Hybrid Cyber-attack Detection in Photovoltaic Farms

Jinan Zhang
Eaton Research Lab
Golden, CO, USA
jinanzhang@eaton.com

Jin Ye
University of Georgia
Athens, GA, USA
jin.ye@uga.edu

Wenzhan Song
University of Georgia
Athens, GA, USA
wsong@uga.edu

Jianming Lian
Oak Ridge National Laboratory
Oak Ridge, TN, USA
lianj@ornl.gov

Dongbo Zhao
Eaton Research Lab
Golden, CO, USA
dongbozhao@eaton.com

He Yang
University of Georgia
Athens, GA, USA
heyang95@uga.edu

2023 IEEE Energy Conversion Congress and Exposition (ECCE) | 979-8-3503-1644-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ECCE53617.2023.10362667

***Abstract*—To address the cyber-physical security in PV farms, a hybrid cyber-attack detection is proposed in this manuscript. To secure PV farms, the proposed method integrates model-based and data-driven methods by fusing the detection score at the device and system levels. First, a model-based cyber-attack detection method is developed for each PV inverter. A residual between the estimation of the Kalman filter and measurement is calculated. By leveraging the calculated residual from all inverters, a squared Mahalanobis distance is developed for device detection score generation. At the system level, a convolutional neural network (CNN) is proposed to detect cyber-attack using the waveform data at the point of common coupling (PCC) in PV farms. To improve the CNN detection accuracy, a set of well-designed features are extracted from the raw waveform data. Finally, a weighted detection score fusion method is proposed to combine device and system detection scores by using their complementary strength. The feasibility and robustness of the proposed method are validated by testing cases and a comparative experiment.**

***Index Terms*—Kalman filter, squared Mahalanobis distance, convolutional neural network, score fusion, hybrid detection, cyber-attack, PV farm security**

I. Introduction

The smart grid, one of the largest cyber-physical systems, is a critical infrastructure for society. Due to the reliance on information and communication technologies, the smart grid faces a significant risk in security [1]. For example, attackers hack the power grid leading to a power outage for 16 hours in Ukraine [2]. Malware Stuxnet compromises critical equipment in utilities is reported in [3]. With a growing number of distributed energy sources (DERs), a new type of cyber-attack compromising DERs inverter also appears [4]. In [5], the authors introduce a non-invasive attack targeting the PV inverter. A noise injection attack in a grid-connected inverter is demonstrated in [6].

PV farm plays a vital role in smart grid operation. With built-in remote function in inverters, PV farms have started to anticipate the grid support service [7]. Once attackers compromise PV farms, it not only destroys the power generation of PV farms but also impacts the stability of the smart grid. To secure the PV farms, attack detection has been designed to alleviate the attack impact at an early stage. Existing works on attack detection are categorized into data-driven and model-based approaches. Data-driven strategies show promise in attack detection without using any physical model information. Because of their reliance on sufficient data, data-driven approaches are typically deployed at the system level. For example, features in the time and frequency domain are proposed to detect cyber-attack using measurement at PCC of photovoltaic (PV) farms [8]. In [9], a deep learning model is developed to detect false data injection attacks in the state estimation of the power grid. Although data-driven methods can achieve a high detection accuracy in offline training, they require a large amount of training data that is unavailable in the real world. Deficient attack cases causing the imbalanced data set may degrade the detection performance of the data-driven method. In addition, some data-driven methods cannot address stealthy attacks without physical model information. On the contrary, the model-based approach makes use of the physical model to estimate system status. By leveraging the residual between estimates and measurement, cyber-attacks are detected. As discussed in [6], the high-frequency noise is analyzed and identified by Kalman filter-based detection approach in the inverter controller. While data-driven and model-based approaches can, to some extent, address cyber attacks at the system and device levels, respectively, a comprehensive framework for cyber attack detection for PV farms is still lacking. It is an open challenge to combine model-based detection methods in each inverter and data-driven methods for PV farms.

In [10], a fusion method is proposed for decision-making. It fuses different decisions into a new or better decision which provides a new fundamental solution for the coordination of model-based and data-driven cyber-attack detection in PV farms. Based on this decision-in and decision-out approach [10], a hybrid cyber-attack detection framework is proposed for PV farms as shown in Fig, 1. In each PV inverter, a model-based cyber-attack detector is developed. With the Kalman filter in the proposed detector, a residual between

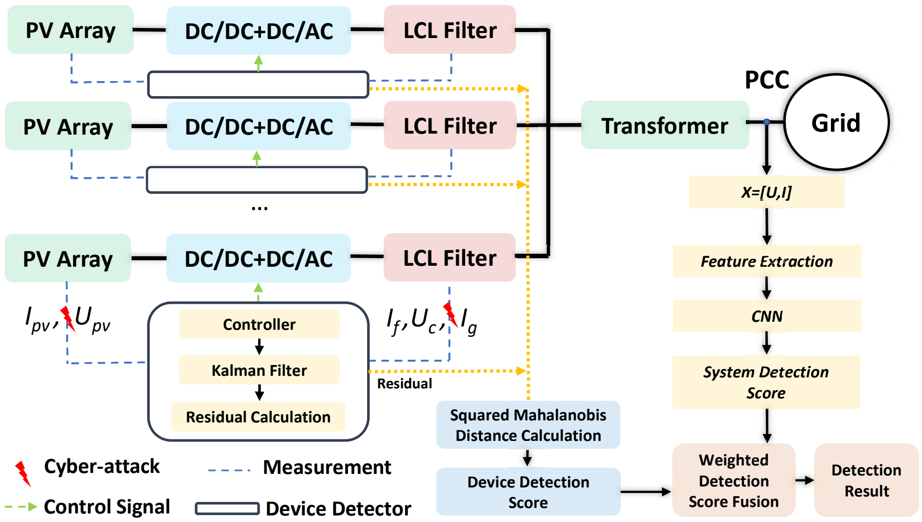

Fig. 1. Schematic diagram of hybrid cyber-attack detection in PV farms.

estimation and measurement is calculated. Then, the squared Mahalanobis distance is developed to fuse the residual of all inverters and generate a device detection score. At the system level, a convolutional neural network (CNN) is developed for system detection score using measurement data at the point of common coupling (PCC). In addition, a set of features is extracted to improve the model training efficiency and detection accuracy. Finally, a weighted detection score fusion method is designed for cyber-attack detection in PV farms.

II. PV Farm and Cyber-attack Modeling

A. PV Farms Modeling

a large-scale PV farm consists of two-stage PV inverters connected in parallel. Within each PV conversion system, the PV array is linked to a DC/DC converter, which then converts the DC power to AC power through a DC/AC inverter. On the grid side of the PV inverter, an LCL filter is employed to effectively mitigate the presence of harmonics in the AC current. The dynamics of the inverter are depicted below.

$$u_{in}^{p} = S^{p}\frac{u_{dc}}{2} \tag{1}$$

where u_{in}^{p} is the inverter-side voltage in phase p, S^{p} is the switch signal in phase p, $p = a, b, c$, u_{dc} is the DC-link voltage. Then, the model of the PV inverter referring to the LCL filter can be derived as

$$\dot{x} = Ax + Bu \tag{2}$$

Where $x = [I_f^a, I_f^b, I_f^c]^T$, I_f^p is the inverter-side inductance current, $u = [U_{in}^a, U_{in}^b, U_{in}^c, U_c^a, U_c^b, U_c^c]^T$, U_{in}^p is the inverter-side voltage, U_c^p is the capacitor voltage.

$$A = \begin{bmatrix} \frac{-R}{L} & 0 & 0 \\ 0 & \frac{-R}{L} & 0 \\ 0 & 0 & \frac{-R}{L} \end{bmatrix} \quad B = \begin{bmatrix} \frac{1}{L} & 0 & 0 & \frac{-1}{L} & 0 & 0 \\ 0 & \frac{1}{L} & 0 & 0 & \frac{-1}{L} & 0 \\ 0 & 0 & \frac{1}{L} & 0 & 0 & \frac{-1}{L} \end{bmatrix} \tag{3}$$

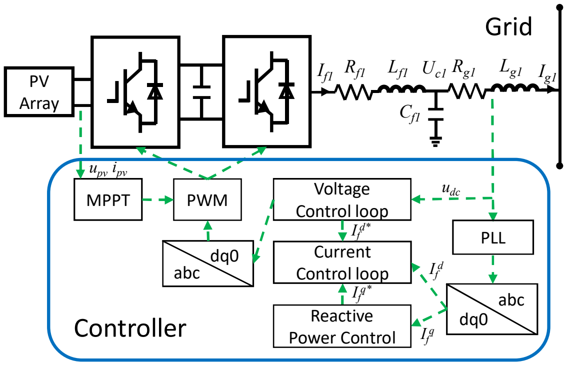

Fig. 2. A PV inverter controller.

As shown in Fig. 2, maximum power point tracking (MPPT) method is designed to force the PV array generate maximum power to power grid. Additionally, a PI-based PV inverter controller, comprising a DC-link voltage control loop, current control loop, and reactive control loop, is developed for the PV system. The DC-link voltage controller is designed to maintain the stability of the capacitor voltage, while the reactive power control loop regulates the generation of the required reactive power. The control reference for $I_f^{d,q}$ is denoted as $I_f^{d*,q*}$.

B. Cyber-attack Modeling

In this paper, a cyber-attack is defined to compromise the measured data in the PV inverter sensor as shown in Fig. 1. To clarify the attack model, the cyber-attack is expressed during attack time as follows.

$$Y_f = \omega Y_o + \alpha \tag{4}$$

where Y_f is the compromised sensor data which is the final input of the controller; Y_o is the original measurement data;

α represents the false data that is injected into the sensor of the inverter, ω is attack gain.

III. Hybrid Cyber-attacks Detection Method

In this section, a hybrid cyber-attack detection method is developed, including device detection score, system detection score, and weighted score fusion techniques.

A. Kalman Filter in PV inverter

Kalman filter is widely used in time-series data analysis and is good at state estimating with noise and uncertainties. In the Kalman filter, the sensor measurements are forwarded to Kalman Filter at a certain time interval. Then, at each time step, the Kalman filter calculates an accurate estimation result of the system state based on the system model from the previous time step and the real-time sensor data. Based on the PV inverter, the inverter can be derived considering the impact of noise and uncertainties which is expressed as follows.

$$\begin{aligned} x[k+1] &= A_d x[k] + B_d u[k] + Bw, Cov(w) = Q \\ y[k] &= C_d x[k] + v, Cov(v) = R \end{aligned} \tag{5}$$

Where Q is the process noise covariance matrix, R is the measurement noise covariance matrix. Based on the above inverter model, the estimation of the Kalman Filter can be derived, which has been described in [11].

B. Device Detection Score

To detect cyber-attacks, the residual between states estimation of Kalman filter and measurement in PV inverters is calculated as follows,

$$\Gamma = X - \hat{X} \tag{6}$$

Where $\Gamma = [\gamma_1, ..., \gamma_n]$ is calculated residual, $X = [x_1, ..., x_n]$ is the measurement signal, x_n is n_{th} PV inverter measurement, $\hat{X} = [\hat{x}_1, ..., \hat{x}_n]$ is the estimation of the Kalman filter, $\hat{x}_n$ is n_{th} PV inverter estimation. With Kalman filter, the calculated residual Γ represents the status variation of PV inverters. To detect cyber-attacks, squared Mahalanobis distance (SMD) is calculated as follows,

$$\delta_{SMD} = (\Gamma - \mu)^T \Sigma^{-1} (\Gamma - \mu) \tag{7}$$

where μ and Σ are the expectation and covariance matrices of Γ under normal conditions, respectively. The Σ is calculated by using a maximum likelihood estimator. Then, the device detection score is derived as

$$S_{device} = tanh(\frac{\delta_{SMD}}{T}) \tag{8}$$

Where $\tanh$ is a hyperbolic tangent function, δ_{SMD} is the squared Mahalanobis distance, T is a detection threshold value of the device detection method in the PV inverter.

C. Data-driven cyber-attacks detection method using CNN

Fig. 1 presents that the measurement at PCC is used for cyber-attack detection at the system level. Several critical features are extracted from measurement data first. Then, all extracted features are labeled and normalized in the data pre-processing. The data-driven model is trained to make an accurate classification using these features. Finally, the cyber-attack is identified using a well-trained neural network. Three-phase voltage and current at PCC are used as the input data of the proposed method, which is denoted by:

$$X_t^{pcc} = [U_a, U_b, U_c, I_a, I_b, I_c]^T \tag{9}$$

where the subscript t represents the time; U_a, U_b, U_c and I_a, I_b, I_c are the 3-phase voltage [V] and current [A] sample measurement at the PCC node, respectively. To improve the efficiency of the data model, a set of critical features is extracted from X_t^{pcc}, which is expressed as

$$X_{ft}^{pcc} = [F_U, M_U, THD_U, F_I, M_I, THD_I]^T \tag{10}$$

where $F_{U,I}$ are the frequency of three-phase voltage and current at PCC, respectively; $M_{U,I}$ are the magnitude of three-phase voltage and current at PCC, respectively; $THD_{U,I}$ are THD of three-phase voltage and current at PCC, respectively.

In recent years, CNN is trained to detect anomalous behaviors, such as [12], [13]. With the noise-resistance, CNN has the potential to process time-series data. In this paper, CNN is used as a data model to detect cyber-attacks in PV farms. In addition, a sigmoid activation function in the output layer is often used for classification. The sigmoid function is expressed as

$$sigmoid(x) = \frac{e^x}{e^x + 1} \tag{11}$$

A classification layer is adopted by using the cross-entropy error to calculate the cost function, as

$$\min_{W} \ J = -\frac{1}{M} \sum_{i=1}^{M} \sum_{j=1}^{n_c} y_j^i \cdot \log(\hat{y}_j^i) \tag{12}$$

where M is the number of training samples; y represents the ground truth; $\hat{y}$ is the predicted result; W represents weights and biases. Because the sigmoid function is used to normalize the output prediction to be a valid probability distribution. Thus, the output of the sigmoid function at the classification layer is used as the system detection score S_{system}.

D. Weighted Detection Score Fusion

To increase detection accuracy, detection capabilities from devices and systems are used simultaneously. The device detection score represents the model-based cyber-attack detection result considering the dynamics in each PV inverter. The system detection score is the output of the data-driven method using the measurement at PCC. To fuse two scores, a weighted detection score is proposed as

$$S_{fusion} = \alpha_d S_{device} + \alpha_s S_{system} \tag{13}$$

TABLE I
$[\omega, \alpha]$ SETTING IN SINGLE ATTACKS

Attack	I_f	Target	Attack Time
Attack 1	$[1, 100]_a, [1, 200]_b, [1, 300]_c$	PV1	[0.2, 1]s
Attack 2	$[1, 100 + 200sin(20\pi t)]_a, [1, 0]_b, [1, 0]_c$	PV1	[0.2, 1]s
Attack 3	$[1, 300 + 100sin(2\pi t)]_a, [1, 200 + 300sin(2\pi t)]_b, [1, 100 + 200sin(2\pi t)]_c$	PV1	[0.2, 1]s
Attack 4	$[1, 300 + 100sin(20\pi t)]_a, [1, 200 + 300sin(60\pi t)]_b, [1, 100 + 200sin(40\pi t)]_c$	PV1	[0.2, 1]s
Attack 5	$[1, 100sin(200\pi t)]_a, [1, 300sin(600\pi t)]_b, [1, 200sin(400\pi t)]_c$	PV1	[0.2, 1]s
Attack 6	$[1, 300sin(200\pi t)]_a, [1, 300sin(600\pi t)]_b, [1, 300sin(400\pi t)]_c$	PV1	[0.2, 1]s
Attack 7	$[1, 0]_a, [1, 300sin(600\pi t)]_b, [1, 0]_c$	PV1	[0.2, 1]s
Attack 8	$[1, 0]_a, [1, 0]_b, [1, 300sin(600\pi t)]_c$	PV1	[0.2, 1]s
Attack 9	$[1, 0]_a, [1, 300sin(600\pi t)]_b, [1, 300sin(600\pi t)]_c$	PV1	[0.2, 1]s
Attack 10	$[1, 200sin(1000\pi t)]_a, [1, 500sin(200\pi t)]_b, [1, 100sin(400\pi t)]_c$	PV1	[0.2, 1]s
Attack 11	$[1, 100sin(110\pi t)]_a, [1, 300sin(30\pi t)]_b, [1, 200sin(42\pi t)]_c$	PV1	[0.2, 1]s
Attack 12	$[1, 100sin(120\pi t)]_a, [1, 300sin(120\pi t)]_b, [1, 200sin(120\pi t)]_c$	PV1	[0.2, 1]s
	$[1, 100sin(120\pi t)]_a, [1, 300sin(120\pi t)]_b, [1, 200sin(120\pi t)]_c$	PV2	[0.2, 1]s
Attack 13	$[1, 400sin(1200\pi t)]_a, [1, 100sin(20\pi t)]_b, [1, 300sin(80\pi t)]_c$	PV1	[0.2, 1]s
	$[1, 0]_a, [1, 500sin(600\pi t)]_b, [1, 0]_c$	PV2	[0.2, 1]s
Attack 14	$[1, 200sin(32\pi t)]_a, [1, 100sin(38\pi t)]_b, [1, 150sin(40\pi t)]_c$	PV1	[0.2, 1]s
	$[1, 100]_a, [1, 200]_b, [1, 300]_c$	PV2	[0.2, 1]s
Attack 15	$[1, 200 + 100sin(26\pi t)]_a, [1, 100 + 300sin(24\pi t)]_b, [1, 150 + 200sin(34\pi t)]_c$	PV1	[0.2, 1]s
	$[1, 200sin(1000\pi t)]_a, [1, 500sin(200\pi t)]_b, [1, 100sin(400\pi t)]_c$	PV2	[0.2, 1]s
Attack 16	$[0.8, 0]_a, [0.8, 0]_b, [0.8, 0]_c$	PV1	[0.2, 1]s
Attack 17	$[0.2, 0]_a, [0.2, 0]_b, [0.2, 0]_c$	PV1	[0.2, 1]s

where α_d and α_s are detection weight, S_{fusion}, S_{device}, and S_{system} are the fusion detection score, device detection score, and system detection score, respectively. The detection result is obtained using following equation.

$$Detection\ Result = \begin{cases} Normal,\ S_{fusion} < T_{fusion}, \\ Attack,\ S_{fusion} > T_{fusion}. \end{cases} \quad (14)$$

Where T_{fusion} is the threshold in the score fusion.

IV. SIMULATION RESULT

A. Simulation Model

To test the proposed detection algorithm, four two-stage PV inverters enabled PV farm is simulated in the MATLAB as shown in Fig. 1. The rated power in each PV inverter is 125kW. The DC-link voltage of the PV inverter is $1500V$. The grid voltage is $480V_{rms}$. To test the proposed detection method in the PV farm, several attacks are designed in Table. I. As shown in Table. I, different set of attack vector $[\omega, \alpha]$ are designed to compromise the sensor measurement in PV inverter 1(PV1) and PV inverter 2(PV2). $[\omega, \alpha]_a$ is the attack vector in phase A measurement.

B. Training, Testing Cases and Accuracy Definition

Under the different attack cases in Table I, a large number of data set in the PV farm is generated. The sampling rate is 20 kHz. For a detailed analysis of the introduced features and detection algorithm, we compare the results of using the two different methods. One only employs CNN to detect cyber-attacks. The other one uses the proposed hybrid cyber-attack detection method which fuses the device detection score of SMD and system detection score from CNN. For convenient expression, we denote the these two methods as CNN and SMD+CNN, respectively.

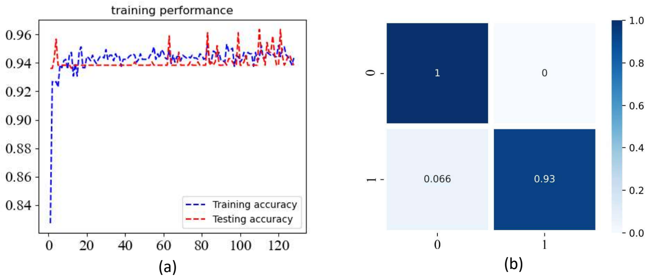

Fig. 3. (a) Training and Testing Accuracy of CNN; (b) fusion matrix of CNN.

In the training process of CNN, the data of attack 1-16 scenarios in TABLE. I is randomly split into a training (70% of data) set and a test (30%) set. To validate the performance of the proposed method, the stealthy attack 17 in TABLE. I, which is not included in the model training, is designed as a validation case for both methods.

To evaluate the performance of detection methods, the testing accuracy is defined as follows:

$$Acc = \frac{N_{nt} + N_{at}}{N_{total}} \quad (15)$$

where N_{nt} and N_{at} represent the number of samples that are correctly identified as normal and attack, respectively; N_{total} represents the total number of testing samples.

C. Detection Result Analysis

The testing accuracy of CNN for attack 1-16 is summarized in Fig. 3. The testing accuracy of the CNN is 96.5%. It is noted that 6.6% of attack data are misclassified to normal condition in Fig. 3(b). This error mainly comes from attack 16. Fig. 4 shows the attack 16 impact on the PV1. Due to

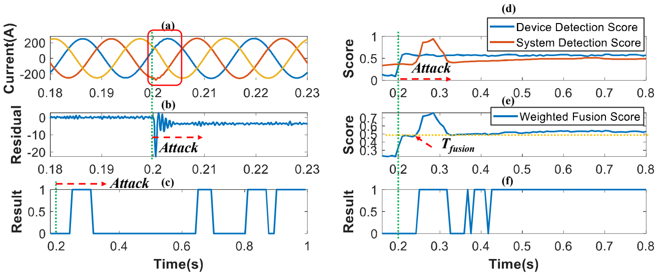

Fig. 4. (a) Output current I_g of PV1; (b) calculated residual γ_1 of PV1; (c) detection result of CNN; (d) Device and system detection score; (e) weighted fusion score; (f) detection result of attack 16 using fusion score.

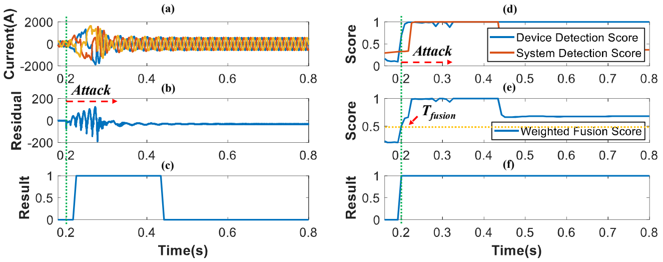

Fig. 5. (a) Output current I_g of PV1; (b) calculated residual γ_1 of PV1; (c) detection result of CNN; (d) Device and system detection score; (e) weighted fusion score; (f) detection result of attack 17 using fusion score.

the minor impact around 0.2s, it is hard for CNN to detect attack. After the 0.25s in Fig. 4(a), there is no distortion and harmonics in the output current. This attack leads to the degraded performance of CNN as shown in Fig. 4(c).

But at the device level, the residual in Fig. 4 (b) illustrates the discrepancy between estimation and measurement. Based on the Kalman filter, the device detector identifies attack 16. Then, the proposed method, SMD+CNN, makes full use of device and system detection scores in the PV farm simultaneously. The corresponding detection result is shown in Fig. 4(d-f). Based on the Eq. (13), the weighted fusion score fusion is calculated in Fig. 4(d,e). Compared to CNN, the attack 16 is identified by the proposed method SMD+CNN as shown in Fig. 4(f). Compared to Fig. 4(c), the detection accuracy for attack 16 is improved from 35.42% to 86.46% in Fig. 4(f).

D. Stealthy Attack Detection Analysis

In this section, stealthy attack 17 is tested using CNN and SMD+CNN, respectively. Fig. 5(a) shows that attack 17 impacts the output of PV1. With extracted features, CNN still identifies the anomaly in the current waveform at PCC in Fig. 5(c). Although the waveform restores to normal after the transit impact, the false data injected by attack 17 does not disappear which is observed by the calculated residual by Kalman filter in Fig. 5(b). Compared to CNN, the SMD+CNN shows better resilience in the stealthy attack 17. As shown in Fig. 5(e-f), the device detection score is fused into the detection result using a weighted fusion score. Fig. 5(f) shows attack 17 is identified by the proposed method.

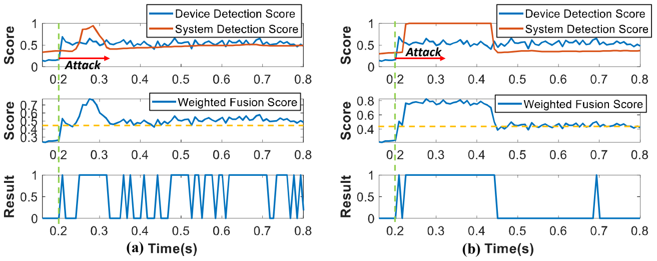

Fig. 6. (a) Device, system detection score, and detection result of attack 16 using hierarchical clustering+CNN; (b) Device, system detection score, and detection result of attack 17 using hierarchical clustering+CNN.

E. Comparison Simulation Result of the Hybrid Method using Clustering and CNN

Clustering is an unsupervised learning technique. Since it does not require data labeling in model training, many works have developed cyber-attack detection and diagnosis by utilizing clustering method. In [14], a hybrid cyber-attack detection method in power grids is proposed by integrating hierarchical clustering and decision tree. Motivated by the high efficiency of the clustering method, a comparative experiment is conducted by replacing SMD with hierarchical clustering. Fig. 6 shows the detection result of hierarchical clustering+CNN in attack 16 and attack 17. The detection accuracy of attack 16 and attack 17 are 63.54% and 31.25%, respectively. Compared to SMD+CNN, hierarchical clustering cannot capture more dynamic information in the device detection score, resulting in a moderate performance after data fusion. This experiment also demonstrates a better performance of the proposed method (SMD+CNN) in cyber-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] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2011.

[2] D. Volz, "Us government concludes cyber attack caused ukraine power outage," *Reuters, February*, vol. 25, 2016.

[3] A. S. Bretas, N. G. Bretas, B. Carvalho, E. Baeyens, and P. P. Khargonekar, "Smart grids cyber-physical security as a malicious data attack: An innovation approach," *Electric Power Systems Research*, vol. 149, pp. 210–219, 2017.

[4] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G.-S. Seo *et al.*, "A review of cyber–physical security for photovoltaic systems," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 4, pp. 4879–4901, 2021.

[5] A. Barua and M. A. Al Faruque, "Hall spoofing: A non-invasive dos attack on grid-tied solar inverter," in *29th {USENIX} Security Symposium ({USENIX} Security 20)*, 2020, pp. 1273–1290.

[6] N. Gajanur, M. D. R. Greidanus, S. K. Mazumder, and M. A. Abbaszada, "Impact and mitigation of high-frequency side-channel noise intrusion on the low-frequency performance of an inverter," *IEEE Transactions on Power Electronics*, vol. 37, no. 10, pp. 11 481–11 485, 2022.

[7] E. Bullich-Massagué, R. Ferrer-San-José, M. Aragüés-Peñalba, L. Serrano-Salamanca, C. Pacheco-Navas, and O. Gomis-Bellmunt, "Power plant control in large-scale photovoltaic plants: design, implementation and validation in a 9.4 mw photovoltaic plant," *IET Renewable Power Generation*, vol. 10, no. 1, pp. 50–62, 2016.

[8] L. Guo, J. Zhang, J. Ye, S. J. Coshatt, and W. Song, "Data-driven cyber-attack detection for pv farms via time-frequency domain features," *IEEE Transactions on Smart Grid*, vol. 13, no. 2, pp. 1582–1597, 2021.

[9] X. Niu, J. Li, J. Sun, and K. Tomsovic, "Dynamic detection of false data injection attack in smart grid using deep learning," in *2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2019, pp. 1–6.

[10] B. Dasarathy, "Sensor fusion potential exploitation-innovative architectures and illustrative applications," *Proceedings of the IEEE*, vol. 85, no. 1, pp. 24–38, 1997.

[11] J. Zhang and J. Ye, "Cyber-attack detection for active neutral point clamped (anpc) photovoltaic (pv) converter using kalman filter," in *2022 IEEE Applied Power Electronics Conference and Exposition (APEC)*, 2022, pp. 1939–1944.

[12] L. Guo, J. Zhang, J. Ye, S. J. Coshatt, and W. Song, "Data-driven cyber-attack detection for pv farms via time-frequency domain features," *IEEE Transactions on Smart Grid*, vol. 13, no. 2, pp. 1582–1597, March 2022.

[13] W. Qiu, Q. Tang, Y. Wang, L. Zhan, Y. Liu, and W. Yao, "Multi-view convolutional neural network for data spoofing cyber-attack detection in distribution synchrophasors," *IEEE Transactions on Smart Grid*, 2020.

[14] A. Aflaki, M. Gitizadeh, R. Razavi-Far, V. Palade, and A. A. Ghasemi, "A hybrid framework for detecting and eliminating cyber-attacks in power grids," *Energies*, vol. 14, no. 18, p. 5823, 2021.