Cyber-physical security framework for Photovoltaic Farms

Jinan Zhang, Qi Li, Jin Ye, Lulu Guo
School of Electrical and Computer Engineering
University of Georgia, Athens, Georgia, USA
Email: jinan.zhang@uga.edu, qi.li@uga.edu, jin.ye@uga.edu, lulu.guo@uga.edu

***Abstract*—With the evolution of PV converters, a growing number of vulnerabilities in PV farms are exposing to cyber threats. To mitigate the influence of cyber-attack on PV farms, it is necessary to study attacks' impact and propose detection methods. To meet this requirement, a cyber-physical security framework is proposed for PV farms. Data integrity attacks (DIAs) are studied on different control loops. As μPMU is gaining in popularity, a lower sampling rate of μPMU data is applied to develop a detection algorithm. We have evaluated two data-driven methods, which are support vector machine (SVM) and long short-term memory (LSTM). Finally, the data-driven methods verify the feasibility of μPMU data in attack detection.**

***Index Terms*—PV farm, Data-driven Detection, μPMU, Data Integrity Attack, Attack Impact Analysis**

I. Introduction

As power grids evolve into a cyber-physical system, they become more vulnerable to cyber-attacks than before. A large amount of DERs (distributed energy resources) that are integrated into the grid, such as photovoltaic (PV) farm, wind power plant, and electric vehicles, bring an amount of vulnerabilities and challenges [1]. To resolve this potential threat, PELS (IEEE Power Electronics Society) proposes strengthening the research of the cyber-physical security in power electronics. Data integrity attack (DIA), which is one of the most common cyber-attacks in practical applications, may falsify the sensor measurement by injecting or altering data to change the system's status. In [2], the impact of DIA on the distributed controller in microgrid was analyzed, wherein, the DIA could block the measurement or control signal, causing severe damage to the system. In [3], a systematic method was proposed to assess the integrity attack on the motor drive. In [4], the author proposed a systematic assessment method for cyber-physical security on EMS in electrical vehicles.

As one of the most typical applications of DERs, solar photovoltaic generation systems have been concerned widely. In general, the PV farm works as a power generator, which significantly impacts the power system operation. In [5], the authors constructed a state-space model for PV farms to analyze PV dynamic performance. With the evolution of PV converters, vulnerability assessment of cyber-attacks has become necessary. In [6], the author analyzed the impact of cyber-attacks on PV and ESS in the microgrid, but this work only focused on the assessment of attacks at the system level. Up to date, the attack impact analysis research in the converter level has yet to be explored.

978-1-7281-9591-9/20/$31.00 ©2020 IEEE

Besides the impact evaluation of DIAs in PV farms, cyber-attack detection is also necessary for an operator to identify and eliminate integrity attacks timely in practical applications. Among the detection methodologies in the literature, a data-driven method is widely employed. In [7], a data-driven method was proposed to distinguish differences between several faults in the power grid. In [8], a multidimensional online approach was presented to detect cyber-attacks. In [9], a diagnosis methodology was presented for DIAs in PV farm based on multilayer long short-term memory networks. According to the above works, the extracted feature from waveform data was applied to the detection algorithm. With the popularity of μPMU, μPMU data is obtained easily from the system dispatch center, which brings a new possibility for data-driven detection methods.

To mitigate the false data integrity attacks on the PV farm, this paper focuses on the DIA on large-scale PV systems. The DIAs on different control loops are analyzed. Two detection methods will then be used to verify the feasibility of μPMU in cyber-attack detection.

II. Modeling of Photovoltaic Farms

As shown in Fig. 1, a two-stage two-level PV system is built, including PV array, DC/DC converter, DC/AC inverter, DC/DC controller and DC/AC controller.

A. PV Array Model

In Fig. 1, an equivalent circuit is applied to represent the PV array. To describe the PV current-voltage relationship, a dynamic equation of PV array is derived as follow:

$$I_{pv} = I_{ph} - I_s(e^{\frac{U_{pv}+I_{pv}R_s}{a}} - 1) - \frac{U_{pv}+I_{pv}R_s}{R_{sh}} \quad (1)$$

where I_{ph} and I_s are the photovoltaic and saturation currents of the array, respectively; R_s is the equivalent series resistance of the array; R_{sh} is the equivalent parallel resistance; a is the diode ideal constant; $[I_{ph}, I_s, R_s, R_{sh}, a]$ are calculated by using the following equations.

$$\begin{aligned} I_{ph} &= I_{ph0}G[1 + a_{Isc}(T - T_0)], \\ I_s &= I_{s0}(\frac{T}{T_0})^3 e^{47.1(1-\frac{T_0}{T})}, \\ a &= a_0\frac{T}{T_0}, R_s = R_{s0}, R_{sh} = R_{sh0}/G \end{aligned} \quad (2)$$

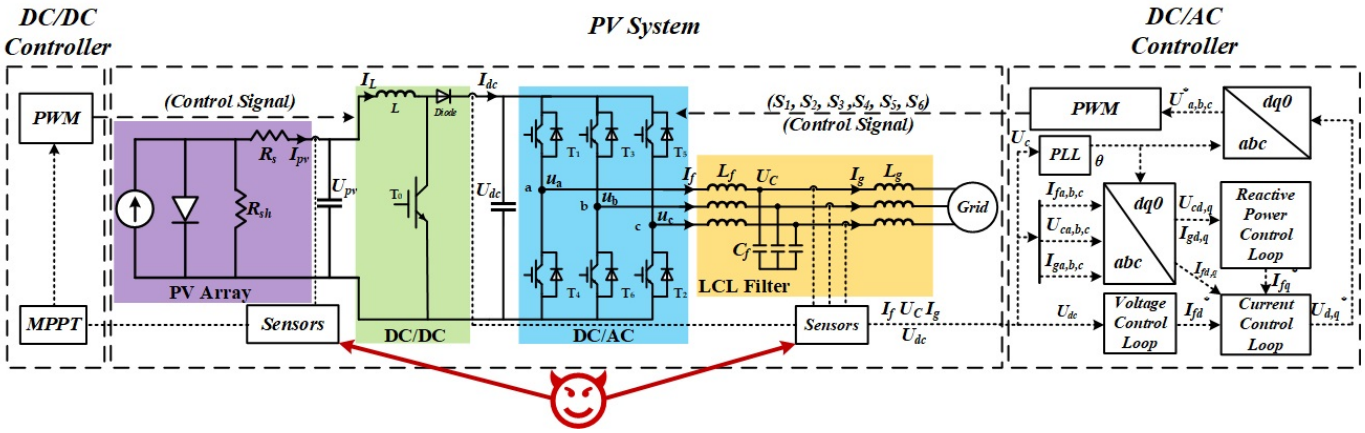

Fig. 1: Two-stage two level PV converter circuit.

where $T_0 = 298.15$ is the STC temperature; $G(pu)$ represents the irradiance; a_{Isc} is the short circuit current temperature coefficient; $[I_{ph0}, I_{s0}, R_{s0}, R_{sh0}, a_0]$ can be extracted at standard test conditions (STC).

B. DC/DC Converter Model

The DC/DC circuit is used to connect the PV array with an inverter in Fig. 1. The DC/DC controller generates the optimal duty cycle for boost converter to track the maximum power point (MPP). The DC/DC converter is modeled as

$$\begin{aligned} \dot{U_{pv}} &= \frac{I_{pv} - I_L}{C_{pv}} \\ \dot{I_L} &= \frac{U_{pv} - (1-D)U_{dc}}{L} \end{aligned} \tag{3}$$

where I_L is the inductance current; U_{dc} is the dc voltage of capacitor; D is the duty cycle and C_{pv}; L represents the component of DC/DC circuit. In steady state, the relationship between U_{pv} and U_{dc} can be derived as

$$\frac{U_{dc}}{U_{pv}} = \frac{1}{1-D} \tag{4}$$

C. DC/AC Inverter Model

The differential equation of the DC link capacitor can be expressed as follows:

$$C_{dc}\dot{U_{dc}} = (1-D)I_L - \frac{3}{2}\frac{U_{cd}I_{gd} + U_{cq}I_{gq}}{U_{dc}} \tag{5}$$

where U_{dc} is dc link capacitor voltage; U_{cd}, U_{cq} are the LCL capacitor voltage in d,q frame; I_{gd}, I_{gq} are the grid side current of LCL in d,q frame. The inverter and LCL filter can be represented by the following state equations:

$$\begin{aligned} \dot{I_{fd}} &= \frac{1}{L_f}(U_{id} - U_{cd}) + \omega I_{fq} \\ \dot{I_{fq}} &= \frac{1}{L_f}(U_{iq} - U_{cq}) - \omega I_{fd} \\ \dot{U_{cd}} &= \frac{1}{C_f}(I_{fd} - I_{gd}) + \omega U_{cq} \\ \dot{U_{cq}} &= \frac{1}{C_f}(I_{fq} - I_{gq}) - \omega U_{cd} \\ \dot{I_{gd}} &= \frac{1}{L_g}(U_{cd} - U_{gd}) + \omega I_{gq} \\ \dot{I_{gq}} &= \frac{1}{L_g}(U_{cq} - U_{gq}) - \omega I_{gd} \end{aligned} \tag{6}$$

where ω is system frequency, $I_{fd,q}$ is inverter side current in the LCL filter, and L_f is the inductance in LCL filterp.

D. Controller for DC/DC Converter

DC/DC converter is used to connect the PV array to DC/AC inverter. Generally, the DC/DC converter is designed as a boost converter that extracts the maximum power from the PV array. MPPT is a widely used algorithm in the DC/DC controller. In this paper, an incremental conductance method is used. It utilizes the incremental conductance ($\Delta I/\Delta V$) of the PV array to compute the sign of the change in power to voltage ($\Delta P/\Delta V$). In this method, the maximum power point is derived by comparing incremental conductance ($\Delta I/\Delta V$) to the array conductance (I/V). When the two conductances are the same ($I/V = \Delta I/\Delta V$), the output voltage is the MPP voltage. The flowchart of the MPPT scheme is shown in Fig. 2.

E. Controller for DC/AC Inverter

Typically, the inverter controller is designed to transfer the power from the DC circuit to the AC grid. In Fig. 1, the DC/AC controller includes DC link voltage control loop, reactive control loop, and current control loop. The DC link controller is responsible for maintaining the capacitor voltage and determining the I^*_{fd}. The reactive power control loop is

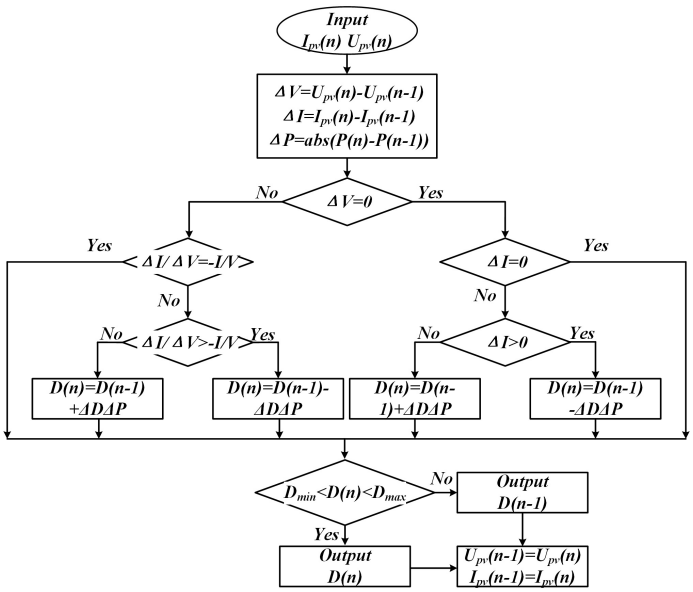

Fig. 2: Flowchart of MPPT Algorithm

designed so that the PV system could generate an amount of reactive power and determines I_{fq}^*. Thus, I_{fd}^* and I_{fq}^* can be expressed as follows:

$$\begin{aligned} I_{fd}^* &= k_{pv}(U_{dc}^* - U_{dc}) + \frac{k_{iv}(U_{dc}^* - U_{dc})}{s} \\ I_{fq}^* &= k_{pq}(Q^* - Q) + \frac{k_{iq}(Q^* - Q)}{s} \end{aligned} \tag{7}$$

where k_{pv}, k_{iv}, k_{pq} and k_{iq} are the PI parameter, U_{dc}^* is DC link voltage reference, Q^* is reactive power reference. In practical applications, PV converters do not generate any reactive power. Therefore, in this paper, we assume that $I_{fq}^* = 0$. The inner current control loop also employs the PI controller independently to regulate I_{fd}, I_{fq} to their references. Then, the current control loop can be modeled as

$$\begin{aligned} U_{id}^* &= k_{pi}(I_{fd}^* - I_{fd}) + \frac{k_{ii}(I_{fd}^* - I_{fd})}{s} - \omega L_f I_{fq} \\ U_{iq}^* &= k_{pi}(I_{fd}^* - I_{fd}) + \frac{k_{ii}(I_{fd}^* - I_{fd})}{s} + \omega L_f I_{fd} \end{aligned} \tag{8}$$

where k_{pi}, k_{ii} are the PI paremeter, $I_{fd,q}^*$ is the inductance current in LCL filter, $I_{fd,q}^*$ is the inductance current reference in d,q frame.

III. Cyber-Attacks Model and Impact Analysis

To investigate the impact of DIAs in the PV converter, we model the DIAs and analyze the dynamic performance of the two-stage PV converter during attack duration, the conclusion of which will benefit developing a data-driven detection method.

A. DIA Model

To clarify the impact of cyber-attack on the PV converters, the vulnerability of PV is given in Fig. 1. The attackers can compromise the DC/DC or DC/AC controller and falsify the sensor measurements. In general, a DIA can be expressed as

$$\mathbf{Y_F}(t) = \alpha * \mathbf{F}(t) + \beta * \mathbf{Y}_0(t - t_{delay}) \tag{9}$$

where $\mathbf{Y_F}$ is the compromised data vector that is eventually the input of controller; $\mathbf{Y}_0$ is the original measurement; $\mathbf{F}$ is a general compromised data vector which can be independent or determined by $\mathbf{Y}_0$; α is a multiplicative factor matrix that defines the weight of the attack vector; β is a multiplicative factor that defines the weight of the real vector; t_{delay} is the delay time injection. Here, $Y_0(t)$ is defined as

$$Y_0(t) = [U_{pv}(t), I_{pv}(t), U_{dc}(t), I_f(t), U_c(t), I_g(t)]^T. \tag{10}$$

In the above definition, α is the multiplicative factor matrix, and can be expressed as a 12×12 matrix

$$\alpha = diag\ [\alpha_{upv}, \alpha_{ipv}, \alpha_{udc}, \alpha_{il_{1\times3}}, \alpha_{uc_{1\times3}}, \alpha_{ig_{1\times3}}]. \tag{11}$$

B. Impact Analysis of DIAs on DC/DC converter

When an attacker compromises the DC/DC sensor, the measurements would be mistakenly used in the controller, degrading the DC/DC controller performance. According to the above analysis in sectionII-D, attacks on DC/DC converter should be designed elaborately so that PV system operation status can be changed. To further study the impact of integrity attacks on DC/DC converter, we consider the MPPT algorithm's mechanism. We assume that ΔI and ΔV are two malicious injections aiming to falsify the DC/DC sensor measurements. As shown in Fig. 2, the output duty cycle in the controller must meet the following constraints of MPPT algorithm:

$$D_{min} < D < D_{max}. \tag{12}$$

Once the duty cycle exceeds the limit, the control signal remains unchanged in the controller. To destroy the DC/CD controller, ΔI and ΔV should meet the following conditions:

$$-\Delta I \Delta U > \frac{D_{min} - D}{\Delta D},\ \frac{\Delta I}{\Delta U} > -\frac{I}{U} \tag{13}$$

or

$$\Delta I \Delta U < \frac{D_{max} - D}{\Delta D},\ \frac{\Delta I}{\Delta U} < -\frac{I}{U} \tag{14}$$

where D is duty cycle generated by MPPT after attack; ΔD is duty cycle step size.

To clarify the dynamic process of cyber-attack on DC/DC controller, two DIAs are simulated in PV converters modeled in the above section.

Attack 1: $\alpha = diag\ [1\ -0.9\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$, $\beta = 1$, $F = Y_0(t)$, $t_{delay} = 0$, $G = 1$, $T = 298.15K$, $t_{attack} = 0.3 - 0.6s$. Fig. 3 shows performance of DC/DC controller and measurement variation in sensors. As the input of the DC/DC controller, both voltage and current of PV array are changed at 0.3s. Based on the MPPT algorithm, $-I/V > \Delta I/\Delta V$, the DC/DC controller should generate a larger duty cycle to track the MPP, which is also obtained from the Fig. 3(c). Thus, the power level is falsified by cyber-attacks. Although the efficiency of PV converter is reduced, this attack does not generate any harmonics in the waveform.

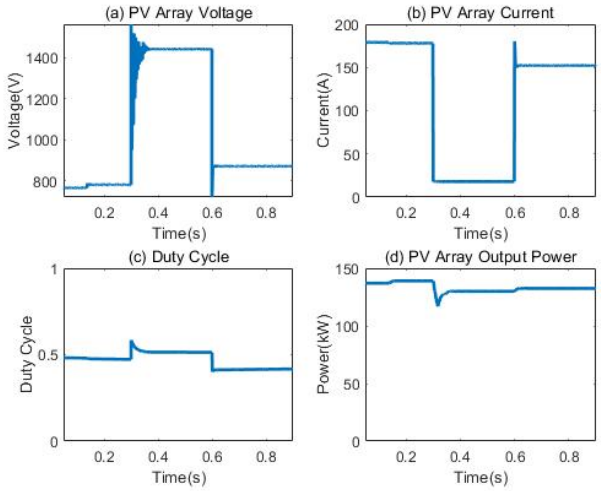

Fig. 3: PV Array Voltage, Current, Duty Cycle and Output Power due to DIA 1 in DC/DC controller

Attack 2: $\alpha = diag\ [-0.9\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$, $\beta = 1$, $F = Y_0(t)$, $t_{delay} = 0$, $G = 1$, $T = 298.15K$, $t_{attack} = 0.3 - 0.6s$. According to Fig. 4(d), this attack does not cause any changes to the controller operation. More specifically, the PV array voltage decreases, and the PV array current increases. Thus, based on Fig. 4(a,b), there is $-I/V < \Delta I/\Delta V$. The duty cycle should be reduced to track the MPP. Due to the limitation of the duty cycle in the MPPT algorithm, the output duty cycle remains the same in the Fig. 4(c). According to the above two attacks, we conclude that DC/DC integrity attack can only change the power level of PV converters when it meets equations (13) or (14).

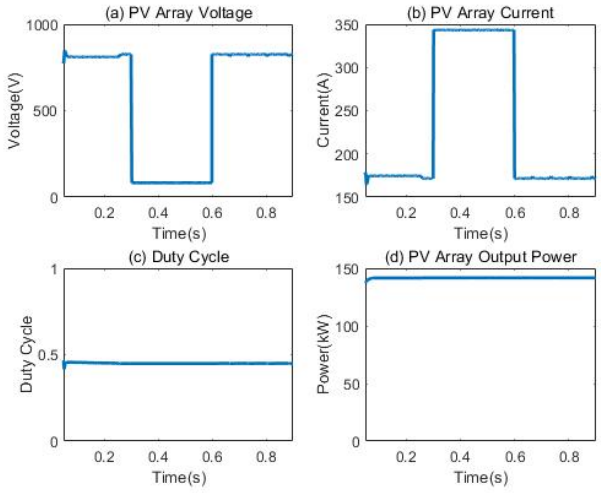

Fig. 4: PV Array Voltage, Current, Duty Cycle and Output Power due to DIA 2 in DC/DC controller

C. Impact Analysis of DIAs on outer DC Link Voltage Control

As analyzed in sectionII-E, both DC voltage control and reactive power control determine the reference of the inner current control loop. In a real application, the PV converter does not generate reactive power and $I_{fq}^* = 0$. Thus, the impact of DIA on the DC link is analyzed in this section. The DC link capacitor works as a bridge that connects DC circuit and DC/AC inverter. DC voltage disturbance impacts the PV array output and inverter performance. As discussed in the previous section, U_{dcF} is defined to represent the DC link voltage after an attack. Considering the value of U_{dcF}, the impacts of two scenarios are discussed in the following passage.

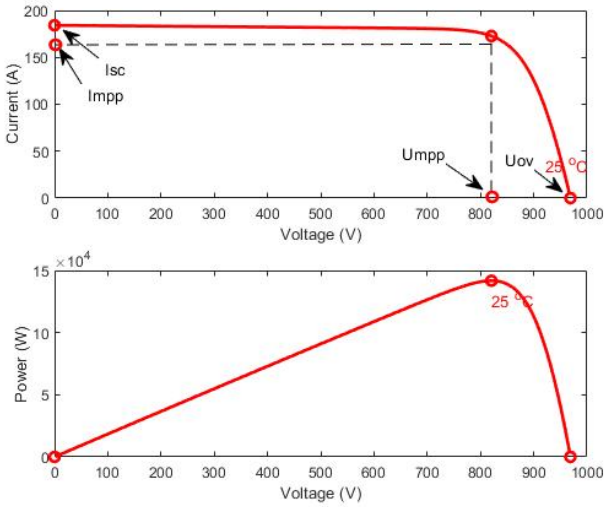

Fig. 5: PV Array P-U Curve and I-U Curve

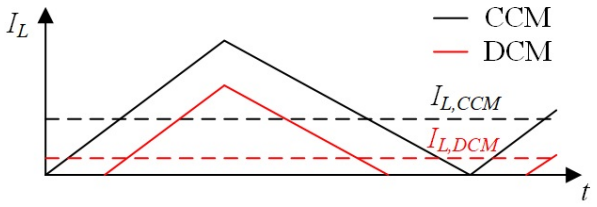

Fig. 6: Inductor current in CCM and DCM operation

1) $U_{dcF} > U_{dc}$: When $U_{pv} > U_{mpp}$, the PV array output current decreases with the increasing U_{pv}. When $U_{pv} = U_{ov}$ (see Fig. 5), the PV array never generates any current to DC/DC converter, which also causes DC/DC converter to enter DCM. In the steady mode, I_L is determined by I_{pv}. Thus, the average value of inductance current is expressed as $\bar{I_L} = I_{pv}$. Fig. 6 shows the PV converter CCM and DCM operation. When I_{pv} is less than $I_{L,CCM}$ as shown in Fig. 6, DC/DC converter operates in DCM. According to the equations (1) and (2), I_{pv} can be represented by $f(U_{pv})$. Therefore, if we apply the equation (4) and (12), then the DC/DC converter is

in DCM operation when the U_{dcF} should meet the following constraints: $f(U_{dcF}(1-D_{max})) < I_{L,CCM}$. Otherwise, when $U_{dcF} > U_{dc}$, the DIA only changes power level and decrease PV converter operation efficiency.

2) $U_{dcF} < U_{dc}$: In this scenario, the DC/DC converter could not enter into DCM operation state, since $U_{dcF}(1 - D_{min}) > U_{ov}$. With the decreased U_{dcF}, the MPPT algorithm still works to track the MPP. Based on the equation (7), I^*_{fd} increases to transfer the PV output power to AC grid. As the saturation limitation in PI control, the PV converter will operate at a stable point due to this integrity attack.

To illustrate the impact of DIA in DC link controller, two simulation results are described in the following paragraph.

Attack 1: $\alpha = diag\ [0\ 0\ -1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T, \beta = 1, F = Y_0(t), t_{delay} = 0, G = 1, T = 298.15K, t_{attack} = 0.3 - 0.6s$. As shown in Fig. 7, DC link voltage increases due to attack, which leads to an increase in PV array voltage. The DC/DC converter enters into the DCM operation state, which can be obtained from the inductance current in Fig. 7(b). Because the PV array could not generate any power to the converter, the DC link needs to absorb energy from the AC grid. Hence, there is an amount of disturbance in the output power and I_g which are shown in the Fig. 7(c,d). Thus, this attack destroys the converter controller.

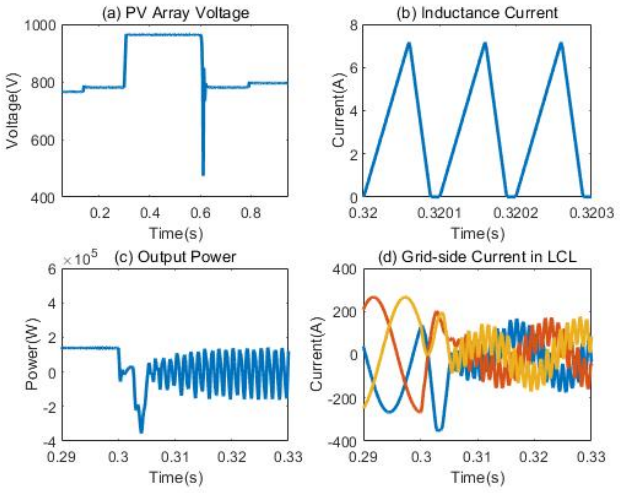

Fig. 7: PV Array Voltage, Inductor Current, Output Power and I_g due to DIA on DC link Voltage Control

Attack 2: $\alpha = diag\ [0\ 0\ 0.33\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T, \beta = 1, F = Y_0(t), t_{delay} = 0, G = 1, T = 298.15K, t_{attack} = 0.3 - 0.6s$. As shown in Fig. 8, DC link voltage decreases due to attack. But the PV converter is still stable. Inductance current shows the converter operates in CCM in Fig. 8(b). Thus, this attack only reduces PV array output power, which is also obtained from Fig. 8(c,d).

D. DIAs' Impact Analysis in Inner Current Control

The inner current control loop can be expressed as

$$\begin{bmatrix} I_{fd} \\ I_{fq} \end{bmatrix} = G_i(s) \begin{bmatrix} I^*_{fd} \\ I^*_{fq} \end{bmatrix} \tag{15}$$

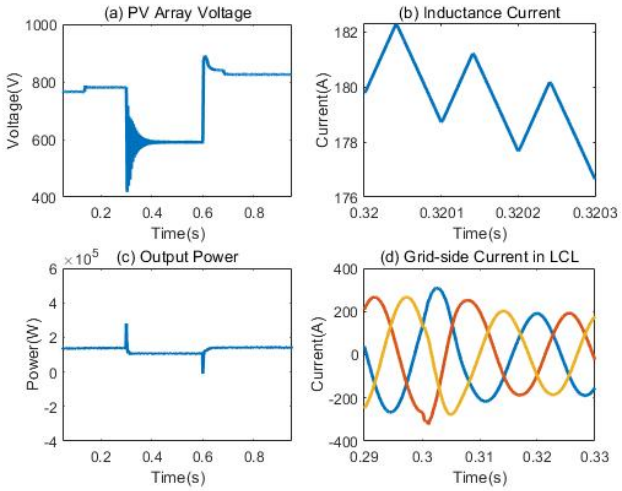

Fig. 8: PV Array Voltage, Inductor Current, Output Power and I_g due to DIA on DC link Voltage Control

$$G_i(s) = \frac{G_{ipi}(s)G_p(s)G_{PWM}(s)}{1 + G_{ipi}(s)G_p(s)G_{PWM}(s)} \tag{16}$$

where $G_{ipi} = k_p + k_i/s$, $G_p = 1/(sL_{fi})$; $G_i(s)$ is the closed transfer function; I^*_{fd}, I^*_{fq} is inductance current reference; G_{PWM} represents the inverter and PWM. In this paper, $U_{id} = U^*_{id}$. Thus, G_{PWM} is assumed as 1 here. DIA falsifies the sensor measurement, the G_i can be manipulated as

$$G_{iF}(s) = \frac{G_{ipi}(s)G_p(s)G_{PWM}(s)}{1 + G_{ipi}(s)G_p(s)G_{PWM}(s)G_F(s)} \tag{17}$$

where $G_{iF}(s)$ is the closed transfer function of current controller, and $G_F(s)$ is a function of α_{il} and β. In recent years, a number of papers have assessed the stability of the current control loop [10], [11]. These methods can be used to evaluate DIA's impacts on the current controller. Due to page limitation, this method is not presented in the paper.

IV. Data-driven Cyber-attack Detection

To the best of our knowledge, μPMU data is rarely used in the data-driven detection algorithm. In this section, we focus on assessing the feasibility of using μPMU data for data-driven attack detection. We will implement two different kinds of popular supervised data-driven methods, e.g., Support Vector Machine (SVM), and Long Short-Term Memory (LSTM) [12], [13]. To obtain enough μPMU data samples, the PV converter model in section II is used to construct a large-scale PV farm in MATLAB. Seven paralleled PV converters are connected to a power grid. Thus, the capacity of this PV farm is 980kW. An amount of cases, including normal condition, DIAs in controller, and replay attack, are simulated to form training data set. The μPMU is installed at the PCC node to measure the voltage and current of PV farm.

A. Machine Learning

1) Support Vector Machine: The basic idea of the support vector machine is to create a boundary or a hyperplane to

separate the data into several classes. Intuitively, the further from the hyperplane data points lie, the more confident we are that they have been correctly classified. In general, it's not easy to have a directly separable set of training data. That is where the kernel trick comes in, whose idea is mapping the non-linear separable dataset into a higher dimensional space where we could find a hyperplane to separate the data. SVM exhibited state-of-the-art performance on classification problems. However, SVM does not perform well for large datasets such as image classification, and the training time is much higher.

B. Deep Learning

1) Long short-term memory: LSTM is a variant of the recurrent neural network(RNN). It was developed to solve the vanishing gradient problem of RNN by adding a way to carry the past information across the time steps. In this case, information is saved for later, thus preventing older data from gradually vanishing during training. LSTM is versatile that can process not only single data points but also entire sequences of data, especially time-series data. It shows powerful capability when handling scenarios like natural language processing (NLP), speech recognition.

C. μPMU Dataset Analysis

The μPMU data are collected from the PMU sensors. Although the sampling rate of μPMU data is much less compared to the original waveform, the three features of the magnitude, frequency, and phase angle of the waveform are directly obtained from the hardware calculation of PMU device. At each sampling time instance, an 18-dimensional μPMU data vector is obtained. We denote three-phase (a, b, c) voltage (V) μPMU data (θ, F, M represent phase angle, frequency and magnitude, respectively) as: θ_{V_a}, F_{V_a}, M_{V_a}, θ_{V_b}, F_{V_b}, M_{V_b}, θ_{V_c}, F_{V_c}, M_{V_c} and three-phase current (I) μPMU data as: θ_{I_a}, F_{I_a}, M_{I_a}, θ_{I_b}, F_{I_b}, M_{I_b}, θ_{I_c}, F_{I_c}, M_{I_c}.

All the data at each time point constitute a μPMU data sample, which can be represented as a 1-D time sequence: $X = (X_1^{\mu\text{PMU}}, X_2^{\mu\text{PMU}}, ..., X_t^{\mu\text{PMU}})$, where $X_t^{\mu\text{PMU}}$ represents the μPMU data sampled at time t. The equation $X_t^{\mu\text{PMU}} = (\theta_{V_a}^t, F_{V_a}^t, M_{V_a}^t ..., \theta_{I_c}^t, F_{I_c}^t, M_{I_c}^t)$, shows the features that μPMU sample data have (18 features in total). For every μPMU data sample, we constructed a normalized high-dimensional matrix $X_{t\times s}$, where t represents the window size of the sample data and s represents the number of features. In our case, $t = 10$ (0.08 sec) and $s = 18$ (18 features in total), respectively. Eventually, each sample data to be input to the models denote by the matrix $X_{10\times 18}$.

D. Case Study

SVM and LSTM are used to conduct experiments on attack detection and attack diagnosis, respectively. For attack detection, the data are divided into 2 cases (normal and abnormal), which is a binary classification problem. For attack diagnosis, the data are divided into 5 cases (normal, DIA in DC/AC controller, DIA in DC/DC controller, replay attack, delay attack), which is a multi-classification problem. The overall block diagram is shown in Fig. 9, describing the workflow of the implemented data-driven evaluation methods. The experiment results are presented below after we conducted a 10-fold cross-validation. Tables. I and II show the detection and diagnosis performance of the two algorithms.

From the Tables. I and II, in comparison, LSTM outperforms SVM model in all metrics (99.42% and 98.98% accuracy in detection and diagnosis, respectively). Although SVM gets similar results as LSTM on attack detection, when it comes to attack diagnosis, the gap between these two methods is revealed. The performance of the SVM declined while the robustness of the LSTM is still strong. We contribute this to LSTM's powerful capability of extracting features and latent information. In short, both the implemented two data-driven methods perform well in the attack detection and diagnosis for our PV farm, which shows the potential for μPMU data to be used in the security area of the power system.

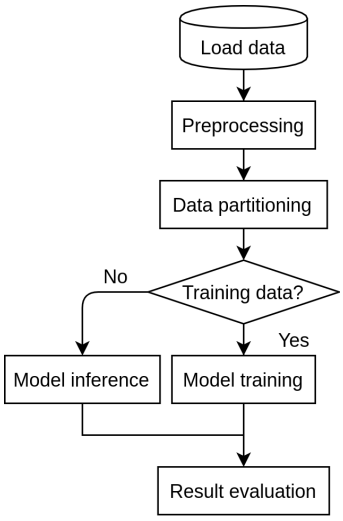

Fig. 9: The overall block diagram showing the workflow of the implemented data-driven evaluation methods.

TABLE I: Detection performance evaluation

Model\Metrics	Acc	Prec	Rec	F_1
SVM	0.9880	0.9908	0.9789	0.9847
LSTM	0.9942	0.9935	0.9929	0.9945

TABLE II: Diagnosis performance evaluation

Model\Metrics	Acc	Prec	Rec	F_1
SVM	0.9753	0.9473	0.9414	0.9443
LSTM	0.9898	0.9742	0.9891	0.9892

V. Conclusion

This paper analyzes the impact of DIAs on different control loops in the PV farm. For validation, the DIA model is built, and a two-stage two-level PV converter is modeled. To obtain

the impacts of DIA, both theoretical analysis and case studies are shown in this paper. To mitigate the DIAs' impact, a data-driven method is proposed using μPMU data. As one of the first attempts at using μPMU data, we evaluate two data-driven methods, which are SVM and LSTM. Finally, these two methods verify the feasibility of μPMU data in attack detection.

ACKNOWLEDGMENT

This research was partially supported by the U.S. Department of Energy's Solar Energy Technology Office under award number DE-EE0009026 and U.S.National Science Foundation NSF-ECCS-1946057.

REFERENCES

[1] 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.

[2] J. Liu, Y. Du, S.-i. Yim, X. Lu, B. Chen, and F. Qiu, "Steady-state analysis of microgrid distributed control under denial of service attacks," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2020.

[3] B. Yang, L. Guo, F. Li, J. Ye, and W.-Z. Song, "Vulnerability assessments of electric drive systems due to sensor data integrity attacks," *IEEE Transactions on Industrial Informatics*, 2019.

[4] L. Guo, B. Yang, J. Ye, H. Chen, F. Li, W.-Z. Song, L. Du, and L. Guan, "Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles," *IEEE Transactions on Industrial Informatics*, 2020.

[5] E. I. Batzelis, G. Anagnostou, I. R. Cole, T. R. Betts, and B. C. Pal, "A state-space dynamic model for photovoltaic systems with full ancillary services support," *IEEE Transactions on Sustainable Energy*, vol. 10, no. 3, pp. 1399–1409, 2018.

[6] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, "Microgrid risk analysis considering the impact of cyber attacks on solar pv and ess control systems," *IEEE transactions on smart grid*, vol. 8, no. 3, pp. 1330–1339, 2016.

[7] B. Yang, F. Li, J. Ye, and W. Song, "Condition monitoring and fault diagnosis of generators in power networks," in *2019 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2019, pp. 1–5.

[8] F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, and W. Song, "Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2019.

[9] F. Li, Q. Li, J. Zhang, J. Kou, J. Ye, W. Song, and A. H. Mantooth, "Detection and diagnosis of data integrity attacks in solar farms based on multi-layer long short-term memory network," *IEEE Transactions on Power Electronics*, pp. 1–1, 2020.

[10] X. Wang, F. Blaabjerg, M. Liserre, Z. Chen, J. He, and Y. Li, "An active damper for stabilizing power-electronics-based ac systems," *IEEE Transactions on Power Electronics*, vol. 29, no. 7, pp. 3318–3329, 2013.

[11] W. Cao, "Impedance-based stability analysis and controller design of three-phase inverter-based ac systems," 2017.

[12] S. B. Kotsiantis, I. Zaharakis, and P. Pintelas, "Supervised machine learning: A review of classification techniques," *Emerging artificial intelligence applications in computer engineering*, vol. 160, pp. 3–24, 2007.

[13] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. MIT press, 2016.