Real-Time Estimation and Defense of PV Inverter Sensor Attacks With Hardware Implementation

Kaikai Pan, *Member, IEEE*, Zhiyun Wang, Jingwei Dong, Peter Palensky, *Senior Member, IEEE*, and Wenyuan Xu, *Fellow, IEEE*

***Abstract*—Sensor attacks on grid-tie photovoltaic (PV) inverters can cause severe damage. Considering uncertain environments and unknown model mismatches, real-time estimation and defense for sensor attacks on actual PV inverters are challenging. In this article, we propose an optimization-driven robust estimator within the attack frequency range using the $\mathcal{H}_\infty$ index, while the model mismatch effect on estimation is also minimized. To improve the real-time response under varying environments, an analytical solution from a convex quadratic programming reformulation is constructed. Guided by the estimation, we further develop a closed-loop compensation strategy with a tracking controller and a low-pass filter. Through code porting, our proposed defense strategy has been implemented in a microcommercial PV inverter. Hardware implementations show that our defense approach can effectively mitigate sensor attacks and maintain stable inverter operation.**

***Index Terms*—Hardware implementation, photovoltaic (PV) inverter, real-time robust estimation, sensor attacks, time-varying.**

I. Introduction

THE embedded sensors in photovoltaic (PV) inverters are crucial for safe power conversion. However, PV inverters are frequently installed in less secure areas and the growing presence of third-party entities can complicate the security landscape, heightening the risk of sensor attacks via physical and cyber methods [1]. For instance, the physical attack "Hall Spoofing" [2] injects errors into current sensors of inverters using an external magnetic field, and the cyber attack "Horus" [3] exposes sensor data to integrity attacks. They can cause the victim inverter to reduce output power, shut down and even physically burn out. Thus, it is urgent to develop real-time estimation and defense approaches to protect PV inverters.

Previous studies have investigated the defense methods against sensor attacks from data-driven and model-based perspectives. Research works have utilized multiclass support vector machines [4], and long and short-term memory networks [5] to achieve attack detection. However, data-driven approaches are highly dependent on the quantity and quality of the accessible data and thus can be intractable somehow. To our knowledge, digital signal processors (DSPs) have been commonly utilized in PV inverters [6]. They are characterized by modest computing power and storage, exemplified by the TMS320F28035 in our experiment (60 MHz CPU frequency, 128 kB of flash memory, and 20 kB of RAM). Such constraints pose challenges in implementing complex data-driven algorithms. For model-based approaches, research in [7] has proposed a Kalman filter and adaptive cumulative sum chart to detect the low-frequency spoofed sensor data. The work in [8] studies the impact of side-channel noise intrusion on inverters with a model-based mitigation strategy. Yet many of them overlooked model parameter variations due to environmental factors, as well as mismatches between the mathematical model and the physical inverter, leading to performance degradation and challenges in hardware implementation.

To tackle these, we develop a real-time sensor attack estimator for the parameter-varying PV inverter and establish a lightweight defense approach. First, we introduce a time-varying model of the inverter and obtain the model parameters through system identification. Then, we propose an optimization-driven robust estimator using the $\mathcal{H}_\infty$ index and alleviating model mismatch effects on attack estimation. We further propose an analytical form of the estimator to cope with real-time environmental variations. Next, the estimation outcome is utilized to devise a feed-forward compensation strategy into the inverter's control loop. Hardware implementations show that our proposed estimator and defense approach effectively mitigate potential severe damage.

Kaikai Pan, Zhiyun Wang, and Wenyuan Xu are with the College of Electrical Engineering, Zhejiang University, Hangzhou 310058, China (e-mail: pankaikai@zju.edu.cn; zhiyw@zju.edu.cn; wyxu@zju.edu.cn).

Jingwei Dong is with the Division of Systems and Control, Department of Information Technology, Uppsala University, 75105 Uppsala, Sweden (e-mail: jingwei.dong@it.uu.se).

Peter Palensky is with the Department of Electrical Sustainable Energy, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology (TU Delft), 2600 Delft, The Netherlands (e-mail: p.palensky@tudelft.nl).

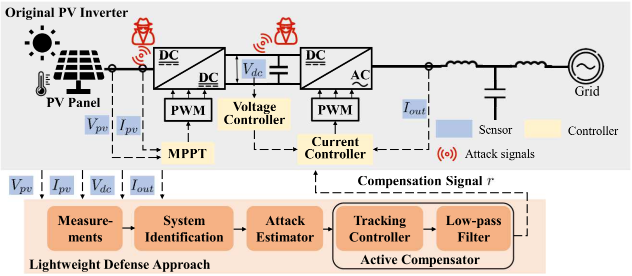


Fig. 1. Grid-tie PV inverter under sensor attacks.

II. The Time-Varying PV Inverter Model

Fig. 1 illustrates that attackers can launch physical or cyber attacks on inverter's voltage and current sensors. A physical two-stage PV inverter can be modeled by integrating the physical plant and the control loop, which has been developed in the previous work [9], [10]. To construct a more realistic inverter model, we consider that the optimal output voltage and current of PV panels may vary with environmental factors (e.g., temperature and irradiance), leading to a time-varying operating point of the inverter. Thus, the linear time-varying inverter model under sensor attacks can be described by

$$\begin{aligned} x(k+1) &= A(w_k)x(k) + B_u u(k) + B_f f(k) + B_r r(k) \\ y(k) &= Cx(k) + D_f f(k) + D_r r(k) \end{aligned} \tag{1}$$

where $x(k)$ denotes physical states of the inverter and also control intermediate variables, $u(k)$ is the input signal, $r(k)$ is the compensation signal to be designed later, and $y(k)$ represents measured output of voltage and current. Here $f(k)$ denotes sensor attacks on the output of PV panels, the dc-bus voltage, and the inverter output current. $A(w_k)$ is the parameter-varying matrix with the environmental factor w (from a set $\mathcal{W} \in \mathbb{R}^{n_w}$). The coefficients matrices B_u, B_f, B_r, C, D_f, and D_r have compatible dimensions.

We first analyze the hardware circuits and the available open-source control code to obtain part of the model parameters. Then we gather hours of input and output data from the physical inverter in a constant environmental setting. These data are utilized for system identification, based on Levenberg–Marquardt's least-squares search method with fixed partial parameters [11]. Once all the system parameters for the current case are acquired, the system matrix $A(w_k)$ can be recalculated by the physical relationships, accounting for changes in w. In many practical scenarios, attack signals often target at specific frequencies to deliver customized damage [12]. Note that the attack signal in this article refers to the signal superimposed on the sensor measurement. Our goal is to devise a robust estimation and defense approach within a specific attack frequency range, based on the input signal $u(k)$ and the measurement $y(k)$. To achieve that, we first rerepresent (1) with a more compact difference algebraic equation (DAE) formulation

$$H\left(w_k, \mathfrak{q}\right) X(k) + L\left(\mathfrak{q}\right) z(k) + F\left(\mathfrak{q}\right) f(k) = 0 \tag{2}$$

where $\mathfrak{q} = e^{j\theta}$ represents the time shift operator and θ denotes the frequency within the range $[\vartheta_1, \vartheta_2]$. By defining $z(k) := [y(k)^T \;\; u(k)^T]^T$, $X(k) := [x(k)^T \;\; r(k)^T]^T$, the polynomial matrices $H\left(w_k, \mathfrak{q}\right)$, $L\left(\mathfrak{q}\right)$, $F\left(\mathfrak{q}\right)$ in $\mathfrak{q}$ can be expressed as

$$H\left(w_k, \mathfrak{q}\right) := \begin{bmatrix} -\mathfrak{q} + A\left(w_k\right) & B_r \\ C & D_r \end{bmatrix}, L\left(\mathfrak{q}\right) := \begin{bmatrix} 0 & B_u \\ -I & 0 \end{bmatrix},$$

$$F\left(\mathfrak{q}\right) := \begin{bmatrix} B_f \\ D_f \end{bmatrix}.$$

III. Defense of PV Inverter Sensor Attacks

For the DAE (2), we introduce an estimation signal e consisting of linear transfer functions in the following form:

$$e(k) := R(w, \mathfrak{q})z(k) := a^{-1}(\mathfrak{q})N(w, \mathfrak{q})L(\mathfrak{q})z(k) \tag{3}$$

where $R(w, \mathfrak{q})$ is the transfer function from the available signal to the estimator. We propose a formulation that $R(w, \mathfrak{q}) := a^{-1}(\mathfrak{q})N(w, \mathfrak{q})L(\mathfrak{q})$ where $N(w, \mathfrak{q})$ is the polynomial with coefficients to be designed for a fixed denominator $a(\mathfrak{q})$ with a low order to reduce overhead in real-time implementation. The estimation signal is designed to decouple the unknown dynamics to minimize the impact of environmental factors and system states on the estimation, which indicates

$$a^{-1}(\mathfrak{q})N(w, \mathfrak{q})H\left(w_k, \mathfrak{q}\right) = 0, \forall w \in \mathcal{W}, \theta \in [\vartheta_1, \vartheta_2]\,. \tag{4}$$

By design, our estimation signal can be varied with w to ensure that the above equation holds at every moment. For an accurate estimation, the estimation signal is expected to follow and approximate the attack signal f. By combining (2) and constraint (4), we aim to find a stable $R(w, \mathfrak{q})$ such that

$$e(k) = -a^{-1}(\mathfrak{q})N(w, \mathfrak{q})F(\mathfrak{q})f(k) \approx f(k), \quad \theta \in [\vartheta_1, \vartheta_2] \tag{5}$$

$$G_{ef}(\mathfrak{q}, w)f(k) - I \approx 0, \theta \in [\vartheta_1, \vartheta_2] \tag{6}$$

where $G_{ef}(\mathfrak{q}, w) = -a^{-1}(\mathfrak{q})N(w, \mathfrak{q})F(\mathfrak{q})$. Notably, achieving $G_{ef}(\mathfrak{q}, w)f(k) - I = 0$ for all $\theta \in [\vartheta_1, \vartheta_2]$ is unattainable due to its infinite equality constraints. To render the constraint tractable, we introduce the finite $\mathcal{H}_\infty$ norm for (6)

$$||G_{ef}(\mathfrak{q}, w)f(k) - I||_{\mathcal{H}_\infty(\theta)} \leq \eta, \;\; \theta \in [\vartheta_1, \vartheta_2] \tag{7}$$

where η is the upper bound. Using η as the optimization objective can narrow the gap between the estimation and the attack signal. Moreover, *accounting for interference and nonlinearity inevitably results in a model mismatch between the linear model (1) and the actual PV inverter.* We introduce a model mismatch signature matrix $\bar{Q}$ [13] into the optimization objective to mitigate the effects of model mismatch on attack estimation. $\bar{Q}$ is a positive semi-definite real matrix obtained through prior inverter operations.

The design of the estimator parameters can be transformed into an optimization problem by expressing the constraint (7) as linear matrix inequalities through the GKYP lemma. To achieve a timely estimation and response, we construct an optimization-driven robust estimator with an analytical solution for the estimator parameters. We relax the constraint (7) by letting $G_{ef}(\mathfrak{q}, w)$ approximate the identity matrix at selected frequency points instead of the whole range $[\vartheta_1, \vartheta_2]$. More specifically, the optimal parameters of the estimator $N^*(w)$ can be derived by solving the problem

$$N^*(w) := \underset{N(w)}{\arg\min} \sum_{i=1}^{n} (\alpha_i + \beta_i) + \mu N(w)\bar{Q}N(w)^T$$

$$\text{s.t.} \qquad N(w)H(w) = 0 \tag{8a}$$

$$\operatorname{Re}\left(G_{ef}\left(e^{j\theta_i}, w\right) - 1\right)^2 \leq \alpha_i, \forall i = (1, 2, ..., n) \tag{8b}$$

$$\operatorname{Im}\left(G_{ef}\left(e^{j\theta_i}, w\right)\right)^2 \leq \beta_i, \qquad \forall i = (1, 2, ..., n) \tag{8c}$$

where μ is the weighting factor, $\operatorname{Re}(\cdot)$ and $\operatorname{Im}(\cdot)$ denote the real and imaginary parts of a complex number, n is the number of selected frequency points, and θ_i is the ith frequency point. Note that a one-dimensional attack signal is considered in (8), but it can be extended to multidimensional sensor attacks. This design exhibits computational tractability, owing to its formulation as a convex quadratic optimization (QP) problem. Considering the Lagrange dual of (8), an analytical solution of (8) can be obtained

$$N^*(w, \lambda) = -\frac{1}{\lambda}\sum_{i=1}^{n} \operatorname{Re}(\Psi_i)\left(\sum_{i=1}^{n} \lambda^{-1}(Re(\Psi_i)^2 + \operatorname{Im}(\Psi_i)^2) + \lambda^{-1}\mu\bar{Q} + H\left(w\right)H^T\left(w\right)\right)^{-1} \tag{9}$$

where $\Psi_i = a(\mathfrak{q})^{-1}F(\mathfrak{q})\big|_{\mathfrak{q}=e^{j\theta_i}}$ and (9) reaches the optimal solution of (8) as λ tends to ∞. When the environmental factors change, the estimator can quickly recalculate to get $N^*(w)$ based on the change of $H\left(w\right)$. Thus, we offer a lightweight approach for a real-time robust estimator that can promptly adapt to parameter changes and model mismatches.

We provide a remark on the lower bound of optimality. *The selective approach imposes constraints only on a subset of the frequency points. This estimator obtains a lower bound on optimality for the original optimization problem. However, the degradation in performance at nonselected frequencies can be minor for a large n (it still exhibits computational traceability due to the convexity) and a uniform selection strategy.*

Based on the estimator, we further propose an active compensator that integrates a tracking controller along with a low-pass filter, as shown in Fig. 1. As the compensation signal comes after the attack signal, we add a differential operator into the tracking controller part to prevent the compensation signal from lagging behind the attack. This design could counteract the attack effects. The tracking controller uses a proportional differentiation algorithm and can be described as a one-pole-one-zero discrete-time transfer function

$$G_c = \frac{k_{c1}\mathfrak{q} + k_{c2}}{\mathfrak{q} + 1} \tag{10}$$

where k_{c1} and k_{c2} are proportional and differential coefficients. Further, a second-order discrete-time low-pass filter suppresses potential high-frequency noise. Thus the whole active compensator can be expressed as

$$G_{com} = \frac{k_{n3}\mathfrak{q}^3 + k_{n2}\mathfrak{q}^2 + k_{n1}\mathfrak{q} + k_{n0}}{k_{d3}\mathfrak{q}^3 + k_{d2}\mathfrak{q}^2 + k_{d1}\mathfrak{q} + k_{d0}} \tag{11}$$

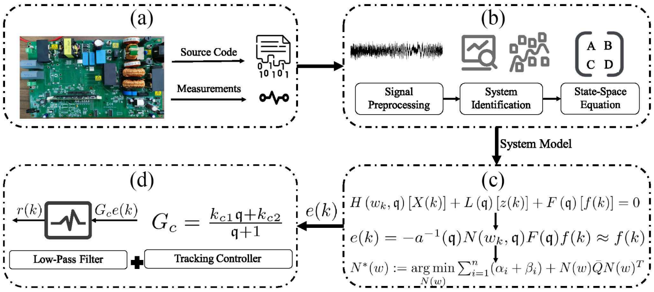

(a)
Source Code
Measurements
(b)
A B
C D
Signal Preprocessing
System Identification
State-Space Equation
System Model
(c)
$H\left(w_k, \mathfrak{q}\right)\left[X(k)\right] + L\left(\mathfrak{q}\right)\left[z(k)\right] + F\left(\mathfrak{q}\right)\left[f(k)\right] = 0$
$e(k) = -a^{-1}(\mathfrak{q})N(w_k, \mathfrak{q})F(\mathfrak{q})f(k) \approx f(k)$
$N^*(w) := \underset{N(w)}{\arg\min} \sum_{i=1}^{n}(\alpha_i + \beta_i) + N(w)\bar{Q}N(w)^T$
$e(k)$
(d)
$r(k)$
$G_c e(k)$
$G_c = \frac{k_{c1}\mathfrak{q}+k_{c2}}{\mathfrak{q}+1}$
Low-Pass Filter
Tracking Controller

Fig. 2. Flowchart of the implementation procedure. (a) Inverter signal collection. (b) System identification. (c) Attack estimator. (d) Active compensator.

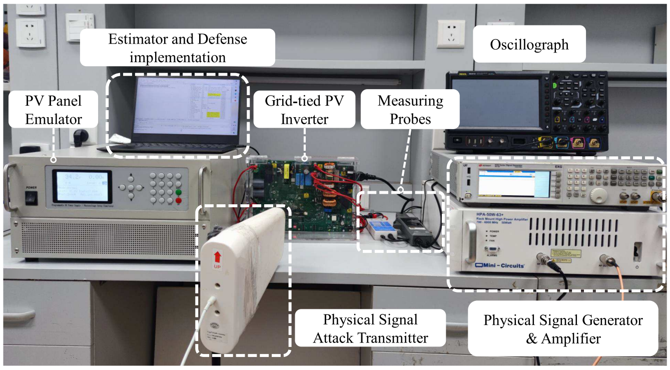

Estimator and Defense implementation
Oscillograph
PV Panel Emulator
Grid-tied PV Inverter
Measuring Probes
Physical Signal Attack Transmitter
Physical Signal Generator & Amplifier

Fig. 3. Experimental setup.

where k_{ni} and $k_{di}(i = (0, 1, 2, 3)$ relates to k_{c1}, k_{c2} and the cut-off frequency. To defend against sensor attacks, the active compensator delivers the compensation signal r to the control loop. For a better illustration, the hardware and software implementation of our approach is outlined in Fig. 2.

IV. Experiments and Discussion

To verify the proposed defense approach for sensor attacks on PV inverters, we conducted hardware experiments on a microcommercial PV inverter. The hardware experimental setup includes a TI C2000 Solar Micro Inverter with its driven DSP controller, PV panel emulator, and physical attack signal generator & transmitter, as shown in Fig. 3. The oscillograph displays the real voltage and current by the measuring probes.

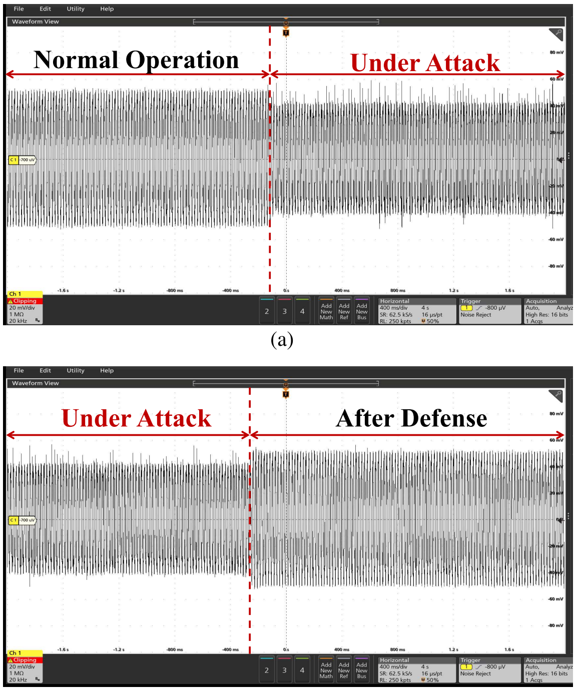
A. Experimental Results

To evaluate under real sensor attacks, we perform a physical attack using an innovative electromagnetic interference (EMI) method. The principle of the attack can be found in [14]. For the efficient EMI injection, we use an EXG vector signal generator as the signal source (9 KHz–6 GHz). The amplifier HPA-50W-63+ is used to amplify the output signal to 10 W. Then we use a high gain log-periodic directional antenna to transmit EMI signals with +14 dBi. By frequency sweeping, we can identify the frequency of EMI signals that the sensors on the PV output side, DC-bus side, and AC side are “sensitive” to, as shown in Table I. This physical attack can inject up to 354% anomalous

TABLE I

EMI Impact on Inverter Sensors

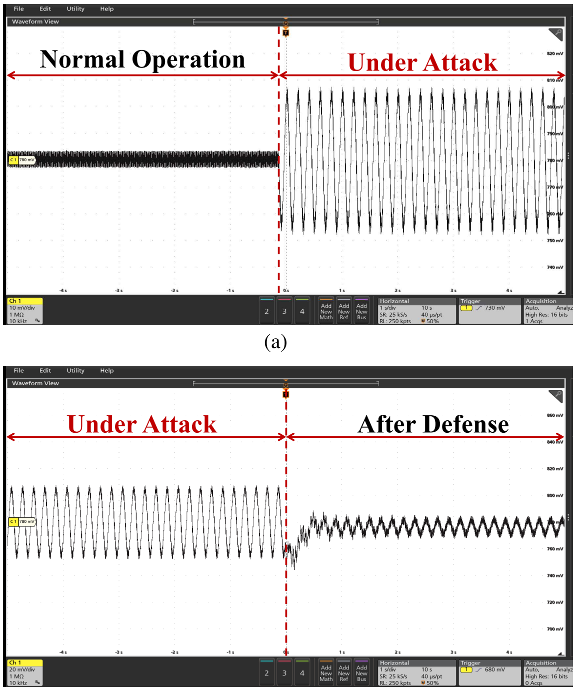
Sensor Position	Sensor Type	Sensor Model	Measurement Range	Test Parameters		Output		
				Freq (MHz)	Pow (W)	Original Value	Devation	Devation Rate (%)
Ipv	DC Current	ACS712	0–20 A	850	10	2.2 A	1.65 A	75
Vbus	DC Voltage	OPA2171	0–418 V	1140	10	385 V	33.44 V	9
Iout	AC Current	LTSR6-NP	−20 A–20 A	1280	10	0.24 A	0.85 A	354



(a)

(b)

Fig. 4. Real current after the step attack and defense. (a) Effect of the step attack. (b) Affter our defense method.



(a)

(b)

Fig. 5. Real dc-bus voltage before and after the defense. (a) Effect of the sinusoidal attack. (b) After our defense method.

measurements at a power of 10 W, causing a serious threat to the inverter operation. We illustrate the effectiveness of our defense through two attack forms: step and sinusoidal. A step attack can be implemented with a constant-intensity EMI signal at a fixed frequency point, while a sinusoidal one is achieved through amplitude modulation of the EMI signal using a modulation signal at 5 Hz.

In the hardware implementations, we set the estimator degree $d_N = 7$, the denominator $a(\mathsf{q}) = (\mathsf{q} + 0.5)^{d_N}$. The selected frequency points are 0, 10, 20, 30, 40, 50, and 60 Hz. The optimal parameter of the estimator is obtained by solving (9). Next, we port the code of our lightweight defense approach to the DSP controller of the micro commercial inverter. We implement a step attack on the PV panel output current sensor and a sinusoidal attack at 5 Hz on the DC bus voltage sensor. Note that the attack on the I_{out} immediately triggers the off-grid protection, making it difficult to implement our defense strategy. The attack on the PV panel output current sensor could interfere with the operation of the MPPT algorithm and impede the inverter from achieving maximum power. The changes in real inverter output current under a step attack are illustrated in Fig. 4. Here the current probe converts the actual current value by 1 A/100 mV. The reduced output current indicates a decrease in inverter output power. Under normal operation, the average output power is 90 W, which is reduced to 62 W after the attack. Thirty-one percent of the wasted output power could cause power shortages in microgrids. Fortunately, our defense method can restore it to 88 W, eliminating the majority of the power reduction in 100 ms. The time to mitigate the attack is much faster than the time for grid scheduling and control. Fig. 5(a) and 5(b) illustrates the real dc-bus voltage before and after our defense method. The high voltage differential probe measurement reduces the actual value of the current by a factor of 500. The results show that the sinusoidal form of the attack causes dramatic fluctuations in the dc-bus voltage, which can lead to inverters going off-grid by triggering the over/under-voltage protection. Once more, our defense approach can mitigate the fluctuations after a 230 ms transient process. Here we can use the peak-to-peak values to describe the severity of the fluctuations. After "removing" the normal fluctuations, our defense method reduces the voltage fluctuations to 19.2% of the attack case and keeps dc bus voltages within the acceptable limits. We have uploaded a video demo to the link [15] to show the process. We note that it remains challenging for the defense to completely mitigate the effects of attacks in hardware experiments. This is mainly because, although we have alleviated the model mismatch effects on attack estimation in (8), it is hard to eliminate it completely through the selection of the weighting factor μ. Nevertheless, as demonstrated by experimental results, our defense method still effectively mitigates the attack impact and ensures stable inverter operations.

B. Discussion

1) Output Power: The microcommercial inverter we used in the experiments supports a maximum output power of 280 W. However, due to safety considerations and constraints on grid-connected power in the laboratory, evaluation with high power may damage the inverter and other devices. Therefore, we evaluate the effectiveness of our defense approach within the permissible range of the inverter's output power.

2) Scalability: Considering the safety, the experiments in this article are carried out on a low-power microinverter. For other PV inverters, the power and frequency of the EMI signal for effectively launching sensor attacks may vary. Despite the differences in inverter hardware, one can integrate physical priors and employ a system identification to obtain the inverter model. Then, through our proposed method in (1)–(11), the estimator and compensator parameters can be derived.

3) Sensor Faults: The inverters' sensors may also face multiple types of faults. For stuck and drift faults, the fault signal can be represented as a step or ramp, whose frequency components are concentrated around 0 Hz. We can use the current design to estimate and compensate faults. For the gain fault, one may not achieve an accurate estimation as (8a) is not met, but can analyze the indicative signal e to detect the fault.

V. Conclusion

This article have proposed a viable solution for robust estimation and defense against sensor attacks on actual PV inverters, considering environmental changes and model mismatches. We develop an optimization-driven approach and present an analytical solution form of the estimator to enhance real-time response. We further develop a closed-loop compensation strategy to mitigate the impact of sensor attacks. We hope that our work raises awareness of power inverter security and proposes implementable defense strategies.

References

[1] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Trans. Power Electron.*, vol. 38, no. 2, pp. 2364–2383, Feb. 2023.

[2] A. Barua and M. A. A. Faruque, "Hall spoofing: A non-invasive attack on Grid-Tied solar inverter," in *Proc. USENIX Secur. Symp.*, 2020, pp. 1273–1290.

[3] S. Khandelwal, "Critical flaws found in solar panels could shut down power grids," *The Hacker News*, Aug. 2017. Accessed: Jan. 11, 2024. [Online]. Available: https://thehackernews.com/2017/08/solar-panel-power-grid.html

[4] A. A. Khan, O. A. Beg, M. Alamaniotis, and S. Ahmed, "Intelligent anomaly identification in cyber-physical inverter-based systems," *Elect. Power Syst. Res.*, vol. 193, pp. 1–13, Apr. 2021.

[5] P. Ganesh et al., "Learning-based simultaneous detection and characterization of time delay attack in cyber-physical systems," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3581–3593, Jul. 2021.

[6] H. Athari, M. Niroomand, and M. Ataei, "Review and classification of control systems in grid-tied inverters," *Renewable Sustain. Energy Rev.*, vol. 72, pp. 1167–1176, 2017.

[7] J. Zhang, M. D. R. Greidanus, S. K. Mazumder, J. Ye, W. Song, and H. A. Mantooth, "Model-based detection scheme for spoofed sensor data in grid-connected inverters," *IEEE Trans. Ind. Electron.*, vol. 71, no. 3, pp. 3224–3228, Mar. 2024.

[8] S. K. Mazumder, M. D. R. Greidanus, J. Liu, and H. A. Mantooth, "Vulnerability of a VOC-based inverter due to noise injection and its mitigation," *IEEE Trans. Power Electron.*, vol. 38, no. 2, pp. 1445–1450, Feb. 2023.

[9] S. Bacha, I. Munteanu, and A. I. Bratcu, *Power Electronic Converters Modeling and Control* in Advanced Textbooks in Control and Signal Processing, London, UK: Springer, vol. 454, 2014, p. 454.

[10] N. Pogaku, M. Prodanovic, and T. C. Green, "Modeling, analysis and testing of autonomous operation of an inverter-based microgrid," *IEEE Trans. Power Electron.*, vol. 22, no. 2, pp. 613–625, Mar. 2007.

[11] F. Dkhichi, B. Oukarfi, A. Fakkar, and N. Belbounaguia, "Parameter identification of solar cell model using levenberg–marquardt algorithm combined with simulated annealing," *Solar Energy*, vol. 110, pp. 781–788, Dec. 2014.

[12] 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 Trans. Power Electron.*, vol. 37, no. 10, pp. 11481–11485, Oct. 2022.

[13] K. Pan, P. Palensky, and P. M. Esfahani, "Dynamic anomaly detection with high-fidelity simulators: A convex optimization approach," *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1500–1515, Mar. 2022.

[14] M. D. R. Greidanus, S. D'Silva, S. Gupta, D. Sur, S. K. Mazumder, and M. B. Shadmand, "Electromagnetic side-channel noise intrusion on solid-state transformer," *IEEE Trans. Power Electron.*, vol. 39, no. 8, pp. 9244–9256, Aug. 2024.

[15] "Attack and defense demo." Accessed: Jun. 20, 2024. [Online]. Available: https://tinyurl.com/DefenseofInverterDemoVideos