Event-triggered Self-learning Control Scheme For Power Electronics Dominated Grid

Mohsen Hosseinzadehtaher, *Student Member, IEEE*, Amin Y. Fard, *Student Member, IEEE*, and Mohammad B. Shadmand, *Senior Member, IEEE*
Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, IL, USA
mhosse5@uic.edu, ayouse9@uic.edu, shadmand@uic.edu

***Abstract* — The growing penetration of distributed energy resources (DERs) requires renovation of the conventional power grid into a new paradigm, so-called power electronics dominated grid (PEDG). Alongside the features introduced within this new concept, the PEDG is more prone to cyber-physical malicious activities because of the distributed communication infrastructure and accessibility of the resources. Some of these malicious activities e.g., stealthy attacks, are unobservable for the supervisory system until the control system diverges. Some of these attacks might result in loss of DER generation that could cause frequency deviations beyond permissible boundaries specified by the DERs grid integration standards. To fulfill frequency restoration in the event of stealthy attacks, this paper proposes an artificial-intelligence-based shadow control for inverter-interfaced DERs to improve the grid's resiliency. During the normal operation of the PEDG, all DERs inject active power considering various criteria including, maximum available power, state of the charge, rate of power reserve, etc. As an unusual deviation on the frequency or its rate of change occurs, the artificial-intelligence-inspired shadow control of the grid cluster is activated to re-balance active power across the grid within a short timeframe while slow-response synchronous generators are trying to catch up. The ANN module of the proposed shadow control provides accurate feedbacks for the DER controller to support the grid frequency for any potential disturbances. The proposed shadow control framework is verified on a 14-bus PEDG system.**

***Keywords* – artificial intelligence, artificial neural network, power electronics dominated grid, frequency restoration, shadow control.**

I. Introduction

Unlike the conventional power grid that large centralized power plants using non-renewable fuels (e.g., oil, coal, nuclear fuel, etc.) are the main providers, distributed energy resources (DERs) are expected to become the primary providers in the modernized power grid [1]. This upgrade yields to a new energy paradigm so-called, power electronics dominated grid (PEDG) [2]. Although the concept of PEDG enables rising penetration of renewable resources across the grid, it introduces some challenges in privacy [3], stability [4], control [5], cyber-physical security [6-8], and planning [9]. These challenges need to be addressed to accelerate full implementation of this paradigm.

To ensure full control over the PEDG, the control hierarchy of the conventional power system, which is a three-layered control framework is adopted [10]. Power quality and stability of the grid are guaranteed by primary and secondary layers of the control hierarchy via high-bandwidth control techniques [11], while the tertiary layer confirms optimal operation of the entire system [12]. Satisfactory cooperation of the numerous agents i.e., smart inverters, sensors, smart meters, etc. across the PEDG requires adequate communications among these control layers that means a high traffic distributed communication infrastructure. The dispersed nature of communication infrastructure makes the entire PEDG more susceptible to cyberattacks. Various types of cyber events are studied in the literature including false data injection (FDI), denial of service (DoS) [13], man-in-the-middle malicious activities, stealthy attacks [14], and advanced persistent attacks. Each of these attack categories target different goals, differing from gaining illegal financial benefits to cascading failures of the grid, yielding to large-scale power outages. To prevent, detect, and mitigate these attacks, the PEDG must be equipped with intrusion detection systems (IDSs) [15]. Although various types of IDSs are proposed and implemented with proper performances, stealthy attacks on the state variables of the system are unobservable by the supervisory layers until their harmful intentions are attained on the system [16]. One of the main targets of the stealthy attacks on the power system is the frequency by deteriorating the active power balance across the grid that could cause vast outages [17].

Generally, in the power grid, the balance between demand and supply could be jeopardized due to major inaccuracies in generation/demand prediction algorithms, natural disasters, cyberattacks, etc. For maintaining a resilient and stable operation of the PEDG, demand and supply must stay balanced unceasingly [18]. In the conventional power system, considering the dynamics of the system frequency, which are mainly formed by the rotating inertia of synchronous machines [19], if a sudden loss of generation occurs, the rotating energy stored in the rotor is transformed into electrical power to meet the existing demand, which causes a transitory frequency drop. This frequency drop must be mitigated in a timely manner, otherwise the DERs will pushed to go islanded according to the grid integration standards e.g., IEEE 1547 [20]. Also, it is mandated by North American Reliability Corporation (NERC) that the first level of under-frequency load shedding (UFLS) relays should be triggered if the frequency drops down more than 0.7 Hz and the synchronous generator must be disconnected if the frequency goes beyond 61.8 Hz in a 60-Hz system.

Considering the distributed nature of the PEDG, frequency issue becomes more challenging due to the lower level of inertia in the PEDGs (< 2s) in comparison to traditional power grids (~

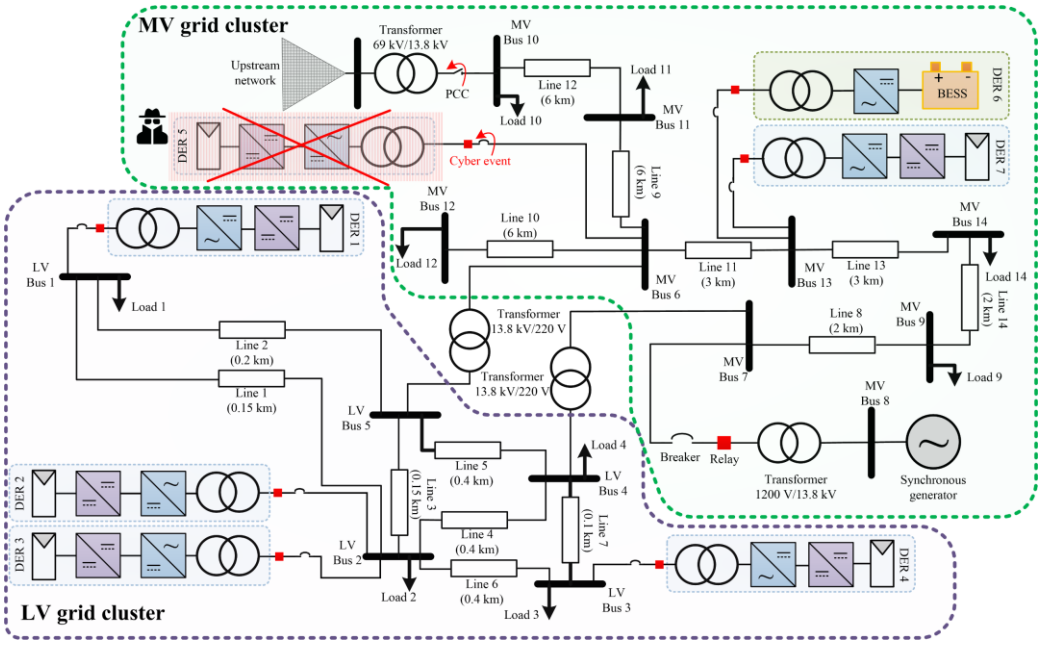

Fig. 1. The 14-bus PEDG under study.

10s) [21]. It must be taken into the account that in the islanded operation of the PEDG, not only the entire inertia level is low, but also there is no support from the upstream network. Thus, it is vital to equip the PEDG with robust, fast, and reliable frequency restoration control. If the frequency restoration control system is not able to cope with occurred disturbances within a short timeframe, protection relays will be triggered and a load shedding or a wide-area blackout might take place. Furthermore, based on the power system safety codes, the relays are set and coordinated in a manner that are sensitive to the rate of change of frequency (ROCOF), as well. It should be remarked that the entire system inertia controls the initial ROCOF when disturbances arise. Stealthy attacks on the state variables of the PEDG like inductor currents or capacitor voltages, attempt pushing some of the DERs across the grid to go islanded. Due to low inertia of the system, this would yield to substantial frequency deviations.

Numerous research articles have focused on frequency restoration from different perspectives [22]. Fundamentally, the frequency excursion problem in conventional power systems is regulated by leveraging two different control approaches. One is related to the synchronous generators' output control and the other focuses on the energy consumption control to restore frequency deviations, where the latter is recognized as load interruption [23]. Though, in the PEDG, mitigating substantial fluctuations on the frequency due to stealthy attacks needs a fast and precise approach to detect the required active power due to the generation loss, and compensate this amount in a timely manner, which is not achievable with the bulky-rotation-mass-based generation.

This paper proposes a novel shadow control scheme which leverages the advantages of artificial intelligence techniques for enhancing PEDG resiliency. A cohesive data-extracted methodology built-in a shadow control (CDMSC) scheme is developed with inherent features of the artificial neural networks (ANNs) to enhance the dynamic response of the system. When an stealthy attack occurs, the state variables easily become unstable while the observable and measurable global variables do not breach their standard ranges or at least violation occurs with some delay. Due to this unobservability and the intrinsic latency in common supervisory control techniques, there is a possibility that local DERs will be pushed islanded while the supply-demand balance is jeopardized before the supervisory layer of control take any effective action. The proposed CDMSC approximates the grid's inertia by ANN module, accurately. Different practical frequency dynamics, ROCOF and inertia constant are considered in the training process to ensure all possible scenarios on a realistic power system. Moreover, several disturbances including, load disturbances and potential loss of generation are considered in this process. It should be remarked that oscillation pattern of frequency is dictated by the synchronous generators in the understudy system; thus, considered disturbances are used as inputs of swing equation and the required power is calculated based on the frequency excursion and ROCOF. This data is used as test data in training process. A feed-forward ANN with two layers is applied in main core of the shadow control scheme towards an event-triggered self-learning controller that is guiding supervisory controller. Bayesian algorithm is utilized in the training process and optimum numbers of hidden neurons are founded by several evaluation of training mechanism.

The remainder of the paper is structured as follows; the understudy 14-bus PEDG is described in section (II). Section (III) details the concept of stealthy attacks and their impacts on the PEDG. In section IV, the concept of ANN-based shadow control scheme is explained in detail. Mathematical formulation of the proposed shadow control scheme such as system's dynamic equations and training process are provided in section (V). Several case studies are designed and performed on the 14-bus PEDG, accordingly, the results for validating the proposed shadow control scheme are presented in section (VI), and ultimately this article is concluded in section (VII).

II. System Description

To study the proposed ANN-based shadow control, a realistic 14-bus power system is considered as depicted in Fig. 1. The 14-bus system has two voltage levels as medium voltage (MV) and low voltage (LV), where MV is at the 13.8 kV and LV is 220 V. The entire system has the capability of connection/disconnection to/from the upstream network at 69 kV level via a substation connected to bus 10. In the islanded operation mode, an 800 kVA synchronous generator along with seven DERs feed the loads across the grid. The entire loading of the system is 500 kW, where 150 kW is provided by the synchronous machine and the rest is coming from the DERs. All the DERs are equipped with frequency relays and circuit-breakers to disconnect the DER in the occurrence of unpermitted frequency fluctuations. The MV and LV sections of the grid are interconnected through two 13.8 kV/200 V transformers, while the system has the capability of getting partitioned into two self-sufficient PEDG clusters with different voltage levels. In the considered attack model, the intruders using stealthy approaches push the DER 5 to disconnect from the grid. The rating of DER 5 is 270 kVA, as the main provider of the system. To maximize the attack impact, the attackers target the largest provider of the system. After disconnection of the DER, the frequency of the system drops suddenly due to significant mismatch between active power generation and consumption. If the system only relies on the synchronous generator for compensating the active power, due to high inertia synchronous generator, the frequency will drop below allowable boundaries and all the frequency relays would be triggered, which results in a backout across the grid. In the proposed approach, the shadow control of the cluster is activated due to the unexpected change in the system frequency. The ANN module of the shadow control accurately estimates the generation loss, and DER 6 which is a battery energy storage system (BESS) provides the lost generation. Using the proposed approach, not only load shedding is not needed, but also the fast response of the inverter-based DER restores the grid frequency and keeps all the DERs connected.

III. Impacts of Stealthy Attack Without Resilient Self-Learning Control

Stealthy attacks are extremely menacing for the PEDG stability especially when the system inertia is comparatively low or mixed. The situation could be even more crucial if stealthy attacks occur in various grid access points. The main feature of the stealthy attacks is deceiving the supervisory layer such that the measured parameter alterations are unobservable while other system state variables are being diverged. This manipulation will result in failure of the entire system when the supervisory layer is not able to do any prevention nor detection strategies. A successful stealthy attack can be designed by formulating the approximated state-space model of a system even by having imperfect system information. In this work, stealthy attacks are implemented on several inverters of PEDG and the control input signals are manipulated by employing attack disturbance signals into the system controller.

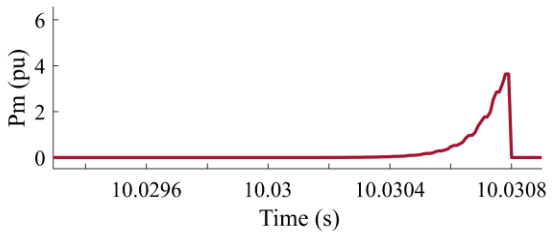

Fig. 2. The considered stealthy attack on PEDG access point: the attack is done on the governor controller and manipulate the regulated mechanical power fed to the turbine.

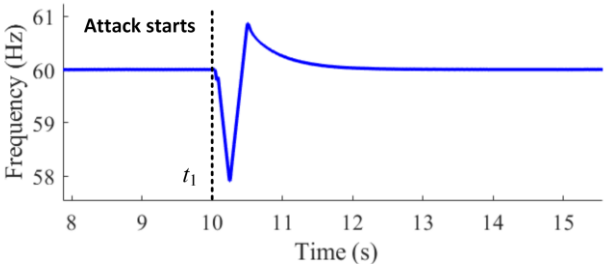

Fig. 3. System frequency dynamic: attack initiated at t_1 = 10s and ends after 0.0308 s. System becomes unstable after 0.25 s due to the large frequency deviation.

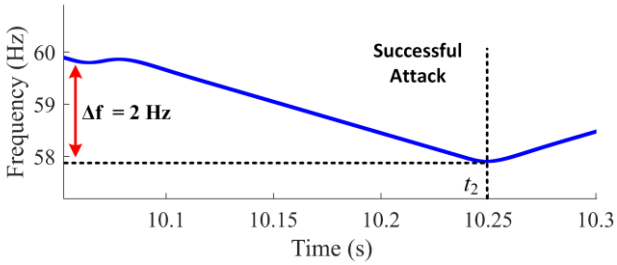

Fig. 4. System frequency dynamic: attack initiated at t_1 = 10s and ended after 0.0308 s. System become unstable at t_2 = 10.25 s, frequency deviation is more than 2 Hz and the frequency protection relays are triggered.

To have a better perspective on the effects of stealthy attacks on the understudy 14-bus PEDG, as a case study, a stealthy intrusion is applied on the governor of the synchronous generator. Fig. 2 depicts the attack signal model applied on the governor control. Similar attacks could happen on the DERs as well since the attacker could have access to the local controller of an inverter across of the PEDG. To show the effectiveness of attacks on the DERs, AC bus frequency dynamic is investigated from different aspects. Fig. 3 shows the frequency dynamic before and after the attack occurrence. The system frequency is 60 Hz during the normal operation of the system. At instant t_1 =10 s, the attack starts, and its duration is 0.0308 seconds. Considering the power system protection standards, frequency excursion of more than 2 Hz is defined as a risky violation for the system, thus the protection systems will be triggered, and the synchronous generator are separated from the system; consequently, this will increase the power-supply unbalance level and the entire energy system may experience the blackout if disturbances are not mitigated in timely manner. To analyze frequency dynamic with more details, the zoomed-in version of

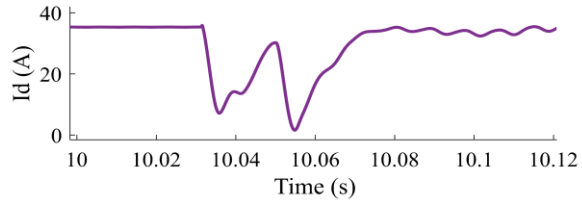

Fig. 5. *d*-component of the inverter current as the predefined state variable.

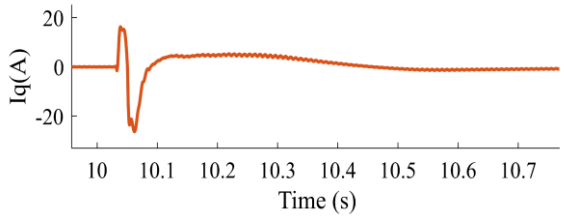

Fig. 6. *q*-component of the inverter current as the predefined state variable.

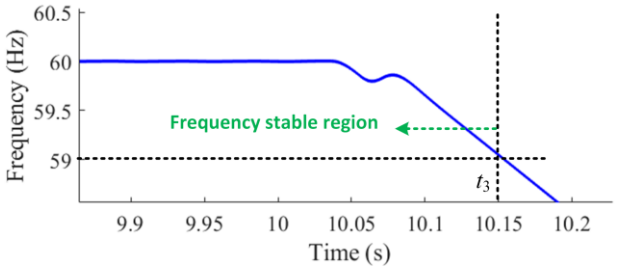

Fig. 7. System frequency dynamic: attack is done at t_1 = 10s and ended after 0.0308 s. System operates in stable region before t_3 = 10.15 s.

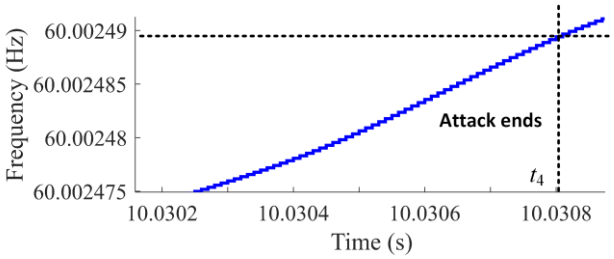

Fig. 8. Zoomed-in form of system frequency dynamic at the end of the attack duration: attack started at t_1 = 10s and ended at t_4 = 10.0308 s. system is stable when attack is ended, and the supervisory control layer cannot detect stealthy attack.

Fig. 3 is illustrated to accurately demonstrate system dynamics during the attack. Fig. 4 shows that after 0.25 s, the system is not stable, and the relays have been activated. As expected in stealthy attacks, state variables are diverged faster than the measured variables. These fast divergences trigger the local protection. Consequently, cascaded inverters tripping may occur which results in major blackout. This significant unbalance will result in huge frequency excursion and the supervisory layer is not able to take any protective action for restoring the system frequency. For describing this scenario, two state variables of the system which are *q* and *d* components of the inverter currents are shown in Fig. 5 and Fig. 6. As seen, the state variables have diverged faster than the observable variables to the supervisory controller which are the frequency and voltage of the AC bus. To shed light on this event, the frequency behavior of the system

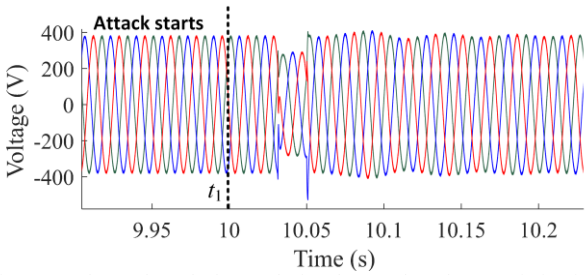

Fig. 9. AC bus voltage before and after the attack, voltage variation is in the acceptable standard range during the attack.

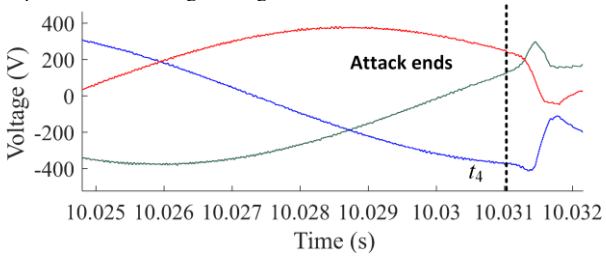

Fig. 10. System frequency dynamic: attack occurs at t_1 = 10s and ends at t_4 = 10.0308 s. System becomes unstable after 0.25 s due to the large frequency deviation.

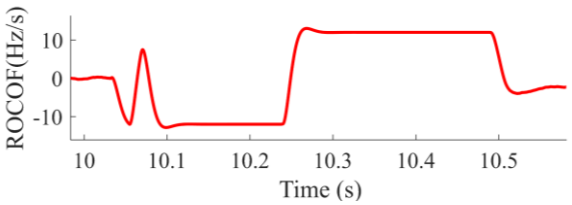

Fig. 11. Rate of change of frequency during stealthy attack

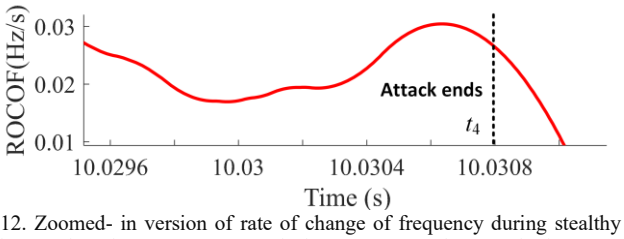

Fig. 12. Zoomed- in version of rate of change of frequency during stealthy attack. Attack ends at t_4 = 10.0308s, before t_4, ROCOF has standard pattern, so the relays will not be sensitive during the attack.

during attack interval are shown in Fig.7 and Fig. 8. Fig. 7 states that before reaching to t_3 = 10.15 s, the supervisory controller cannot detect that any attacks on the grid while Fig. 5 and Fig. 6 illustrate that the state variables have violated the standard ranges after the attack ends at t_4 = 10.0308 s.

Fig. 9 and Fig. 10 attest that the AC bus voltage variations remain in an standard range while the state variables have been diverted. Moreover, ROCOF are seen in Fig. 11 and Fig. 12. These figures demonstrate that during the attack, ROCOF is negligible too; thus, the supervisory control will not observe the stealthy attacks while state variables are violating the standard ranges. This case study demonstrates the significance to have a self-learning control scheme for mitigating the impact of unobservable intrusions such as the stealth attack presented in this section. The proposed shadow controller brings an extra

layer of intelligence to the supervisory layer for mitigating the unobservable stealthy attacks via a self-learning mechanism.

IV. The Proposed ANN-based Shadow Control Framework

To mitigate the consequences of the stealthy attacks on the DERs of the PEDG, the system cannot rely on the high inertia synchronous generators, since by the time they catch up with the amount of the lost generation due to a cyber event, the frequency relays are triggered and the system has faced a large-scale blackout. The proposed solution in this paper employs the fast controller of the BESS to cope with the active power lost. High-bandwidth control schemes e.g., model predictive control (MPC) can be utilized to implement primary control layer for DERs with fast dynamic response. The proposed shadow control framework provides corrective active power for healing the system at very fast timescale, thus the primary control layer of DER should have high bandwidth such as MPC. In this paper, the previously developed MPC is utilized as the primary PQ controller for the DERs [12]. Since the supervisory layer of the system would not be able to observe the stealthy attacks, an ANN-based shadow control scheme is designed which only needs feedback from the cluster frequency and its ROCOF. The proposed cohesive data-driven-based scheme so-called CDMSC observes the frequency of the cluster and the rate it is being changed. Since the only input that the proposed shadow control scheme requires is the frequency, it would not be compromised. By proving the active power reference for the BESS of the cluster, the frequency can be restored in an ultra-fast timescale, thus mitigating the stealth attack impact.

V. Training Mechanism

A two-layer feed-forward ANN is trained for providing the BESS power reference in response to potential disturbances. The major challenge is the training process for providing proper active power references to regulate frequency and ROCOF in a highly non-linear system such as PEDG. Fig. 13 shows the training performance of ANN with a negligible error of 0.0044. The performance is calculated based on the mean square error (MSE) criteria. It should be mentioned that the database has been divided randomly in a way that 70% of data is used for training process, 15% for validation, and 15% for testing process. For having a better understanding of training performance, the histogram of errors is plotted in Fig. 14. In this work 60,000 sample data have been provided for input and target data which are sufficient for a network to be trained. To clarify the training process, the root-causing of the frequency deviation should be investigated. The synchronous generator is the primary source for shaping the frequency profile of the islanded PEDG due to its rotating mass. Frequency will be affected by any changes in supply-demand balance based on the swing equation, which is given by,

$$T_m - T_e = 2H\,\Delta\dot{\omega} + D\,\Delta\omega \qquad (1)$$

where T_m, T_e are mechanical torque which drive the turbine and retarding torque because of electrical loads, respectively. D is defined as damping coefficient. $\Delta\omega$ and $\Delta\dot{\omega}$ are deviation from synchronous speed and acceleration,

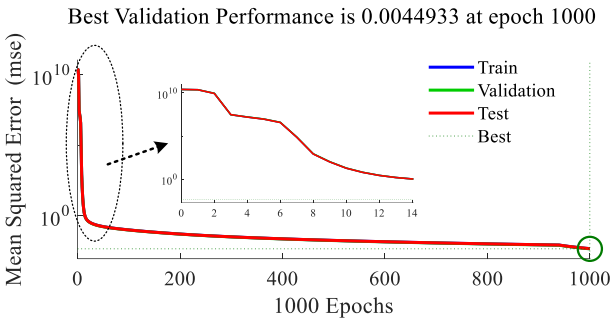

Fig. 13. Training performance of neural network by 1000 epochs, Bayesian regularization algorithm has been used for training.

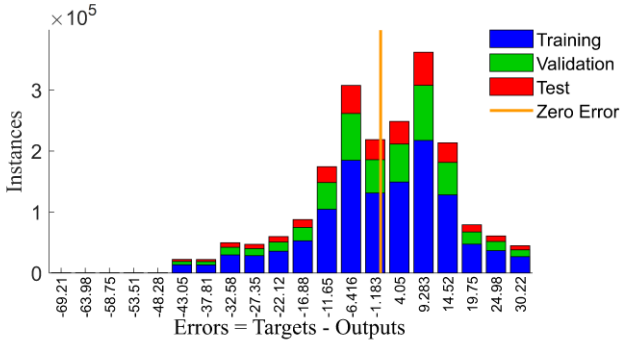

Fig. 14. Histogram of the differences between target values and output values

respectively. Converting the torque parameter to power and ignoring the damping factor, swing equation is given by,

$$P_m - P_e = J\omega_m\left(\frac{d}{dt}\left(\frac{d}{dt}(\theta_m)\right)\right),\ \theta_m = \omega_s t + \delta_m \qquad (2)$$

where P_m , P_e and ω_m are the mechanical power, electrical power, and angular velocity of the rotor, respectively. $J\omega_m$ is defined as the inertia constant of machine at synchronous speed of ω_s . Also, θ_m is defined as the angular position of the rotor with respect to a stationary axis and δ_m is the angular position with respect to the synchronously rotating reference frame. Equation (2) can be written based on the kinetic energy of rotating mass of rotor, which is given by,

$$\begin{aligned} P_m - P_e &= \frac{d}{dt}(E_k),\ E_k = \frac{1}{2}J\left(\omega_m\right)^2 \\ P_m - P_e &= J\omega_m\frac{d}{dt}(\omega_m),\ \Delta P = (4J\pi^2)f\frac{d}{dt}(f) \end{aligned} \qquad (3)$$

where ΔP is the required power to be injected to the system if it has positive value. However, if this value is negative, the system has extra power and should be absorbed by energy storage systems. In (3), f is the system frequency and df/dt is defined as the ROCOF. The proposed ANN is learned by Bayesian regularization algorithm with thousands of epochs. Different models of frequency deviation are defined and used as the inputs of swing equation. Then, feasible solutions along with different inputs are registered in a database to be used as training data for ANN. Furthermore, different inertia constants are considered in swing equations. This fact makes the trained network as a promising tool for providing robust and fast power command.

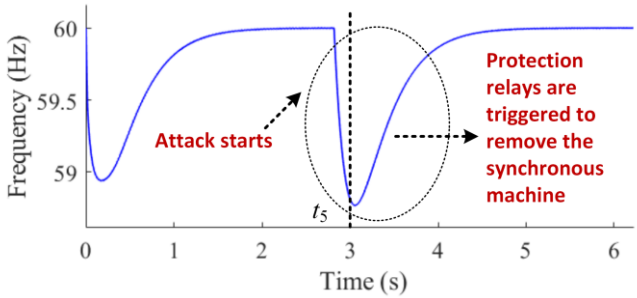

Fig. 15. AC bus frequency before and after the attack in absence of shadow control scheme, frequency variation is not in the acceptable standard range and the system collapses.

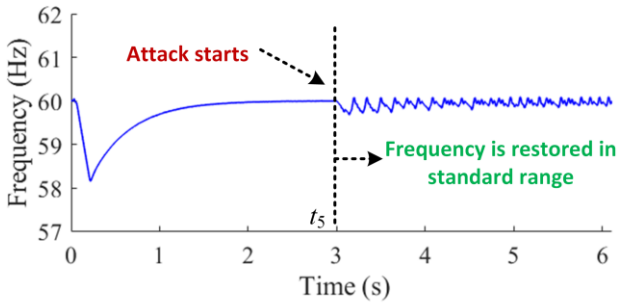

Fig. 16. AC bus frequency before and after the attack with employing the shadow control scheme, frequency variation is in the acceptable standard range and the system operates normally.

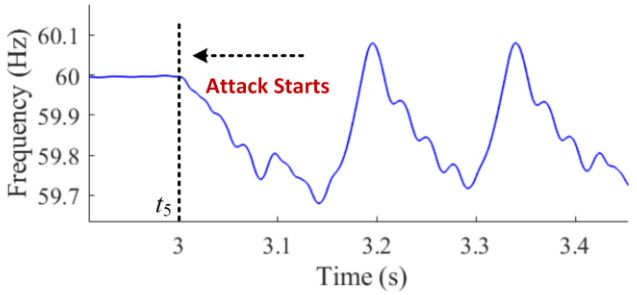

Fig. 17. Zoomed in version of AC bus frequency around t_5 = 3 s. Shadow controller is employed and the frequency variation is in the acceptable standard range.

VI. Result And Discussion

In this section, the functionality of the proposed event-triggered ANN-based shadow control scheme is validated on the understudy 14-bus PEDG. The proposed shadow control scheme observes the global variables of the system and is activated when the supervisory layer does not take an effective action to support the system during disturbances. As explained, when a stealthy attack occurs, the inverters' state variables are diverged and manipulated PV inverters are removed from the grid by the protection system. The proposed shadow control supports the system frequency stability by injecting the required active power. Fig. 15 shows the system frequency during grid's normal operation when there is no shadow controller. At t_5 =3s, a stealthy attack is occurred, and a major part of grid generation is lost. As seen, frequency severely drops and violates the

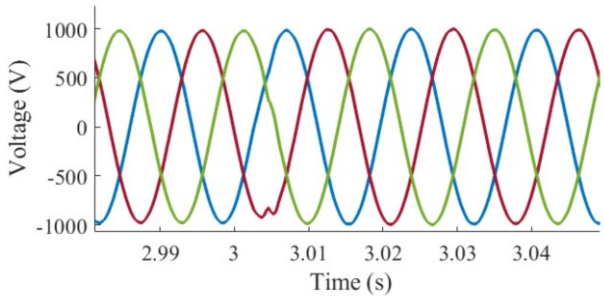

Fig. 18. AC bus voltage before and after the attack, voltage variation is in the acceptable standard range during the attack.

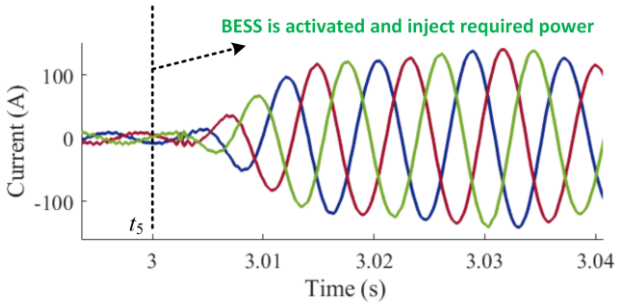

Fig. 19. Injected current by BESS to the grid after the attack, current is increased fast based on shadow controller command.

standard range. Although the synchronous machine tries to inject required amount of power but cannot support the grid in a timely manner due to its inherent slow dynamic response. In fact, the protection system removes the generator from the grid. To illustrate the effectiveness of the proposed shadow controller, the same stealthy attack scenario is repeated. Fig. 16 shows that sever frequency excursion is restored in a timely manner before the grid collapses. Fig. 17 shows the zoomed-in system frequency dynamics around t_5 = 3 s. This figure demonstrates that the frequency deviation is kept in the allowable range and the system operation continues without any challenges. Considering the harsh disturbances on the system, it is crucial to evaluate the voltage dynamics. Fig. 18 illustrate the AC bus voltage dynamic. As depicted, during the attack, voltage stability has been ensured due to the BESS's support guided by the shadow controller. The functionality of the shadow controller at the time of attack is illustrated in Fig. 19, where it illustrates the required injected current to the grid. As seen, the current is increased quickly while the grid codes are violated. Therefore, it is concluded that the proposed event-triggered technique can decline the ROCOF and nadir frequency in a proper time and the grid stability and resiliency is guaranteed during the potential disturbances.

VII. Conclusion

Vulnerabilities of the new energy paradigm, the PEDG, in the event of cyberattacks are among the most crucial challenges. Stealthy attacks, due to their unobservable natures by the supervisory layer, are among the most destructive cyber incidents. The stealthy attacks could deteriorate the balance between active power generation and consumption by pushing the DERs across the grid to go islanded. This will result in

severe frequency drop. Although the existing synchronous generators will try to compensate loss of generation, due to their high inertia and slow response, the frequency relays might trigger and cascading failure occurs across the grid, yielding to large-scale blackouts. To overcome this challenge, an event-triggered ANN-based shadow control scheme is proposed in this paper to ensure frequency restoration in the case of stealthy attacks. The proposed data-driven shadow control observes the frequency and its rate of change and behaves according to the real-time situation of the grid. In the case of loss of generation, the proposed shadow control is activated autonomously since it observes the frequency and ROCOF. Then, by accurately approximating the required active power, the BESS of located in the PEDG cluster compensates the active power. A two-layer feed-forward ANN is trained for the shadow controller. To test the proposed shadow control scheme, a real 14-bus PEDG with seven DERs is considered. The results without the proposed approach in the case of stealthy attacks illustrated divergence of the state variables yielding to unstable operation of the entire PEDG cluster. Results by employing the proposed ANN-based shadow control depicts significant improvements in the frequency restoration of the 14-bus system.

ACKNOWLEDGEMENT

This work was supported by the U.S. National Science Foundation under Grant ECCS-2033956.

REFERENCES

[1] B. Kroposki *et al.*, "Achieving a 100% Renewable Grid: Operating Electric Power Systems with Extremely High Levels of Variable Renewable Energy," *IEEE Power and Energy Magazine,* vol. 15, no. 2, pp. 61-73, 2017, doi: 10.1109/MPE.2016.2637122.

[2] A. Khan, M. Hosseinzadehtaher, M. B. Shadmand, S. Bayhan, and H. Abu-Rub, "On the Stability of the Power Electronics-Dominated Grid: A New Energy Paradigm," *IEEE Industrial Electronics Magazine,* vol. 14, no. 4, pp. 65-78, 2020, doi: 10.1109/MIE.2020.3002523.

[3] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security & Privacy,* vol. 7, no. 3, pp. 75-77, 2009, doi: 10.1109/MSP.2009.76.

[4] A. Khan, S. D. silva, A. Y. Fard, M. B. Shadmand, and H. A. Abu-Rub, "On Stability of PV Clusters with Distributed Power Reserve Capability," *IEEE Transactions on Industrial Electronics,* pp. 1-1, 2020, doi: 10.1109/TIE.2020.2987291.

[5] S. D'silva, A. Khan, M. F. Umar, M. B. Shadmand, and H. Abu-Rub, "On Stability of Hybrid Power Ramp Rate Control for High Photovoltaic Penetrated Grid," in *2020 IEEE Energy Conversion Congress and Exposition (ECCE)*, 11-15 Oct. 2020 2020, pp. 2806-2813, doi: 10.1109/ECCE44975.2020.9235460.

[6] A. Y. Fard, M. B. Shadmand, and S. K. Mazumder, "Holistic Multi-timescale Attack Resilient Control Framework for Power Electronics Dominated Grid," in *2020 Resilience Week (RWS)*, 19-23 Oct. 2020 2020, pp. 167-173, doi: 10.1109/RWS50334.2020.9241270.

[7] A. Y. Fard, M. Hosseinzadehtaher, M. B. Shadmand, and S. K. Mazumder, "Cyberattack Resilient Control for Power Electronics Dominated Grid with Minimal Communication," presented at the The IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG 2021), Chicago, IL, USA, 2021.

[8] A. Khan, M. Hosseinzadehtaher, M. B. Shadmand, D. Saleem, and H. Abu-Rub, "Intrusion Detection for Cybersecurity of Power Electronics Dominated Grids: Inverters PQ Set-Points Manipulation," in *2020 IEEE CyberPELS (CyberPELS)*, 13-13 Oct. 2020 2020, pp. 1-8, doi: 10.1109/CyberPELS49534.2020.9311538.

[9] M. Hosseinzadehtaher, A. Khan, M. B. Shadmand, and H. Abu-Rub, "Anomaly Detection in Distribution Power System based on a Condition Monitoring Vector and Ultra- Short Demand Forecasting," in *2020 IEEE CyberPELS (CyberPELS)*, 13-13 Oct. 2020 2020, pp. 1-6, doi: 10.1109/CyberPELS49534.2020.9311534.

[10] A. Bidram and A. Davoudi, "Hierarchical Structure of Microgrids Control System," *IEEE Transactions on Smart Grid,* vol. 3, no. 4, pp. 1963-1976, 2012, doi: 10.1109/TSG.2012.2197425.

[11] M. Hosseinzadehtaher, A. Khan, M. Easley, M. B. Shadmand, and P. Fajri, "Self-healing Predictive Control of Battery System in Naval Power System with Pulsed Power Loads," *IEEE Transactions on Energy Conversion,* pp. 1-1, 2020, doi: 10.1109/TEC.2020.3014294.

[12] 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,* vol. 57, no. 1, pp. 824-834, 2021, doi: 10.1109/TIA.2020.3037287.

[13] A. Hansen, J. Staggs, and S. Shenoi, "Security analysis of an advanced metering infrastructure," *International Journal of Critical Infrastructure Protection,* vol. 18, pp. 3-19, 2017.

[14] 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 2020, pp. 1-6, doi: 10.1109/KPEC47870.2020.9167599.

[15] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Transactions on Power Systems,* vol. 28, no. 2, pp. 1052-1062, 2013, doi: 10.1109/TPWRS.2012.2224144.

[16] P. Cheng, Z. Yang, J. Chen, Y. Qi, and L. Shi, "An Event-Based Stealthy Attack on Remote State Estimation," *IEEE Transactions on Automatic Control,* vol. 65, no. 10, pp. 4348-4355, 2020, doi: 10.1109/TAC.2019.2956021.

[17] X. He, X. Liu, and P. Li, "Coordinated False Data Injection Attacks in AGC System and Its Countermeasure," *IEEE Access,* vol. 8, pp. 194640-194651, 2020, doi: 10.1109/ACCESS.2020.3033566.

[18] M. Braun *et al.*, "The Future of Power System Restoration: Using Distributed Energy Resources as a Force to Get Back Online," *IEEE Power and Energy Magazine,* vol. 16, no. 6, pp. 30-41, 2018, doi: 10.1109/MPE.2018.2864227.

[19] J. Liu, Y. Miura, and T. Ise, "Comparison of Dynamic Characteristics Between Virtual Synchronous Generator and Droop Control in Inverter-Based Distributed Generators," *IEEE Transactions on Power Electronics,* vol. 31, no. 5, pp. 3600-3611, 2016, doi: 10.1109/TPEL.2015.2465852.

[20] "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003),* pp. 1-138, 2018, doi: 10.1109/IEEESTD.2018.8332112.

[21] H. Gu, R. Yan, and T. K. Saha, "Minimum Synchronous Inertia Requirement of Renewable Power Systems," *IEEE Transactions on Power Systems,* vol. 33, no. 2, pp. 1533-1543, 2018, doi: 10.1109/TPWRS.2017.2720621.

[22] S. Xu, Y. Xue, and L. Chang, "Review of Power System Support Functions for Inverter-Based Distributed Energy Resources- Standards, Control Algorithms, and Trends," *IEEE Open Journal of Power Electronics,* vol. 2, pp. 88-105, 2021, doi: 10.1109/OJPEL.2021.3056627.

[23] H. Huang and F. Li, "Sensitivity Analysis of Load-Damping Characteristic in Power System Frequency Regulation," *IEEE Transactions on Power Systems,* vol. 28, no. 2, pp. 1324-1335, 2013, doi: 10.1109/TPWRS.2012.2209901.