A Robust Method to Secure Multi-Inverter Grid Tied PV and Battery Energy Storage Systems Against Cyber Intrusions

Hasan Ibrahim *Member, IEEE,* Jaewon Kim, *Member, IEEE,* Shaozhe Wang, *Member, IEEE,* Prasad Enjeti, *Fellow, IEEE*

***Abstract*—This paper details a robust method to secure a multi-inverter grid tied system that interfaces photovoltaic (PV) and battery energy storage against potential cyber-attacks. The method can be applied to any third-party inverter systems without a need to modify their internal controls. A small random private excitation signal termed "watermark" is injected into the DC input voltage terminals (via a series transformer) connected to the PV/battery inverter system. An external robust cyber intrusion detector (CID) hardware consisting of a digital signal processor (DSP) generates the "watermark" and also receives the sensor signals that control the setpoints of the PV/battery grid tied system. The CID algorithm is shown to detect all possible cyber intrusions (such as false data injection(FDI)) on external sensor signals such as P and Q measured by a smart meter that control the overall system operation. The proposed CID computes online system ID and two variance tests in real time on each sensor signal and is able pinpoint intrusion location in a multi-inverter system. Results on a hardware in the loop (HIL) of a two-inverter grid connected system demonstrate effectiveness of the proposed CID system for FDI and unobservable FDI. Test results on a laboratory prototype will be discussed in the conference presentation.**

***Index Terms*—Cybersecurity, dynamic watermarking, malicious sensors, cyber-physical system, solar-rich distribution systems, watermarking (WM), Hardware in the loop (HIL)**

I. Introduction

Large (MW) rated solar PV and battery grid interfaces have the potential to revolutionize the way we generate and consume electricity, providing a more sustainable, reliable, and cost-effective energy system. Multi-inverter systems are commonly used in large solar PV and battery grid interfaces [2]. As the deployment of multi-inverter systems continues to grow, their inter connectivity adds to flexibility with superior grid forming/following features so does the potential for cyber attacks [3]. Since the operation of the PV/battery grid interface inverters depend on the reported measurements from external sensors (example: smart meters), they are highly susceptible to potential cyber-attacks where malicious agents can compromise the sensors or the communication networks carrying the sensor measurements [3]. To address these concerns, government agencies and industry leaders are working together to develop and implement robust cyber security measures for grid-connected multi-inverter systems [4]. These measures aim to mitigate the risk of cyber attacks and ensure the integrity and security of these systems.

Fig. 1 shows a typical solar PV/battery grid interface system diagram with installations such as Houston, Texas by CenterPoint Energy and Enel Green Power North America's Roadrunner in other regions of Texas. Typically a "Plant Controller" [5] receives the data from various sensors, system operators and controls the set points of each PV/Battery grid interface. In [2], [6] a comprehensive review of several methods of various types of cyber intrusions / attacks is presented. Securing sensor data via encryption methods such as public key cryptography are discussed. Other methods detail modifications to controls within the commercial hardware [6] to provide defense mechanisms against FDIA rendering them unsuitable when an installation employs building blocks such as inverters/system controllers from different vendors. Use of private Blockchain methodology has been suggested [2] to authenticate the validity of sensor data. Many approaches known in the literature [2] do not address complex attack scenarios such as unobservable FDIA, also known as replay attack [7].

The authors' previous work [8], [9], explored the implementation of the watermarking signal injection method into the inverter control signals. This is possible if one has access to the embedded processor controlling the grid interfaced inverter system. However, a majority of PV/battery installation systems (see Fig. 1) employ commercial inverters that do not have access to inverter control hardware.

In the proposed work [1], [10], a small random private excitation signal termed "watermark" is injected into the DC input voltage terminals (via a series transformer, see Fig. 1) connected to the PV/battery inverter system. Fig. 1 illustrates an external cyber intrusion detector (CID) hardware consisting of a digital signal processor (DSP), that generates the "watermark" $e[k]$ and also receives the sensor signals that control the setpoints of the PV/battery grid tied system. The CID algorithm is shown to detect all possible cyber intrusions (such as false data injection(FDI)) on external sensor signals such as P and Q measured by a smart meter that control the overall system operation. The proposed CID computes online system ID and two variance tests in real time on each sensor signal and is able pinpoint intrusion location in a multi-inverter system. Since the watermark signal is injected (externally) into the available dc input terminals (via a series transformer), the proposed is versatile and can be adapted to

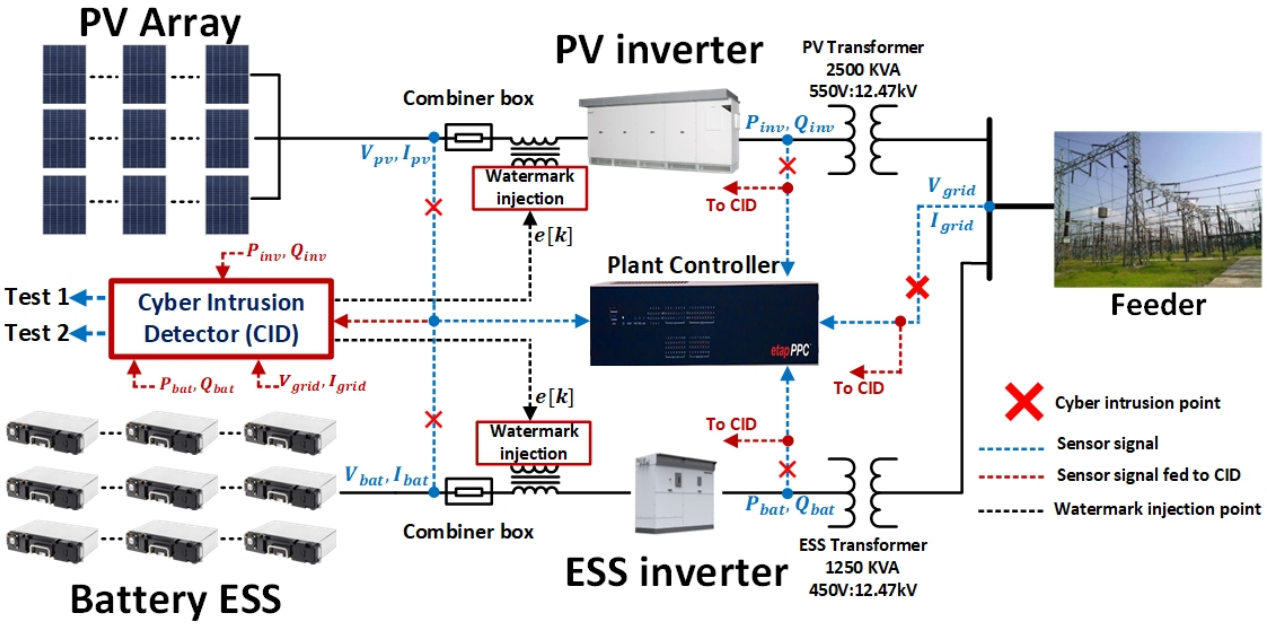

Fig. 1: Block diagram of a typical solar PV / Battery energy storage system interfaced to the grid. Such systems are monitored/controlled via a "plant controller". The proposed Cyber Intrusion Detector (CID) [1] is shown as an add-on option to observe the system's signals and rapidly detect possible cyber intrusions (false data injection) in measurements.

any commercial grid connected inverter hardware [1]

II. Proposed CID with Watermarking Method

Fig. 1 shows the block diagram of an multi inverter PV/Battery system interface to the grid. As shown, the effective functioning of the system is depend on reported sensor measurements to provide state information of the system to the plant controller so that it can generate appropriate control laws to operate the system. However, the security of these systems can be compromised when those sensor measurements are corrupted via false data injection, that lead to inappropriate set points to PV/battery subsystems. This vulnerability (due to false data injection) is compounded when sensor measurements are transmitted over networks (such as MODBUS) and FDIA is launched. In [7] a replay attack on sensor data (real time sensor measurement was replaced by a prerecorded signal) on centrifuges is a prominent real-world cyber-attack example.

A. Dynamic Watermarking Tests

In a dynamic system with multiple sensors, some could be malicious and some could be honest. If a malicious sensor i that reports incorrect measurements, i.e., $z_i[k] \not\equiv y_i[k]$, where $z[k]$ is the measurements reported from the sensor and $y[k]$ is the system's actual values. Such malicious sensors distorting measurements can cause critical damage to Cyber-Physical Systems(CPS) such as *Stuxnet* [7].

We consider the watermark signal $e[k]$, a random private excitation signal $e[k] \sim \mathcal{N}(0, \sigma_e^2 I)$, injected into the DC input voltage in our system and a linear stochastic system with sensor output vector $z[k]$, control input vector $u[k]$, and white Gaussian noise $w[k]$ with zero mean and Covariance matrix $\sigma_w^2 I$. Two Dynamic Watermarking tests on sensor measurements as shown below:

Test 1:

$$\lim_{T\to\infty} \frac{1}{T} \sum_{k=0}^{T-1} e_1[k](z[k+1] - Az[k] - Bu[k]) = B_i \sigma_e^2. \quad (1)$$

Test 2:

$$\lim_{T\to\infty} \frac{1}{T} \sum_{k=0}^{T-1} (z[k+1] - Az[k] - Bu[k])(z[k+1] - Az[k] - Bu[k])^T = \sigma_e^2 BB^T + \sigma_w^2 I_n. \quad (2)$$

In the multi inverter system architecture, multiple watermarking signals, $e_1[k]$, $e_2[k]$, ... etc, see Fig. 1, are injected on the input signal as shown in Fig. 1. Each WM signal has its unique random distribution that distinguishes them apart. Multiple Tests 1 & 2 will be computed for each inverter using the associated watermark signal with that specific inverter.

B. System Identification

To compute the two Dynamic Watermarking tests, a proper system identification method is essential for controlling multi-scale systems and providing safe operations. Multiple system IDs will be calculated for each inverter. We employed the *Least Squares Method* for the system identification [11]–[13]. The form of the prediction model is as follows:

$$\hat{z[k+1]} = \alpha_0 z[k] + \alpha_1 z[k-1] + ... + \alpha_n z[k-n] + \beta_0 u[k] + \beta_1 u[k-1] + ... + \beta_m u[k-m] \quad (3)$$

,where $z[k]$ is the output of the system, $u[k]$ is the input of the system, $A_n = [\alpha_0 \alpha_1 ... \alpha_n]^T$, and $B_m = [\beta_0 \beta_1 ... \beta_m]^T$ are the parameters associated with input and output of the prediction model. The dimensions of the input and output vectors m and n are also unknown.

III. Experimental Results

In this section, an experimental study to assess the effectiveness of a watermarking signal $e_1[k]$ in ensuring the security for two separate grid connected 3 kW inverter system is discussed. We conduct three key experiments to validate its robustness and the functionality of the proposed Cyber Intrusion Detector (CID). The first experiment involves testing the watermarking signal $e_1[k]$ and $e_2[k]$ on two 3 kW inverter prototypes respectively. We inject the watermark into the control input and closely monitor its impact on the inverter's control mechanism. The primary objective is to verify that the watermarking process does not compromise the regular operation of the inverters and that the algorithm successfully detects and identifies points of intrusion. In the second experiment, we implement a Hardware-in-the-Loop (HIL) system, integrating the inverter with a virtual simulation model. Here, the watermarking signal is injected into the input DC voltage signal, simulating real-world conditions. By thoroughly evaluating the system's performance and validating its integrity, we ensure that the watermarking signal remains effective in complex operational scenarios. In the final experiment, we inject the watermark into the input voltage signal of the multiple 3 kW inverter system to test and validate the proposed Cyber Intrusion Detector (CID), more results on this experiment will be collected and presented during the conference.

A. Test results on a 3kW two inverter laboratory grid connected system

In this section, the proposed detection algorithm's robustness and functionality are validated using two 3kW grid tied inverter systems in the laboratory (Fig. 2). The experimental setup aims to emulate real-world conditions to test the system's resilience against cyber attacks. In the attack scenario, the adversary gains access to the system's current sensor data and manipulates it to falsely report a change in the current's signal transmitted to the controller, simulating a false data injection (FDI) attack. The hardware setup, shown in Fig. 2, is as follows: To represent the grid, a 120 V rms AC source is utilized, and a 15 Ohm resistor is connected in parallel with the AC source to enable the consumption of 960 W of real power. The selected inverter for the experiment is the PE-Expert 4, developed by Myway [14], which is commonly used in grid-connected systems. In the hardware results presented in this section, the oscilloscope settings are as follows: sec/div is set to 40m, the voltage in CH1 div is 200, and the inverter current div is 20. The variance tests will vary depending on each attack scenario. To validate the performance of the proposed CID, two attacks were performed, the harmonic injection attack and the amplitude manipulation attack.

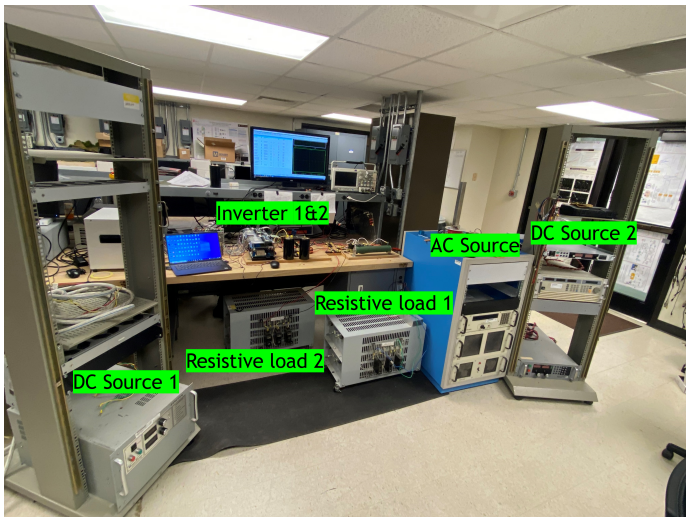

Fig. 2: Lab hardware setup for two 3kW grid tied inverter systems powered by PV/battery emulators

1) Amplitude manipulation attack:

In this scenario the attacker gains access to the system's sensor data and manipulates it to falsely report a change in the current's amplitude. The controller will try to respond by changing the amplitude to negate the effects of the reported data. As indicated in Fig 3, the attack is initiated on inverter 2. Fig 3 shows variance tests 1 and 2 on both inverters. Since inverter 1 was not attacked, the variances did not show a change, however, in inverter 2 case the variances shows a jump once the attack commences. Such attacks may cause severe damage to the grid such as triggering unwanted security measurements as discussed in the man in the middle attack scenario in [15]. This test demonstrates the CID algorithm's capability to promptly identify the amplitude manipulation attack and distinguish between the behavior of attacked and unaffected inverters.

2) Harmonic injection attack:

Another attack scenario evaluated is the harmonic injection attack, which involves the adversary injecting malicious harmonic signals into the system to manipulate its behavior. Figure 4 showcases the experiment during the harmonic injection attack. Variance tests 1 and 2 are conducted on both inverters to monitor their response. As expected, inverter 2, which remains unattacked, shows minimal changes in variance. However, in the case of inverter 1, which is subjected to the attack, the variance tests display significant fluctuations. This discrepancy in variance values between the attacked and unaffected inverters signifies the presence of the harmonic injection attack, confirming the effectiveness of the detection algorithm.

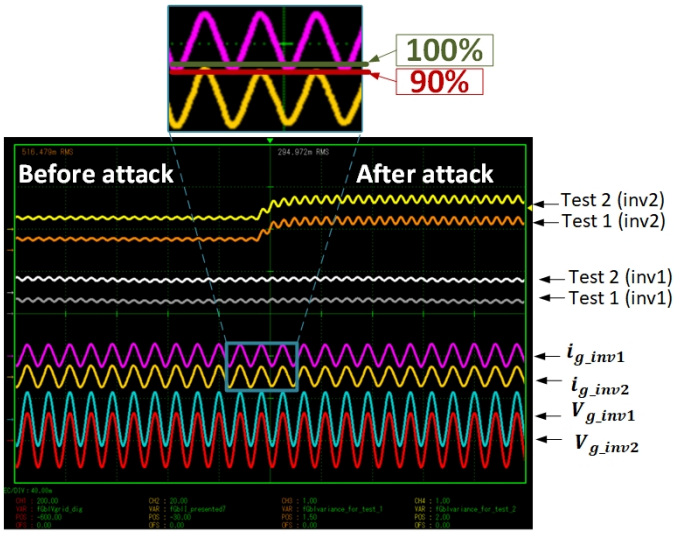

Fig. 3: Experimental results on two inverter system (Fig. 2). Inverter 2 is operating under healthy condition while inverter 1 is being attacked via current amplitude reducing type FDIA.

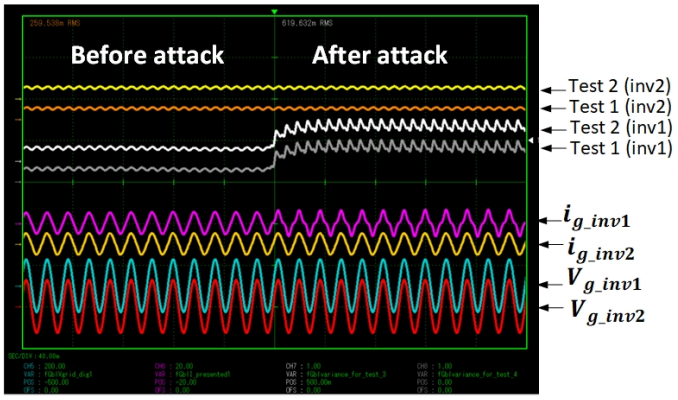

Fig. 4: Experimental results on two inverter system (Fig. 2). Inverter 1 is operating under healthy condition while inverter 1 is being attacked via harmonic injection

B. Test results on Hardware in the Loop (HIL) Multi Inverter System

In order to validate the effectiveness of the proposed cyber security method, shown in Fig. 1, a Hardware-in-the-Loop (HIL) experiment was conducted. The primary objective of this experiment was to demonstrate the ability of the watermarking signal, generated by a TI DSP (Digital Signal Processor), to be injected on the input DC, Fig. 1 and Fig. 6, and propagate through the plant model to showcase the system identification (ID) process for detecting cyber attacks. The experimental setup, shown in Fig. 5, comprised a multi inverter systems plant model simulated in the HIL box, shown in Fig. 6 , and an external TI DSP for signal injection and system identification. The watermarking signal, generated by the TI DSP, was externally injected into the HIL box to be superimposed onto the plant model's input signal. Additionally, the DSP was equipped with the algorithm responsible for building the system ID, explained in section IIB, based on the input and output signals of the simulated system. The generated watermarking signal propagates through the system as intended, remaining embedded in the output signals of the model. This successful propagation is a crucial aspect of the proposed cyber security method, as it ensures the watermarking signal's presence during the subsequent system identification process. Additionally, during the experiment, the HIL box outputs the system's signals from the simulated multi inverter model and feeds to the TI DSP, which employs the system identification algorithm to build a reference system ID based on the unaltered model's behavior. This reference ID serves as a baseline for comparison during subsequent stages. To validate the performance of the proposed CID, two FDI attacks were performed, the harmonic injection attack and the amplitude manipulation attack.

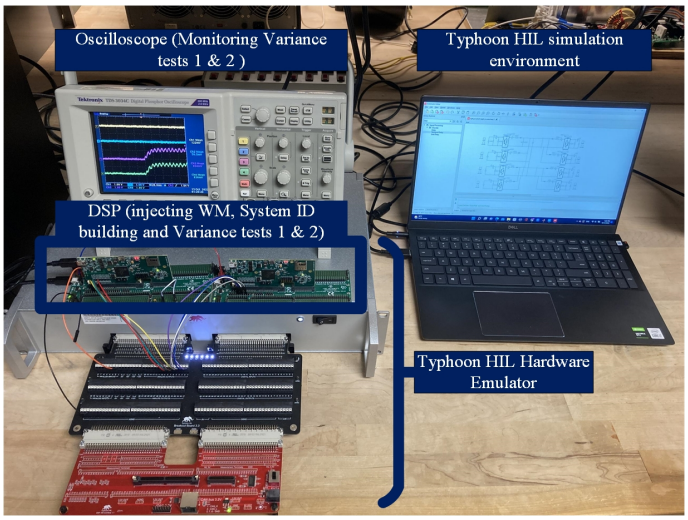

Fig. 5: Test setup for multiple grid tied inverter system on Typhoon HIL system.

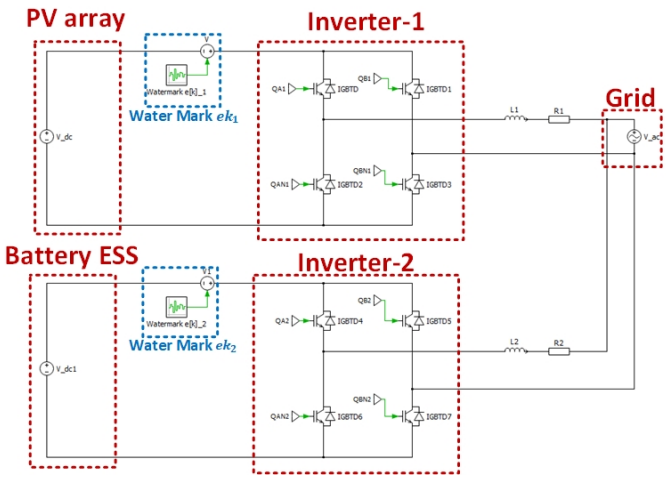

Fig. 6: HIL multiple inverter model, similar to the typical solar farm archticture shown in Fig.1. The model shows multiple inverters supplied by two DC supplies. It also show multiple unique watermarking signal $e[k]$ injection points on the input voltage signal for each inverter

1) Harmonic injection attack:

In the demonstrated attack scenario, the current sensor is accessed and manipulated by a malicious agent to report false harmonics in the system to the controller to deceive the system and potentially manipulate its behavior. As indicated in Fig 7, the attack is initiated on one of the multiple inverters, namely inverter 2. Fig 7 (a) shows variance tests 1 and 2 on both inverter 1 and 2. The system identification algorithm in the TI DSP detected these malicious signals, and upon comparison with the reference system ID, variance Tests 1 & 2 showed a significant jump on the attacked inverter, inverter 1, which indicated the start of an attack. The algorithm is shown to not only detect the attack but also accurately identify the location of the attack thereby providing valuable insights for potential mitigation strategies. By identifying the specific inverter affected by the attack, prompt corrective measures can be taken to ensure the system's security and integrity.

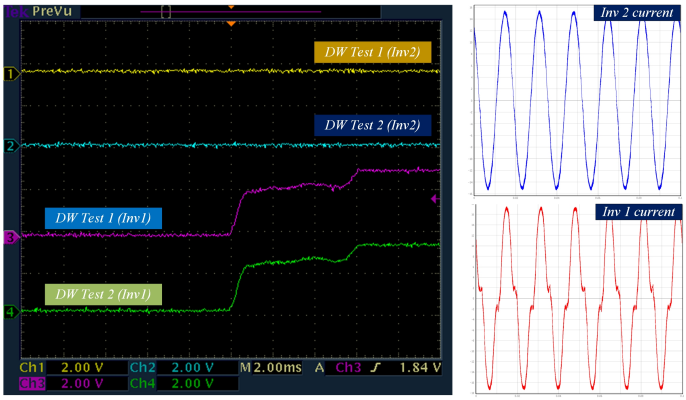

Fig. 7: Test results on multiple inverter HIL system (Figs. 5 and 6). Inverter 2 current sensor signal data is corrupted with harmonics. The variance Test 1 and 2 show an increase indicating FDIA.

2) Amplitude manipulation attack: In this attack scenario, a malicious agent gains access to the current sensor and manipulates the reported current measurements to deceive the system and trigger a false response. This attack can be likened to a "Man in the Middle" attack, where the malicious agent intercepts and alters the communication between the sensor readings and the controller [15]. As depicted in Figure **??**, the attack is initiated on one of the inverters, in this case, inverter 2. Figure 8 (a) presents variance tests 1 and 2 conducted on both inverter 2 and inverter 1. The system identification algorithm running on the TI DSP detects the maliciously altered current measurements and identifies the presence of the attack through significant jumps observed in the variance tests on the attacked inverter, inverter 2, Fig.8. Similar to the harmonic attack, the CID not only successfully detects the harmonic injection attack but also accurately pinpoints the location of the attack.

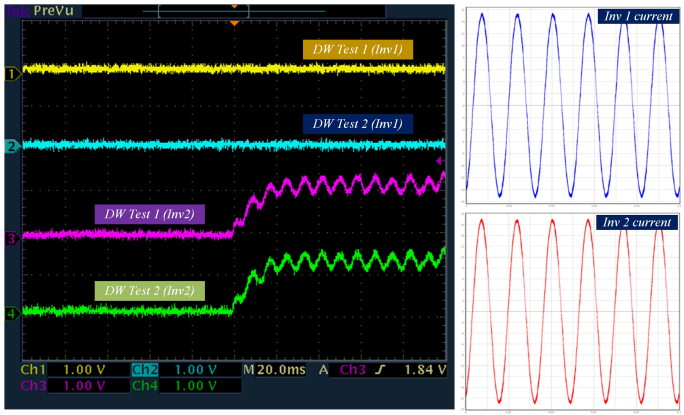

Fig. 8: Test results on multiple inverter HIL system (Figs. 5 and 6). Inverter 2 current sensor signal data is corrupted by altering the current amplitude measurement. The variance Test 1 and 2 show an increase indicating FDIA.

IV. Conclusion

In this paper a robust method to secure multi inverter grid tied photovoltaic (PV) and battery energy storage systems against cyber intrusions has been presented. The proposed intrusion detection system is an add-on option, does not require any modification to the existing PV/Battery grid connection / existing controls and has been shown to detect complex cyber intrusions such as false data injection attack (FDI). Test results on a 3kW two inverter laboratory grid connected system as will as a HIL system, demonstrate effectiveness of the proposed CID systems.

References

[1] P. Enjeti, P. R. Kumar, and L. Xie, "Methods and system for detecting compromised sensors using dynamic watermarking," Patent, U.S. Provisional Patent Application Serial No. 63/352,131, filed June 14, 2022 Texas A&M University System.

[2] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy," *IEEE Access*, vol. 10, pp. 35 846–35 875, 2022.

[3] R. H. Lasseter, Z. Chen, and D. Pattabiraman, "Grid-forming inverters: A critical asset for the power grid," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 8, no. 2, pp. 925–935, 2020.

[4] "Ieee standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)*, pp. 1–138, 2018.

[5] "Electrical power system analysis software: Power management system." [Online]. Available: https://etap.com/

[6] J. Ye *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, 2022.

[7] P. K. Kerr, J. Rollins, and C. A. Theohary, *The Stuxnet computer worm: Harbinger of an emerging warfare capability.* Congressional Research Service Washington, DC, 2010.

[8] H. Ibrahim, J. Ramos-Ruiz, J. Kim, W. H. Ko, T. Huang, P. Enjeti, P. R. Kumar, and L. Xie, "An active detection scheme for sensor spoofing in grid-tied pv systems," in *2021 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2021, pp. 1433–1439.

[9] W.-H. Ko, J. Ramos-Ruiz, T. Huang, J. Kim, H. Ibrahim, P. Enjeti, P. R. Kumar, and L. Xie, "Robust dynamic watermarking for cyber-physical security of inverter-based resources in power distribution systems," *IEEE Transactions on Industrial Electronics (Accepted - to be published).*

[10] F. H. Alotaibi, H. Ibrahim, J. Kim, P. R. Kumar, and P. Enjeti, "Designing an intrusion detection for an adjustable speed drive system controlling a critical process," *IEEE Access*, pp. 1–1, 2023.
[11] L. Ljung, *System Identification: Theory for the User*. USA: Prentice-Hall, Inc., 1986.
[12] F. Ding and T. Chen, "Identification of hammerstein nonlinear armax systems," *Automatica*, vol. 41, no. 9, pp. 1479–1489, 2005.
[13] J. Ding, F. Ding, X. P. Liu, and G. Liu, "Hierarchical least squares identification for linear siso systems with dual-rate sampled-data," *IEEE Transactions on Automatic Control*, vol. 56, no. 11, pp. 2677–2683, 2011.
[14] J. Ramos-Ruiz, H. Ibrahim, J. Kim, W. H. Ko, T. Huang, P. Enjeti, P. R. Kumar, and L. Xie, "Validation of a robust cyber shield for a grid connected pv inverter system via digital watermarking principle," in *2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2021, pp. 1–6.
[15] G. Tertytchny, H. Karbouj, L. Hadjidemetriou, C. Charalambous, M. K. Michael, M. Sazos, and M. Maniatakos, "Demonstration of man in the middle attack on a commercial photovoltaic inverter providing ancillary services," in *2020 IEEE CyberPELS (CyberPELS)*, 2020, pp. 1–7.