_{Thi}P_{PCCi} - R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\right)^2 \\ &+\left(R_{Thi}P_{PCCi} + \omega L_{Thi}Q_{PCCi}\right)\cos^2(\delta_{Thi})\end{aligned}}\end{aligned} \tag{14}$$

Now, $\|\vec{v}_{PCCi}\|_2 = \sqrt{A_i^2 + B_i^2}$ describes the different operation regions of the i^{th} targeted local PCC bus in a three dimensional surface for a given Thevenin representation of the rest of TVPP network. In this case, the SOR of the targeted i^{th} PCC bus is the projection of the surface on the P_{PCCi} and Q_{PCCi} plane where $\|\vec{v}_{PCCi}\|_2 \in \mathbb{R}$. Also, subspace of the SNOR is described by projection of the surface with range of $0.9V_g < \|\vec{v}_{PCCi}\|_2 < 1.1V_g$ on the P_{PCCi} and Q_{PCCi} plane. On the other hand, any operation set-points that satisfies $\|\vec{v}_{PCCi}\|_2 \notin \mathbb{R}$ is in the

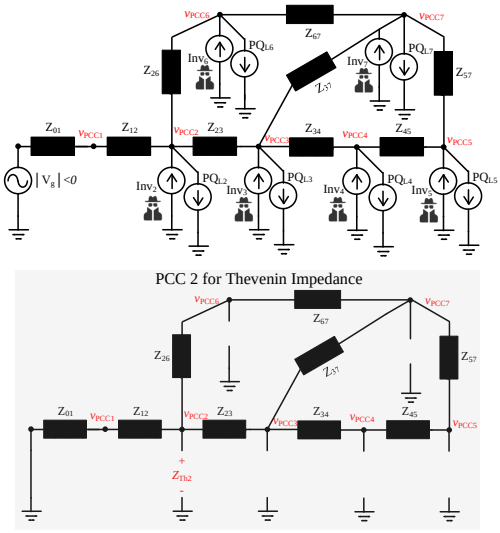


Fig. 5. Eight bus single-phase TVPP example and the Thevenin impedance of PCC2.

UOR. Yet, these operation regions cannot be utilized in real-time. As finding the Thevenin voltage of the rest of the network requires repeated load flow solutions.

To extend this analysis to real-time, the inclusion of nearby PCC buses PQ set-points on the i^{th} targeted PCC bus is deliberated by finding the expression of the Thevenin voltage in (4) as a function of all the other grid-feeding inverters PQ set-points except the targeted i^{th} grid-feeding inverter. In fact, with such consideration the targeted PCC voltage is expressed with a multi-dimensional manifold. This process is repeated for every local PCC bus in the TVPP network and then the intersection of all PCC buses SOR is considered as the whole TVPP SOR. Similarly, the intersection of all PCC buses SNOR is the entire VPP SNOR. Thereby, any operation set-point that is outside the SOR is considered in UOR (which means violation of the developed main theorem). However, application of Thevenin and superposition theories are not applicable directly since the grid-feeding inverters operation depends on its local PCC voltage existence. This is detailed by a graphical example in the next subsection.

C. *Graphical Example of the Derived Real-Time Opeartion Regions*

The inclusion of nearby grid-feeding inverters (i.e., DEGs) influence is determined by finding the closed form solution of the Thevenin voltage depicted (2)-(14). To understand this, an example is taken here of the TVPP network shown in Fig. 4. This example can be extended to any network with an arbitrary number of grid-feeding inverters. In this case, the Thevenin voltage of the grid-feeding inverter at local PCC bus 2 is as (15). Then, this Thevenin voltage is combined with (13) and (14) considering the index i equal to 2.

$$\begin{aligned}
&\left\|\vec{v}_{PCC2}\right\|_2 = \sqrt{A_2^2 + B_2^2}, \vec{v}_{Th_2} = \left(\vec{v}_{Bus_3} - \vec{v}_g\right)\left(Z_{Th_2}\right)^{-1} + \vec{v}_g, \vec{v}_g = \left|V_g\right| \angle 0 \\
&\vec{v}_{Bus_3} = 0.5\left|V_g\right| + j\left(R_{Th_3} Q_{PCC3} - \omega L_{Th_3} P_{PCC3}\right)\left|V_g\right|^{-1} \\
&+\sqrt{0.25\left|V_g\right|^2 - \left(\left(R_{Th_3} Q_{PCC3} - \omega L_{Th_3} P_{PCC3}\right)\left|V_g\right|^{-1}\right)^2 + \left(R_{Th_3} P_{PCC3} + \omega L_{Th_3} Q_{PCC3}\right)} \\
&Z_{Th_2} = Z_{01} + Z_{12}, R_{Th_2} = \mathrm{Re}\left\{Z_{Th_2}\right\}, L_{Th_2} = \mathrm{Im}\left\{Z_{Th_2}\right\}\omega^{-1} \\
&Z_{Th_3} = Z_{01} + Z_{12} + Z_{23}, R_{Th_3} = \mathrm{Re}\left\{Z_{Th_3}\right\}, L_{Th_3} = \mathrm{Im}\left\{Z_{Th_3}\right\}\omega^{-1}
\end{aligned} \tag{15}$$

Similarly, the voltage at the local PCC bus 3 is a function of all PQ set-points in the network and can be described by (13) and (14) with index i equal to 3 and (16).

$$\begin{aligned}
&\left\|\vec{v}_{PCC3}\right\|_2 = \sqrt{A_3^2 + B_3^2}, \vec{v}_{Th_3} = \vec{v}_{Bus2} \\
&\vec{v}_{Bus2} = 0.5\left|V_g\right| + j\left(R_{Th_2} Q_{PCC2} - \omega L_{Th_2} P_{PCC2}\right)\left|V_g\right|^{-1} + \\
&\sqrt{0.25\left|V_g\right|^2 - \left(\left(R_{Th_2} Q_{PCC2} - \omega L_{Th_2} P_{PCC2}\right)\left|V_g\right|^{-1}\right)^2 + \left(R_{Th_2} P_{PCC2} + \omega L_{Th_2} Q_{PCC2}\right)}
\end{aligned} \tag{16}$$

Also, the voltage at main TVPP bus is a function of all PQ set-points in the network and described by (17).

$$\begin{aligned}
&\left\|\vec{v}_{PCC1}\right\|_2 = \left\|\left(\vec{v}_{Bus2} - \vec{v}_g\right)\left(Z_{Th_0}\right)\left(Z_{Th_2}\right)^{-1} + \left(\vec{v}_{Bus3} - \vec{v}_g\right)\left(Z_{Th_0}\right)\left(Z_{Th_3}\right)^{-1} + \vec{v}_g\right\|_2 \\
&Z_{Th_0} = Z_{01}, R_{Th_0} = \mathrm{Re}\left\{Z_{Th_0}\right\}, L_{Th_2} = \mathrm{Im}\left\{Z_{Th_0}\right\}\omega^{-1}
\end{aligned} \tag{17}$$

In this example, each PCC bus is five dimensional manifold. A correction is needed in finding the main TVPP multi-dimensional manifold. This correction is related to the usage of the source $\vec{v}_g$ twice in the superposition analysis. Furthermore, this correction is depicted graphically in Fig. 4. This correction can be applied to any general network architecture radial or mesh. In fact, a more complex TVPP network is taken as an example to illustrate this correction on superposition theory application for obtaining local PCC bus 2 Thevenin voltage in

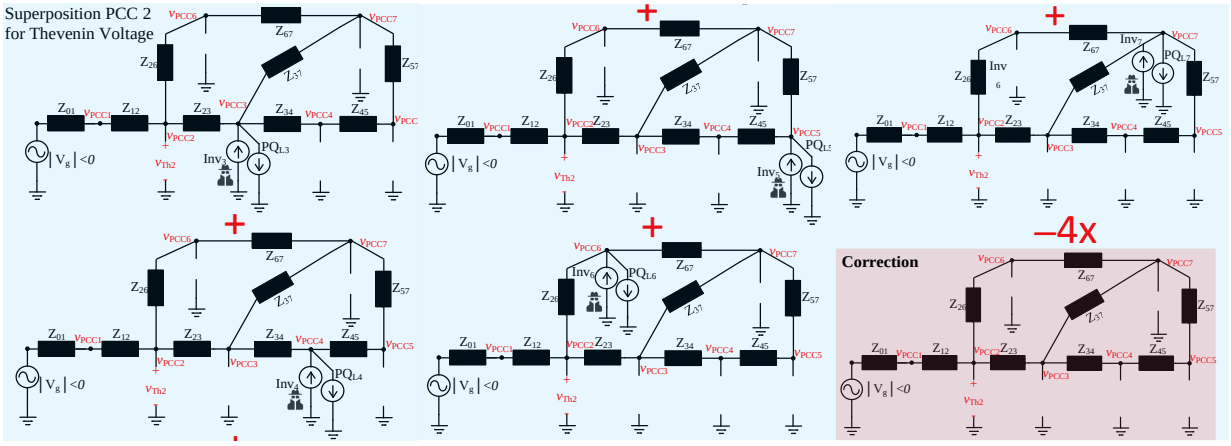


Fig. 6. Eight bus single-phase TVPP example with the correction for Thevenin voltage on superposition theory to obtain PCC2.

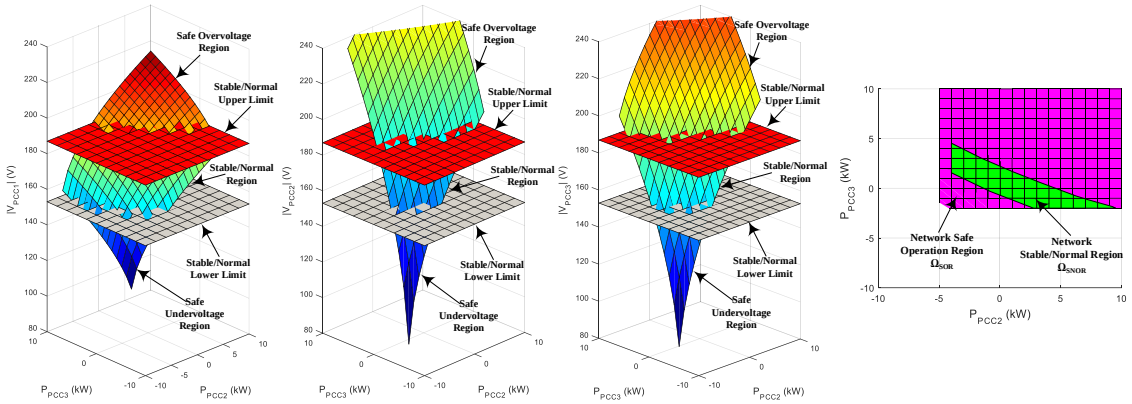


Fig. 7. Operation regions of (a) PCC 1, (b) PCC 2, (c) PCC 3, and (d) SOR and SNOR of the four PCC bus single-phase TVPP for scenario I

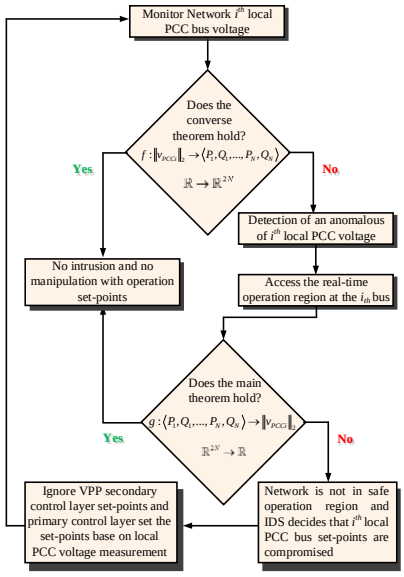


Fig. 8. Intrusion detection system.

Fig. 5. Furthermore, the Thevenin voltage for local PCC bus 2 is summation of $\vec{v}_{Th_2}$ in all the five equivalent circuits shown in Fig. 6. However, the correction in this example is to subtract four times the impact of $\vec{v}_g$ on the local PCC bus 2. This approach allows obtaining local PCC bus 2 as a function of all TVPP PQ set-points. Note that, this analysis focused on superposition is because the basis of this analysis is on repetitive utilization of subsection II.B results.

Moreover, without loss of generality, let us consider Q_{PCC2} and Q_{PCC3} are zero. Then, the realization of the different operation regions for each local PCC bus in Fig. 4 is reduced from a five-dimensional manifold to a three-dimensional surface depicted in Fig. 7(a), (b) and (c) for each PCC bus. Let Ω_1 be the projection of the surface $\vec{v}_{PCC1}$ on the P_{PCC2} and P_{PCC3} plane. Then, Ω_{PCC1} is describing the operation set-points that belongs to SOR or SNOR at $\vec{v}_{PCC1}$. Similarly, Ω_{PCC2} is describing SOR or SNOR at $\vec{v}_{PCC2}$ and Ω_{PCC3} at $\vec{v}_{PCC3}$. Moreover, the network SOR (Ω_{SOR}) is given as intersection of all individual buses SORs (i.e., $\Omega_{SOR} = \Omega_{PCC1} \cap \Omega_{PCC2} \cap \Omega_{PCC3}$). The VPP network SOR ($\Omega_{SOR}$) is depicted in Fig. 7(d) and the network SNOR is depicted by the green area in Fig. 7(d).

Table I: Individual grid-feeding inverter DEGs ratings

Parameter	Symbol	Value
Rated Power	S_{Rated}	20 kVA
Switching Frequency	f_{sw}	10 kHz
Nominal Grid Frequency	ω	376.8 Rad/s
Voltage Peak	V_g	$120\sqrt{2}$ V
DC-Bus Voltage	V_{DCi}	420 V
DC-link Capacitor	C_{DCi}	2 mF
Filter Inductor	L_i	0.5 mH
Filter Inductor Resistance	R_i	0.05 Ω

IV. Proposed Intrusion Detection System Based on the Identified Real-Time Operation Regioins

Summary of the proposed IDS logic for sanity check of the PQ set-point assignment from secondary layer controller is illustrated in Fig. 8 that is leveraging the developed real-time operation regions. Initially, in Fig. 8 an anomalous i^{th} local PCC voltage is considered by the voltage monitoring system once the converse theorem is violated. In other words, the morphism $f:\|\vec{v}_{PCCi}\|_2 \rightarrow \langle P_{PCC1}, Q_{PCC1}, \dots, P_{PCCN}, Q_{PCCN}\rangle, \mathbb{R} \rightarrow \mathbb{R}^{2N}$ is not satisfied. Then, the primary control layer access to the real-time operation regions to authenticate the main theorem (i.e., $g:\langle P_{PCC1}, Q_{PCC1}, \dots, P_{PCCN}, Q_{PCCN}\rangle \rightarrow \|\vec{v}_{PCCi}\|_2, \mathbb{R}^{2N} \rightarrow \mathbb{R}$). If the main theorem does not hold. Then, the i^{th} local PCC bus PQ set-points that are generated by the VPP slow time scale secondary control layer are compromised as $f \neq g^{-1}$. In other words, f and g are nonisomorphism pair and the network is operating in UOR. After that, the set-points passing from the compromised secondary control layer are disregarded and the grid-feeding inverters are changing the set-points and monitor if the local PCC voltage of the bus is regaining safe operation (i.e., move the network to SOR).

The steps to generate the analytic expression of each PCC bus in the single-phase TVPP as a function of all the network DEGs' PQ operation set-points are as follows:

1 - Each local PCC bus can be described by (13) and (14). These equations includes the remaining non-targeted PCC buses operation set-points in the Thevenin voltage expression.

2 - Then, finding the Thevenin voltage expression analytically requires application of superposition multiple times. However, a correction must be done at the end to eliminate the effect of using some sources multiple times. The repetition of these sources is used for sake of solvability. In other words, this

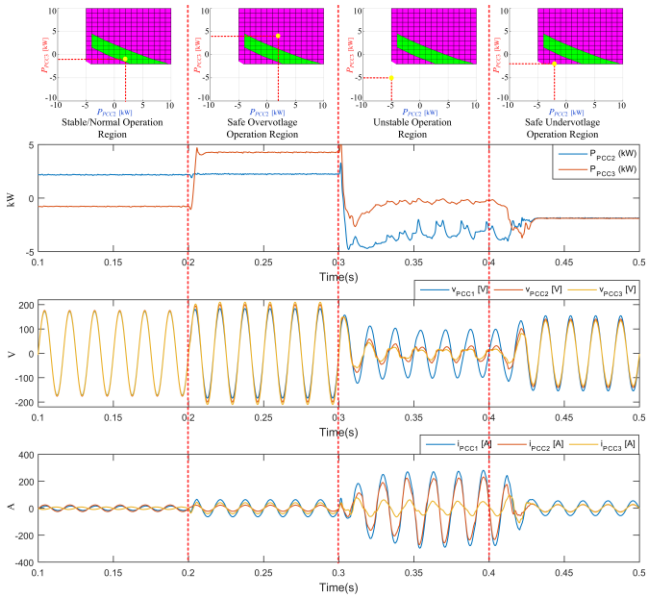


Fig. 9. Scenario I effectiveness using the identified real-time operation regions for intrusion detection in TVPP of Fig. 4.

approach is followed to utilize repetitively the analogy introduced in section II-B.

3 - After that, for each local PCC bus a multi-dimensional manifold is acquired. These manifolds are used to define the SOR of each local PCC bus when $\|\vec{v}_{PCCi}\|_2 \in \mathbb{R}$ is satisfied (This is the developed main theorem when $\mathbb{R}^{2N} \rightarrow \mathbb{R}$). This is graphically representing the projection of the manifold on the independent variables domain. Also, the subspace that defined SNOR is the projection portion of SOR where the range is of $0.9V_g < \|\vec{v}_{PCCi}\|_2 < 1.1V_g$. In addition, any operation point outside SOR is in UOR of the local PCC bus, i.e. $\|\vec{v}_{PCCi}\|_2 \notin \mathbb{R}$.

4 - The intersection of all local PCC SORs obtains the SOR of the whole single-phase TVPP. This SOR region is used to enable understanding in real-time compromised VPP secondary control layer generated PQ set-points that are passing to the primary control layer of the unobservable DEGs.

The challenge that might arise is what if finding the Thevenin impedance or reduction of the impedance network during each stage of superposition is non-solvable due to network connection complexity. This can be elucidated with using the general two point impedance theory introduced in [21], [22] by using the network Laplacian matrix.

V. Resutls and Discussion

The theoretical analyses established are validated by simulation of two scenarios. In these two scenarios, the DEGs in the TVPP network are rated according to Table I. Particularly, the inverters representing DEGs in the TVPPs are rated to 10 kVA, 60 Hz nominal frequency operation, 10 kHz switching frequency, 420 V nominal DC link voltage, and 0.5 mH filter inductor. These DEGs are controlled in grid-feeding mode of operation through the primary current control scheme illustrated above in Fig. 2. In these scenarios, once an anomalous local PCC voltage is observed by a specific DEG's proactive IDS, this DEG's IDS authenticates the VPP secondary control layer generated set-points through accessing

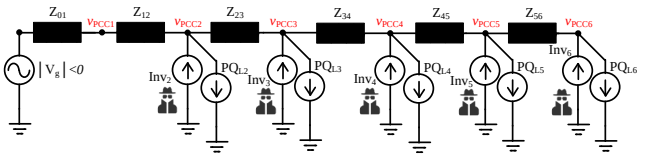


Fig. 10. Seven bus single phase TVPP for scenario II

the real-time operation regions in the primary control layer. If the authentication fails, this DEG disregards the set-points passing from the VPP secondary control layer. After that, the set-points are decided based on local PCC voltage control to regain safe operation.

The first scenario is validating the developed operation regions graphically through a simulation of the four bus single-phase TVPP presented in Fig. 4 with malicious stealthy cyber attackers. These stealthy attackers are changing the set-points passing to the primary control layer gradually to violate the stability limits of the TVPP. The operation regions for this TVPP are identified in Fig. 7. Then, the second scenario is application of the proposed multi-dimensional manifolds with the proposed IDS to a seven bus single-phase TVPP of Fig. 9.

A. *Malicious Stealthy Cyber-Attack Scenario I*

The malicious stealthy cyber-attack scenario depicted in Fig. 9 validates the different operation regions derived and shows the effectiveness of using these operation region for intrusion detection. Initially, the single-phase TVPP of Fig. 4 is operating in the network SNOR with P_{PCC2} = 2 kW, P_{PCC3} = -1 kW (see Fig. 9 from 0.1 s to 0.2 s). Then, the stealthy intruder manipulates the DEGs operation set-points passing from the secondary control layer by utilizing the reserved generation (i.e. PV power reserve, or energy storage) at PCC2. The new operation set-points results in surplus of 4 kW at PCC2 bus (see Fig. 9 from 0.2 s to 0.3 s). At this duration, the TVPP is moved to the overvoltage SOR and the attacker fails to jeopardize the operation of the network also the IDS is not performing any action as no anomalous voltage is observed. After that, at time instant 0.3 s in Fig. 9 the attacker manipulates the generation at PCC2 and PCC3 by reducing the generation so the net power appearing at PCC2 and PCC3 is -5 kW. Now, the TVPP is witnessing unstable operation seen in the voltage waveforms, power oscillations, and overcurrent after 0.3 s in Fig. 9. In this situation, the IDS first fails to authenticate the converse theorem and then fails to authenticate the main theorem through the real-time operation regions of Fig. 7. Thereby, the last operation set-points belong to the UOR and the stealthy intrusion is detected by the IDS. After that, PCC2 and PCC3 grid-feeding inverter are controlling their local PCC voltage through the set-points and disregard the VPP secondary control layer generated set-points after 0.4 s in Fig. 9. The new operation PQ set-points are obtained by using the generation reserved at PCC2 and PCC3 to 2 kW and 4 kW. As consequence, the TVPP regains operation in the undervoltage SOR after 0.4 s in Fig. 9.

B. *Malicious Stealthy Cyber-Attack Sencario II*

Now, for the scenario of the TVPP with seven buses that is shown in Fig. 10, each local PCC bus is described with eleven dimensional manifolds. Furthermore, in this scenario initially the TVPP is operating in the SNOR of the network (see Fig. 11

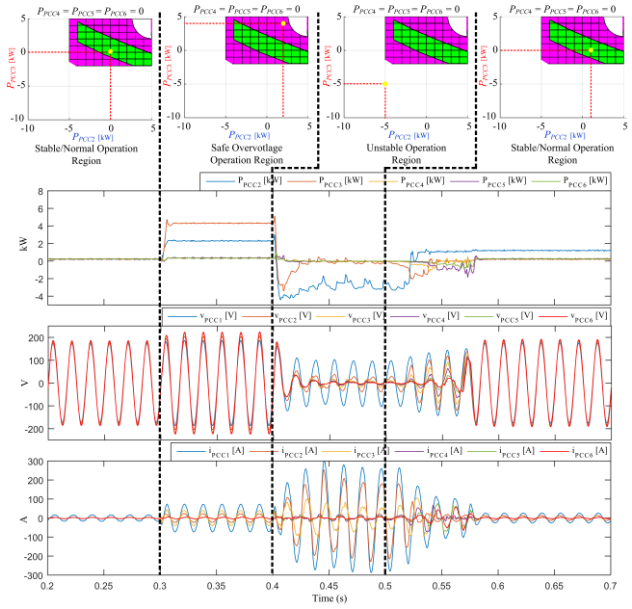


Fig. 11. Scenario II for the seven bus single-phase TVPP shown in Fig. 10 the TVPP operator is utilizing the operation regions after detecting anomalous voltage at PCC2 and PCC3.

before time instant 0.3 s). All consumers DEGs are meeting their local loads and not injecting any power into their local PCC terminals. After that, power reversal occurs at PCC2 and PCC3 after time instant 0.3 s in Fig. 11 due to a manipulation by a cyber intruder at the secondary layer. At this duration, the set-points 2 kW for PCC2 4 kW for PCC3 belong to the SOR and the intruder fails to jeopardize the network operation. Then, after 0.4 s in Fig. 11, PCC2 and PCC3 are pushed to unstable operation by the intruder. This new operation set-point -5 kW for PCC2 and PCC3 are in the UOR and the intruder is successful to induce an unstable operation. The IDS will alert the DEG that an anomalous voltage is detected and nonisomorphism pair will be concluded with authenticating the converse and the developed main theorem, then the DEGs are moved to local primary control mode based on PCC voltage condition to push the TVPP to the SNOR (see Fig. 11 after time instant 0.5 s). For this example, the local PCC buses and the main TVPP bus eleven dimensional manifolds are described by (18) – (23).

$$\left\|\vec{v}_{PCC1}\right\|_2 = \left\|\vec{v}_g + \sum_{i=2}^{6}\left(\vec{v}_{Busi} - \vec{v}_g\right)\left(Z_{Th_0}\right)\left(Z_{Th_1}\right)^{-1}\right\|_2, \vec{v}_g = \left|V_g\right|\angle 0$$

$$\vec{v}_{Busi} = 0.5\left|V_g\right| + j\left(R_{Th_i}Q_{PCCi} - \omega L_{Th_i}P_{PCCi}\right)\left|V_g\right|^{-1} + \sqrt{0.25\left|V_g\right|^2 - \left(\left(R_{Th_i}Q_{PCCi} - \omega L_{Th_i}P_{PCCi}\right)\left|V_g\right|^{-1}\right)^2 + \left(R_{Th_i}P_{PCCi} + \omega L_{Th_i}Q_{PCCi}\right)} \quad (18)$$

$$Z_{Thi} = \sum_{x=0,y=1}^{x=N-1,y=N} Z_{xy}, R_{Th_i} = \mathrm{Re}\left\{Z_{Thi}\right\}, L_{Th_i} = \mathrm{Im}\left\{Z_{Thi}\right\}\omega^{-1}, N = 6$$

$$\left\|\vec{v}_{PCC2}\right\|_2 = \sqrt{A_2^2 + B_2^2}, \vec{v}_{Th_2} = \vec{v}_g + \sum_{i=3}^{6}\left(\vec{v}_{Busi} - \vec{v}_g\right)\left(Z_{Th_2}\right)\left(Z_{Th_1}\right)^{-1} \quad (19)$$

$$\left\|\vec{v}_{PCC3}\right\|_2 = \sqrt{A_3^2 + B_3^2}, \vec{v}_{Th3} = \vec{v}_{Bus2} + \sum_{i=4}^{6}\left(\vec{v}_{Busi} - \vec{v}_g\right)\left(Z_{Th_3}\right)\left(Z_{Th_1}\right)^{-1} \quad (20)$$

$$\left\|\vec{v}_{PCC4}\right\|_2 = \sqrt{A_4^2 + B_4^2}, \vec{v}_{Th4} = \vec{v}_{Bus2} + \vec{v}_{Bus3} - \vec{v}_g + \sum_{i=5}^{6}\left(\vec{v}_{Busi} - \vec{v}_g\right)\left(Z_{Th_4}\right)\left(Z_{Th_1}\right)^{-1} \quad (21)$$

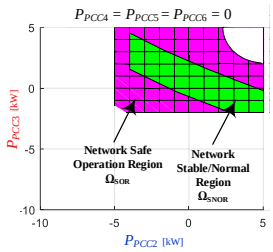


Fig. 12. Seven bus single phase TVPP for scenario II operation regions.

$$\left\|\vec{v}_{PCC5}\right\|_2 = \sqrt{A_5^2 + B_5^2}, \vec{v}_{Th5} = \left(\vec{v}_{Bus6} - \vec{v}_g\right)\left(Z_{Th_5}\right)\left(Z_{Th_1}\right)^{-1} - 2\vec{v}_g + \sum_{i=2}^{4}\vec{v}_{Busi} \quad (22)$$

$$\left\|\vec{v}_{PCC6}\right\|_2 = \sqrt{A_6^2 + B_6^2}, \vec{v}_{Th6} = -3\vec{v}_g + \sum_{i=2}^{5}\vec{v}_{Busi} \quad (23)$$

Based on (18)-(23) and the initial operation set-points in the second scenario the operation regions are depicted in Fig. 12 for scenario II.

It worth mentioning that once the IDS identified malicious PQ set-point and the DEG disregard the secondary layer controller set-point assignment, the DEG network may not operate in optimal operation set-point anymore which was the task of secondary layer controller, but it prevents the collapse of the network which may have catastrophic impact on the VPP. Thus, the objective of the proposed approach is prevention of the catastrophic grid failure and large blackouts by real-time intrusion detection at early stage while the grid operates are being alerted for further diagnosis, devices and controllers reset, etc.

VI. Conclusion

The overall objective of this work is to realize a real-time IDS for a power grid with fleet of VPPs. A real-time operation regions identification framework is proposed that describes each local PCC bus as multi-dimensional manifold where all the network PQ set-points are considered as the independent domain variables that are constructing the feasible PCC bus voltage range. Then, this work also exemplifies a correction so the Thévenin analysis obtained with superposition theory is applicable to multi-inverter network. Then, these multi-dimensional manifolds were used to identify three operation regions for each internal local PCC and main PCC bus in the TVPP as the following: (i) safe operation region (SOR), (ii) stable/normal operation region (SNOR), and (iii) unstable operation region (UOR). These operation regions are utilized in designing an intrusion detection system (IDS) to facilitate a linkage between unobservable DEGs and the upstream network for detecting stealthy intruders manipulating the secondary control layer. The concept of this work is constructed on validating a developed main theorem and its converse theorem. The main theorem states that in the network SOR all network operation set-points are morphismed to unique real valued local PCC bus voltages. While the converse theorem states that in the network SOR all local PCC bus voltages are morphismed to unique operation set-points. Hence, the detection of a nonisomorphism pair of the main theorem and the converse theorem concludes operating in the UOR induced by malicious intruder. Finally, two scenarios were simulated illustrating the effectiveness of the proposed theory.

REFERENCES

[1] A. Khan, M. Hosseinzadehtaher, M. B. Shadmand, S. Bayhan, and H. Abu-Rub, "On Stability of Power Electronics Dominated Grid," *IEEE Industrial Electronics Magazine*, no. 4, 2020.

[2] B. Mirafzal and A. Adib, "On Grid-Interactive Smart Inverters: Features and Advancements," *IEEE Access*, vol. 8, pp. 160526-160536.

[3] S. Y. Hadush and L. Meeus, "DSO-TSO cooperation issues and solutions for distribution grid congestion management," *Energy Policy*, vol. 120, pp. 610-621, 2018.

[4] Q. Ai, S. Fan, and L. Piao, "Optimal scheduling strategy for virtual power plants based on credibility theory," *Protection and Control of Modern Power Systems*, vol. 1, no. 1, p. 3, 2016.

[5] C. Kieny, B. Berseneff, N. Hadjsaid, Y. Besanger, and J. Maire, "On the concept and the interest of virtual power plant: Some results from the European project Fenix," in *2009 IEEE Power & Energy Society General Meeting*, 26-30 July 2009 2009, pp. 1-6.

[6] "CFCL BlueGen units for virtual power plant project in Netherlands," *Fuel Cells Bulletin*, vol. 2012, no. 7, p. 3, 2012.

[7] E. G. Kardakos, C. K. Simoglou, and A. G. Bakirtzis, "Optimal Offering Strategy of a Virtual Power Plant: A Stochastic Bi-Level Approach," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 794-806, 2016.

[8] Y. Wang, X. Ai, Z. Tan, L. Yan, and S. Liu, "Interactive Dispatch Modes and Bidding Strategy of Multiple Virtual Power Plants Based on Demand Response and Game Theory," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 510-519, 2016.

[9] H. Yang, D. Yi, J. Zhao, and Z. Dong, "Distributed Optimal Dispatch of Virtual Power Plant via Limited Communication," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3511-3512, 2013.

[10] A. Thavlov and H. W. Bindner, "Utilization of Flexible Demand in a Virtual Power Plant Set-Up," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 640-647, 2015.

[11] A. Baringo, L. Baringo, and J. M. Arroyo, "Day-Ahead Self-Scheduling of a Virtual Power Plant in Energy and Reserve Electricity Markets Under Uncertainty," *IEEE Transactions on Power Systems*, vol. 34, no. 3, pp. 1881-1894, 2019.

[12] A. Y. Fard, M. Easley, G. T. Amariucai, M. B. Shadmand, and H. Abu-Rub, "Cybersecurity Analytics using Smart Inverters in Power Distribution System: Proactive Intrusion Detection and Corrective Control Framework," in *2019 IEEE International Symposium on Technologies for Homeland Security (HST)*, 5-6. 2019, pp. 1-6.

[13] S. Harshbarger, M. Hosseinzadehtaher, B. Natarajan, E. Vasserman, M. Shadmand, and G. Amariucai, "(A Little) Ignorance is Bliss: The Effect of Imperfect Model Information on Stealthy Attacks in Power Grids," in *2020 IEEE Kansas Power and Energy Conference (KPEC)*, 13-14 July 2020, pp. 1-6,

[14] C. Xu, F. C. Huff, and P. Francino, "Optimal load dispatch based on generator reactive capability curve," in *2006 IEEE Power Engineering Society General Meeting*, 18-22 June 2006.

[15] D. Pudjianto, C. Ramsay, and G. Strbac, "Virtual power plant and system integration of distributed energy resources," *IET Renewable Power Generation*, vol. 1, no. 1, pp. 10-16.

[16] P. Cuffe, P. Smith, and A. Keane, "Capability Chart for Distributed Reactive Power Resources," *IEEE Transactions on Power Systems*, vol. 29, no. 1, pp. 15-22, 2014.

[17] A. V. Jayawardena, L. G. Meegahapola, D. A. Robinson, and S. Perera, "Capability chart: A new tool for grid-tied microgrid operation," in *2014 IEEE PES T&D Conference and Exposition*, 14-17 April 2014 2014, pp. 1-5.

[18] F. L. Müller, J. Szabó, O. Sundström, and J. Lygeros, "Aggregation and Disaggregation of Energetic Flexibility From Distributed Energy Resources," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1205-1214, 2019.

[19] Z. Tan, H. Zhong, Q. Xia, C. Kang, X. S. Wang, and H. Tang, "Estimating the Robust P-Q Capability of a Technical Virtual Power Plant Under Uncertainties," *IEEE Transactions on Power Systems*, vol. 35, no. 6, pp. 4285-4296, 2020.

[20] J. W. Simpson-Porco, "Lossy DC Power Flow," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 2477-2485, 2018.

[21] W. J. Tzeng and F. Y. Wu, "Theory of impedance networks: the two-point impedance andLCresonances," *Journal of Physics A: Mathematical and General*, vol. 39, no. 27, pp. 8579-8591, 2006.

[22] F. Y. Wu, "Theory of resistor networks: The two-point resistance," *J. Phys. A: Math. Gen.*, vol. 37, no. 26, p. 6653, 2004.

APPENDIX

A. Stability of the i^{th} Grid-Feeding Inverter Primary Control Layer Used for DEGs in the Single-Phase TVPP

Consider the i^{th} single-phase grid-feeding inverter that is connected to its local PCC terminals in Fig. 1. The active power (P_i) and reactive power (Q_i) injected into the network by this inverter can be measured by using the second order generalized integrator (SOGI) presented as (A.1) and (A.2), respectively.

$$P_i = \frac{1}{2} i^{\alpha}_{PCCi} v^{\alpha}_{PCCi} + \frac{1}{2} i^{\beta}_{PCCi} v^{\beta}_{PCCi} \tag{A.1}$$

$$Q_i = \frac{1}{2} i^{\alpha}_{PCCi} v^{\beta}_{PCCi} - \frac{1}{2} i^{\beta}_{PCCi} v^{\alpha}_{PCCi} \tag{A.2}$$

By differentiating equations (A.1) and (A.2), the state-space model that includes active and reactive power as state variables can be determined,

$$\frac{dP_i}{dt} = \frac{1}{2}\left(v^{\alpha}_{PCCi} \frac{di^{\alpha}_{PCCi}}{dt} + i^{\alpha}_{PCCi} \frac{dv^{\alpha}_{PCCi}}{dt} + v^{\beta}_{PCCi} \frac{di^{\beta}_{PCCi}}{dt} + i^{\beta}_{PCCi} \frac{dv^{\alpha}_{PCCi}}{dt} \right) \tag{A.3}$$

$$\frac{dQ_i}{dt} = \frac{1}{2}\left(v^{\beta}_{PCCi} \frac{di^{\alpha}_{PCCi}}{dt} + i^{\alpha}_{PCCi} \frac{dv^{\beta}_{PCCi}}{dt} - v^{\alpha}_{PCCi} \frac{di^{\beta}_{PCCi}}{dt} - i^{\beta}_{PCCi} \frac{dv^{\alpha}_{PCCi}}{dt} \right) \tag{A.4}$$

Furthermore, the expression for the derivatives of the stationary reference frame PCC currents i^{α}_{PCCi} and $i^{ß}_{PCCi}$ in (A.3) and (A.4) are deduced by applying Kirchhoff voltage law at the loop of common coupling depicted in Fig. 1. Hence, the PCC currents derivatives are as (A.5) and (A.6).

$$\frac{di^{\alpha}_{PCCi}}{dt} = L_i^{-1} m_{\alpha i} v_{DCi} - L_i^{-1} v^{\alpha}_{PCCi} - L_i^{-1} R_i i^{\alpha}_{PCCi} \tag{A.5}$$

$$\frac{di^{\beta}_{PCCi}}{dt} = L_i^{-1} m_{\beta i} v_{DCi} - L_i^{-1} v^{\beta}_{PCCi} - L_i^{-1} R_i i^{\beta}_{PCCi} \tag{A.6}$$

where $m_{\alpha i}$ and $m_{ßi}$ are stationary reference frame modulation indices of the i^{th} inverter, L_i is the filter inductance of the i^{th} inverter, and R_i is the filter resistance of the i^{th} inverter. Similarly, expression of the derivates of the stationary reference PCC voltages v^{α}_{PCCi} and $v^{ß}_{PCCi}$ in equations (A.3) and (A.4) are given as (A.7) and (A.8).

$$\frac{dv^{\alpha}_{PCCi}}{dt} = -\omega v^{\beta}_{PCCi} \tag{A.7}$$

$$\frac{dv^{\beta}_{PCCi}}{dt} = \omega v^{\alpha}_{PCCi} \tag{A.8}$$

where ω is the angular frequency of the network. Therefore, substituting (A.5), (A.6), (A.7) and (A.8) into (A.3) and (A.4) results in the time varying MIMO state-space system given by (A.9) and (A.10). The system is time varying because the stationary reference modulation indices $m_{\alpha i}$ and $m_{ßi}$ are multiplied by the PCC voltages. In addition, this MIMO state space control inputs are coupled in both states.

$$\frac{dP_i}{dt} = -R_i L_i^{-1} P_i - \omega Q_i + 0.5 L_i^{-1}\left(m_{\alpha i} v_{DCi} v^{\alpha}_{PCCi} + m_{\beta i} v_{DCi} v^{\beta}_{PCCi} - v^2_{PCCi} \right) \tag{A.9}$$

$$\frac{dQ_i}{dt} = -R_i L_i^{-1} Q_i + \omega P_i + 0.5 L_i^{-1}\left(m_{\alpha i} v_{DCi} v^{\beta}_{PCCi} - m_{\beta i} v_{DCi} v^{\alpha}_{PCCi} \right) \tag{A.10}$$

where v_{PCCi} is the Euclidean norm of v^{α}_{PCCi} and $v^{ß}_{PCCi}$. However, if the two inputs are defined as (A.11) and (A.12), then, the state-space in (A.9) and (A.10) transform into a simple linear time invariant (LTI) MIMO state-space as (A.13) and (A.14).

$$u_{Pi} = m_{\alpha i} v_{DCi} v^{\alpha}_{PCCi} + m_{\beta i} v_{DCi} v^{\beta}_{PCCi} - v^2_{PCCi} \tag{A.11}$$

$$u_{Qi} = m_{\alpha i} v_{DCi} v^{\beta}_{PCCi} - m_{\beta i} v_{DCi} v^{\alpha}_{PCCi} \tag{A.12}$$

$$\frac{dP_i}{dt} = -R_i L_i^{-1} P_i - \omega Q_i + 0.5 L_i^{-1} u_{Pi} \tag{A.13}$$

$$\frac{dQ_i}{dt} = -R_i L_i^{-1} Q_i + \omega P_i + 0.5 L_i^{-1} u_{Qi} \tag{A.14}$$

Now, consider the error on the instantaneous active and reactive power for the i^{th} inverter as (A.15) and (A.16),

$$e_{Pi} = P_{Refi} - P_i \tag{A.15}$$

$$e_{Qi} = Q_{Refi} - Q_i \tag{A.16}$$

where P_{Refi} is the reference commanded active power and Q_{Refi} is the reference commanded reactive power. Moreover, the cancellation of the coupling terms in (A.13) and (A.14) is achieved by taking the following control law that includes feedback and feedforward as (A.17) and (A.18).

$$u_{Pi} = \underbrace{2 L_i \omega Q_i}_{\text{Feedforward}} + \underbrace{2 L_i v_{Pi}}_{\text{Feedback}} \tag{A.17}$$

$$u_{Qi} = \underbrace{-2 L_i \omega P_i}_{\text{Feedforward}} + \underbrace{2 L_i v_{Qi}}_{\text{Feedback}} \tag{A.18}$$

The feedback term v_P in (A.17) is obtained with a Proportional Integral (PI) controller as (A.19) that tracks the desired active power reference.

$$v_{Pi} = K_{Ppi} e_{Pi} + K_{Pii} \int_0^t e_{Pi}(\tau) d\tau \tag{A.19}$$

Similarly, the feedback term v_Q in (A.18) is deduced with a PI controller as (A.20), this PI controller assures tracking the desired reactive power reference.

$$v_{Qi} = K_{Qpi} e_{Qi} + K_{Qii} \int_0^t e_{Qi}(\tau) d\tau \tag{A.20}$$

Moreover, substituting (A.19) into (A.17) and then placing the resulting expression into (A.13) yields the error dynamics of the active power that is given by (A.21).

$$\frac{de_{Pi}}{dt} = -\left(K_{Ppi} + R_i L_i^{-1} \right) e_{Pi} - K_{Pii} \int_0^t e_{Pi}(\tau) d\tau \tag{A.21}$$

Likewise, inserting (A.20) into (A.18) and then substituting the resulting expression into (A.14) yields the error dynamics of the reactive power as (A.22).

$$\frac{de_{Qi}}{dt} = -\left(K_{Qpi} + R_i L_i^{-1} \right) e_{Qi} - K_{Qii} \int_0^t e_{Qi}(\tau) d\tau \tag{A.22}$$

The active and reactive power error dynamics in (A.21) and (A.22) indicate that if the controller gains K_{Ppi}, K_{Pii}, K_{Qpi} and K_{Qii} are positive, the primary control layer is exponentially globally asymptotically stable. This is proved by linear quadratic Lyapunov stability theorem as follows, (A.21) and (A.22) are expressed by the state-space (A.23).

$$\frac{dX}{dt} = AX$$

$$X \in \mathbb{R}^4, A \in \mathbb{R}^{4 \times 4}$$

$$X = \begin{bmatrix} e_{Pi} & \frac{de_{Pi}}{dt} & e_{Qi} & \frac{de_{Qi}}{dt} \end{bmatrix}^T$$

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -K_{Pii} & -\left(K_{Ppi} + R_i L_i^{-1} \right) & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -K_{Qii} & -\left(K_{Qpi} + R_i L_i^{-1} \right) \end{bmatrix} \tag{A.23}$$

$$P=\begin{bmatrix} K_{Pii}{}^2+\left(K_{Ppi}+R_iL_i^{-1}\right)^2+K_{Pii} & \frac{1}{2K_{Pii}} & 0 & 0 \\ \frac{-1}{2K_{Pii}} & \frac{1}{K_{Pii}\left(K_{Ppi}+R_iL_i^{-1}\right)}-1 & 0 & 0 \\ 0 & 0 & K_{Qii}{}^2+\left(K_{Qpi}+R_iL_i^{-1}\right)^2+K_{Qii} & \frac{1}{2K_{Qii}} \\ 0 & 0 & \frac{-1}{2K_{Qii}} & \frac{1}{K_{Qii}\left(K_{Qpi}+R_iL_i^{-1}\right)}-1 \end{bmatrix} \quad \text{(A.25)}$$

Then, to prove the stability of the closed loop control with positive gains, the selection a positive definite matrix symmetrical matrix ($Q \in \mathbb{R}^{4x4}$), results in a positive definite symmetrical matrix ($P \in \mathbb{R}^{4x4}$) for satisfying the (A.24).

$$PA + A^TP = -Q \quad \text{(A.24)}$$

To show this, let us select $Q = I^{4x4}$ which is positive definite symmetrical matrix. Then, the solution of (A.24) is given in (A.25).

If the gains $K_{P_{pi}}$, $K_{P_{ii}}$, $K_{Q_{pi}}$ and $K_{Q_{ii}}$ are according to (A.26),

$$\begin{aligned} K_{Ppi} &> -R_iL_i^{-1}\ ,\ K_{Pii} > 0 \\ K_{Qpi} &> -R_iL_i^{-1}\ ,\ K_{Qii} > 0 \end{aligned} \quad \text{(A.26)}$$

Then, $P > 0$ (i.e., positive definite matrix since all leading minors and the determinant are positive). Therefore, the equilibrium point (0,0,0,0) is globally exponentially asymptotically stable. Hence, converging to the error dynamics to the equilibrium point (0,0,0,0) means the original system is converging to $\left(P_{Refi}, 0, Q_{Refi}, 0\right)$ as $t \to \infty$. To retrieve the original system inputs which are the inverter stationary reference modulation indices $m_{\alpha i}$ and $m_{ßi}$,

$$\begin{bmatrix} m_{\alpha i} \\ m_{\beta i} \end{bmatrix} = \frac{1}{\left\|v_{PCCi}\right\|_2^2}\begin{bmatrix} v_{PCCi}^{\alpha} & v_{PCCi}^{\beta} \\ v_{PCCi}^{\beta} & -v_{PCCi}^{\alpha} \end{bmatrix}\begin{bmatrix} \left(u_{Pi}+\left\|v_{PCCi}\right\|_2^2\right)v_{DCi}{}^{-1} \\ u_{Qi}v_{DCi}{}^{-1} \end{bmatrix} \quad \text{(A.27)}$$

L_2 norm $\|v_{PCCi}\|_2$ in (A.27) is $\|v_{PCCi}\|_2 \neq 0$ in network steady state stable voltage conditions, since the fundamental component of v_{PCCi} is well-posed and the signals v^{α}_{PCCi} and $v^{ß}_{PCCi}$ are always orthogonal due to SOGI utilization. Finally, the modulation index that controls the single-phase grid-feeding inverter is given as (A.28).

$$m_i = \begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} m_{\alpha i} \\ m_{\beta i} \end{bmatrix} \quad \text{(A.28)}$$

The controller structure is illustrated in Fig. 2.

A. *Implication of L_2 norm $\|v_{PCCi}\|_2 = 0$ in Unstable TVPP Voltage Conditions Induced by Cyber Intruder Set-Points*

The impact of unstable network voltage conditions can be understood from the conditions where the L_2 norm $\|v_{PCCi}\|_2$ of (A.27) is equal to zero or the existence of the active and reactive power measurement for the primary controller feedback in (A.1) and (A.2). Specifically, when there is an ill-posed local PCC voltage imposed on the terminals of the grid-feeding inverter due to a cyber-attacker requesting malicious set-points at the secondary control layer, the L_2 norm expressed in (A.29) is equal to zero.

$$\left\|v_{PCCi}\right\|_2 = \sqrt{v_{PCCi}^{\alpha}{}^2 + v_{PCCi}^{\beta}{}^2} \quad \text{(A.29)}$$

Zero L_2 norm means singularity in this situation, which results in non-existing stationary reference modulation indices (i.e., no solution for (A.27)). Also, with no PCC voltage, measuring the active and reactive power by (A.1) and (A.2) for the primary controller feedback will not be possible. Hence, unstable voltage conditions will cause TVPP DEGs operation failure. Hence, this proves that any instability witnessed in this TVPP is originated from unstable network voltage conditions and not from the primary control layer.