Cybersecurity Analytics for Virtual Power Plants

Ahmad Khan, *Student Member*, IEEE, Mohsen Hosseinzadehtaher, *Student Member*, IEEE,
Mohammad B. Shadmand, *Senior Member*, IEEE, Sudip K. Mazumder, *Fellow*, IEEE
Dept. of Electrical & Computer Engineering,
University of Illinois at Chicago, Chicago, IL, USA
ahmad20@uic.edu, mhossie5@uic.edu, shadmand@uic.edu, mazumder@uic.edu

***Abstract*— This article presents a framework to realize cybersecure virtual power plant (VPP). The foundation of this cybersecurity analytics is established on a developed normal operation region identification methodology. This normal operation region is exploited as a confirmation strategy to distinguish malicious set-points that are determined by VPP cyber-layer. These malicious set-points are spawned by a cyber-attacker influencing the VPP cyber-layer. The normal operation region is based on a derived one-to-one mapping between the network internal point of common coupling (PCC) bus voltages and the cyber-layer generated set-points. This derived mapping is compared with an inverse mapping through internal PCC bus voltage monitoring for anomalies. Once, an inconsistency is witnessed by the cybersecurity analytics between the one-to-one mapping and the inverse mapping, then the initial voltage anomaly detected by the monitoring system is due to an intrusion. The developed theory is validated through simulation of a cyber attacker gradually violating the network stability boundary through manipulating the operation set-points.**

***Index Terms*—Virtual power plant, power electronics-dominated grid, cybersecurity analytics**

I. Introduction

The envisioned energy paradigm will implicate high deployment of renewable based generation through the utilization of distributed energy generators (DEGs) [1-3]. At the low voltage side of the grid, grid-connected inverters are the dominant type of DEGs. Grid-connected inverters are following the inertial response of the network through their internal point of common coupling (PCC). In addition, these DEGs' capabilities are narrowed down to supplying current into the internal PCC terminals without considering upstream network prerequisites [4]. In other words, DEGs at the low voltage side are unobservable to utility operators and vice versa. Thereby, it is essential to execute real-time system level coordination and management to enable optimal utilization of these unobservable DEGs that are deployed at the low voltage side [5].

The virtual power plant (VPP) concept is exemplifying to be an inspiring exemplar that will expedite DEGs efficient integration with the utility grid. According to [6], VPP is a collection of numerous size of DEGs that are aggregated into a single consortium. Thereby, the VPP is an intermediate operator that facilitate the effective interconnection between transmission and distribution system operators. In fact, VPP perception introduction runs higher observability and controllability on DEGs and enables the optimal utilization of inverters based generation features. Several practical VPPs are reported around the world such as the European VPPs detailed implementations in [7] and [8].

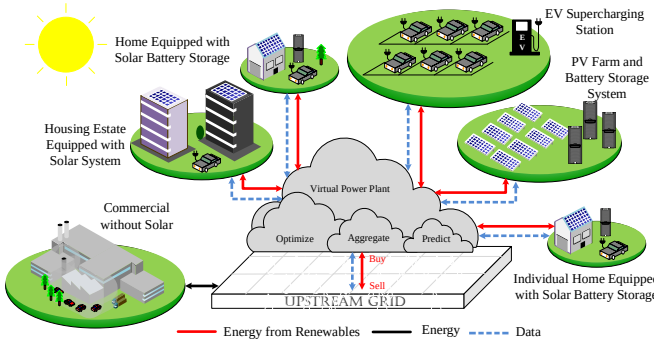

Fig. 1. VPP concept illustration

Nevertheless, this futuristic grid layout is anticipated to be vulnerable to malicious cyber-attacks [9-12]. As more generation portion and intelligent devices will function outside the conventional power plant administrative layout [13, 14]. For instance, cyber-attackers might take advantage of the VPP infrastructure to initiate catastrophic events disrupting the utility grid operation and create serious damages [15, 16]. The detection of such type of cyber-attack is extremely difficult at early stages. Thereby, this article improves the cybersecurity aspects of a VPP (see Fig. 1). Explicitly, by detection of a cyber-attacker manipulating the VPP cyber layer operation set-points gradually to violate network stability bound. Furthermore, the cybersecurity analytics proposed is based on a developed normal operation region identification framework. This normal operation region provides a one-to-one mapping between the network internal PCC bus voltage and the VPP cyber-layer generated set-points. This derived mapping is compared with an inverse mapping through internal PCC bus voltage monitoring for anomalies. Once, an inconsistency is witnessed by the cybersecurity analytics between the one-to-one mapping and the inverse mapping, the voltage anomaly is due to a cyber-attack. Then, after cyber-attack detection, the VPP control system is alerted.

Network stability bounds identification is an offline process. For instance, conventional generator stability bounds are assessed with capability curve concept [17]. This curve provides the range of the dispatchable active and reactive power set-point that guaranties the generator stable operation. The idea of the capability curve is extended to VPP perception with exploiting upstream network constrains in [18]. Universally, the capability curve is acquired by repetitive power flow

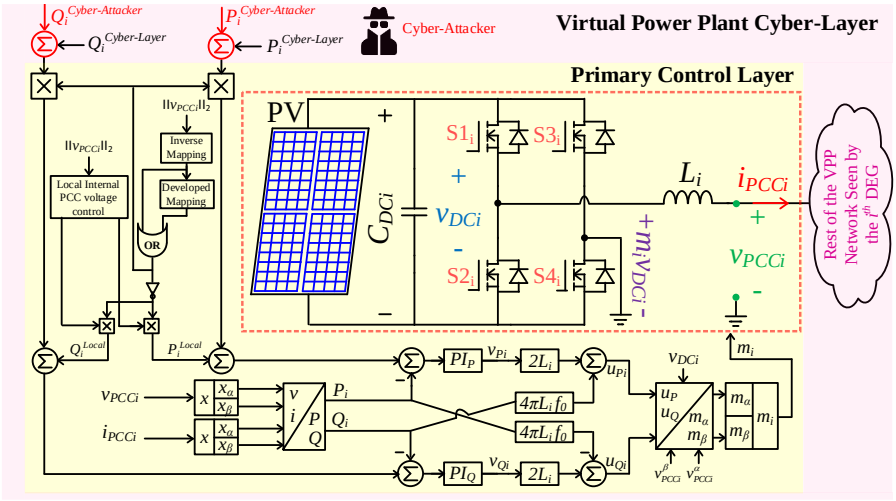

Fig. 2. Primary control layout considered for DEGs detailing the cybersecurity analytics and switch level depiction [19], [20].

solutions for several operational scenarios that are chosen arbitrarily. Then, the realistic solution scenarios are mapped to points in the capability curve. Thereby, up to the authors' knowledge, exploiting the existing body of knowledge of the capability curves for rapid cyber-attack detection against operational set-points manipulation and breaches is not feasible.

The rest of the article is organized as follows: Section II is normal operation regions derivation and construction of the developed one-to-one mapping, attack model description, and description of the cybersecurity analytics system. Section III discusses the results. Finally, section IV concludes the paper.

II. Cyber-Attack Hypothesis, Normal Operation Region Derivation, and Cybersecurity Analytics

A. Cyber-Attack Hypothesis and Malicious Set-Points Impact

Based on the time scale separation principle in Fig. 2 DEG layout, the VPP in Fig. 1 from the perspective of the slow time scale cyber-layer is represented as Fig. 3(a). Now, consider that a cyber-attacker is manipulating the operation set-points of the i^{th} concerned internal PCC bus that are assigned by the cyber-layer to the primary control of the DEG. From this cyber-attacker perspective, the impact of his manipulation can only be comprehended from the measurements. This is because the cyber-attacker lacks knowledge associated with the network topology or nearby DEGs. Given this absence of this knowledge by the cyber-attacker, the cyber-attacker could induce catastrophic effect by pushing the i^{th} concerned internal PCC bus to operate outside its stability bound by slowly and randomly changing the operation set-points.

B. Developed One-To-One Mapping Between Internal PCC Bus Voltages and the Cyber-Layer Operation Set-Points

From the perspective of an i^{th} specific DEG in the network, the remaining VPP network elements are seen as a Thèvenin voltage source ($\vec{v}_{Thi}$) with a series Thèvenin impedance ($Z_{Thi} = R_{Thi} + jX_{Thi}$) after the i^{th} internal PCC bus terminal (see Fig. 3(b)). Therefore, mathematically the internal PCC voltage ($\vec{v}_{PCCi}$) is represented by (1).

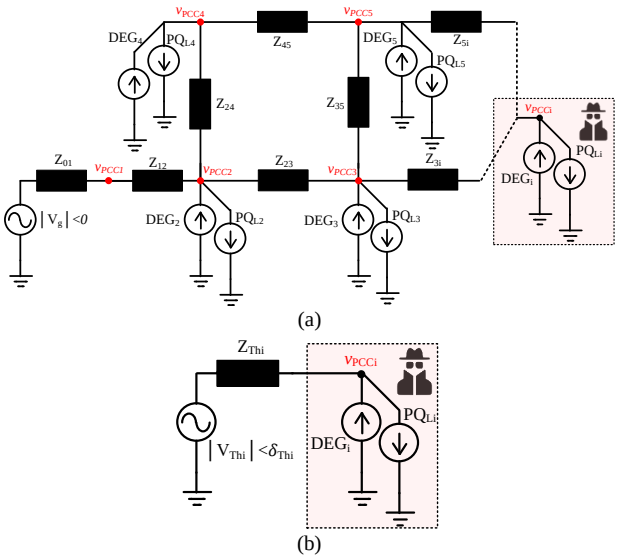

Fig. 3. (a) VPP general network, (b) illustrating the i^{th} local PCC bus equivalent circuit at the secondary control layer time scale.

$$\vec{v}_{PCCi} = (R_{Thi} + jX_{Thi})\vec{i}_{PCCi} + \vec{v}_{Thi} = \|V_{PCCi}\|_2 \angle\delta_{PCCi} = \xi_i + j\psi_i$$
$$\vec{v}_{Thi} = \|V_{Thi}\|_2 \angle\delta_{Thi} = \|V_{Thi}\|_2 \cos(\delta_{Thi}) + j\|V_{Thi}\|_2 \sin(\delta_{Thi}) \quad (1)$$

where $\vec{i}_{PCCi}$ is the net current supplied at the i^{th} internal PCC bus. $\vec{v}_{PCCi}$ is correlated to the set-points of the cyber-layer through the internal PCC current ($\vec{i}_{PCCi}$) as in (2)

$$\vec{i}_{PCCi} = (P_{PCCi} - jQ_{PCCi})\vec{v}^{*}_{PCCi}{}^{-1} \quad (2)$$

where $\vec{v}^{*}_{PCCi}$ is the complex conjugate of $\vec{v}_{PCCi}$, P_{PCCi} is the total supplied active power at the i^{th} concerned internal PCC bus, and Q_{PCCi} is the total supplied reactive power at the i^{th} concerned internal PCC bus. Unifying (2) and (1) results in (3).

$$\vec{v}_{PCCi} = (R_{Thi} + jX_{Thi})(P_{PCCi} - jQ_{PCCi})\vec{v}^{*}_{PCCi}{}^{-1} + \vec{v}_{Thi} \quad (3)$$

Equation (3) is rearranged to (4) considering (1).

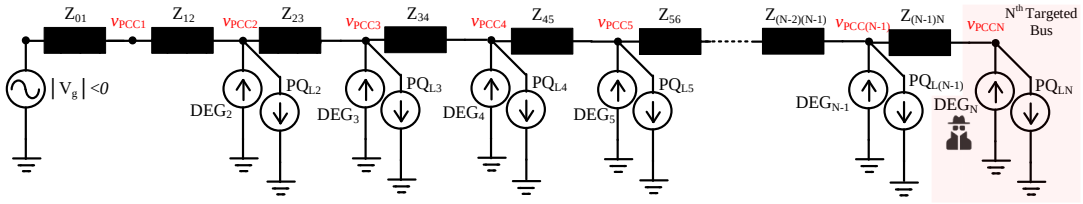

Fig. 4. Example of N DEGs TVPP for Thèvenin voltage closed form derivation

Algorithm 1: Cybersecurity Analytics System

Function [*Intrusion*] = **IDS** $[v_{PCCi}, P_{PCC1}, Q_{PCC1}, \dots, P_{PCCN}, Q_{PCCN}]$

1: Continuously monitor the internal PCC bus voltages

$$\|\vec{v}_{PCCi}\|_2 \rightarrow \langle P_{PCC1}, Q_{PCC1}, \dots, P_{PCCN}, Q_{PCCN}\rangle$$

If $(\|\vec{v}_{PCCi}\|_2 \rightarrow \langle P_{PCC1}, Q_{PCC1}, \dots, P_{PCCN}, Q_{PCCN}\rangle$ **! =** $\mathbb{R} \rightarrow \mathbb{R}^{2N})$

Internal PCC bus voltage is anomalous

2: Utilize the normal operation region one-to-one mapping

$$\langle P_{PCC1}, Q_{PCC1}, \dots, P_{PCCN}, Q_{PCCN}\rangle \rightarrow \|\vec{v}_{PCCi}\|_2$$

If $(\langle P_{PCC1}, Q_{PCC1}, \dots, P_{PCCN}, Q_{PCCN}\rangle \rightarrow \|\vec{v}_{PCCi}\|_2$ **! =** $\mathbb{R}^{2N} \rightarrow \mathbb{R})$

The anomaly detect is due to an intruder. Then, *Intrusion* = 1 and

Else

Intrusion = 0

Else

Intrusion = 0

$$\begin{aligned}&\xi_i^2+\psi_i^2 = R_{Thi}P_{PCCi}+X_{Thi}Q_{PCCi}+\\&\|V_{Thi}\|_2\left(A_i\cos(\delta_{Thi})+B_i\sin(\delta_{Thi})\right)\\&+j\left(X_{Thi}P_{PCCi}-R_{Thi}Q_{PCCi}+\|V_{Thi}\|_2\left(A_i\sin(\delta_{Thi})-B_i\cos(\delta_{Thi})\right)\right)\end{aligned} \tag{4}$$

It is fairly straightforward to obtain a closed form solution for the parameters ξ_i and Ψ_i from (4) for a particular Thèvenin depiction of the other elements in the network.

$$\begin{aligned}&\xi_i = 0.5\|V_{Thi}\|_2\cos(\delta_{Thi})+\left(R_{Thi}Q_{PCCi}-X_{Thi}P_{PCCi}\right)\|V_{Thi}\|_2^{-1}\sin(\delta_{Thi})\\&+\sqrt{\begin{aligned}&0.25\|V_{Thi}\|_2^2\cos^2(\delta_{Thi})+\left(\left(X_{Thi}P_{PCCi}-R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\right)^2\sin^2(\delta_{Thi})\\&+\left(X_{Thi}P_{PCCi}-R_{Thi}Q_{PCCi}\right)\cos(\delta_{Thi})\sin(\delta_{Thi})\\&-\left(\left(X_{Thi}P_{PCCi}-R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\right)^2\\&+\left(R_{Thi}P_{PCCi}+X_{Thi}Q_{PCCi}\right)\cos^2(\delta_{Thi})\end{aligned}}\end{aligned} \tag{5}$$

$$\begin{aligned}&\psi_i = \left(X_{Thi}P_{PCCi}-R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\sec(\delta_{Thi})+0.5\|V_{Thi}\|_2\sin(\delta_{Thi})\\&+\left(R_{Thi}Q_{PCCi}-X_{Thi}P_{PCCi}\right)\|V_{Thi}\|_2^{-1}\sin(\delta_{Thi})\tan(\delta_{Thi})+\\&\tan(\delta_{Thi})\sqrt{\begin{aligned}&0.25\|V_{Thi}\|_2^2\cos^2(\delta_{Thi})+\left(\left(X_{Thi}P_{PCCi}-R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\right)^2\sin^2(\delta_{Thi})\\&+\left(X_{Thi}P_{PCCi}-R_{Thi}Q_{PCCi}\right)\cos(\delta_{Thi})\sin(\delta_{Thi})\\&-\left(\left(X_{Thi}P_{PCCi}-R_{Thi}Q_{PCCi}\right)\|V_{Thi}\|_2^{-1}\right)^2\\&+\left(R_{Thi}P_{PCCi}+X_{Thi}Q_{PCCi}\right)\cos^2(\delta_{Thi})\end{aligned}}\end{aligned} \tag{6}$$

$\|\vec{v}_{PCCi}\|_2 = \sqrt{\xi_i^2+\Psi_i^2}$ describes the stability bound of the i^{th} concerned internal PCC bus for a particular Thèvenin depiction of the rest of network. The normal operation region of the concerned i^{th} PCC bus is the projection of $\|\vec{v}_{PCCi}\|_2$ on the P_{PCCi} and Q_{PCCi} plane (i.e., the domain when $\|\vec{v}_{PCCi}\|_2 \in \mathbb{R}$). Yet, this normal operation region cannot be exploited for rapid analysis. This is because the Thèvenin source representing the remaining elements in the network is obtained numerically with power flow. To extend this analysis, the insertion of adjacent PCC buses set-points on the i^{th} concerned PCC bus is described by obtaining the expression of the Thèvenin source in (1) as a function of all the other grid-connected DEGs set-points. This results in generalizing the concerned internal PCC bus voltage

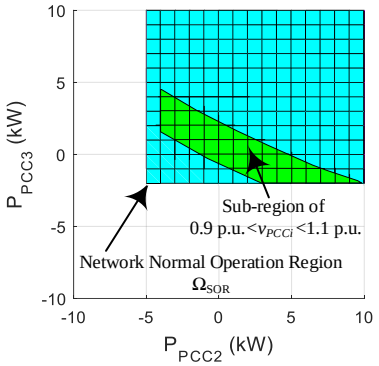

Fig. 5. Normal operation region of the whole network

to a manifold. This process is repetitive for every individual internal PCC bus in the network and then the intersection of all PCC buses normal operation regions is considered as the whole network normal operation region. The whole network normal operation region is the developed one-to-one mapping between the network internal point of common coupling PCC bus voltages and the cyber-layer generated set-points. Furthermore, to understand the Thèvenin closed form, the network with N DEGs shown in Fig. 4 is taken as an example. The aim is to find the manifold of the DEG at the N^{th} internal PCC bus in Fig. 4. The N^{th} internal PCC bus manifold is given in (7).

$$\begin{aligned}&\left\|\vec{v}_{PCC_N}\right\|_2 = \sqrt{\xi_N^2+\psi_N^2}\ ,\ \vec{v}_{Th_N} = (3-N)\vec{v}_g+\sum_{i=2}^{N-1}\vec{v}_{Bus_i}\ ,\ \vec{v}_g = |V_g|\angle 0\\&\vec{v}_{Bus_i} = 0.5|V_g|+j\left(R_{Th_i}Q_{PCCi}-X_{Th_i}P_{PCCi}\right)|V_g|^{-1}+\\&\sqrt{0.25|V_g|^2-\left(\left(R_{Th_i}Q_{PCCi}-X_{Th_i}P_{PCCi}\right)|V_g|^{-1}\right)^2+\left(R_{Th_i}P_{PCCi}+X_{Th_i}Q_{PCCi}\right)}\\&Z_{Th_i} = \sum_{j=0\ ,\ k=1}^{j=N-1\ ,\ k=N} Z_{jk}\ ,\ R_{Th_i} = \mathrm{Re}\{Z_{Th_i}\}\ ,\ X_{Th_i} = \mathrm{Im}\{Z_{Th_i}\}\end{aligned} \tag{7}$$

The, normal operation region (Ω_{NOR_N}) of this DEGs at N^{th} internal PCC bus is defined as (8).

$$\begin{aligned}&\Omega_{NOR_N} = \mathrm{Proj}_{P_2,Q_2,P_3,Q_3,\dots,P_N,Q_N}\left(\left\|\vec{v}_{PCC_N}\right\|_2\right)\ \Big|\ \left\|\vec{v}_{PCC_N}\right\|_2 \in \mathrm{R}\\&\text{For } \forall\ P_2,Q_2,P_3,Q_3,\dots,P_N,Q_N \in \mathrm{R}\end{aligned} \tag{8}$$

Similar conclusions for the normal operation region are deducible to all other internal PCC buses in the network. Thereby, the whole network normal operation region (Ω_{NOR}) is described by (9).

$$\Omega_{NOR} = \Omega_{NOR_1}\cap\Omega_{NOR_2}\cap\Omega_{NOR_3}\cap\dots..\ \Omega_{NOR_{N-1}}\cap\Omega_{NOR_N} \tag{9}$$

A four bus VPP example is considered, the network normal operation region depicted in Fig. 5.

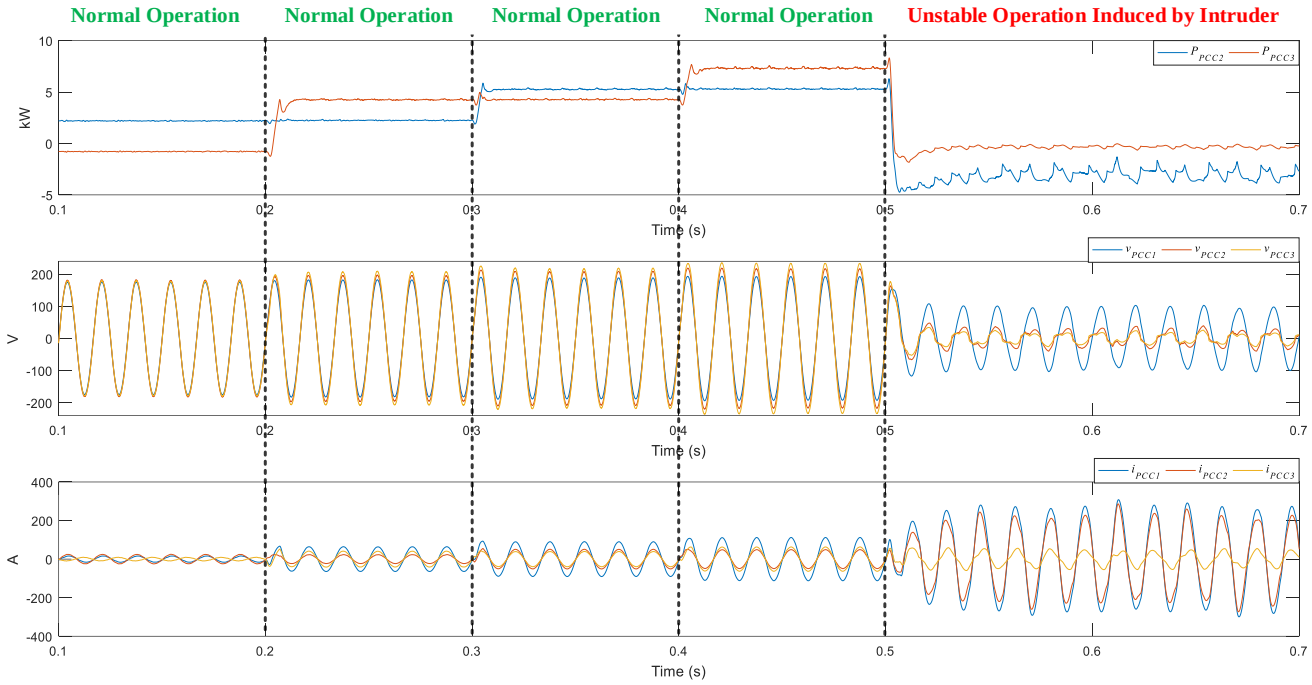

Fig. 6. Cyber-attack scenario I without activating the proposed cybersecurity analytics system

C. *Cybersecurity Analytics Framework*

The cybersecurity analytics system is depicted in Algorithm 1. As aforementioned earlier that this cybersecurity analytics system is mainly founded on the normal operation region deduced in the previous subsection in (1)-(9). Particularly, the normal operation region is the derived one-to-one mapping between the network internal PCC bus voltages and the cyber-layer generated set-points. This derived mapping is compared with an inverse mapping through internal PCC bus voltage monitoring for anomalies. Once, an inconsistency is witnessed by the cybersecurity analytics system between the one-to-one mapping and the inverse mapping, the voltage anomaly is due to an intrusion. Then, the VPP is alerted.

III. RESUTLS AND DISCUSSION

The cybersecurity analytics system performance is validated through simulation of two cyber intrusion scenarios. The grid-connected inverter DEGs in the VPP are rated to 20 kVA apparent power, 10 kHz switching frequency, 420 V DC bus voltage, 0.5 mH filter inductor with equivalent series resistance of 50 mΩ , and 2 mF decoupling capacitor. The utility grid is 120 V_{RMS} at 60 Hz. Moreover, the two scenarios of Fig. 6 and Fig. 7 are identical regarding set-points gradual manipulation by the cyber-attacker seeking for network stability boundary violation. However, in scenario II the DEGs are equipped with the developed cybersecurity analytics system.

A. *Scenario I*

In the scenario I that is depicted in Fig. 6, the cyber-attacker is seeking for violating the network stability boundary. Initially, v_{PCC2} is operating at 2 kW and v_{PCC3} is sinking 1 kW. These initial operating points belong to the normal operation region. Then, after time instant 0.2 sec in Fig. 6, the cyber-attacker increases the operation set-point passing to the primary control layer from the VPP cyber-layer to 4 kW at v_{PCC3}. This new manipulated set-point assignment by the cyber-attacker fails to violate the stability boundary of network. After that, the cyber-attacker further pushes the operation set-point at v_{PCC2} to 5 kW after time instant 0.3 sec in Fig. 6. Again the cyber-attacker fails to jeopardize the operation of the network as this set-point falls within the normal operation region boundary. Therefore, the cyber-attacker once again changes the set-point of v_{PCC3} to 7 kW after time instant 0.4 sec in Fig. 6. However, still he is incapable of jeopardizing the network stability. Hence, the cyber-attacker decides to moves v_{PCC2} and v_{PCC3} to sinking 5 kW after time instant 0.5 sec. In this situation, the cyber-attacker successfully jeopardize the network operation as this set-point is outside the normal operation region boundary (see Fig. 5)). In fact, it is obvious that the network enters into voltage collapse situation after time instant 0.5 sec in Fig. 6.

B. *Scenario II*

In scenario II, the exact same operation set-point variation with respect to time evolution of scenario I is occurring (see Fig. 7). However, in scenario II the DEGs are equipped with the proposed cybersecurity analytics. Therefore, once the cyber-attacker breaches the network stability bounder after 0.5 sec in Fig. 7, the DEGs are moved to internal PCC voltage control mode to regain internal PCC bus voltage normal operation (see Fig. 7 after 0.5 sec). In other words, the cyber-layer set-points are ignored. Note that, the network is no longer operating in optimal operation, but the cybersecurity analytics system avoids catastrophic impacts on the network due to early intrusion detection and alerting the VPP owner for further diagnoses.

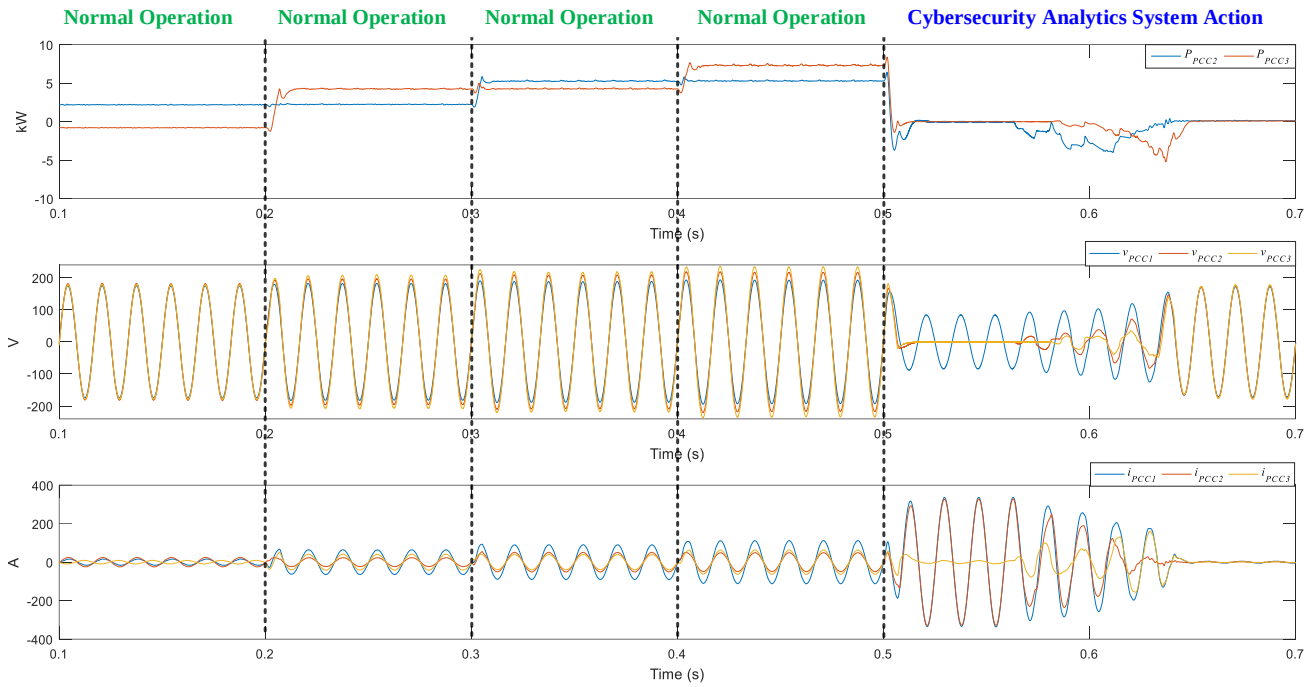

Fig. 7. Cyber-attack scenario II with activating the proposed cybersecurity analytics system

IV. Conclusion

This article presented a cybersecurity analytics system for a VPP. The foundation of this cybersecurity analytics system is established on a developed normal operation region identification methodology. This normal operation region is exploited as a confirmation strategy to distinguish malicious set-points that are demanded by the network cyber-layer. These malicious set-points are spawned by a cyber-attacker influencing the VPP cyber-layer set-points. The normal operation region is based on a derived one-to-one mapping between the network internal PCC bus voltages and the cyber-layer generated set-points. This derived mapping is compared with an inverse mapping through internal PCC bus voltage monitoring for anomaly. Once, an inconsistency is witnessed by the cybersecurity analytics system between the one-to-one mapping and the inverse mapping, the voltage anomaly is due to an intrusion. Then, after intrusion detection the DEGs alert the VPP. The developed theory is validated through simulation of a cyber-attacker gradually violating the network stability boundary through manipulating the operation set-points.

References

[1] A. Khan *et al.*, "On the Stability of the Power Electronics-Dominated Grid," *IEEE Industrial Electronics Magazine*, 2020.

[2] O. H. Abu-Rub *et al.*, "Towards Intelligent Power Electronics-Dominated Grid via Machine Learning Techniques," *IEEE Power Electronics Magazine*, 2021.

[3] A. Y. Fard and M. B. Shadmand, "Multitimescale Three-Tiered Voltage Control Framework for Dispersed Smart Inverters at the Grid Edge," *IEEE Transactions on Industry Applications*, 2021.

[4] B. Mirafzal and A. Adib, "On Grid-Interactive Smart Inverters: Features and Advancements," *IEEE Access*, 2020.

[5] S. Y. Hadush and L. Meeus, "DSO-TSO cooperation issues and solutions for distribution grid congestion management," *Energy Policy*, 2018.

[6] Q. Ai *et al.*, "Optimal scheduling strategy for virtual power plants based on credibility theory," *Protection and Control of Modern Power Systems*, 2016.

[7] C. Kieny *et al.*, "On the concept and the interest of virtual power plant: Some results from the European project Fenix," *2009 IEEE PES General Meeting*, 2009.

[8] "CFCL BlueGen units for virtual power plant project in Netherlands," *Fuel Cells Bulletin*, 2012.

[9] A. Khan *et al.*, "Intrusion Detection for Cybersecurity of Power Electronics Dominated Grids: Inverters PQ Set-Points Manipulation," *2020 IEEE CyberPELS*, 2020.

[10] M. Hosseinzadehtaher *et al.*, "Anomaly Detection in Distribution Power System based on a Condition Monitoring Vector and Ultra-Short Demand Forecasting," *2020 IEEE CyberPELS*, 2020.

[11] Z. Zhang *et al.*, "An Observer Based Intrusion Detection Framework for Smart Inverters at the Grid-Edge," in *2020 IEEE ECCE*, 2020.

[12] T. Hossen *et al.*, "Self-Secure Inverters Against Malicious Setpoints," in *2020 IEEE EPEC*, 2020.

[13] A. Y. Fard *et al.*, "Cybersecurity Analytics using Smart Inverters in Power Distribution System: Proactive Intrusion Detection and Corrective Control Framework," in *2019 IEEE HST*, 2019.

[14] A. Y. Fard *et al.*, "Holistic Multi-timescale Attack Resilient Control Framework for Power Electronics Dominated Grid," in *2020 RWS*, 2020.

[15] S. Harshbarger *et al.*, "(A Little) Ignorance is Bliss: The Effect of Imperfect Model Information on Stealthy Attacks in Power Grids," in *2020 IEEE KPEC*, 2020.

[16] M. Mola *et al.*, "Distributed Event-Triggered Consensus-Based Control of DC Microgrids in Presence of DoS Cyber Attacks," *IEEE Access*, 2021.

[17] C. Xu *et al.*, "Optimal load dispatch based on generator reactive capability curve," in *2006 IEEE PES General Meeting*, 2006.

[18] D. Pudjianto *et al.*, "Virtual power plant and system integration of distributed energy resources," *IET Renewable Power Generation*, 2007.

[19] A. Khan *et al.*, "PLL-less Active and Reactive Power Controller for Grid-Following Inverter," in *2020 IEEE ECCE*, 2020.

[20] A. Khan *et al.*, "Single Stage PLL-less Decoupled Active and Reactive Power Control for Weak Grid Interactive Inverters," *IFAC-PapersOnLine*, 2020.