Novel Control Solutions for DoS Attack Delay Mitigation in Grid Connected and Standalone Inverters

Greidanus, Mateo; Sahoo, Subham; Mazumder, Sudip K; Blaabjerg, Frede

Published in:
2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)

DOI (link to publication from Publisher):
10.1109/PEDG51384.2021.9494230

Publication date:
2021

Document Version
Early version, also known as pre-print

Novel control solutions for DoS attack delay mitigation in grid-connected and standalone inverters

Mateo D. Roig Greidanus
Department of Electrical and Computer Engineering
University of Illinois Chicago
Chicago, USA
mgreid2@uic.edu

Subham Sahoo
Department of Energy Technology
Aalborg University
Aalborg, Denmark
sssa@et.aau.dk

Sudip Mazumder
Department of Electrical and Computer Engineering
University of Illinois Chicago
Chicago, USA
mazumder@uic.edu

Frede Blaabjerg
Department of Energy Technology
Aalborg University
Aalborg, Denmark
fbl@et.aau.dk

***Abstract*—This paper introduces two novel control solutions, which allow localised delay compensation for grid-connected and standalone inverters. As the prediction horizon of the existing controllers are quite small as compared to large communication delays and information unavailability due to denial-of-service (DoS) attacks, the proposed strategy offers a robust delay mitigation range using localized dynamics. Its design philosophy is leveraged via a prediction policy using the inner control loop dynamics. Based on different control objectives in grid-connected and standalone mode, the proposed solutions have been augmented into the control system accordingly. Finally, its robustness under various communication delay and DoS attacks have been tested.**

***Index Terms*—Denial-of-service, hierarchical control, mitigation, inverter, communication network**

I. Introduction

Denial-of-service (DoS) attacks is among the well-discussed cyber attacks on hierarchical controllers of distributed energy resources (DERs) in connection with the electrical grid [1]. Such attacks are characterized by affecting the availability of the information on the communication layer [2]. However, it is in the physical layer where the effects of such attacks are essentially noticed.

DoS-type cyber attacks are notorious for being simple to perform and difficult to detect in their initial states [3]. This inherent characteristic, however, is highly noticeable depending on the number of nodes and the degree of distribution of the communication network. The complexity of the communication framework in DERs is intrinsically linked to the number of inverter modules, the number of communication nodes, and the amount of exchanged information [4]. Therefore, as the number of control layers, inverter systems operating in parallel, and the number of smart meters increase, the complexity of the communication system also increases. Hence, DoS attack can be easily conducted without being detected.

In cyber-physical systems of DERs, the quality of the energy delivered depends directly on unbiased sharing of information between the control agents. Hierarchical control systems are generally designed to meet different requirements of the power grid. However, the functions of the controllers vary depending on the architecture of the electrical network and how they are connected to it [5]. Thus, the effects of a DoS attack on the communication of such systems may degrade the delivered power and may pronounce into instability later [6]. Regardless of the variables affected, the effects of the cyberattack are linked to the nature of the connection of the DERs to the power grid. Strictly speaking, if the DERs are tied to the power grid, the hierarchical control structure works differently than a system islanded from the grid. Likewise, the effects of a cyberattack on the communication network in grid-tied DER systems are different from the effects of similar intrusions on an isolated electrical network.

To deal with DoS attacks with prohibited information, current research efforts focus on three categories: (a) by investigating the methodology for the attack and challenges [7]; (b) on techniques for detection of such occurrences [8], [9]; (b) and mitigating strategies to remove such attacks [10], [11]. The resilient operation of the control system has been studied for DERs connected to the grid or operating in standalone mode [12], [13]. However, due to the different nature of the structures, there is still a lack of work that shows a resilient operation for both frameworks. Taking that into account, this work aims to show robust strategies that mitigate the delay of DoS attack effects in both architectures.

Since the cyber intricacies can be stochastic in nature, a rapid delay mitigation technique can be an efficient solution to handle the said issue. This paper proposes the use of event-triggering techniques to detect an abnormal delayed response in the communication system. Thus, if a limit is violated, a

978-0-7381-4237-1/21/$31.00

new control action is requested from the proposed controllers to mitigate the effects of the attack until normal operation is resumed.

II. Problem Description and Review

The cyber layer, in intelligent power generation systems, guarantees the functioning of the system within the standards established by the power grid operator. The cyber layer comprehends the control algorithms, the calculation of the data, and the exchange of information by the communication networks. All of these parts command, together, the physical layer to ensure that the energy is effectively delivered to the load. Howbeit, both the communication and the concentration of data in the controllers make the system vulnerable to cyber-attacks [14].

The communication interfaces of the cyber layer send and receive messages under a periodic time-lapse. This communication delay, also called latency, indirectly influences the processing of data by control agents. In terms of control, studies have already shown that, depending on its size, the communication delay has a greater impact on the dynamic response of DER systems [15], [16]. Taking this into account, delays maliciously inserted into the communication network of smart grids aim to exploit this effect.

In hierarchical controllers, which relates to both systems studied in this work, the most internal control loops generally have higher bandwidth and are closer to electrical devices. Local controllers are generally distributed and are highly dependent on aggregated or centralized control agents at higher levels. Higher-level controllers usually send references to be followed by the local controller. Thus, a distortion of the information received by the local controller might have a critical effect on the output response of the system.

Therefore, in this work, for both scenarios considered, assume a time-varying heterogeneous delay in communication network described by τ_d. Also, assume that the delay attacks variables on the secondary controller. This control layer works on trajectory correction of the references received by the local primary controller. Then, the signals are distorted by delay in the form

$$x_d[\bar{t}] = \begin{cases} x[t] & \text{if } t \in [0, t_A) \\ x[t-\tau_d] & \text{if } t > t_A \end{cases} \tag{1}$$

where t_A is the time instant when the attack happens.

It is evident that without a strategy aimed at mitigating the delay, the primary controller would be completely inert and will be unable to compensate for the distorted reference signal. Besides, without an attack detection strategy, the local controller would still be operating under the imposed conditions. Yet, the primary controller is usually the one with the highest bandwidth and highest processing speed [17]. This control layer could clearly take much faster actions than the others to mitigate the attack. However, to do so, the primary controller needs to leave its role as a slave control agent to take an active role in the countermeasure process against the DoS attack. This is one of the main ideas from this work and the next sections will present strategies to mitigate the delay in this regard.

III. Proposed Control Strategies

The strategies to mitigate DoS cyber attacks proposed in this article have characteristics in common. Both are event-driven and have adaptive control mechanisms to alter the control conditions during DoS cyber attacks. Fig. 1 gives a conceptual view of how the event-triggering system would work. Once the communication might be compromised, resilient architectures must have monitoring device systems that, by comparison, should have a metric to identify abnormal behavior. For example, the time lapse for information to arrive or loss of data packets are a clear indication that the system does not behave as expected. Therefore, in this section, alternatives for mitigating attacks in both scenarios will be covered as an outlook.

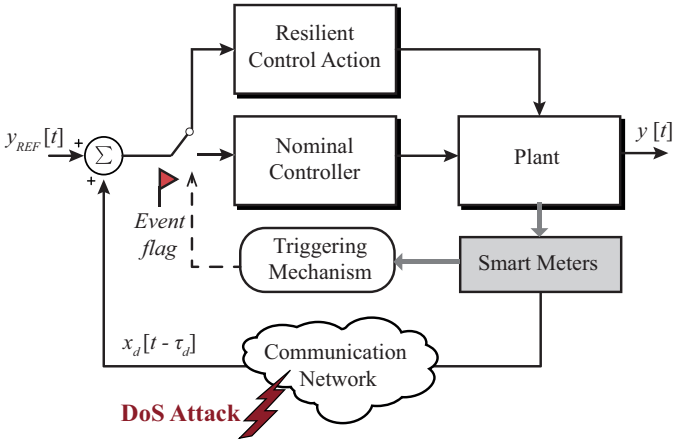


Fig. 1: Schematic of an event-trigger action for the local controller

A. Mitigation of the delay in grid-tied inverter system

The DERs connected to the mains power grid works accordingly as per the commands of a central controller. Since these systems operate in grid-following mode, the variables depend on the voltage and frequency imposed by the electrical network. Still, from a distributed point of view, when these systems operate far from the power grid, there are line impedances between the inverter output and PCC. These impedances cannot be overlooked in the energy delivery process. Taking this into account, the secondary controllers play the role of adjusting the voltage drop and the phase difference for accurate reference tracking. However, if the adjustment values sent by the secondary controller are delivered incorrectly, the system will suffer an imbalance in the supplied energy. Considering this scenario, an attack mitigation strategy is proposed after the identification of the abnormal behavior and evaluating the convergence of the delivered power within a threshold. Then, assuming a control law for the triggering mechanism such that

$$\gamma_{flag} = 1 \iff \{\|y_{REF}[t] - y_d[\bar{t}]\|_2 > \delta \mid \tau_i\} \quad \text{for a time interval } \tau_i \in \{a_i \leq \tau_i < b_i\} \tag{2}$$

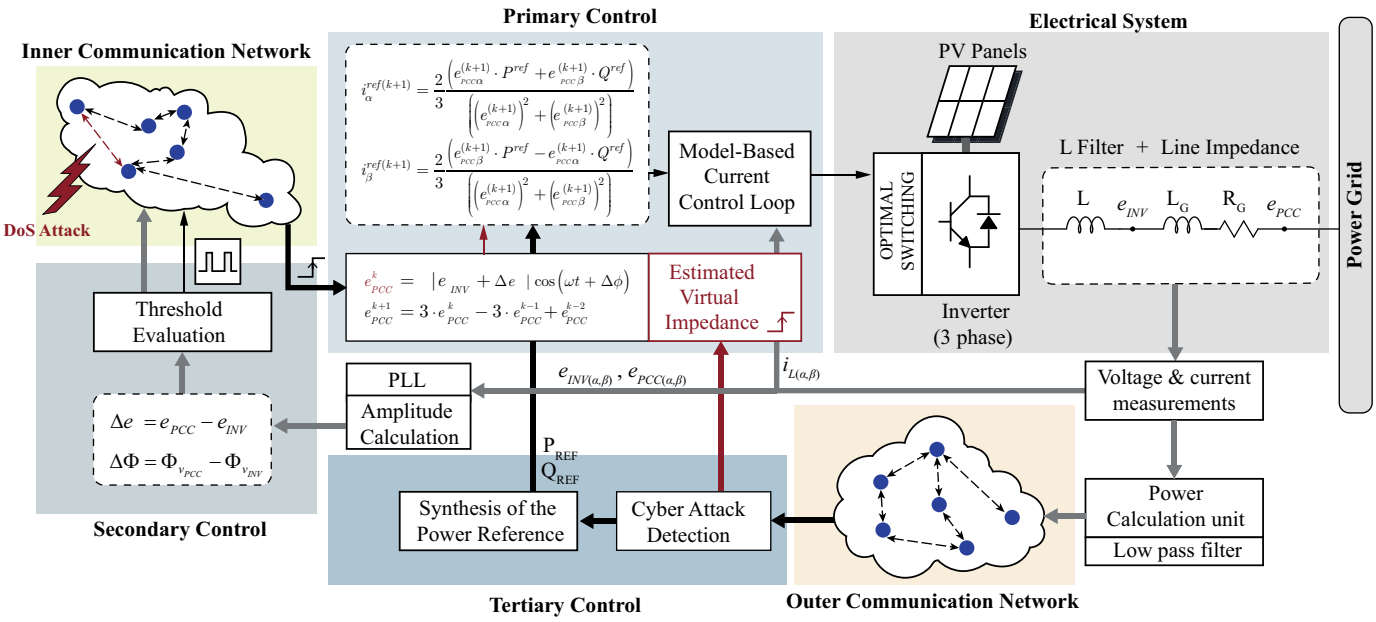


Fig. 2: Schematic of the proposed control strategy for standalone inverters to provide resilience against communication delay – the event-driven strategy adapts the control to estimate voltage on the PCC by Virtual Impedance instead of using the secondary controller during the DoS attack.

where δ is a tolerated threshold within the system can operate, and a_i and b_i define the time interval condition that needs to be attended for the response to be considered normal.

Thus, to mitigate DoS attacks on the system's communication network, this work uses a strategy based on the use of a virtual impedance internal to the primary controller. The method temporarily deflects the signal sent by the secondary controller when estimating the voltage, using a virtual impedance instead. Fig. 2 shows the complete control system considering the proposed strategy.The estimation of the virtual impedance is done in a static manner, in α/β components, based on the measurements of the voltage and current after the inverter output filter such that

$$e_{PCC,\alpha}[t] = -R_{VI} \cdot i_{L,\alpha}[t] - X_{L_{VI}} \cdot i_{L,\alpha} + e_{INV}[t] \quad (3)$$

$$e_{PCC,\beta}[t] = -R_{VI} \cdot i_{L,\beta}[t] - X_{L_{VI}} \cdot i_{L,\beta} + e_{INV}[t] \quad (4)$$

Fig. 3 shows some results of the system operating nominally and under the effect of the DoS attack when no protective measures have been taken. In Fig. 4, the action of the virtual

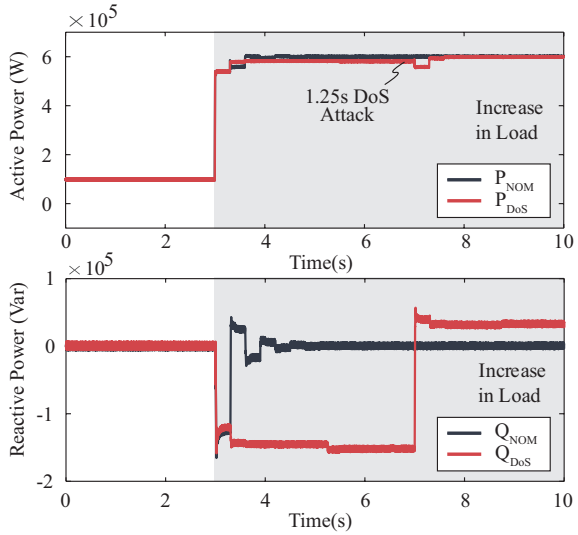


Fig. 3: Comparison of the waveforms of active and reactive power delivered to PCC after half-load step, between nominal condition (P_{NOM} and Q_{NOM}) and during a DoS attack of 1.25s (P_{DoS} and Q_{Dos}).

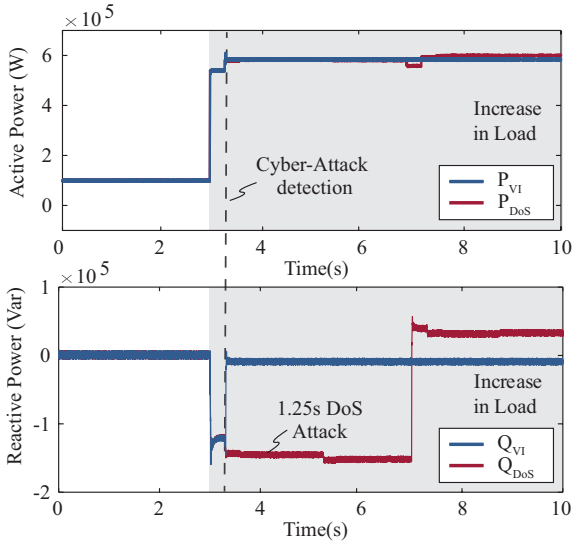


Fig. 4: Comparison of the waveforms of active and reactive power delivered to PCC after half-load step, during a 1.25s DoS attack and when the virtual impedance takes part after the cyber attack detection (P_{VI} and Q_{VI}).

impedance strategy on the primary controller is verified as soon as the abnormality in the system is detected. The attack was induced in the phase shift variable sent by the secondary controller. In this condition, the degradation due to the DoS attack is perceived mainly in the reactive power delivered to the PCC. Thus, comparing the results in the two figures, it shows that the strategy can effectively reduce the effects of the attack verified in the output power.

The strategy using virtual impedance is a temporary alternative and should not meet the control methodology at all times. Due to the distributed nature of the DER system, the choice of impedance values would need to be well chosen and, even so, could produce an undesirable static error in the active power delivered. This last fact justifies the use of the secondary controller in a normal situation. However, it is efficient to mitigate the effects of the degradation of the delivered energy in a short period of time. Hence, giving time for the operator to take any action to restore the system.

B. Mitigation of the delay in isolated network

An example of the system (shown in Fig. 5) with N standalone inverters is considered here, which communicate with each other using a cooperative cyber graph. All DGs are interconnected with each other via tie-line parameters given by R_{ij} and L_{ij} to achieve proportionate active power and reactive sharing. The delayed measurements $x(t-\tau_d)$ mandate prediction of their position in the future. Since the timescale of operation of the secondary controller is generally in seconds, a delay exceeding the predefined limits in this range will lead to oscillatory instability due to continually missed updates and will consequently compromise its performance. This mandates the need of a delay mitigation strategy to compensate for the communication delay between multiple DGs. To minimize the dependence on these factors, this paper firstly exploits the PI consensusability law [18] to predicate the response of the active and reactive control layer in the presence of a disturbance. As the delay compensation occurs in the secondary layer, the corresponding error signals $e_i^{vd}(t)$ and $e_i^{vq}(t)$ prior to the voltage control loop is firstly downsampled to $e_i^{d}(t)$ and $e_i^{q}(t)$, respectively (as shown in Fig. 5) using

$$e_i^d = \sum_{b=0}^{B-1} e_i^{vd}[nD-b].h[b] \tag{5}$$

$$e_i^q = \sum_{b=0}^{B-1} e_i^{vq}[nD-b].h[b] \tag{6}$$

where $h[b]$ is an impulse response with B as the window length and D being the downsampling factor. It is worth notifying that downsampling is a common resampling tool, which decimates the input signal by D sample to reduce the resolution. It is often carried out to decrease the memory requirements. In this context, it is carried out to match the dynamic performance of the error quantities prior to the voltage control loop e_i^{vd}, e_i^{vq} and the error prior to the secondary controller u_k. This step is mandated to synchronize the abovementioned signals due to the multi-time scale property. A pictorial description of the downsampling operation is provided in Fig. 6, where e^{Volt} is downsampled into two output signals, where the new resolution is scaled by two values of D, i.e, 2 and 4.

To affirm the presence of large and random delays, the downsampled signals in '(5) and (6) are compared with the local cooperative inputs $u_i^p(t)$ and $u_i^q(t)$ in the local instant.

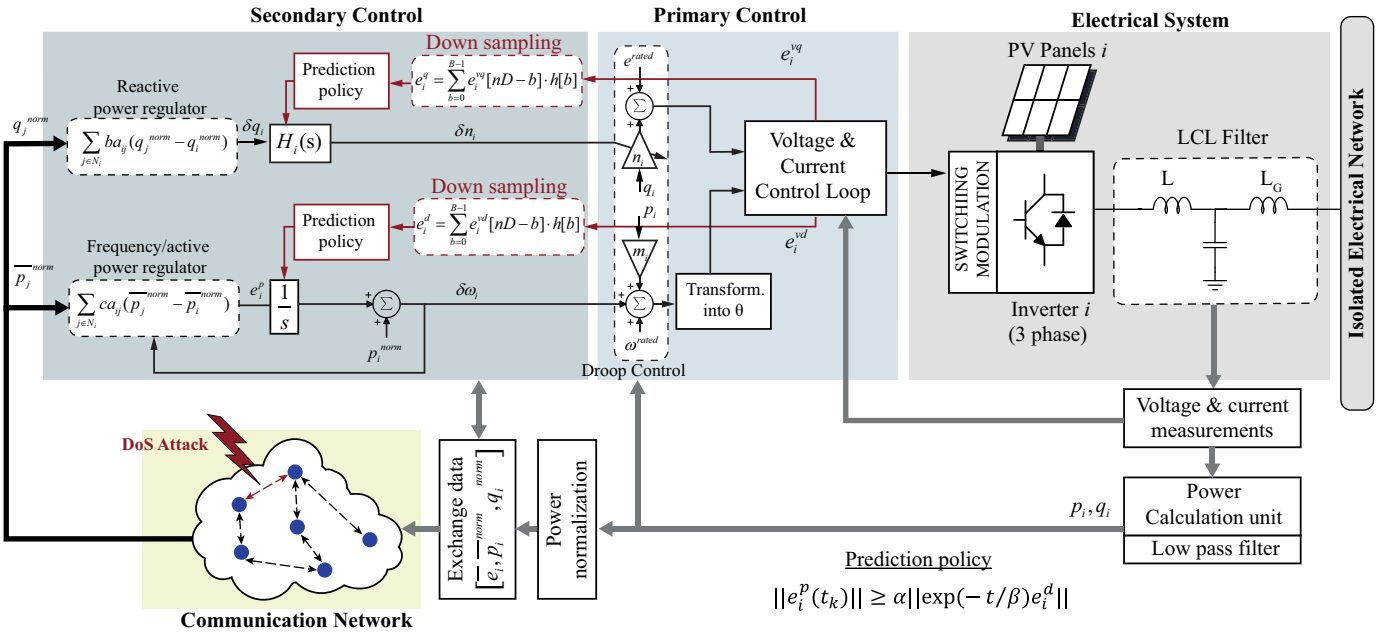


Fig. 5: Schematic of the proposed control strategy for standalone inverters to provide resilience against communication delay – the prediction policy provides a decisive input if the down-sampled input can be used. The down-sampling input can be tuned by varying the down-sampling factor D and B as the window length.

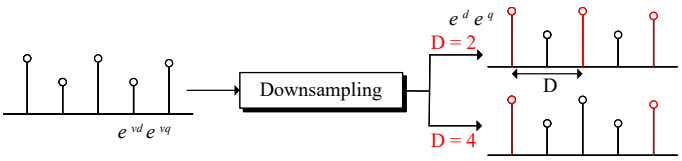


Fig. 6: Downsampling of $\{e^{vd}, e^{vq}\}$ into a decimated output $\{e^{d}, e^{q}\}$, respectively – Higher the value of the scaling factor D, its resolution keeps decreasing.

After this stage, the *prediction policy* operates to reconstruct the final delay compensation signals in $\mathbf{e}_i(t_k) = \{e_i^p(t_k), e_i^q(t_k)\}$ locally based on the condition

$$\mathbf{e}_i(t_k) = [e_i^p(t_k), e_i^q(t_k)] - \mathbf{u}_k \tag{7}$$

Finally, this error is then fed into the *prediction policy* stage; which reconstructs another signal to compensate for large delays. Hence, the prediction policy condition can be given by

$$||\mathbf{e}_i(t_k)|| \geq \alpha ||\exp(-t/T)\mathbf{e}_i^{dq}|| \tag{8}$$

where $\mathbf{e}_i^{dq} = [e_i^d \;\; e_i^q]$, α is a tunable parameter and $T(=K_p/K_i)$ is the controller time constant of $H_1(s)$ and $H_2(s)$ PI control loop. Finally, if the condition in (8) is satisfied, then it generates triggers. These triggers are then used to reconstruct $\mathbf{e}_k(t_k)$ using a `Sample and Hold` block with t_k as the triggering instant. Finally, the reconstructed signals in $\mathbf{e}_i^{reconstruct}(t_k)$, acting as the delay compensating signals, are fed back into the secondary voltage control loop via tunable gains k_1 and k_2, respectively. These model-free predicted inputs are given by

$$e_i^{delp}(t_k) = k_1 e_i^{reconstructp}(t_k) \tag{9}$$

$$e_i^{delq}(t_k) = k_2 e_i^{reconstructq}(t_k) \tag{10}$$

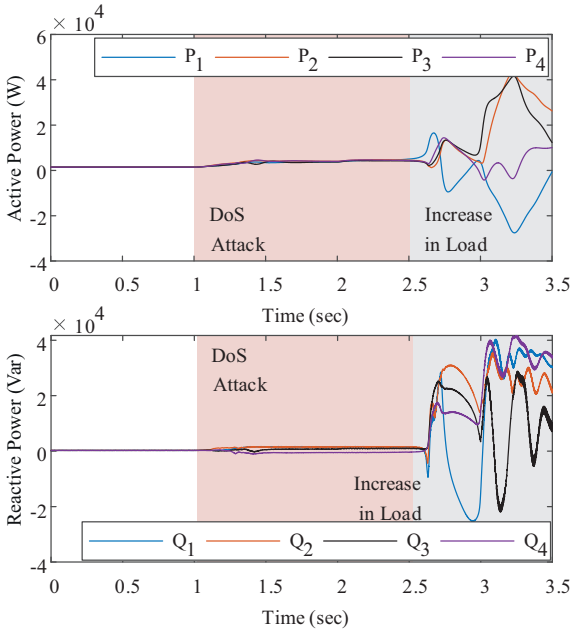
where, $\mathbf{e}_i^{reconstruct}(t_k) = [e_i^{reconstructp}(t_k), \; e_i^{reconstructq}(t_k)]$. Finally, as shown in Fig. 5, these inputs are added back into the control inputs of the secondary controller using:

$$u_i^{pf}(t) = u_i^p(t) + e_i^{delp}(t_k) \tag{11}$$

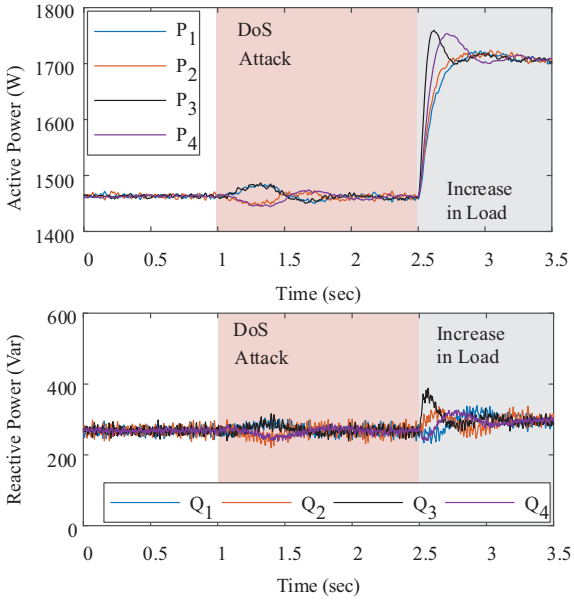
$$u_i^{qf}(t) = u_i^q(t) + e_i^{delq}(t_k) \tag{12}$$

where, u_i^{pf} and u_i^{qf} are the final secondary control inputs designed using the proposed prediction policy. The efficacy to handle large delays can be accounted specifically to the *prediction policy*; where the error calculation stage validates an interruption in updated information. As a result, the prediction horizon due to the proposed strategy becomes much larger compared to the existing approaches.

In the system outlined in Fig. 5 with $N = 4$ standalone parallel inverters, the performance of the proposed delay mitigation technique is evaluated under a maximum communication delay of 0.65 sec in Fig. 7. In Fig. 7(a), the performance of the parallel controllers is affected when a DoS attack is conducted on the incoming communication links of DG I. As a result, the



(a) without the proposed controller



(b) in the presence of proposed controller

Fig. 7: Performance of $N = 4$ standalone inverters under a communication delay of 0.65 sec when a DoS attack is conducted at t = 1s

primary response is followed which leads to drop in frequency following the loss of spanning tree connectivity. However, with the increase in load, the system becomes unstable due to oscillating active and reactive power. However, due to the proposed robust *prediction policy*, the performance in attaining proportionate active and reactive power sharing is significantly improved for the same communication delay even for DoS attacks. This improvement can be attributed to the reconstructed signals $e_i^d(t_k)$ and $e_i^q(t_k)$ for every disturbance.

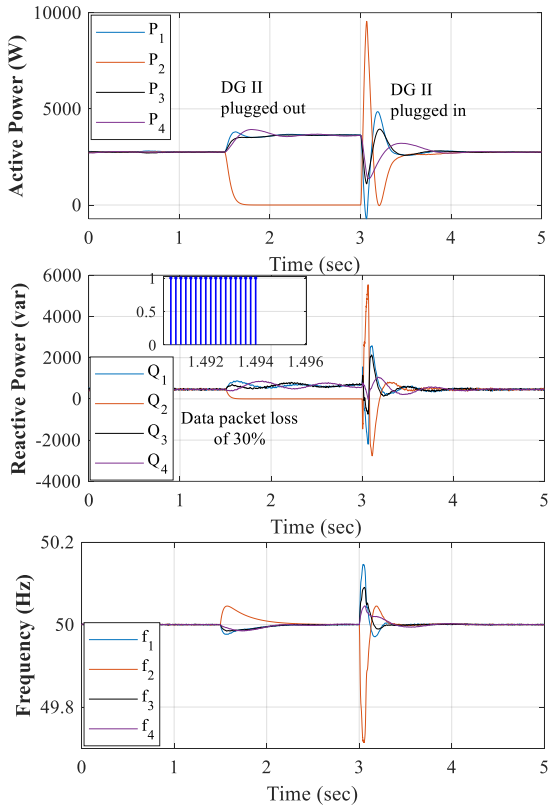


Fig. 8: Performance of $N = 4$ standalone inverters under a communication delay of 0.8 sec and 30% data packet loss when a DoS attack is conducted at t = 1.5 sec.

As soon as the error calculation formalizes that a large delay is prohibiting the next update of measurements, the reconstructed signals using the proposed delay mitigation controller restore consensus between each signal.

In the same system with $N = 4$ standalone DGs, the performance of the proposed delay mitigation strategy is tested in Fig. 8 under a large communication delay of 0.8 sec alongside 30% data packet loss in the communication channel between two DGs. Furthermore, a large signal disturbance in the form of plug and play capability of a DG is performed to test the operational reliability when one of the DGs is plugged out. It can be seen in Fig. 8 that despite the presence of large delay, the proposed *prediction policy* ensures a formidable response, which allows proportionate active power sharing when DG II is plugged out. Furthermore when DG II is plugged in, all standalone inverters resume sharing equally. It can also be seen that the reactive power is proportionately shared without any seemingly steady-state convergence problems.

IV. Discussion and Concluding Remarks

This paper proposes two novel delay mitigation strategies to handle communication delays due to DoS attacks in networked systems for grid-connected and islanded parallel inverters by reconstructing a compensating signal locally. For the grid following inverter, this article proposes an adaptive control strategy, triggered by an attack identification event, to temporarily replace the conventional control and reduce the degradation of the energy supplied to the grid. Whereas for the grid-forming inverter, an event-based reconstructed downsampled signal is used to provide resilience against large delays.

It intends to show that different strategies are necessary to deal with communication delays due to attacks in the control system, depending on the architecture of the DERs in relation to the network. Resilient control systems have characteristics and peculiarities intrinsically related to the physical layer. Therefore, there is no single design methodology for either detecting or mitigating cyber attacks. However, this paper is centralized on two basic conditions that help to address this issue. The first is that detection and mitigation are two processes that need to work together. And the second is that the bandwidth of the control system plays a crucial role in the speed of the DoS attack mitigation operation on hierarchical controllers. Therefore, whatever the hierarchical controller or strategy, the concern with these two issues is crucial to find out robust countermeasure solutions to cyberattacks.

Acknowledgment

This material is based in part upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technology Office (SETO) Award Number DE-EE0009026. This work is also supported in part by the U.S. National Science Foundation under award number 1644874.

References

[1] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks*, vol. 169, p. 107094, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128619311235

[2] S. N. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6522–6530, 2019.

[3] B. Kumar Joshi, N. Joshi, and M. Chandra Joshi, "Early detection of distributed denial of service attack in era of software-defined network," in *2018 Eleventh International Conference on Contemporary Computing (IC3)*, 2018, pp. 1–3.

[4] S. K. Mazumder, K. Acharya, and M. Tahir, "Towards realization of a control-commnunication framework for interactive power networks," in *2008 IEEE Energy 2030 Conference*, 2008, pp. 1–8.

[5] S. Ansari, A. Chandel, and M. Tariq, "A comprehensive review on power converters control and control strategies of ac/dc microgrid," *IEEE Access*, vol. 9, pp. 17 998–18 015, 2021.

[6] X. Zhong, I. Jayawardene, G. K. Venayagamoorthy, and R. Brooks, "Denial of service attack on tie-line bias control in a power system with pv plant," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 1, no. 5, pp. 375–390, 2017.

[7] A. Sundararajan, A. Chavan, D. Saleem, and A. I. Sarwat, "A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security," *Energies*, vol. 11, no. 9, 2018. [Online]. Available: https://www.mdpi.com/1996-1073/11/9/2360

[8] S. Liu, P. Siano, and X. Wang, "Intrusion-detector-dependent frequency regulation for microgrids under denial-of-service attacks," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2593–2596, 2020.

[9] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters–challenges and vulnerabilities," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2019.

[10] M. Long, C.-H. Wu, and J. Hung, "Denial of service attacks on network-based control systems: impact and mitigation," *IEEE Transactions on Industrial Informatics*, vol. 1, no. 2, pp. 85–96, 2005.

[11] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Multilayer resilience paradigm against cyber attacks in dc microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 3, pp. 2522–2532, 2021.

[12] A. Bidram, B. Poudel, L. Damodaran, R. Fierro, and J. M. Guerrero, "Resilient and cybersecure distributed control of inverter-based islanded microgrids," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 3881–3894, 2020.

[13] S. Gholami, S. Saha, and M. Aldeen, "A cyber attack resilient control for distributed energy resources," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017, pp. 1–6.

[14] S. Mazumder, A. Kulkarni, S. Sahoo, F. Blaabjerg, A. Mantooth, J. Balda, Y. Zhao, J. Ramos-Ruiz, P. Enjeti, P. Kumar, L. Xie, J. Enslin, B. Ozpineci, A. Annaswamy, H. Ginn, F. Qiu, J. Liu, B. Smida, C. Ogilvie, J. Ospina, C. Konstantinou, M. Stanovich, K. Schoder, M. Steurer, T. Vu, L. He, and E. Pilo de la Fuente, "A review of current research trends in power-electronic innovations in cyber-physical systems," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–1, 2021.

[15] M. A. Setiawan, F. Shahnia, R. P. Chandrasena, and A. Ghosh, "Data communication network and its delay effect on the dynamic operation of distributed generation units in a microgrid," in *2014 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, 2014, pp. 1–6.

[16] S. Liu, X. Wang, and P. X. Liu, "Impact of communication delays on secondary frequency control in an islanded microgrid," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 4, pp. 2021–2031, 2015.

[17] A. K. Sahoo, K. Mahmud, M. Crittenden, J. Ravishankar, S. Padmanaban, and F. Blaabjerg, "Communication-less primary and secondary control in inverter-interfaced ac microgrid: An overview," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–1, 2020.

[18] R. Carli, A. Chiuso, L. Schenato, and S. Zampieri, "A pi consensus controller for networked clocks synchronization," *IFAC Proceedings Volumes*, vol. 41, no. 2, pp. 10 289–10 294, 2008.