Identification of a Delay Attack in the Secondary Control of Grid-Tied Inverter Systems

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

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

Nanditha Gajanur
Department of Electrical and Computer Engineering
University of Illinois at Chicago
Chicago, USA
ngajan2@uic.edu

***Abstract*—This work is developed for the identification of a denial-of-service cyberattack on the secondary controller of inverter systems which is connected to the power grid. The identification is made through the dynamic response of the reactive power (Q) of the system under attack. By observing the dynamic characteristic of Q, it is possible to correlate the attack with the nominal response of the hierarchical controller. The article shows that the occurrence of the attack can be identified through a supervisory control that runs a model in parallel. The article argues that after an early identification of the attack, a local controller can take action to mitigate its effects on the system's response.**

***Index Terms*—Identification, Denial-of-Service, Cyber attack, Reactive power**

I. Introduction

Smart systems of grid-tied distributed energy resources are characterized by the use of information and communication technologies. The whole power generation is interconnected in the physical and cyber layers such that any change in one layer of the system has effects in the other. Meanwhile, such intelligent structures are expected to be resilient, resistant to attack or external interference, capable of self-healing, and, meanwhile, must supply high-quality power to the network [1], [2]. On that account, the complexity of the interconnections is directly related to the degree of intelligence required, while adding to the vulnerabilities of the system [3].

In grid-connected generation systems, hierarchical controllers are generally employed to ensure that the energy generated is fully supplied at the point of common coupling (PCC) to the grid [4], [5]. The control structure, in turn, makes use of sensors and measurement equipment. Each step of monitoring and control of the system variables employs the use of communication with known protocols and latencies. Thus, the cyber layer plays an important role in sending data and connecting the algorithms that control the flow of energy supplied to the power grid. Then, it is not difficult to assess that the vulnerability of a communication system to cyberattacks is correlated to the reliability and resilience of the overall system [6].

There are well-established standards that regulate the operation of inverters connected to the electrical network, as well as others that regulate communication systems. Yet, there is a report of a lack of integration between standards when there is a concern with the resilience of such systems to possible cyber-attacks [7], [8]. Taking this into account, some recent articles have discussed some cyber-attack scenarios, challenges, and multilayered protection strategies to mitigate the impact of cyber-attacks on DERs systems, whether addressing the problem with communication protocols or through control strategies [9], [10]. However, there is still a limited amount of work in identifying these attacks in DERs.

Cyber-attacks can jeopardize the communication network of the smart grid in several ways. They can compromise the control devices, alter the information transmitted or affect the availability of the communication network [11], [12]. These attacks can be randomly inserted as well as strategically deployed [13]. The problem aggravates when these attacks are not noticeable to the system operator; when they do not induce a violation in operationality boundaries and, still affect the quality and value of the energy delivered.

In any case, the security of the cyber-physical system depends primarily on identifying the occurrence of the attack. This identification, in general, needs to be done through observation and smart recognition of response patterns. Some recent work has presented data-driven methods such as machine learning and deep learning algorithms in pattern recognition and attack identification [14], [15]. These algorithms have shown great accuracy in detecting attacks. However, there is still lack of field validation for real situations. The main reason for that is the complexity in using these algorithms due to the high computational cost [16], [17]. Another issue of the works presented above is that they detect from a superior point of view and with access to all the affected variables. Undoubtedly, there is an interest in performing the identification of Denial-of-Service (DoS) attacks in real-time, quickly, and accurately. However, if identification can be done locally, attack mitigation actions can also be carried out faster. Model-based strategies are still a starting point for detecting deviations in the system's behavior. However, this model needs to be accurate enough to identify the system patterns. This means that the reference model should not be misled, even during transitional stages in the operation of the system.

Given the background, this paper presents and discusses

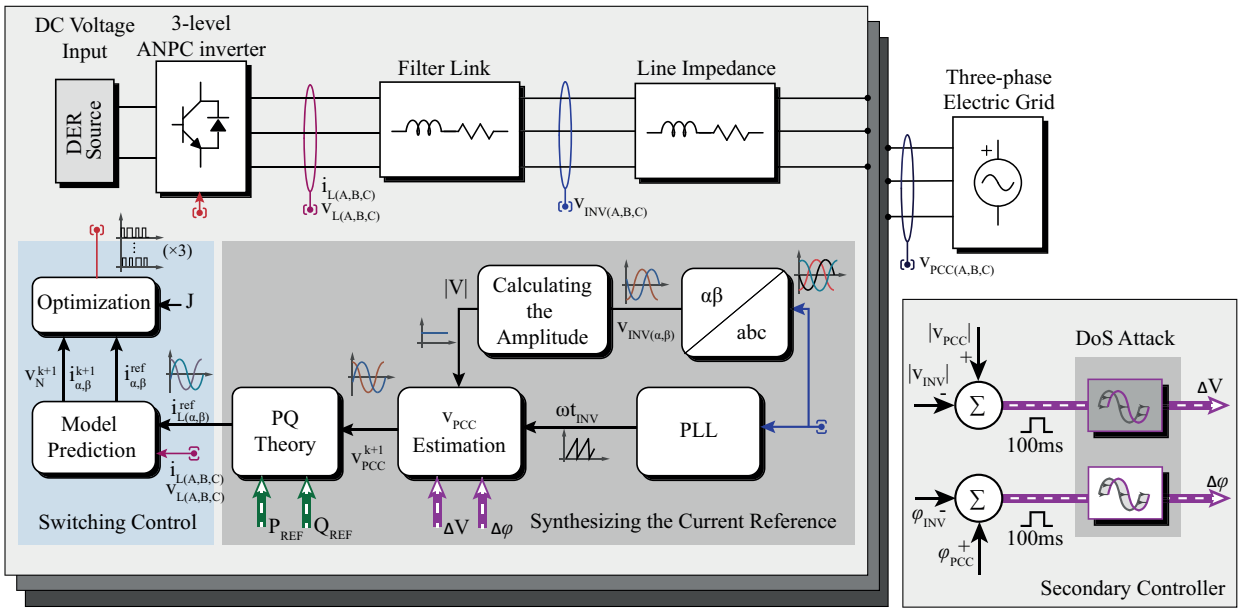

Fig. 1. Schematic of the inverter connected to the grid and control system with references from secondary and tertiary control. The latter provides the active and reactive power references subsequent to an optimal dispatch calculation.

some results of a system subject to a DoS attack, as illustrated in Fig.1, in the form of a delay purposely inserted in the secondary controller of an inverter connected to the grid. The DoS attack, as presented in this paper, induces a silent steady-state response. Unless the system is subject to a transient, its effects will not be noticeable to an observer not prepared to identify it. However, the authors seeks to show that these attacks should have a characteristic impact signature on variables of the physical layer depending on which variable is being affected in the communication layer. The results, to be discussed later in this work, shows that these attacks degrade the power delivered to the power grid. Based on these results, this paper will propose an early identification of the cyber-attack method from the observation of the affected variables and the correlation between the expected and the actual response. In the end, this work proposes an adaptive local controller to mitigate the impact of the delay, after identifying it, for a more reliable operation of the inverter system.

II. System and Problem Description

In this article, consider the scenario in which the DERs are connected to the power grid at a common coupling point. Moreover, the system is capable of power-sharing of the load. The control architecture is fashioned to supply power to the grid according to the demand of a central controller. In the analyzed electrical system, the generation and processing of energy are done at average power in the range of hundreds of kW. Between the inverters and the PCC, there are short-distance transmission line impedances. These line impedances result in voltage drops and phase shifts that need to be compensated for delivering the expected energy to the grid. Also, the control system is designed to provide voltage and current with good quality, meeting the standards defined by the power grid operator.

The problem description is inherently linked to the system's control structure. DoS attacks affect the communication network between the control layers of the smart grid. For this reason, initially, this work presents the nominal structure of control of the system and, next, it details the effects of this cyber attack.

A. Control Structure

The hierarchical controller is structured in such a fashion that the layers, with complementary functions, work together to address the aforementioned issues. These functions concern the synthesis of the reference, the restoration of the deviations, and the regulation of the voltage or current with reference-following [18]. In general, primary controllers can be implemented locally, without the need for communication, while having higher bandwidth for data processing. The secondary and tertiary controllers, on the other hand, generally use some form of communication between other control agents that can be organized centrally or distributed [19].

With the characteristics mentioned above, the hierarchical control system is illustrated in Fig.1. The power references come from a central tertiary controller. The secondary controller, with the help of phasor measurement units (PMUs), adjusts the voltage amplitude and phase deviations between the PCC and the inverter output. The tertiary and secondary controls communicated with the primary control at a given data processing rate. Finally, there is a local (primary) controller. The latter, based on the voltage and power references, synthesizes the current reference and performs an optimized control of the inverter current. Altogether, this hierarchical

control functions as a grid-following structure, with the final purpose of providing the power demanded by the load.

In the considered system, the primary controller performs the synthesis of the reference current and controls it. The switching control is done by model-based prediction and optimization. This model considers the inverter´s structure from the DC input until the output terminals of the L filter. Thus, from the inner característics of the inverter system, the control model can be described according to the following equations:

$$v_{NP}^{k+1} = v_{NP}^{k} - \frac{T_s}{C} \cdot \left(i_{La} |S_a| + i_{Lb} |S_b| + i_{Lc} |S_c| \right); \quad (1)$$

$$i_{L\alpha}^{k+1} = \left(1 - \frac{RT_s}{L}\right) \cdot i_{L\alpha}^{k} + \frac{T_s}{L} \left(v_{L\alpha} - v_{INV\alpha} \right); \quad (2)$$

$$i_{L\beta}^{k+1} = \left(1 - \frac{RT_s}{L}\right) \cdot i_{L\beta}^{k} + \frac{T_s}{L} \left(v_{L\beta} - v_{INV\beta} \right), \quad (3)$$

where v_{NP} represents the voltage at the neutral point of the ANPC inverter, i_L is the current at the inverter output in both three-phase and alpha-beta coordinates, v_L and v_{INV} are the voltages at the previous point and after the L filter, respectively. L represents the inductance of the output filter, C the capacitors of the DC-link of the inverter, and T_s is the discrete sampling time of the controller.

The optimization process is solved by minimizing a cost function $\mathbb{J}$ among all the switching state vectors. This cost function is defined as follows

$$\mathbb{J} = \Upsilon_1 \cdot \left| i_{L\alpha}^{ref} - i_{L\alpha}^{k+1} \right| + \Upsilon_2 \cdot \left| i_{L\beta}^{ref} - i_{L\beta}^{k+1} \right| + \Upsilon_3 \cdot \left| v_{NP}^{k+1} \right|, \quad (4)$$

where $\Upsilon_1 - -\Upsilon_3$ weighs the errors for the cost function minimization process.

The current references are synthesized, according to the p-q theory instantaneous power equations [20], such that

$$i_{\alpha}^{k+1} = \frac{2}{3} \frac{\left(v_{PCC\alpha}^{k+1} \cdot \mathrm{P}^{ref} + v_{PCC\beta}^{k+1} \cdot \mathrm{Q}^{ref} \right)}{\left(\left(v_{PCC\alpha}^{k+1} \right)^2 + \left(v_{PCC\beta}^{k+1} \right)^2 \right)}; \quad (5)$$

$$i_{\beta}^{k+1} = \frac{2}{3} \frac{\left(v_{PCC\beta}^{k+1} \cdot \mathrm{P}^{ref} - v_{PCC\alpha}^{k+1} \cdot \mathrm{Q}^{ref} \right)}{\left(\left(v_{PCC\alpha}^{k+1} \right)^2 + \left(v_{PCC\beta}^{k+1} \right)^2 \right)}. \quad (6)$$

In the above equations, the references for active and reactive power come from the tertiary controller. v_{PCC}, on the other hand, is estimated according to the deviation compensation measurements of the secondary controller. The $[k+1]$ prediction of v_{PCC} is made by a second-order extrapolation, to reduce the delay of the digital control so that

$$v_{PCC}^{k+1} = 3 \cdot v_{PCC}^{k} - 3 \cdot v_{PCC}^{k-1} + v_{PCC}^{k-2}. \quad (7)$$

The estimation of v_{PCC} in time at the current sample time is obtained by

$$v_{PCC}^{k} = |V_{INV} + \Delta V| \cos(\omega t + \Delta\phi). \quad (8)$$

In (8) the compensation for voltage amplitude and phase deviations, ΔV and $\Delta\phi$ respectively, comes from the secondary controller. In this work, it is in the communication between these two layers of control that the DoS attack takes place.

B. Delay attack in the communication network

The data between the control layers are transmitted at a certain sample rate through the communication network. A DoS-type attack is characterized by the interruption of data transmission during a certain period of time [21]. Assume that the latency between the primary and secondary control agents is defined over a certain sampling rate $s_n = n \cdot k$ $(n = 0, 1, 2, \ldots)$. Assume a time-varying heterogeneous delay in communication network described by $\tau_n(s_n)$. With this delay, the references in phase $(\Delta\phi)$ and amplitude (ΔV) deviations that arrive to the primary controller adopt the form

$$\hat{\chi}_n[s_n] = \begin{cases} \chi[s_n] & \text{if } t \in [0, t_A) \\ \chi[s_n - \tau_n] & \text{if } t > t_A \end{cases} \quad (9)$$

For the system described above, there are basically two variables that are affected by cyber-attacks. However, for systems connected in parallel, a coordinated attack can affect the communication network between the primary and secondary layers of more than one inverter at the same time. These attacks may not necessarily happen on the same variable or with the same amount of delay. In fact, an intelligent attacker has no interest in the cyberattack being easily detected. Thus, more important than modeling a hypothetical situation is to verify the impact of assuming that condition.

III. Investigation of the Delay Impact

The identification of abnormal behavior in the system's dynamics can be done by observing the transient response of a specific variable and by comparing it to the known expected response. Among the measurable variables, several must be affected in some way by the insertion of a delay type disturbance in the communication network. However, the identification of the attack is only possible if any of these variables are comparable. In other words, if any of the variables has a predetermined and constant expected steady-state value, the variation in it can provide a reliable measure for identifying specific patterns or dynamic response signatures.

In DER systems, especially when it involves forms of intermittent generation, it is generally desirable to insert only the active power into the grid. A reactive power reference would be passively zero, which would make this variable an interesting metric for the identification of the aforementioned delay attack. Considering that, Fig. 2 and Fig. 3 show the trace of the reactive power deviations over time and subject to different delay conditions in the secondary control variables. The graphs were plotted after a step in the power reference from zero to half load of rated active power.

In the figures below, the reference for reactive power from the tertiary controller is set to remain at zero. Ideally, after the transient dynamics, the deviations of the reactive power delivered should also be close to zero. However, even when there is a nominal latency in the communication, the transient behavior of the reactive power supplied still deviates from this expected value. Therefore, the main issue concerns how to distinguish a nominal behavior from an atypical response.

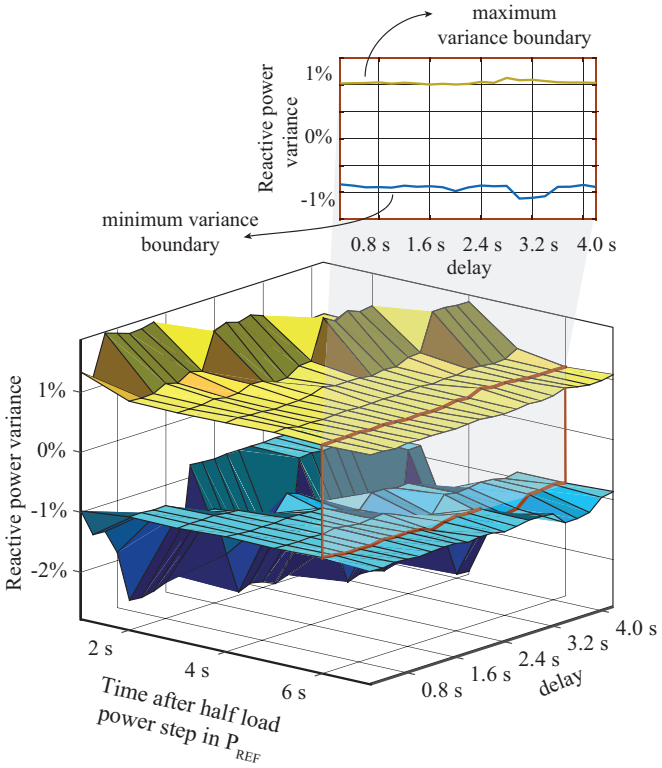

Fig. 2. Reactive power deviation from nominal at PCC in a situation of denial-of-service attack in the voltage amplitude adjustment coming from the secondary controller.

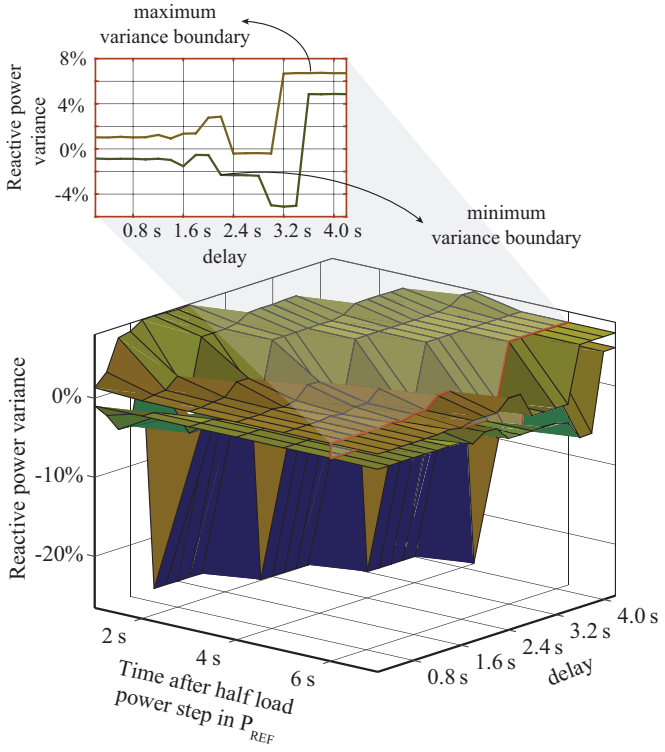

Fig. 3. Reactive power deviation from nominal at PCC in a situation of denial-of-service attack in the phase adjustment coming from the secondary controller.

It can be noted that the convergence to the stationary condition differs depending on where the delay is applied. Whether in the deviation of the amplitude or phase of the voltage, there is a specific pattern for the dynamic response. Although no tendency to instability in the system is noticeable, it is visible that there is a degradation of the settling of the reactive power. As a result of this degradation, there is a loss in the quality of the energy delivered. As expected, the parametric graphs also show that the dynamic behavior of the reactive power delivered varies according to the inserted delay τ_n. Furthermore, it can be noted that there is a distinct dynamic signature depending on the dimension of the delay attack on the communication network. This abnormal behavior would not be perceived in the voltage and current waveforms, as shown in the results obtained in Fig. 4. For this reason, the choice of reactive power as a metric for the identification of the DoS attack is justified.

IV. Identification of the DoS attack

In the previous section, it was verified that the DoS attack degrades the reactive power delivered to the network. Besides, it was found that the behavior of the system has specific dynamic behavior. This behavior shows a signature of the system response depending on the dimension of the inserted delay in the communication network. This finding can help identify an attack and then take an event-oriented action to mitigate the effects on it. Thus, suppose here that the complete model of the plant is known. Also, a supervisory control has access to the power references, as well as the reactive power outputs of the system. Hence, based on the nominal response of the system, it is possible to estimate a model that represents the expected behavior of the system for an arbitrary input condition. For this purpose, this work proposes the use of a Hammerstein-Wiener piecewise linear model as shown in Fig. 5 to estimate the plant. The advantage of using such a structure is that the estimation of the linear model can capture physical knowledge about the behavior of the system. Also, it is possible to add non-linearities of the process, which, in

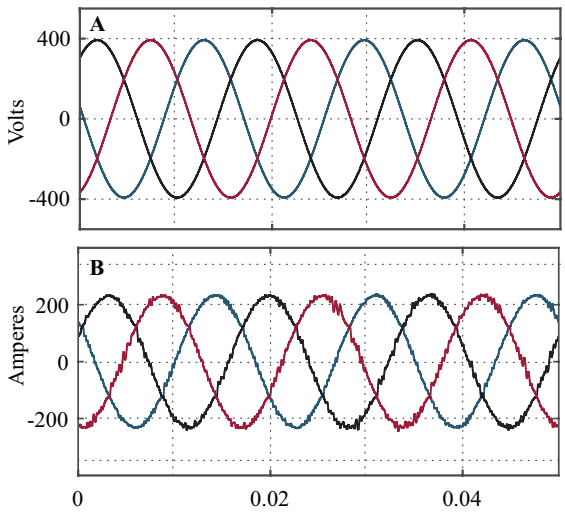

Fig. 4. Inverter's waveforms obtained by real-time simulation in OPAL-RT hardware in the loop. A) Voltage at PCC; B) Inverter's current

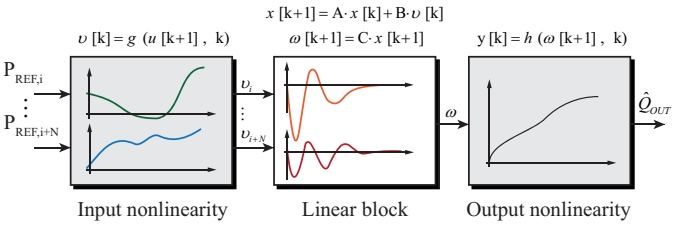

Fig. 5. Hammerstein-Wiener model structure

the plan of this work, comes mainly from the latency in the communication between the control layers.

To validate the plant model against the estimate, the following results are obtained with two ANPC inverters operating in parallel and connected to the grid as shown in the diagram in Fig. 1. With the knowledge of the reference powers from the tertiary controller (model input) and reactive power as an output, the estimate was obtained according to the Hammerstein-Wiener structure, as mentioned before. For the sake of comparison, both the real-time and the estimated model responses are compared during the transient conditions, as shown in Fig. 6. The figure shows these dynamics of the system after a series of transients that happen every two seconds. At time 0s, the active power references are

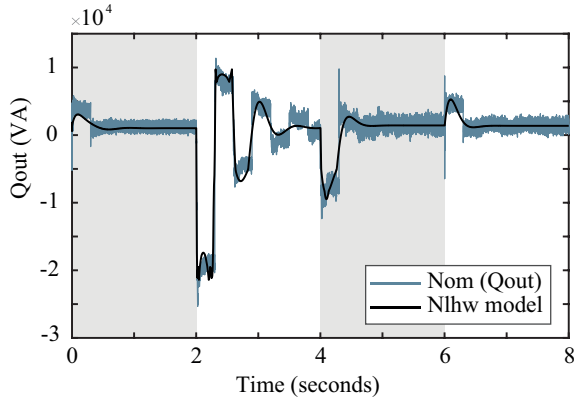

Fig. 6. Comparison between dynamic behavior of the reactive power delivered to the power grid (in blue), and the prediction response found using the model estimated with the Hammerstein-Wiener method (in black).

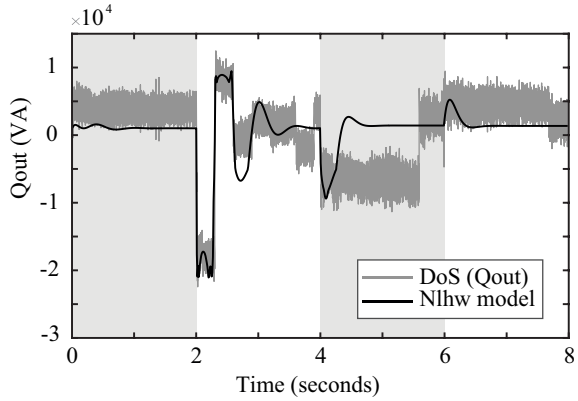

Fig. 7. Comparison between dynamic behavior of the reactive power delivered under attack (in gray), and the prediction response found using the model estimated with the Hammerstein-Wiener method (in black).

$P_{REF1} = 30\% \cdot P_{NOM}$ and $P_{REF2} = 10\% \cdot P_{NOM}$, for inverters 1 and 2 respectively, and where $P_{NOM} = 125kW$. At time 2s, a 40% step-up of the nominal power reference P_{REF1} occurs coming from the tertiary control of the inverter system. In time 4s there is a new step-up of 90% of P_{NOM}, now in P_{REF2} of inverter 2. Then, finally, in time 6s there is a step-down the power reference of inverter 2 of 50% of the nominal load.

The correlation between the estimated model's response and the measured response is sufficient for a supervisory control to take delay mitigation action on the primary controller of the inverter. The issue is what the difference would be in an attack situation. Thus, under the same transient conditions in the power reference coming from the tertiary controller, Fig. 7 shows the behavior of the estimated model in comparison to the real response under attack. A coordinated DoS attack was defined for this simulation so that a malicious delay of $\Delta\hat{V}[s_n] = \Delta V[s_n - 400\text{ms}]$ is inserted in the first inverter. Likewise, a delay attack of $\Delta\hat{\phi}[s_n] = \Delta\phi[s_n - 400\text{ms}]$ is inserted in the second inverter. In this condition, even with the delay distributed and differently inserted in the two inverters, there is still a deviation from the measured response to the estimated model prediction running in parallel. The signature of the predicted answer (in black) is explicit. Even when the degradation in the reactive power is not so great and the time of accommodation of the reactive power to the equilibrium is short, there is still a deviation that can be noticed by the supervisory controller.

V. Conclusions

In a hierarchical control system where multiple DERs are connected to the power grid, a cyber attack can be silent and difficult to identify. In this article, we argue that it is possible to detect locally if there is a DoS attack in the communication between the primary and secondary control layers. The signatures of the reactive power trace show that the dynamic response of the system under attack differs substantially from the nominal value. Thus, a supervisory controller operating locally can identify the occurrence of an attack when there is a transient response of the power reference. The immediate identification of a DoS attack will be helpful for the mitigation actions to be taken, whether through control actions or system protection protocols. The sooner the attack is identified, the sooner it will also be possible to take actions to mitigate it, as demonstrated in the results presented.

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. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under Solar Technologies Office (SETO) Agreement No. EE0008349. This work is also supported in part by the U.S. National Science Foundation under award number 1644874.

REFERENCES

[1] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, 2010.

[2] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[3] J. M. Taylor and H. R. Sharif, "Security challenges and methods for protecting critical infrastructure cyber-physical systems," in *2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*, 2017, pp. 1–6.

[4] J. C. Vasquez, J. M. Guerrero, J. Miret, M. Castilla, and L. G. de Vicuña, "Hierarchical control of intelligent microgrids," *IEEE Industrial Electronics Magazine*, vol. 4, no. 4, pp. 23–29, 2010.

[5] Y. Du, X. Lu, H. Tu, J. Wang, and S. Lukic, "Dynamic microgrids with self-organized grid-forming inverters in unbalanced distribution feeders," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 8, no. 2, pp. 1097–1107, 2020.

[6] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 28–42, 2013.

[7] O. T. Soyoye and K. C. Stefferud, "Cybersecurity risk assessment for california's smart inverter functions," in *2019 IEEE CyberPELS (CyberPELS)*, 2019, pp. 1–5.

[8] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal, and M. J. Reno, "Power system effects and mitigation recommendations for der cyberattacks," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 3, pp. 240–249, 2019. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-cps.2018.5014

[9] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 28–39, 2016. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-cps.2016.0018

[10] Y. Xue, M. Starke, J. Dong, M. Olama, T. Kuruganti, J. Taft, and M. Shankar, "On a future for smart inverters with integrated system functions," in *2018 9th IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2018, pp. 1–8.

[11] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[12] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38–45, 2012.

[13] K. G. Lore, D. M. Shila, and L. Ren, "Detecting data integrity attacks on correlated solar farms using multi-layer data driven algorithm," in *2018 IEEE Conference on Communications and Network Security (CNS)*, 2018, pp. 1–9.

[14] F. Li, Q. Li, J. Zhang, J. Kou, J. Ye, W. Song, and H. A. Mantooth, "Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network," *IEEE Transactions on Power Electronics*, vol. 36, no. 3, pp. 2495–2498, 2021.

[15] Q. Li, F. Li, J. Zhang, J. Ye, W. Song, and A. Mantooth, "Data-driven cyberattack detection for photovoltaic (pv) systems through analyzing micro-pmu data," in *2020 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2020, pp. 431–436.

[16] M. R. Camana Acosta, S. Ahmed, C. E. Garcia, and I. Koo, "Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks," *IEEE Access*, vol. 8, pp. 19 921–19 933, 2020.

[17] S. Azad, F. Sabrina, and S. Wasimi, "Transformation of smart grid using machine learning," in *2019 29th Australasian Universities Power Engineering Conference (AUPEC)*, 2019, pp. 1–6.

[18] X. Lu, J. M. Guerrero, K. Sun, J. C. Vasquez, R. Teodorescu, and L. Huang, "Hierarchical control of parallel ac-dc converter interfaces for hybrid microgrids," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 683–692, 2014.

[19] 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.

[20] H. Akagi, "Generalized theory of the instantaneous reactive power in three-phase circuits," *IEEJ IPEC-Tokyo'83*, vol. 1375, 1983.

[21] C. Deng, "Distributed resilient control for cyber-physical systems under denial-of-service attacks," in *2019 23rd International Conference on Mechatronics Technology (ICMT)*, 2019, pp. 1–5.