An Active Detection Scheme for Sensor Spoofing in Grid-tied PV Systems

Hasan Ibrahim *Member, IEEE,* Jorge Ramos-Ruiz, *Member, IEEE,* Jaewon Kim, *Member, IEEE,* Woo Hyun Ko, *Member, IEEE,* Tong Huang, *Member, IEEE,* Prasad Enjeti, *Fellow, IEEE* P. R. Kumar, *Fellow, IEEE* and Le Xie, *Senior Member, IEEE*

***Abstract*—In this paper an active detection scheme for sensor spoofing (manipulated externally via a cyber attack) in grid-tied PV systems is discussed. The core of the proposed active detection scheme is to introduce a private (secret) watermarking signal into the control inputs of the DC-DC converter and DC-AC inverter stages to detect any malicious spoofing (manipulation) of voltage/current sensor measurements controlling both the DC-DC converter maximum power point tracking (MPPT) stage and the DC-AC inverter of the grid-tied PV system. Several types of possible spoofing mechanisms (attack models) are discussed. The proposed sensor spoofing attack detector system consists of injecting a small magnitude of digital watermarking signal (DWS) and conduct three statistical watermark tests on the reported sensor measurements to determine if a) the proposed system is healthy and operating as expected b) if sensor signals were spoofed (manipulated) externally or c) if a particular sensor is malfunctioning due to a faulty hardware. It is shown via extensive simulations that the proposed DWS approach is robust in detecting malicious external manipulation of sensors controlling the grid tied PV system. A testing platform is currently under development and the experimental results will be discussed in the conference presentation.**

***Index Terms*—Cybersecurity, dynamic watermarking, malicious sensors, cyber-physical system, solar-rich distribution systems, digital watermarking signal (DWS)**

I. Introduction

Grid-tied PV systems has been increasing significantly and inverter-interfaced distributed generation (DG), such as solar photovoltaic (PV) inverters, is shaping the future of distribution power systems [1], [2]. Power electronics inverters are needed to convert the inherit DC voltage of solar panels into grid compatible AC voltage. As the number of power electronics devices in the electrical grid increase, therefore, the number of smart sensors and transducers in the electrical grid will also increase. Since each sensor is a possible vulnerable point for a malicious agent to perform sensor spoofing that may compromise the electrical grid, it is imperative to equip the PV inverters with a robust cyber shield for detecting for such malicious attacks.

References [3]–[5] detail various forms of sensor spoofing via external manipulations to disrupt the grid tied PV system resulting in disruption of service. In [3], a method of sensor spoofing of the inverter current sensor via an external magnetic field to disrupt Hall effect sensor is detailed. In [4], a Man in the Middle (MiTM) attack is performed by manipulating the response of the ancillary service controller, such attack can lead to unwanted triggering of protection relays. In [5], GPS spoofing attacks were studied, proving that this can lead to missed detection of disturbances, that eventually leading to blackouts. Sensor spoofing may also introduce power curtailments and economic losses [6], [7]. It is imperative to equip the PV inverters with a robust sensor spoofing methods and is the subject matter of this paper.

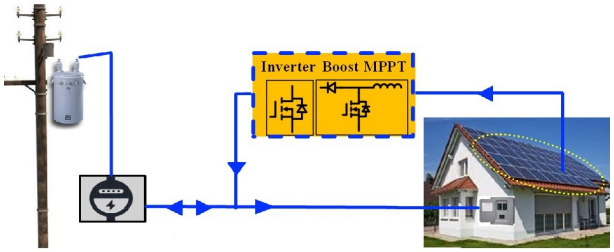

Fig. 1: An example grid-tied PV system

In the authors previous work [8], a sensor spoofing detection scheme for DC-AC inverter stage was introduced, analyzed and experimentally tested on a grid tied systems. In this paper, the proposed sensor spoofing detection mechanism via digital watermarking system (DWS) is further extended to both DC-DC converter stage and DC-AC inverter stage thereby adding several additional sensors. Furthermore, an additional feature to DWS method is added to differentiate between a sensor spoofing (deliberate external manipulation) vs sensor malfunction/failure due to a faulty sensor. The proposed sensor spoofing attack detector system consists of a small magnitude of DWS $e[k]$ has a Gaussian distribution superimposed on the control command of both DC-DC and DC-AC converter stages. It should be noted that the magnitude of the DWS $e[k]$ superimposed on the control command is small, and does not affect the steady state and/or dynamic performance of the power conversion stages. The Attack detector computation box (implemented on a DSP) conducts three statistical watermark verification tests on ALL the reported sensor measurements to determine (see Fig.2) a) if the proposed system is healthy and operating as expected b) if sensor signals were spoofed (manipulated) externally via cyber attack and is the reason for system to malfunction or c) if a particular sensor is malfunctioning due to a faulty sensor. It is shown via extensive simulations that the proposed DWS approach is robust in detecting malicious external manipulation of sensors controlling the grid tied PV system. A testing platform is currently under

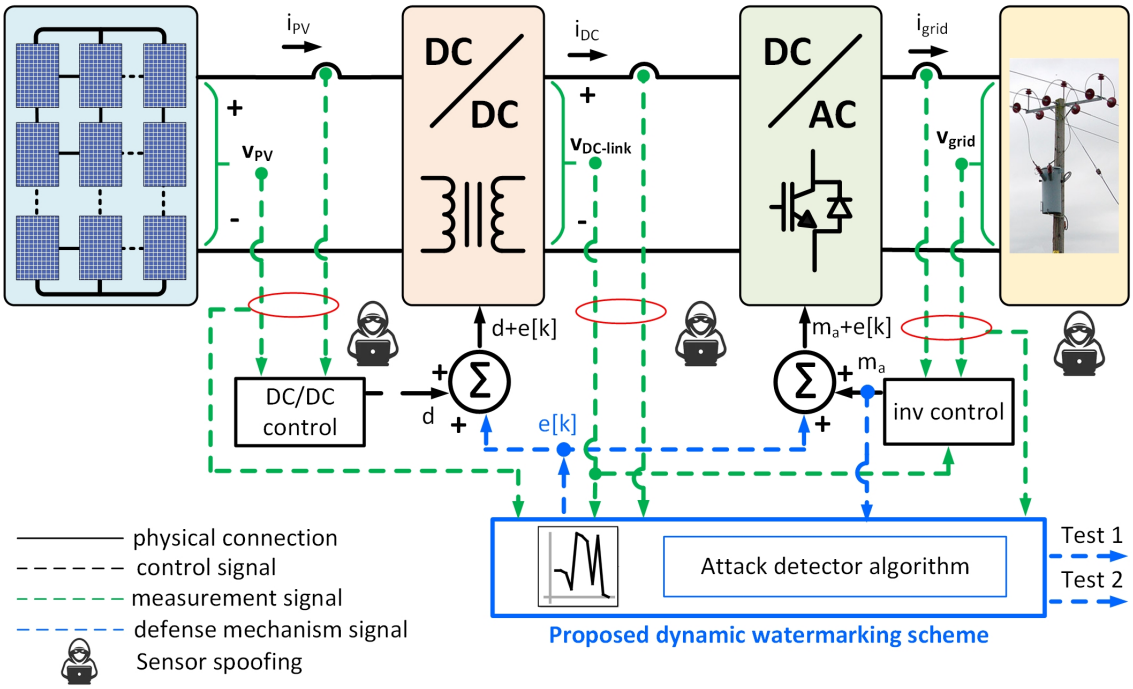

Fig. 2: Block diagram of a grid tied PV system showing possible sensor spoofing (manipulations) by an external attacker

development and the experimental results will be discussed in the conference presentation.

II. Proposed Digital Watermarking System (DWS) Design for a Grid Connected PV System

Fig.1 shows the block diagram of a grid connected PV system. Fig.2 shows a detailed schematic along with sensor measurements required for the control of the DC-DC and DC-AC conversion stages in the system. The dc output from the PV panels are interfaced to a DC-DC boost converter that is controlled in closed loop to regulate the output (dc) voltage and simultaneously enable maximum power point tracking (MPPT) [9]. The DC-DC boost stage is followed by a pulse width modulated (PWM) DC-AC inverter, output filter and is connected to the utility grid. The output of the MPPT stage forms the available power input command to the DC-AC inverter stage. The current and voltage sensors regulate the power flow from the PV to utility grid.

The proposed DWS system consists of injecting (superimposing) a private (secret) random excitation signal $e[k]$ that has a Gaussian distribution (see Fig.2) on the signal that controls the switch duty cycle "d" of the DC-DC converter stage and the modulation index "m_a"on the DC-AC inverter stage that controls the switch on/off states. It should be noted that magnitude of the random excitation signal $e[k]$ is small and does not affect the performance of the system. However, the watermark signal $e[k]$ propagates through the power conversion stages and manifests in the voltage/current signals that are sensed. Should any of the sensors that control the power conversion stages be compromised (spoofed and/or altered by the attacker), a series of statistical tests (detailed in Sections III) to check each of reported sensor measurement readings are compatible with the injected (superimposed) watermark to determine any malicious tampering.

A. Digital Watermarking Algorithm Development for the Grid Connected PV System

As discussed before, Fig.2 shows the system topology. The core idea of dynamic watermarking is to superimpose a private random excitation signal $e[k]$ that has a Gaussian distribution, onto the duty cycle control input: "d" (in the case of DC-DC converter) and modulation index "m_a" (in the case of DC-AC inverter). We call this private random excitation signal and/or a "watermark" since it is undetectable, similar to a watermark on a sheet of paper, furthermore, it is unknown to the attacker. Mathematical proofs and theory of operation of the digital watermarking method for a cyber physical system along with a few applications are detailed in [10], [11].

B. DC-DC Converter Analysis with Digital Watermarking

Fig.3 shows the DC-DC boost converter stage small signal equivalent circuit using the three terminal PWM switch model [12]. Fig.3(b) shows the piece wise linear equivalent circuit. The transfer function of output voltage $v_{out}(s)$ for changes in the duty cycle command $\hat{d}(s)$ is given by,

$$\frac{v_{out}(s)}{\hat{d}(s)} = \frac{\frac{V_{PV}}{RC(1-D)^2}\left(\frac{R(1-D)^2}{L} - s\right)}{s^2 + \frac{s}{RC} + \frac{(1-D)^2}{LC}} \tag{1}$$

Where R is the equivalent resistance (load) at the output of the DC-DC converter, representing the power delivered to the grid by the DC-AC inverter stage, L denotes the boost

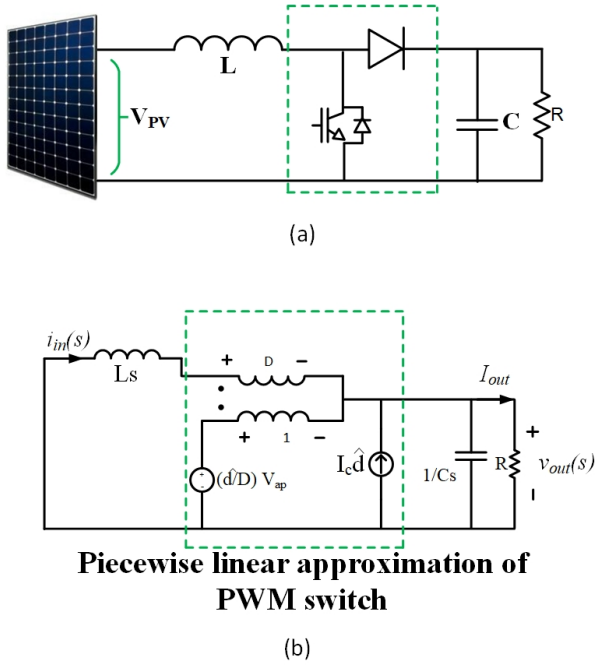

Fig. 3: a) DC-DC boost converter circuit b) small signal equivalent circuit [12]

inductor, C output capacitor, V_{PV} is the solar panel voltage and v_{out} is the output voltage.

The above equation(1) can be simplified by defining,

$$\alpha_1 = \frac{V_{PV}}{LC},\quad \alpha_2 = -\frac{V_{PV}}{RC(1-D)^2},\quad \alpha_3 = \frac{1}{RC},\quad \alpha_4 = \frac{(1-D)^2}{LC}$$

Equation (1) can now be re written as,

$$\frac{v_{out}(s)}{d(s)} = \frac{\alpha_1 + \alpha_2 s}{s^2 + \alpha_3 s + \alpha_4} \tag{2}$$

The time domain differential equation corresponding to (2) is given by,

$$\ddot{v}_{out}(t) = -\alpha_3 \dot{v}_{out}(t) - \alpha_4 v_{out}(t) + \alpha_1 d(t) + \alpha_2 \dot{d}(t) \tag{3}$$

Given the discrete nature of the closed loop control of power electronic systems via digital signal processor (DSP) control with a sampling time Δt, the above equation needs to be transformed to discrete domain. This can be accomplished by employing Tustin method [13], and is given by,

$$v_{out}[k+1] = \alpha_3' v_{out}[k] + \alpha_4' v_{out}[k-1] + \alpha_1' d[k-1] + \alpha_2' d[k] \tag{4}$$

where α_1', α_2', α_3', and α_4' are obtained by the Tustin method.

As outlined in Section II, the watermarking signal $e[k]$ is added to the duty cycle signal $d[k]$(see Fig.2). The modified duty cycle signal is $d_{WM}[k]$ with the addition of watermark signal $e[k]$ is given by,

$$d_{WM}[k] = d[k] + e[k] \tag{5}$$

Now substituting (5) in (4) we obtain the output voltage $v_{(WM)out}[k+1]$ with watermark added to the duty cycle $d_{WM}[k]$ as,

$$v_{(WM)out}[k+1] = \alpha_3' v_{out}[k] + \alpha_4' v_{out}[k-1] + \alpha_1' d_{WM}[k-1] + \alpha_2' d_{WM}[k] \tag{6}$$

Simplifying (6) we obtain,

$$v_{(WM)out}[k+1] = \alpha_3' v_{out}[k] + \alpha_4' v_{out}[k-1] + \alpha_1'(d[k-1] + e[k]) + \alpha_2'(d_[k] + e[k]) \tag{7}$$

Assume the DC-DC converter actual output voltage $v_{out}[k]$ is measured by a sensor, whose value is $z_1[k]$. For a healthy system the voltage sensor output is $z_1[k] \equiv v_{out}[k]$. Should the output voltage sensor be compromised (spoofed) $z_1[k] \not\equiv v_{out}[k]$. The following three tests can then be designed to check if such a compromise has occurred according to the procedure outlined in [10], [11].

*1) **Test 1 for the DC-DC converter**:*

Considering equation (7), $v_{(WM)out}[k+1]$ is output voltage obtained from the model, which includes the watermarking signal and $z_1[k+1]$ is the sensor measurement from the actual system. Test 1 is given by,

$$\lim_{K\to\infty} \frac{1}{K} \sum_{k=0}^{K-1} \Big(z_1[k+1] - v_{(WM)out}[k+1]\Big)^2 = \sigma_\omega^2 \tag{8}$$

Note: Equation (8) is computed repeatedly at each sampling interval of the sensor measurement. During normal operation, i.e. no attack, the output of Test 1 will yield the system noise variance denoted by σ_ω^2 since both the model and actual measurement will be the same. The resulting output of equation (8) is a small value since the variance of system noise is nearly zero. However, when an attack occurs (the sensor output is compromised and/or spoofed) the the actual measurement, $z_1[k+1]$, will no longer match the corresponding value computed from the model, $v_{(WM)out}[k+1]$ computed from (7) , and the output of equation (8) will show an increase in the variance which signifies that an attack has indeed occurred on the output voltage sensor. Section III shows details of various attack scenarios.

*2) **Test 2 for the DC-DC converter**:*

Test 2 is difference between the actual voltage sensor measurement, $z_1[k+1]$ and $v_{out}[k+1]$ and is given by,

$$\lim_{K\to\infty} \frac{1}{K} \sum_{k=0}^{K-1} \Big(z_1[k+1] - v_{out}[k+1]\Big)^2 = \sigma_\omega^2 + (\alpha_1' + \alpha_2')^2 \sigma_e^2 \tag{9}$$

Note in (9) the actual voltage sensor measurement $z_1[k+1]$ includes the effect of watermark and $v_{out}[k+1]$ is output voltage obtained from equation (4) that does not include watermark. In normal operation, i.e no attack, the output of equation (9) should only yield the system noise variance, σ_ω^2, and the watermarking variance σ_e^2, multiplied by constants

as shown$(\alpha_1' + \alpha_2')^2$. When an attack occurs on the sensor output measurement $z_1[k+1] \not\equiv v_{out}[k+1]$ the resulting output of (9) will yield an increase in the variances which indicates an attack. This test is used to detect more complex attacks on the sensors as explained in [10], [11].

*3) **Test 3 for the DC-DC converter:**:*
Test 3 is the difference between Test 2 and Test 1 and given by,

$$Test2 - Test1 = (\alpha_1' + \alpha_2')^2 \sigma_e^2 \tag{10}$$

During normal operation, i.e. no attack, Test 3 will yield the contribution of the watermark. This test is used to distinguish between a cyber-attack and a malfunction of the sensor.

In industrial systems sensors occasionally malfunction and report incorrect data. Examples include: excessive induced noise, increase in measurement error etc. Under such circumstances, both Test-1 and Test-2 output will remain high (above threshold) since the sensor output differs considerably from the computed value from the model. However, Test-3 (equation (10)) will be of low value/or exhibits no change. In such circumstances we can conclude that the sensor is malfunctioning.

C. DC-AC Inverter Analysis

Fig.4 shows the DC-AC inverter stage connected to utility grid via an inductor L_s. Grid impedance is represented by its short circuit impedance L_g and R_L is the equivalent line resistance.

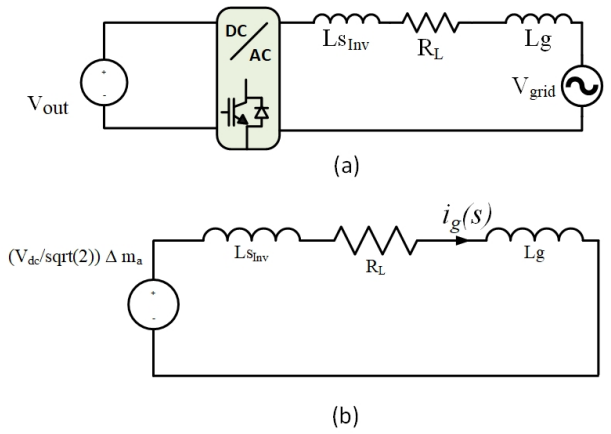

Fig. 4: a)DC-AC inverter connected to utility grid b)small signal circuit equivalent

Transfer function of the small signal boost system is derived in (11)

$$\frac{i_{grid}(s)}{\Delta m_a(s)} = \frac{\frac{V_{dc}}{\sqrt{2}}}{(L_s + L_g)(s + \frac{R}{L_s + L_g})} \tag{11}$$

The above equation (11) can be simplified by defining,

$$\beta_1 = \frac{V_{dc}}{\sqrt{2}(L_s + L_g)} \qquad \beta_2 = \frac{R}{L_s + L_g}$$

Equation (11) can now be re written as,

$$\frac{i_g(s)}{m_a(s)} = \frac{\beta_1}{s + \beta_2} \tag{12}$$

The transfer function (11) corresponds to the following continuous differential equations

$$\dot{i}_g(t) = -\beta_2 i_g(t) + \beta_1 m_a(t) \tag{13}$$

Given the sample time Δt, by the Tustin method, the continuous system can be converted to the following discrete system

$$i_g[k+1] = \beta_2' i_g[k] + \beta_1' m_a[k] \tag{14}$$

where β_1' and β_2' are obtained by the Tustin method based on original system parameters.

As outlined in Section II, the watermarking signal $e[k]$ is added to the modulation index signal $m_a[k]$(see Fig.2). The modified modulation index signal is $m_{a(WM)}[k]$ with the addition of watermark signal $e[k]$ is given by,

$$m_{a(WM)}[k] = m_a[k] + e[k] \tag{15}$$

Now substituting (15) in (14) we obtain the grid current $i_{g(WM)}[k+1]$ with watermark added to the modulation index $m_{a(WM)}[k]$ as,

$$i_{g(WM)}[k+1] = \beta_2' i_g[k] + \beta_1' m_{a(WM)}[k] \tag{16}$$

Simplifying (16) we obtain,

$$i_{g(WM)}[k+1] = \beta_2' i_g[k] + \beta_1' (m_a[k] + e[k]) \tag{17}$$

Assume the DC-AC inverter actual grid current $i_g[k]$ is measured by a sensor, whose value is $z_2[k]$. For a healthy system the voltage sensor output is $z_2[k] \equiv i_g[k]$. Should the grid current sensor be compromised (spoofed) $z_2[k] \not\equiv i_g[k]$. The following three tests can then be designed to check if such a compromise has occurred according to the procedure outlined in [10], [11].

*1) **Test 1 for the DC-AC inverter**:*

Considering equation (17), $i_{g(WM)}[k+1]$ is the grid current obtained from the model, which includes the watermarking signal and $z_2[k+1]$ is the sensor measurement from the actual system. Test 1 is given by,

$$\lim_{K\to\infty} \frac{1}{K} \sum_{k=0}^{K-1} \Big(z_2[k+1] - i_{g(WM)}[k+1] \Big)^2 = \sigma_\omega^2 \tag{18}$$

*2) **Test 2 for the DC-AC inverter**:*

Test 2 is the difference between the actual grid current measurement, $z_2[k+1]$ and $i_g[k+1]$ given by,

$$\lim_{K\to\infty} \frac{1}{K} \sum_{k=0}^{K-1} \Big(z_2[k+1] - i_g[k+1] \Big)^2 = \sigma_\omega^2 + (\beta_1')^2 \sigma_e^2 \tag{19}$$

*3) **Test 3 for the DC-AC inverter**:*
Test 3 is the difference between Test 2 and Test 1 given by,

$$Test2 - Test1 = (\beta_1')^2 \sigma_e^2 \tag{20}$$

III. Results and Discussion

In this section performance of the proposed sensor spoofing for DC-DC Converter stage and DC-AC Inverter stage is detailed. A grid connected PV system with the specifications outlined in Table 1 is simulated and the results are discussed for various attack scenarios.

TABLE I: Design parameters for the Grid-tied PV system

Parameter	***Magnitude***
Rated Power	$5kW$
DC link voltage V_{out}	400 VDC
PV panel voltage V_{PV}	$300V$
L_f	$0.5mH$
C_f	$1mH$
R	32Ω
Switching frequency	10 kHz
$t_{(dc,dc)attack}$	$0.8seconds$
Grid voltage V_{grid}	240 V_{rms}
Grid impedance L_g, R_L	$3mH, 30m\Omega$
Inverter switching frequency	$16kHz$
$t_{(Inv)attack}$	$0.4seconds$

A. DC-DC Converter Stage - Output Voltage Feedback Sensor Compromise

In this section various scenarios under which an output voltage sensor can come under attack (spoofed) and its detection by the proposed DMS Test 1-to-3 are illustrated.

1) Output Voltage V_{out} Sensor is Attacked to Report Over-voltage:
Fig.5 show the simulation results for the output voltage V_{out} sensor signal is increased from nominal 400V to 450V after $t = t_{(dc,dc)attack}$. Such a increase in output voltage can potentially destabilize the system. The data plotted for Test-1 and Test-2 detailed in Section II.B clearly show a sudden increase detecting the attack in less than 1 millisecond after the attack begins. Since the detection delay is significantly small, the defense mechanism is able to identify the attack almost instantaneously.

2) Addition of 2.5% of 1 kHz sinusoidal signal to the V_{out} voltage sensor :
"Fig.6" show the simulation results for the output voltage V_{out} sensor signal after injecting 2.5% of 1 kHz signal is added to the sensor output after $t = t_{(dc,dc)attack}$. Such a increase in output voltage can potentially destabilize the system. The data plotted for Test-1 and Test-2 detailed in Section II.B clearly show a sudden increase detecting the attack in less than 2 millisecond after the attack begins. Since the detection delay is significantly small, the defense mechanism is able to identify the attack almost instantaneously.

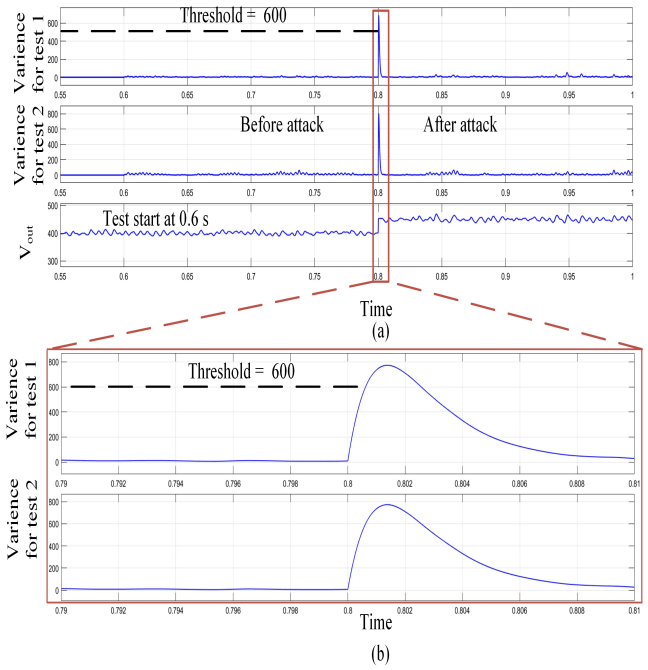

Fig. 5: DC-DC Converter output voltage sensor attack: The correct sensor output (400 V) is increased to 450 V at $t_{(dc,dc)attack}$ = 0.8 seconds to simulate sensor spoofing attack. It is clear that Test-1 and Test-2 show a sudden increase and cross the set threshold limit of 600. It is noted that the detection delay is 1 millisecond

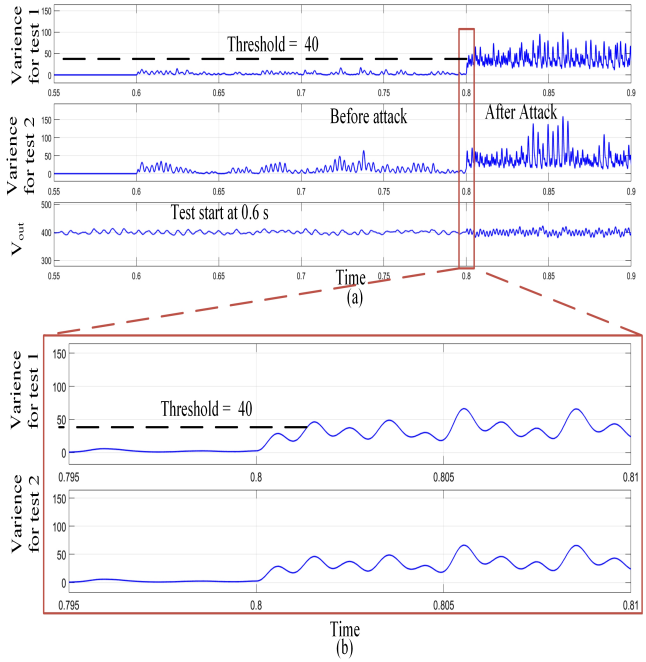

Fig. 6: DC-DC Converter output voltage sensor attack: at $t_{(dc,dc)attack}$ = 0.8 seconds, 2.5% of 1 kHz signal is added to the sensor output. A detection threshold limit is set to 40. a) Detection delay of variance test 1, test 2 and output voltage V_{out}. b) zoomed in on variance test 1 and 2. The attack begins at 0.8 seconds

3) Sensor malfunctioning scenario:

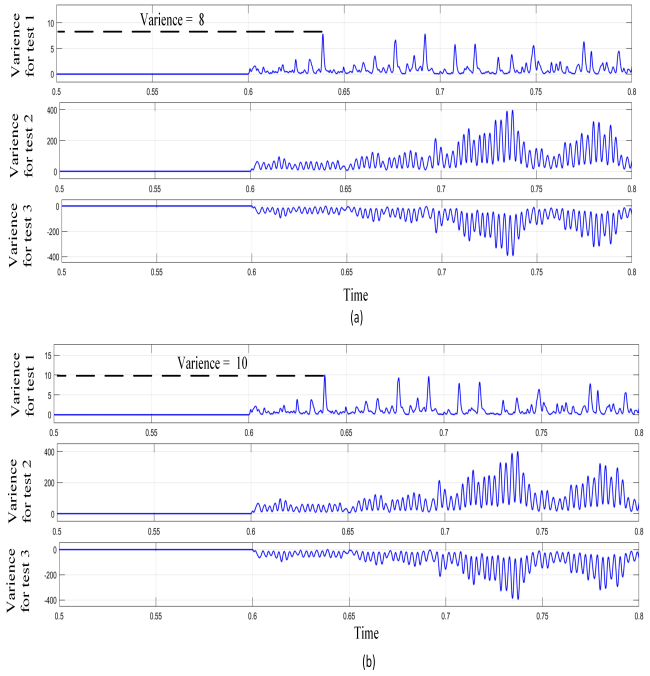

Fig. 7: DC-DC Converter sensor malfunction demonstration test: The correct output voltage sensor value (400v) is increased to (420v) at the start of the simulation, i.e time = 0 seconds, Variance Test start at 0.6 seconds. The threshold limit is set to 9. a) Variance test 1, test 2 and test 3 in normal operation **(400v - no malfunction)** . b)Variance test 1, test 2 and test 3 in malfunctioning operation **(420v - sensor malfunction)**

"Fig.7" show the simulation results for the output voltage V_{out} sensor signal increase from 400v to 420v at the beginning of the simulation. The data plotted for Test-1, Test 2 and Test-3 detailed in Section II.B clearly show that Test 1 and Test 2 variances passes the threshold in Fig.7b and Test 3 variance did not change. Thus we conclude that the sensor is malfunctioning.

Table II summarizes how to distinguish between an attack and a malfunctioned sensor using Test 3

B. DC-AC Inverter Stage Sensor Spoofing Scenarios

Several malicious attack models can be designed, such as Replay Attack, Stealth Attack, Time Delay Attack, Constant Noise Bias Attack, Random Noise Bias Attack, Flipping Sign Attack, and finally, the Harmonic Injections Attack. In this section the attack implemented is the Harmonic Injection Attack where an attacker can superimpose false harmonic measurements to the reported sensor measurements.

1) Harmonic Injection Attack:

"Fig.8" shows the simulation results of the harmonics injections attack. It can be seen that after $t = t_{(Inv)attack}$, the current fed to the grid starts including 3rd and 5th harmonics, potentially decreasing the power factor and efficiency of the inverter significantly. However, the Dynamic Watermarking tests can detect the attack in less than 5 milliseconds after the attack begins. Since the detection delay is significantly small, the defense mechanism is able to identify the attack before one 60 Hz cycle.

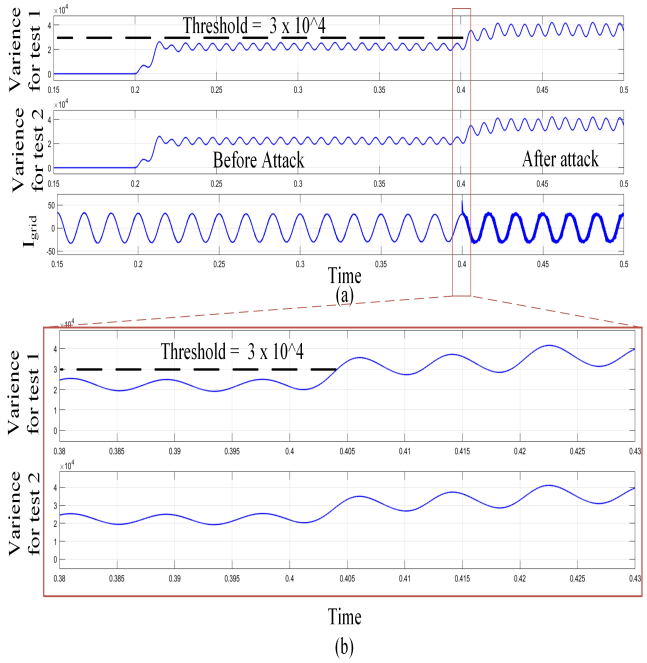

Fig. 8: DC-AC Inverter output current sensor attack: In this test additional harmonics are added to the current sensor output to distort the inject power to the grid. Such an attack is shown to occur after $t_{(Inv)attack}$ = 0.4 seconds. The threshold limit is set to 3×10^4. a) Shows the Test-1, Test-2 output and the current sensor signal I_{grid}. b) is zoomed view indicating the speed of detection

IV. Conclusion

In this paper, analysis and design of an active detection scheme based on digital watermarking technique has been explored for sensor spoofing in grid tied PV systems. It has been shown that by injecting a small magnitude watermark (secret) signal $e[k]$ that has a Gaussian distribution with zero mean superimposed on the control command of both DC-DC and DC-AC converter stages, any tampering of sensor signals that controls the power conversion stages can be detected in microseconds. The fast detection of an attack and/or external compromise of sensor signals allows the implementation of an active defense mechanisms (not discussed in this paper) to protect the grid connected system. The proposed approach can be extended many more sensors and control inputs due to its simplicity in implementation. Several scenarios that detail DC-DC converter output voltage and DC-AC inverter output current sensor spoofing have been shown. In all cases the detection time is shown to be short. A natural extension of the method to detect sensor malfunctioning has also been explained. Simulation results show good agreement with the theory. Experimental results will be presented in the conference.

References

[1] IEA (2017), "World Energy Outlook 2017", IEA, Paris https://www.iea.org/reports/world-energy-outlook-2017.

[2] International Energy Agency, SNAPSHOT OF GLOBAL PHOTOVOLTAIC MARKETS, 2018. Last accessed: February 25, 2019. Available: http://www.iea-pvps.org/fileadmin/dam/public/report/statistics/IEA-PVPS˙-˙A˙Snapshot˙of˙Global˙PV˙-˙1992-2017.pdf.
[3] Barua, A. (2020). Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter. UC Irvine. Retrieved from https://escholarship.org/uc/item/0371448g.
[4] G. Tertytchny et al., "Demonstration of Man in the Middle Attack on a Commercial Photovoltaic Inverter Providing Ancillary Services," 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 2020, pp. 1-7.
[5] I. Akkaya, E. A. Lee and P. Derler, "Model-based evaluation of GPS spoofing attacks on power grid sensors," 2013 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Berkeley, CA, 2013, pp. 1-6.
[6] A. S. Spanias, "Solar energy management as an Internet of Things (IoT) application," 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA), Larnaca, 2017, pp. 1-4.
[7] A. Teymouri, A. Mehrizi-Sani and C. Liu, "Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability," IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, 2018, pp. 2872-2877.
[8] J. Ramos-Ruiz et al., "An Active Detection Scheme for Cyber Attacks on Grid-tied PV Systems," 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 2020, pp. 1-6, doi: 10.1109/CyberPELS49534.2020.9311539.
[9] A. K. Abdelsalam, A. M. Massoud, S. Ahmed and P. N. Enjeti, "High-Performance Adaptive Perturb and Observe MPPT Technique for Photovoltaic-Based Microgrids," in IEEE Transactions on Power Electronics, vol. 26, no. 4, pp. 1010-1021
[10] Jaewon Kim, Woo-Hyun Ko and P. R. Kumar, "Cyber-security with dynamic watermarking for process control systems," in 2019 AIChE Annual Meeting. AIChE, 2019.
[11] B. Satchidanandan and P. R. Kumar, "Dynamic watermarking: Active defense of networked cyber-physical systems," Proceedings of the IEEE, Vol. 105, Issue 2, Feb. 2017, pp. 219-240
[12] V. Vorperian, "Simplified analysis of PWM converters using model of PWM switch. Continuous conduction mode," in IEEE Transactions on Aerospace and Electronic Systems, vol. 26, no. 3, pp. 490-496, May 1990
[13] J. S. Bay, Fundamentals of linear state space systems. McGraw-Hill Science, Engineering & Mathematics, 1999