Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter

Anomadarshi Barua and Mohammad Abdullah Al Faruque, *UC Irvine*

https://www.usenix.org/conference/usenixsecurity20/presentation/barua

This paper is included in the Proceedings of the
29th USENIX Security Symposium.

August 12–14, 2020

978-1-939133-17-5

Open access to the Proceedings of the
29th USENIX Security Symposium
is sponsored by USENIX.

Hall Spoofing: A Noninvasive DoS Attack on Grid-Tied Solar Inverter

Anomadarshi Barua *and* Mohammad Abdullah Al Faruque
Department of Electrical Engineering and Computer Science, University of California, Irvine

Abstract

Grid-tied solar inverters continue to proliferate rapidly to tackle the growing environmental challenges. Nowadays, different smart sensors and transducers are tightly integrated with the grid-tied inverter. This integration opens the "Pandora's Box" of unknown threats that could come from very unconventional ways. This paper demonstrates a noninvasive attack that could come by spoofing the Hall sensor of an inverter in a stealthy way by using an external magnetic field. We demonstrate how an attacker can camouflage his/her attack tool and place it near a target inverter. In doing so, he/she can intentionally perturb grid voltage and frequency and can inject false real and reactive power to the grid. We also show the consequences of the attack on a scaled-down testbed of a power grid with a commercial 140 W grid-tied inverter from Texas Instruments. We are able to achieve a 31.52% change in output voltage, 3.16x (-6dB to -11dB) increase in low-frequency harmonics power, and 3.44x increase in real power. Moreover, we introduce a duty-cycle variation approach for a noninvasive adversarial control that can change the inverter voltage up to 34% and real power up to 38%. We discuss the feasibility of using a 100 kW inverter through discussion. This provides insights behind the generalization of the attack model. In addition, the commercial power system simulation tool Etap 19.0.1 is used to simulate the impact of the attack on a 2.3 MW power grid. To the best of our knowledge, this is the first methodology that highlights the possibility of such an attack that might lead to grid blackout in a weak grid.

1 Introduction

Cyber-physical systems (CPSs) in power grids comprise sophisticated control mechanisms. These mechanisms may produce multidisciplinary security issues capable of compromising the *Availability* and *Integrity* [1, 2, 3] of the power grids. Examples of such attacks on power CPSs include cyberattacks on the Ukrainian power grid [4], DoS attacks on anonymous western utilities in the U.S. power sector [5], the Slammer worm attack on Ohio's Davis-Besse nuclear power plant [6], the Stuxnet malware attack on Iran's nuclear facilities [7], etc. The results of these attacks are very serious, including region-wise blackouts affecting more than 230,000 residents [8] and monetary losses [9].

Nowadays, distributed energy sources are proliferating rapidly and a substantial portion of these sources are highly efficient grid-tied solar inverters[1] [10, 11] equipped with Hall sensors. These Hall sensors, however, can be cleverly spoofed to orchestrate a noninvasive attack on the grid. The attack in question can perturb the normal operation of a power system and may cause grid failures in a weak grid. It is important to note that a strong grid gradually becomes weak due to the continuous integration of distributed energy sources [12]. Strong grids may also behave as weak grids at a particular time of a day (e.g., peak hours). Moreover, micro-grids [13] also behave as weak grids when connected over long cables to a utility grid. A detailed background of strong and weak grids is provided in Section 3.1.

This paper shows that a smart attacker can inject measurement errors into the Hall sensors of an inverter using a noninvasive magnetic spoofing technique with adversarial control. The injected errors can propagate from the compromised Hall sensor to the internal controllers of the inverter and eventually compromise the inverter itself. The compromised inverter can hamper the grid stability and may cause grid failures in a weak grid scenario. This method is similar to the false data injection approach. But in this case, the injection is coming from the physical domain by exploiting the physics of the Hall sensor. *We show that the attacker can intelligently control the false data injection by applying distinct types of external magnetic fields, such as constant, sinusoidal, and square pulsating magnetic fields, on the Hall sensors.* This may perturb the inverter output voltage, frequency, real and reactive power. This perturbation can propagate through the cyber domain and finally impact the physical domain. Hence, this can be termed as an attack from **P**hysical-to-**C**yber-to-**P**hysical (P-2-C-2-P) domain [14]. In power CPSs, this type of cross-domain attack is yet to be explored in depth by the security community.

[1] In this paper, grid-tied solar inverter are used interchangeably with inverter.

Technical Contributions: Our technical contributions are listed as follows that are elaborated in the following sections:

i. A new attack model (**Section 4**) that describes how the availability of the grid-tied inverter is stealthily breached.

ii. Algorithms and a potential design for the relevant attack tool (i.e., Embedded Hall Spoofing Controller) and mathematical models of an inverter's control blocks (**Section 5**).

iii. A testbed (**Section 6**) with a scaled-down model of a power grid, on which the attack model is validated and adversarial control is demonstrated (**Section 7**).

iv. The attack model is further evaluated (**Section 8**) using an industry-standard commercially used *Electrical Power System Analysis Software (Etap 19.0.1)* on a medium-sized 2.3 MW (equivalent to approx. $\sim$ 150 houses) grid.

v. Defense (**Section 9.1**) is proposed and justified, and limitations (**Section 9.2**) of this attack are noted.

2 Related Work

We discuss here different attacks on analog sensors, inertial sensors, and on power systems that exist in the literature.

Attacks on Analog Sensors: Kune et al. [15] spoofed sensors by electromagnetic interference (EMI) to induce defibrillation shocks on implantable cardiac devices. Park et al. [16] used infrared to trigger a medical infusion pump to deliver overdose to patients. Davidson et al. [17] reported how spoofing optical sensors of an unmanned aerial vehicle (UAV) can compromise complete control of the lateral movement. Yan et al. [18] published a contact-less attack on self-driving cars using ultrasound and EMI. Shin et al. [19] showed a spoofing attack on LiDar to create illusions of objects appearing closer in automotive systems. Zhang et al. [20] injected inaudible commands into a microphone using ultrasonic carriers. Lastly, Shoukry et al. [21] used an external magnetic field to spoof the Antilock Braking System (ABS) to change the wheel speed of a vehicle. There are a few fundamental differences between our work and [21]. First, the attacker requires access to place the electromagnetic actuator near the ABS wheel speed sensor and must strongly secure the attack object *ABS Hacker* to the vehicle body, likely with a nut and bolt. Second, the original magnetic field of the vehicle must be shielded before spoofing. The space to place this extra shield near the ABS sensor is critical. Third, the *ABS Hacker* comprises expensive heterogeneous processors. Fourth, the adaptive controller of [21] requires complex tuning of its closed-loop poles and zeros. In contrast to [21], our attack can be noninvasively executed on a cheap Arduino board and does not require strong physical mounting or extra shielding.

Attacks on Inertial Sensors: Son et al. [22] used high power sound noise to compromise the gyroscope of a drone to make it uncontrollable. Wang et al. [23] used a sonic gun to demonstrate acoustic attacks on different inertial sensors. Trippel et al. [24] showed fine-grained adversarial control over MEMS accelerometers using acoustic signals to damage digital integrity. Tu et al. [25] also demonstrated adversarial control over embedded inertial sensors to trigger the actuation of different control systems. In contrast to their methods (e.g., biasing attack, sample rate drifts, etc.), our paper introduces a duty-cycle variation approach for adversarial control that is novel in our attack model in the power CPSs.

Attacks on Modern Power Systems: There are quite a lot of works on traditional **C**yber-to-**P**hysical domain (C-2-P) attacks in the literature, such as malicious false data injection [26], flooding [27], arbitrary command injection [28], time-delay input attack [29], load distribution attack [30]. Ilge Akkaya et al. [31] used GPS spoofing on *Phase Measurement Units* (PMUs) to lead a substation to an erroneous state. In contrast to these works, our work demonstrates an unconventional P-2-C-2-P attack in the power CPSs.

Our work shows how an attacker can cause damage (e.g., blackout) to the connected power grid by intelligently applying constant, sinusoidal, and square pulsating magnetic fields. Moreover, in contrast to the prior works, this paper models the vulnerable blocks of the controller of an inverter and mathematically proves the underlying principle of propagation of attack from sensors to the internal controllers. Our attack impact is more realistic, has more economically damaging effect, and can impact a large region.

3 Background

3.1 Strong and Weak Grid in the Power CPSs

The grid where voltage and frequency are stable and do not vary during load connection/disconnection is known as a strong grid. Historically, rotational generators are present in the power systems. Rotational generators have prime movers to convert rotational kinetic energy into electrical energy. Rotational energy stored in the prime mover of these generators acts as an *inertia* against any sudden change of load in the system; therefore, the voltage/frequency does not vary abruptly within a limit in the grid when a small load is disconnected from the grid. *It is important to note that a strong grid is not ideally strong all the time. The voltage/frequency of a strong grid may vary abruptly if the change of the load is large compared to the generation capacity, or if the rotational energy stored in the prime mover is not sufficient to compensate for the sudden change in the grid. Hence, a strong grid can behave as a weak grid. A weak grid refers to a grid wherein its voltage is highly sensitive to any variation in the load [32].*

Due to the continuous integration of distributed solar/wind inverters, the modern grid is shifting from centralized to distributed generation resulting in poor control and lack of inertia (i.e., rotational turbines). This causes grid weakening over time [12], which is already a concern in the community. In this scenario, an attacker can perturb the grid voltage/frequency using an inverter and this perturbation may disrupt the entire system. Moreover, low generation, long transmission lines, etc., can also contribute to weak grids. We can also find weak grids in isolated places like Baja, Mexico; parts of Alaska; or under-developed areas between strong grids.

3.2 Real Power, Reactive Power and Phase

An inverter can inject real power and reactive power into the grid. *Real power is related to grid frequency and reactive power is related to grid voltage [33].* If the generation of real power is lower than the real power demand, the grid frequency may fall. Whereas, if the generation of reactive power is lower than the required, the grid voltage may fall. Real power is the amount of power in watts (W) being dissipated, and reactive power results from inductive/capacitive loads measured in volt-ampere reactive (VAR) (Appendix 11.2). The phase is the position of a point of a wave in a time instant. Three-phase voltages are 120^o phase apart from each other.

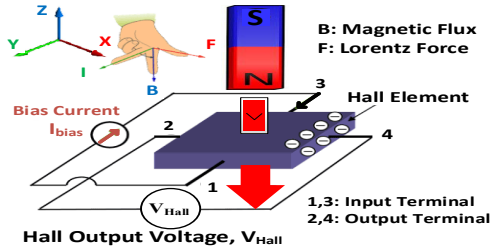

Figure 1: Working principle of a typical Hall sensor.

3.3 Working Principle of a Hall Sensor

Fig. 1 shows the working principle of a typical Hall sensor. It comprises a Hall element, which is made of a thin piece of p-type semiconductor material (e.g. Gallium Arsenide, etc.). Let us assume that a bias current I_{bias} is flowing in +ve Y direction (terminal 1, 3) of the Hall element having thickness d. This Hall element is placed within an applied magnetic field B whose direction is -ve Z-axis. The charge carriers inside the Hall sensors feel a force along +ve X-axis. This force is known as the Lorentz force F. Due to this Lorentz force, the charge carriers will be deflected along the +ve X-axis and a voltage V_{Hall} will be generated across the Hall element. The generated voltage V_{Hall} may be expressed as:

$$V_{Hall} = k(\frac{I_{bias}}{d} \times B) \quad (1)$$

where k is the hall coefficient, which depends upon the properties of the hall element. If d, I_{bias}, and k are constant, V_{Hall} depends only on applied B. This B is proportional to the current/voltage to be measured. *Any external perturbation of B can change V_{Hall}. And this change can give a **false** sense of voltage/current measurement that can propagate to the inverter controller and hamper its normal operation.*

3.4 Why is a Hall Sensor Used in an Inverter?

Inverters measure grid voltage, current, and their phase angles for important control applications. Four methods [34] are mainly used to measure voltage/current: i) Resistive drop/-divider method, ii) Magneto-resistance method, iii) A voltage/current transformer, and iv) A Hall effect sensor.

A resistive drop/divider is not suitable for high voltage/current measurement because of the following reasons: high power loss in the resistor itself, inability to measure small DC current in the presence of large AC current, and absence of proper isolation. A magneto-resistive material is nonlinear and temperature-dependent, therefore, it is not suitable for accurate high current measurement. A voltage/current transformer is not suitable for simultaneous AC/DC measurement and is bulky. It also requires an external resistance to convert current into voltage and has a low efficiency for core loss. *In contrast, the Hall effect sensor has excellent accuracy, high efficiency, very good linearity, low thermal drift, and low response time. It is lightweight, compact, and suitable for simultaneous large AC/DC voltage/current measurement with galvanic isolation.* Therefore, Hall sensors are pervasive in high power inverter applications (Appendix 11.4).

To show the prevalence of Hall sensors in inverters, we investigate six industry-designed inverters (small to medium range) and a large 100 kW inverter. All these inverters (Table 1 and Section 8) have similar functional blocks, and Hall effect sensors are present in the measurement unit. This is because inverters are optimized for ***efficiency and accuracy***, but not for security from this type of unconventional spoofing attack.

Table 1: Presence of Hall sensors in different inverters.

Manufacturer	Inverter Series	Sensor	Power
Texas Instr. [35]	TMDSOLARUINVKIT	Hall	0.14 kW
Texas Instr.[36]	TIDA-01606	Hall	10 kW
STMicro. [37]	STEVAL-ISV003V1	Hall	0.25 kW
Microchip [38]	Grid Connected Inverter	Hall	0.215 kW
SMA[39]	Sunny Boy	Hall	5 kW
SOLAX [40]	SL-TL5000T	Hall	3 kW

4 Attack Model

Fig. 2 depicts our proposed attack model, which can affect the availability of an inverter by spoofing Hall sensors. The components of our attack model are described as follows:

Attacker's Intent: The attacker wants to disrupt the normal operation of a power system by spoofing an inverter noninvasively and wants to cause grid failures in a weak grid.

Attacker's Capabilities: The attacker can surreptitiously place a small box near the target inverter. This box contains a powerful electromagnet integrated with an electronic spoofing controller (i.e., *Embedded Hall Spoofing Controller*). This box is small enough to be camouflaged within a small container, such as flower vase, coffee cup. Placing the camouflaged attack tool near the inverter requires a *brief one-time* access. The box has wireless controls allowing for remote communication. Therefore, the attacker can remotely control the timing of the attack and can pick a vulnerable time (e.g., at peak hour, etc.) to impact the connected power grid. The authorities of the target inverter may not be aware of this attack model and would possibly neglect the security implications of any small camouflaged box placed near an inverter.

Attacker's Access Level: The access near the inverter needed for the attack can be possible in at least three scenarios. **First** (most likely), a malicious employee or a guest, who has access near the inverter, may place the camouflaged attack tool near the inverter. An incident similar to this has

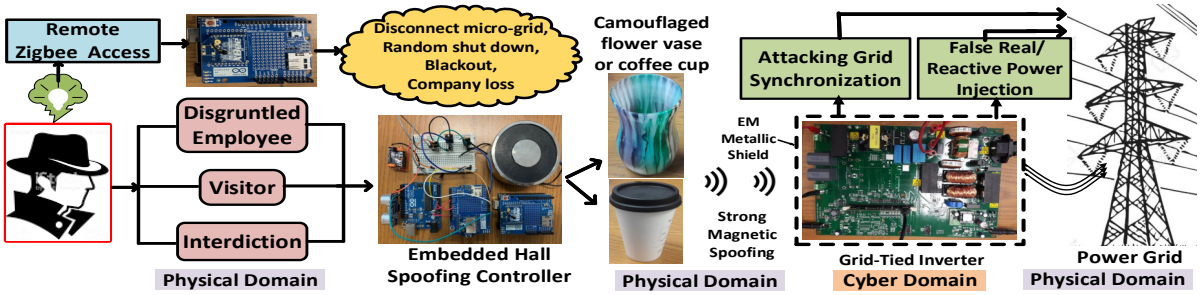

Figure 2: Brief overview of the Hall spoofing attack methodology.

already been reported in past news [41]. A disgruntled ex-employee of an electric utility in Texas posted a note in a hacker journal indicating that his insider knowledge of the system could be used to shut down that region's power grid. Moreover, solar plants are usually located in an isolated place with less security [42]. Getting a *brief one-time* access near the isolated solar plants may not be difficult. Staggs et al. [42] demonstrated how easily an attacker can access a wind plant in the middle of a remote field and can invasively place an attack tool inside of the wind turbine. Our attack model is stronger compared to [42] because of its noninvasive nature. **Second**, the manufacturer may introduce the malicious electromagnet with controllers inside of the solar inverter. **Third** is interdiction, which has been rumored to be used in the past [43, 44, 45, 46] and has been recently proven to be feasible [47]. During interdiction, a competitor can intercept the inverter during delivery or installation and may modify the inverter by placing an electronic device inside and then proceed with delivery or installation to the customer.

Stealthy Nature: The attacker can remotely perturb the inverter by camouflaging the tiny attack tool and can choose the timing of the attack to remain unidentified to maximize the impact. Fig. 3 is an example that shows how the attacker can place the camouflaged attack tool near the target inverter.

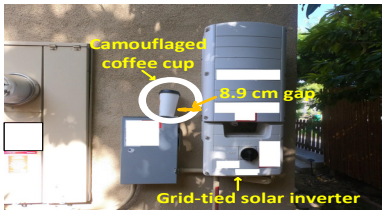

Figure 3: Demonstration of access near a typical inverter.

Outcome of this Attack: The attacker may cause grid failures if the power grid is weak. And for weakly protected systems, the attacker can fry the internal circuitry of the inverter itself. By spoofing the Hall sensor, the attacker can give a false impression that the conditions required for synchronization of the inverter with the grid have been achieved when they have not. This improper grid synchronization may shut down the inverter (Section 7.1). *A micro-grid is a group of interconnected loads and distributed energy resources, which can operate in both grid-connected or island mode* [13]. The attacker can disconnect the micro-grid from the utility grid at a random time or can prevent it from disconnecting even when it is supposed to disconnect (e.g., in the case of an outage). The attacker can choose the timing of the attack and can remotely shut down the inverter in peak hours to create a shortage of real/reactive power with no prior notice to the authority. This scenario can be significant in a weak grid and a micro-grid. As the timing of the attack can be remotely controlled, the attacker can cause a security breach by randomly shutting down the local solar power supply of any important organization, remote airport, army base, etc. The attacker can prevent the inverter from starting and can cause a repetitive shutdown. Simply pressing the restart button of the inverter may not solve the problem until the attack tool is removed. As this attack is stealthy, it can remain unidentified. This trick, which may cause grid instability, can be used to ask for ransom or to blackmail the utility.

Attacker's Safety: As inverters handle high voltage, it is unsafe for the attacker to invasively manipulate them. In this sense, our attack model is safe for the attacker as it enables the attacker to control the operation of the inverter noninvasively.

Attacker's Resources: We assume that the attacker has domain knowledge of the inverter controllers with some high school knowledge of electromagnetism.

Cost: The design cost of the *Embedded Hall Spoofing Controller* and the electromagnet is less than $50. The electronic parts are readily available from Amazon and Digikey.

5 Attack Model Design

This section explains how an attacker can design the attack tool (i.e., *Embedded Hall Spoofing Controller*). This section also mathematically models important basic blocks of an inverter irrespective of the inverter size.

5.1 Embedded Hall Spoofing Controller

The *Embedded Hall Spoofing Controller* consists of an electromagnet, an Arduino Uno, few MOSFETs, a Zigbee RF module, an Ultrasonic Sensor, and Energizer A23 Batteries. A small (height 3.8 cm, radius 3.5 cm) but powerful electromagnet (WF-P80/38) is used as a source of magnetic field. An electromagnet can also be built by winding wires around a strong neodymium (NIB) magnet, which is easily found in a computer hard disk [48]. An ultrasonic sensor (HC-SR04) is interfaced with the Arduino board to measure the distance between the electromagnet and the inverter shield. This distance helps to calculate the required strength of the *Magneto-Motive Force* (MMF) to influence the Hall sensors and stops oversupply of power to extend the battery lifetime. MMF measures

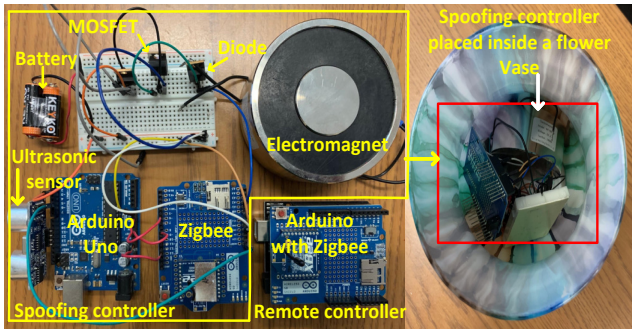

Figure 4: The Embedded Hall Spoofing Controller.

the strength of the generated magnetic flux. A Metal Oxide Semiconductor Field Effect Transistor (MOSFET), P7N20E is used to toggle the electromagnet ON and OFF with variable frequencies using a Pulse Width Modulation (PWM) technique. This PWM helps to generate variable-frequency electromagnetic flux and controls the power input to the electromagnet depending upon the attacker's need and intention. To protect the MOSFET from an inductive surge (due to the switching of the large electromagnet), a free-wheeling diode (U1620G) is connected across the electromagnet.

5.2 Controller Compromising Algorithm

The algorithm, which compromises the inverter controller, runs on the Arduino Uno (Algorithm 1). It is computationally inexpensive and may run on the Arduino for a long period with the battery pack mentioned in Section 5.1. It controls the ultrasonic sensor, Zigbee modules, and ADC, PWM, RX-TX peripherals of the Arduino Uno. After initializing the necessary modules and peripherals, the algorithm first checks for battery voltage level to see whether it is above the threshold. Otherwise, it returns `ErrorCode` after informing the attacker about this issue through Zigbee. Then the distance from the inverter is calculated using the ultrasonic module. If it is outside of the range, it notifies the attacker (`ErrorCode`) through Zigbee. Otherwise, it activates the MOSFET switching block and generates PWM frequency depending upon the attacker's need and intention for different attack scenarios. The attacker can also enable adversarial control and provide duty-cycle to the attack tool through the Zigbee. Depending upon the provided duty-cycle (see Section 7.4), the `PowerController` supplies the required amount of power to the electromagnet. This algorithm also checks for `MagnetCurrent`, which is flowing through the electromagnet. If it is less than the required amount, the algorithm also notifies the attacker.

5.3 Modelling Grid-Tied Inverters

This section mathematically models the basic blocks of the inverter controller. A grid-tied solar inverter can be single-phase or three-phase. Fig. 5 shows the basic blocks of a three-phase inverter. Let us denote the balanced abc-phase (*phase a, b, c*) grid voltages by e_a, e_b, and e_c, which are 120^0 phase apart. These abc-phase grid voltages may be represented by a

Algorithm 1: Solar Inverter Controller Compromising Algorithm.

Input: Control variables: $\{Attack\_level, Adversarial\_control, Duty\_cycle\}$
Output: Pulse Width Modulation Frequency: PWM_{freq}

$n \leftarrow$: $Timesteps$
$ADC\_arduino, PWM\_arduino, RX\_TX\_arduino \leftarrow Initialize$
$Zigbee\_module, Ultrasound\_module \leftarrow Initialize$
for $i \leftarrow 1$ ***to*** n **do**
  $batteryVoltage \leftarrow ADC\_Channel\_1$
  if $batteryVoltage < VoltageThreshold$ **then**
    Inform_attacker (battery_voltage_low)
    return $ErrorCode\_BatteryVoltageLow$
  else
    Inform_attacker (battery_voltage_sufficient)
  $ultrasound\_setup \leftarrow Activate$
  $Distance \leftarrow Ultrasound\_Measurements$
  if $Distance > Distance\_threshold$ **then**
    Inform_attacker (distance_threshold_exceed)
    return $ErrorCode\_DistanceThresholdExceed$
  $PowerController \leftarrow (Duty\_cycle = 100\%)$
  if $Attack\_Level = Constant\_MMF$ **then**
    $MosfetGate \leftarrow PulledUp$
  else if $Attack\_Level = Pulsating\_MMF\_1Hz$ **then**
    $MosfetGate \leftarrow PulledUp$
    $PWM_{freq} \leftarrow 1$
  else if $Attack\_Level = Pulsating\_MMF\_2Hz$ **then**
    $MosfetGate \leftarrow PulledUp$
    $PWM_{freq} \leftarrow 2$
  else
    $MosfetGate \leftarrow PulledDown$
  if $Adversarial\_control = Enable$ **then**
    $PowerController \leftarrow (Duty\_cycle, Distance)$
    Inform_attacker (adversarial_control_enabled)
  else
    $PowerController \leftarrow (Duty\_cycle = 100\%)$
    Inform_attacker (adversarial_control_disabled)
  $MagnetCurrent \leftarrow ADC\_Channel\_2$
  if $MagnetCurrent < CurrentThreshold$ **then**
    Inform_attacker (battery_Charge_low)
    return $ErrorCode\_BatteryChargeLow$

grid voltage space vector $\vec{S}_{abc}$ as follows:

$$\vec{S}_{abc}(t) = \begin{bmatrix} e_a \\ e_b \\ e_c \end{bmatrix} = \begin{bmatrix} E\cos\omega t \\ E\cos(\omega t - 120^0) \\ E\cos(\omega t + 120^0) \end{bmatrix} \quad (2)$$

where E is the amplitude and ω is the angular frequency of the grid voltage. Terms e_a, e_b, and e_c are sensed by three Hall effect voltage sensors *(we name these as grid sensors)* and then are sampled by the Digital Signal Processing (DSP) unit.

The abc-to-dq Transformation Block: This block transforms abc-phase grid voltage $\vec{S}_{abc}$ into direct-quadrature (dq) axis components, which are direct current (DC) quantities. This transformation facilitates the designing of a simple controller, such as the Proportional-Integral (PI) controller, in DC domain [49]. We know the axis of the rotor flux of a rotating machine is known as direct (d) axis, and the quadrature (q) axis lags d axis by 90^o. The *abc-to-dq* transformation is done in two steps: a *Clarke Matrix* (CM) transforms $\vec{S}_{abc}$ into alpha-beta component vector $\vec{S}_{\alpha\beta}$ (e_α and e_β), and a *Park Matrix* (PM) transforms $\vec{S}_{\alpha\beta}$ into dq component vector $\vec{S}_{dq}$ (e_d and e_q). The term $\vec{S}_{dq}$ can be given by (Appendix 11.5):

$$\vec{S}_{dq} = \begin{bmatrix} e_d \\ e_q \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{3}{2}}E \\ 0 \end{bmatrix} \quad (3)$$

where e_d and e_q are the d and q axis components of the abc-phase grid voltages, respectively and they are DC quantities. Please note that $e_q = 0$ for balanced grid voltage.

Let us denote the three-phase inverter output voltages $[u_a, u_b, u_c]$ and output currents $[i_a, i_b, i_c]$ as vectors $\vec{U}_{abc}$ and $\vec{I}_{abc}$, respectively. The inverter output current $\vec{I}_{abc}$ is similarly sensed and sampled by three Hall effect current sensors (*we name these as grid sensors*) and the DSP unit, respectively.

$\vec{U}_{abc}$ and $\vec{I}_{abc}$ vectors are also sinusoidal quantities, and they are converted into their dq axis components using a Clarke and a Park matrix. Let us denote $\vec{U}_{dq}$ and $\vec{I}_{dq}$ as the dq transformations of $\vec{U}_{abc}$ and $\vec{I}_{abc}$, respectively. The term $\vec{U}_{dq}$ comprises u_d and u_q where u_d and u_q are the d and q axis components of $\vec{U}_{abc}$. The term $\vec{I}_{dq}$ similarly comprises i_d and i_q where i_d and i_q are the d and q axis components of $\vec{I}_{abc}$.

A loop filter with inductance L is present between $\vec{S}_{abc}$ and $\vec{U}_{abc}$ for signal smoothing. The relation between $\vec{S}_{abc}$ and $\vec{U}_{abc}$ can be simplified using their dq axis components (e_d, e_q and u_d, u_q) and finally can be expressed as (Appendix 11.6):

$$u_d = e_d + L\frac{di_d}{dt} - \omega L i_q \quad (4)$$

$$u_q = L\frac{di_q}{dt} + \omega L i_d \quad (5)$$

Generation of Reference Currents (i_d^*, i_q^*): Two reference points, which are i_d^* and i_q^*, control the real and reactive power set points of the inverter. The solar panel output voltage V_T and current I_T are sensed by *two separate Hall voltage and current sensors* (*we name these as solar panel sensors*). V_T and I_T are given as inputs to a Maximum Power Point Tracking (MPPT) block that generates reference point i_d^* to track the maximum available real power from the panel. The other reference point i_q^* is generated from the reference reactive power Q^*, which is provided by the facility's energy management systems using a Wide/Local Area Network [50].

Proportional-Integral (PI) Current Controllers: Two separate PI current controllers force the dq axis components i_d and i_q to track the reference set points i_d^* and i_q^*. This tracking generates fractional DC voltages u_d^p and u_q^p as follows:

$$u_d^p = K_p(i_d^* - i_d) + K_i \int (i_d^* - i_d) \quad (6)$$

$$u_q^p = K_p(i_q^* - i_q) + K_i \int (i_q^* - i_q) \quad (7)$$

where K_p and K_i are the proportional and integral constants of the PI controllers. The term i_d^* is related with real power and i_q^* is related with reactive power. By tracking these two quantities, PI controllers control the correct injection of real and reactive power into the grid (Eqn. 6, 7).

Space Vector Pulse Width Modulation (SVPWM) Block: The SVPWM block, which generates appropriate *pulse width modulated* signals, controls the MOSFET switches and generates appropriate 3-phase inverter output voltages u_a, u_b, and u_c. The SVPWM block uses two reference signals u_d^* and u_q^*, which are generated by putting Eqn. 6, 7 into Eqn. 4, 5:

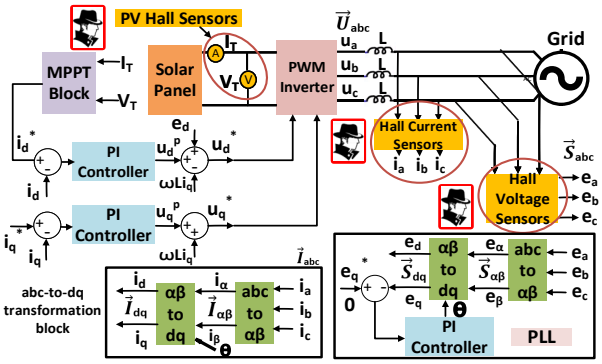

Figure 5: Typical controllers inside of a 3-phase inverter.

$$u_d^* = e_d + u_d^p - \omega L i_q \quad (8)$$

$$u_q^* = u_q^p + \omega L i_d \quad (9)$$

Note that, the reference voltages u_d^* and u_q^* depend on reference currents i_d^* and i_q^*, dq components of grid currents i_d and i_q, angular frequency ω, and filter inductance L.

Phase Locked Loop (PLL) Block: PLL synchronizes the inverter output frequency with the grid frequency by implementing the following equation [51]:

$$\begin{bmatrix} e_d \\ e_q \end{bmatrix} = \begin{bmatrix} \cos\theta^* & \sin\theta^* \\ -\sin\theta^* & \cos\theta^* \end{bmatrix} \begin{bmatrix} e_\alpha \\ e_\beta \end{bmatrix} = k \begin{bmatrix} \cos(\theta - \theta^*) \\ \sin(\theta - \theta^*) \end{bmatrix} \quad (10)$$

where k is a constant, θ and θ^* are the instantaneous phase angles (i.e., frequency) of the grid and inverter output voltage, respectively. The PI controller of the PLL tries to equal e_q with e_q^*. Therefore, if the reference value e_q^* is set to 0 (generated internally), e_q in Eqn. 10 will be also close to 0. This causes $\sin(\theta - \theta^*) = 0$ (i.e., $\theta = \theta^*$) in Eqn. 10. This results in grid-synchronization, because the inverter output voltage $\vec{U}_{abc}$ has the same phase (i.e., $\theta = \theta^*$) as the grid voltage $\vec{S}_{abc}$.

Single Phase Grid Controllers: A single-phase grid-tied inverter has similar blocks as the three-phase, except it does not have Clarke matrix transformation, but it uses *Phase Shifters*. As it has a similar controller, an adversary can similarly affect it using the same attack methodology.

6 Experimental Setup

6.1 A Scaled-Down Testbed of a Power Grid

To avoid safety concerns related to high voltage and high power experiments, we have created a scaled-down version of a real grid in our lab (Fig. 6) to validate our attack model. A 140 W grid-tied inverter kit (part# = TMDSOLARUINVKIT) from Texas Instruments Inc. is used. This is a scaled-down version of a practical solar inverter. This inverter has a Piccolo-B control card (C2000 microcontroller) that implements all the controller blocks (e.g., PLL, Park & Clarke transformations, PI controllers, MPPT, SVPWM, etc.). The supported software kit is downloaded from *ControlSUITE*,

then compiled using *Code Composer Studio 9.1.0* IDE, and then flashed into the solar inverter kit. The Solar panel is emulated by a DC Power source (Part# = PSB 2400L2). An isolated and stable grid is created using another inverter (Part# = BESTEK) with a 300 W load. The 140 W target solar inverter is connected with this stable grid to emulate a weak grid. Oscilloscopes (Part# = Tektronix TDS2022C) with differential probes (Part# = Yokogawa 700924 Probe 1400V / 100 MHz) and multimeters are used to measure the inverter output voltage, current, and power before and after the attack. In order to assist the understanding for readers, attack demonstration and results are shown in a video in the following link: https://sites.google.com/view/usenix-spoofing/home

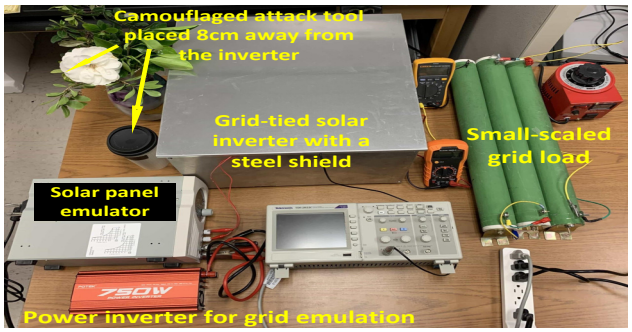

Figure 6: A scaled-down testbed of a power grid.

6.2 Feasibility Analysis of the Attack

The feasibility of this attack methodology depends upon the following three key factors: (i) The location of the Hall sensors, (ii) The barrier and EM shielding around the inverter, and (iii) The amount of MMF required to overcome the barrier and influence the Hall sensors.

As Hall sensors measure the voltage/current, they normally are placed nearby where the solar panel and the grid voltage cables enter the inverter board. Therefore, the *PV Connection side* and the *Grid Connection side* are two suitable locations to place the camouflaged attack tool near the inverter (Fig. 7). The Hall sensors are within 4 cm from the board edge for our experimental inverter. This information regarding the location of the Hall sensors is essential to optimal placement of the attack tool and thus maximizing the attack's impact.

The generated MMF by the electromagnet should be strong enough to overcome the following two barriers: (i) The air gap between the body of the inverter and the electromagnet, and (ii) The metallic shield around the inverter.

Most of the generated MMF is used to overcome the air gap barrier because air has a very high magnetic reluctance. The more the air gap (the distance between the inverter and the electromagnet) is, the more MMF is required to overcome the distance. After penetrating the air, the remaining MMF is used to penetrate the shield around the solar inverter. If the shield is non-magnetic (e.g., aluminum, tin, brass, stainless steel, etc.) or non-metallic (e.g., plastic, polycarbonate, etc.), the remaining MMF can easily penetrate the shield. If the shield is made of ferromagnets (e.g., steel, etc.), the remaining MMF should be strong enough to saturate the ferromagnetic shield, so that its magnetic shielding property gets diminished [52]. For example, 0.6 Tesla magnetic flux density is sufficient to saturate steel shield [53].

Is it possible to generate that much MMF by our *Embedded Hall Spoofing Controller*? We discuss some comparative numbers here to answer this question. It is possible to make a 0.1 Tesla to 2 Tesla powerful lab magnet with 500-9000 turns on an iron core [54]. A coin-sized neodymium magnet has 0.5-1.25 Tesla [55] and a typical loudspeaker magnet has 1-2.4 Tesla [56] magnetic strength. Our experimental electromagnet has approx. ∼4000 turns that can generate up to 0.8 Tesla with the mentioned battery pack. This is sufficient to spoof the Hall sensors of an inverter from at most 10 cm distance. Here we consider a steel shield around the inverter. By investing more money (>$50) on the magnetic core (e.g., neodymium–iron–boron ($Nd_2Fe_{14}B$) rare earth magnet [55]), we can shrink the size of the electromagnet and make it stronger to spoof from 10+ cm distance.

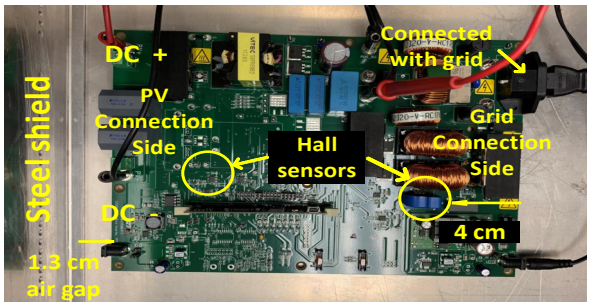

Figure 7: Typical locations of Hall sensors inside an inverter.

7 Attack Model Validation

In this section we validate our proposed attack model, which is explained in Section 4, in our lab testbed for 5 different scenarios. We also explain how the attack propagates from the sensor to the inverter controller by using suitable equations.

It is clear from Section 5.3 that grid voltage $\vec{S}_{abc}$ can control the inverter output voltage $\vec{U}_{abc}$ (Eqn. 8, 9) and phase angle θ (Eqn. 10); inverter output voltage $\vec{U}_{abc}$ and real power P depend on output current $\vec{I}_{abc}$ (Eqn. 8, 9), solar panel voltage V_T, and current C_T; and inverter reactive power Q depends on output current $\vec{I}_{abc}$ and reference i_q^*. The above dependency information is important from the attacker's perspective and can be formulated mathematically as follows:

$$\begin{aligned} \theta &= f(\vec{S}_{abc});\ \ \vec{U}_{abc} = f(\vec{S}_{abc}, \vec{I}_{abc}, V_T, I_T) \\ P &= f(\vec{I}_{abc}, V_T, I_T);\ \ Q = f(\vec{I}_{abc}, i_q^*) \end{aligned} \tag{11}$$

where $f(.)$ is the function notation.

7.1 Attacking Grid Synchronization

Two conditions must be satisfied to synchronize the inverter with the grid [33]: (i) inverter output voltage $\vec{U}_{abc}$ must be slightly higher than the grid voltage $\vec{S}_{abc}$, and (ii) inverter voltage phase θ must be same as the grid voltage phase.

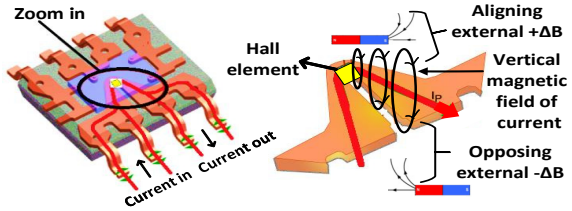

Figure 8: Aligning and opposing spoofing into Hall sensors.

Scenario 1: Let us assume the attacker spoofs only the grid voltage ($\vec{S}_{abc}$) sensors with a constant ±MMF (aligning and opposing polarity). Therefore, the attacker considers injecting magnetic field $\pm\Delta B$ into the Hall grid voltage sensors. The term $+\Delta B$ means that the applied +MMF aligns vertically in the same *direction* of the Hall sensor measurement axis, and $-\Delta B$ means that the applied -MMF aligns vertically in the *opposite* direction of the Hall sensor measurement axis (Fig. 8). An injection of $\pm\Delta B$ results in a ***false*** Hall voltage V^f_{Hall}; therefore Eqn. 1 may be expressed as follows:

$$V^f_{Hall} = k\{\frac{I_{bias}}{d} \times (B \pm \Delta B)\} \tag{12}$$

V^f_{Hall} causes injection of false voltages, which include $\pm\Delta E_a, \pm\Delta E_b$, and $\pm\Delta E_c$ (± for ±MMF), into grid voltage vector $\vec{S}_{abc}$. Therefore, Eqn. 2 is changed as follows:

$$\vec{S}^{false}_{abc}(t) = \begin{bmatrix} e_a \pm \Delta E_a \\ e_b \pm \Delta E_b \\ e_c \pm \Delta E_c \end{bmatrix} \tag{13}$$

where $\pm\Delta E_a, \pm\Delta E_b$, and $\pm\Delta E_c$ may be different from each other. The low-pass filter of the DSP unit cannot filter out these false voltages. So, $\vec{S}^{false}_{abc}$ propagates to the following *abc-to-dq* transformation block. This affects Eqn. 3 as follows:

$$\vec{S}^{false}_{dq} = \begin{bmatrix} e_d \\ e_q \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{3}{2}}E \\ 0 \end{bmatrix} \pm PM \times \begin{bmatrix} \Delta e_\alpha \\ \Delta e_\beta \end{bmatrix} \tag{14}$$

where $PM \times \begin{bmatrix} \Delta e_\alpha \\ \Delta e_\beta \end{bmatrix}$ is a time-varying quantity. Terms Δe_α and Δe_β are the errors propagating from the Clarke matrix transformation block. Therefore, $\vec{S}^{false}_{dq}$ is no longer stable, and as a result, e_d and e_q change with time (i.e., $e_q \neq 0$). This influences the *Right-Hand Side* (R.H.S) of Eqn. 8 and 9. As a result, reference voltages u^*_d and u^*_q are perturbed. This will force SVPWM to create a false inverter output voltage vector $\vec{U}^{false}_{abc}$. It is possible to generate a larger or smaller $\vec{U}^{false}_{abc}$ than allowed. A larger $\vec{U}^{false}_{abc}$ than the grid voltage $\vec{S}_{abc}$ can cause high transient current to be pushed into the grid. If $\vec{U}^{false}_{abc}$ is smaller than $\vec{S}_{abc}$, the inverter acts as a load and current flows into the inverter from the grid. Both cases can shut down the inverter or may damage the inverter by frying the electronics.

Scenario 2: Let us assume the attacker spoofs only the grid current ($\vec{I}_{abc}$) sensors with a constant ±MMF. An injection of ±MMF results in a ***false*** Hall voltage V^f_{Hall}, which causes an injection of $\pm\Delta I_a, \pm\Delta I_b, \pm\Delta I_c$ measurement errors into $\vec{I}_{abc}$. This causes a false output current $\vec{I}^{false}_{abc}$. The low-pass filter of the DSP unit cannot filter out this false signal. This propagates to the following *abc-to-dq* transformation block and creates a false current $\vec{I}^{false}_{dq}$. This affects Eqn. 6 and 7 as follows:

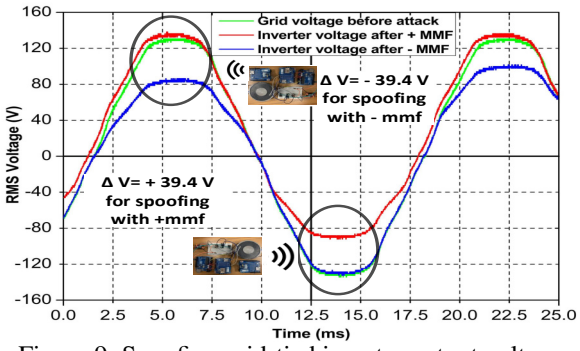

Figure 9: Spoofing grid-tied inverter output voltage.

$$u^f_d = K_p(i^*_d - i^{false}_d) + K_i \int (i^*_d - i^{false}_d) \tag{15}$$

$$u^f_q = K_p(i^*_q - i^{false}_q) + K_i \int (i^*_q - i^{false}_q) \tag{16}$$

Generated false voltages u^f_d and u^f_q influence the R.H.S of Eqn. 8 and 9. As a result, reference voltages u^*_d and u^*_q are perturbed. This will force SVPWM to create false inverter output voltage vector $\vec{U}^{false}_{abc}$. Similar to the consequences in Scenario 1, this may shut down the inverter.

The attack Scenario 2 is demonstrated in our testbed by spoofing a grid current sensor using 0.8 Tesla from a 7.8 cm distance (Fig. 9). The attacker causes an increase in the inverter output voltage from -125 V to -85.6 V (ΔV = + 31.52%) by +MMF spoofing and causes a decrease from +125 V to +85.6 V (ΔV = - 31.52%) by -MMF spoofing. This creates a sudden mismatch between the inverter output voltage and the grid voltage. This mismatch forces the inverter to shut down.

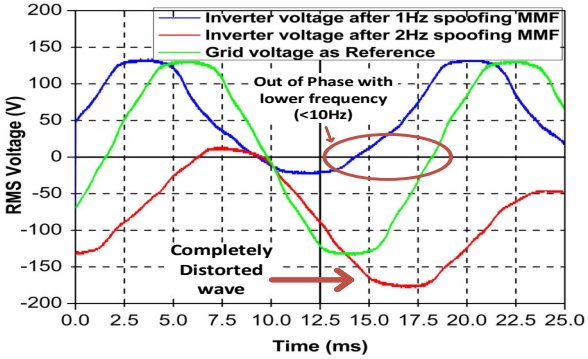

Figure 10: Spoofing grid-tied inverter output frequency.

Scenario 3: Let us assume the attacker spoofs only the grid voltage ($\vec{S}_{abc}$) sensors with a sinusoidal MMF (*note that the last two scenarios are for constant MMF*). An injection of a sinusoidal MMF results in a ***false*** Hall voltage $V^f_{Hall}(t)$, which causes an injection of $\Delta E_a(t)$, $\Delta E_b(t)$, $\Delta E_c(t)$ measurement errors into $\vec{S}_{abc}$. Therefore, Eqn. 2 is changed as follows:

$$\vec{S}^{false}_{abc}(t) = \begin{bmatrix} e_a + \Delta E_a(t) \\ e_b + \Delta E_b(t) \\ e_c + \Delta E_c(t \end{bmatrix} = \begin{bmatrix} E^f_{1a}\cos(\omega t + \theta^f_a) \\ E^f_{2a}\cos(\omega t + \theta^f_b) \\ E^f_{3a}\cos(\omega t + \theta^f_c) \end{bmatrix} \tag{17}$$

where E^f_{1a}, E^f_{2a}, E^f_{3a} and θ^f_a, θ^f_b, θ^f_c are false amplitudes and phase angles, respectively. Thus $\vec{S}^{false}_{abc}$ has different phase angles and amplitudes than $\vec{S}_{abc}$. The low-pass filter of the DSP unit cannot filter out this injected low frequency (< 2Hz) error, and the error propagates to the following PLL block of the controller. Hence, the R.H.S of the Eqn. 10 is given by:

$$\begin{bmatrix} e_d \\ e_q \end{bmatrix} = \begin{bmatrix} \cos\theta^* & \sin\theta^* \\ -\sin\theta^* & \cos\theta^* \end{bmatrix} \begin{bmatrix} e^f_\alpha \\ e^f_\beta \end{bmatrix} = k \begin{bmatrix} \cos(\theta^f - \theta^*) \\ \sin(\theta^f - \theta^*) \end{bmatrix} \quad (18)$$

where e^f_α and e^f_β are propagated errors that cause false phase angle θ^f of the grid voltage. The PLL of the inverter tries to lock with the attacker provided phase angle θ^f (i.e., $\theta^* = \theta^f$). This causes a frequency mismatch between the grid and the inverter voltage. This frequency mismatch causes frequency oscillations and may cause grid failures in weak grids.

The attack Scenario 3 is demonstrated in our testbed and the outcome is shown in Fig. 10. The attacker injects 0.8 Tesla magnetic pulse (1Hz) from a 7.8 cm distance into the grid voltage sensors. This causes the inverter output frequency to go out of phase. The output voltage shape is completely distorted when the attack tool is placed within 1 cm of the inverter (extreme scenario). Fig. 11 shows the *Fast Fourier Transform (FFT)* analysis of the inverter output voltage. The frequency spectrum reveals the strong presence of low-frequency components (<10Hz) and indicates that low frequency (1Hz) power is 3.16x (-6dB to -11dB) more than the fundamental frequency (60Hz) power during the attack. This distorted output wave shuts down the inverter, and blackout occurs in the testbed.

7.2 False Real/Reactive Power Injection

The attacker can attack $\vec{I}_{abc}$, V_T, or I_T sensor depending upon his resources to perturb the real power or reactive power injection (Eqn. 11). Note that, three current sensors are placed in the AC section of the inverter to measure $\vec{I}_{abc}$, and one voltage sensor and one current sensor are placed in the DC section of the inverter (*note that we name these as solar panel sensors*) to measure the solar voltage V_T or the current I_T.

Scenario 4: Let us assume the attacker wants to perform a real power injection attack; therefore, the attacker considers attacking either V_T or I_T sensor by spoofing with a constant

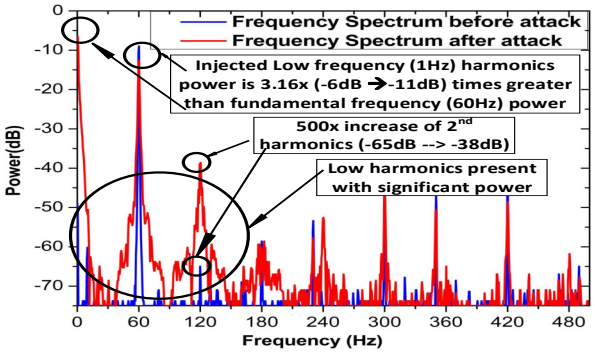

Figure 11: The frequency spectrum of the inverter output voltage before and after the attack Scenario 3.

MMF (a.k.a. exerting external ΔB). This may create a false Hall voltage V^f_{Hall}. The false V^f_{Hall} causes a false solar panel voltage V^f_T or a current I^f_T as follows:

$$V^f_T = V_T + \Delta V_T \text{ and } I^f_T \quad = I_T + \Delta I_T \quad (19)$$

where ΔV_T or ΔI_T are due to the attacker's false MMF injection into the sensor. This false signal V^f_T or I^f_T is fed into the MPPT algorithm. Several algorithms [57], such as Perturb and Observe, Incremental Conductance, Parasitic Capacitance, and Constant Voltage are used as MPPT algorithms and none of these can filter out the injected error $\Delta V_T/\Delta I_T$. As a consequence, the MPPT block generates a false reference current i^{*f}_d. The PI current controller (Section 5) tracks (Eqn. 6) the false i^{*f}_d and generates false u^f_d as follows:

$$u^f_d = K_p(i^{*f}_d - i_d) + K_i \int (i^{*f}_d - i_d) \quad (20)$$

u^f_d can change the input reference voltage of the SVPWM (Eqn. 8, 9) causing more or less injection of real power than required into the grid. This phenomenon may alter the demand response of the grid and can be critical in a weak grid. The results of this scenario are discussed in detail in Section 7.3.

Scenario 5: Let us assume the attacker wants to perform a reactive power injection attack; therefore, the attacker considers attacking the $\vec{I}_{abc}$ sensors (Eqn. 11). The attacker can use pulsating square ($\sqcap$) MMF (as a square wave generation is easier than the sine wave generation) to spoof the $\vec{I}_{abc}$ sensors. It creates pulsating perturbation $\Delta I_\sqcap(t)$ with frequency $\omega_\sqcap$, which may be expressed as: $\Delta I_\sqcap(t) = sgn(\sin(\omega_\sqcap t))$, where *sgn* is the signum function. The pulsating error $\Delta I_\sqcap(t)$ may cause pulsating voltage $V^{f\sqcap}_{Hall}(t)$ (Eqn. 12). This false $V^{f\sqcap}_{Hall}(t)$ results in an injection of pulsating $\Delta I_{a\sqcap}(t)$, $\Delta I_{b\sqcap}(t)$, $\Delta I_{c\sqcap}(t)$ measurement errors into $\vec{I}_{abc}$ as follows:

$$\vec{I}^{false}_{abc}(t) = \begin{bmatrix} I\cos\omega t + sgn(\sin(\omega_\sqcap t)) \\ I\cos(\omega t - 120^0) + sgn(\sin(\omega_\sqcap t)) \\ I\cos(\omega t + 120^0) + sgn(\sin(\omega_\sqcap t)) \end{bmatrix} \quad (21)$$

The pulsating false current $\vec{I}^{false}_{abc}(t)$ creates a pulsating q-axis current $i^\sqcap_q$ after the *abc-to-dq* transformation (Section 5). PI current controller cannot properly track the i^*_q due to the pulsating nature of $i^\sqcap_q$. As a result, a pulsating error voltage is produced (Eqn. 7) that causes a pulsating push of reactive power into the grid. This may cause fluctuation in the grid voltage. And for a weak grid scenario, this fluctuation for a long time may be detrimental for the grid health. As our setup does not have reactive power injection capability, we have shown the impacts of this scenario via simulation using a commercially used software Etap (Section 8.2).

7.3 Attack-Impact with Spoofing-Distance

Fig. 12 shows the impact of the attack scenarios for different spoofing-distances for 0.8 Tesla magnetic field. Here, spoofing-distance means the distance between the electromagnet and the sensor. Note that attack scenarios 1, 2, 3 are created by spoofing the grid voltage/current sensors, and scenario 4

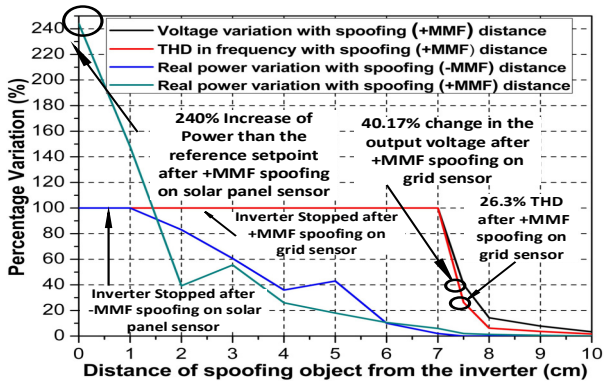

Figure 12: Attack effects with different spoofing-distance.

is created by spoofing the solar panel voltage/current sensors. For scenarios 2 and 3, 40.17% output voltage variation and 26.3% Total Harmonic Distortion (THD) in output frequency are noted, respectively, for 7.5 cm of spoofing-distance. *The THD value refers to the magnitude of harmonics (i.e., due to injected errors) present in the frequency.* The inverter is shut down if the spoofing-distance is less than 7 cm for scenarios 2 and 3. This is shown as a flat line (100% variation) in Fig. 12. For attack scenario 4, real power injection increases from 45 W to 155 W (240% increase) for +MMF spoofing, and the inverter is shut down for -MMF spoofing for 1cm spoofing-distance. The attack impact prevails up to 10 cm for scenarios 2, 3 and up to 8 cm for scenario 4 in our experimental setup. Note that MMF follows the inverse square law with distance ($MMF \propto 1/distance^2$). However, inverter power, voltage, and frequency may not change by following the inverse square law. The reason for this is that the relevant controllers are non-linear and they may add higher order poles and zeros. Fig. 12 supports this claim. It shows that real power, voltage, and frequency change in inverse of higher order (greater than inverse square) with distance. Moreover, voltage and frequency vary significantly compared to power. This indicates that voltage and frequency are more sensitive than power to distance.

7.4 Controlling Inverter Voltage and Power

The generated MMF from the electromagnet depends upon power, and this power is supplied by the battery pack. The attacker can remotely send adversarial commands (i.e., duty-cycle) using the Zigbee to control the input power to the electromagnet (i.e., *spoofing-power*). The *Embedded Hall Spoofing Controller* can vary the *spoofing-power* according to the received adversarial command. This results in varying MMF exerted to the inverter. As our attack model is noninvasive, the direct feedback from the compromised Hall sensor to the *Embedded Hall spoofing Controller* is absent. Rather, the ultrasonic sensor provides specific information about the distance between the inverter and the attack tool. This information acts as a weak feedback to control the *spoofing-power* and this can be utilized to control the inverter voltage and power from a specific distance.

Duty-Cycle Variation: The *spoofing*-power can be controlled from a specific distance by using a PWM technique. PWM is used to vary the duty-cycle (i.e., active/on-time) of the relevant MOSFET. Fig. 13 shows that by varying the duty-cycle of a signal of 100Hz from 0% to 100%, the attacker can change the power input to the electromagnet from 0 W to 50 W and can control the output voltage and the real power of the inverter (Eqn. 12, 15, 16, and 20 give more insights). This experiment is conducted by placing the electromagnet 5 cm away from the sensors. When the magnetic field is applied to grid sensors, the output voltage of the inverter changes in sub-linear fashion from 0% to 34%, up to 32 W of input power to the electromagnet. The inverter stops working after this point, and this is shown as a flat line (100% variation). When the magnetic field is applied to solar panel sensors, the real power output of the inverter changes in sub-linear fashion from 0% to 38%, up to 50 W of input power to the electromagnet. The battery pack can provide this amount of power as this power is required only for a few seconds. Fig. 13 shows that the 35 W power applied to grid sensors may turn off the inverter, but the same power applied to solar panel sensors may not do the same. This indicates that the inverter is more sensitive to its grid voltage variation than its real power variation.

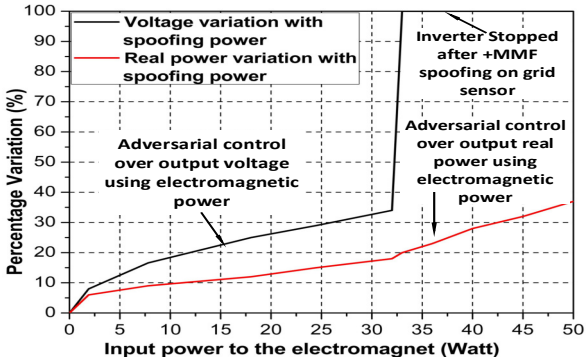

Figure 13: Attack effects with different spoofing-power.

8 Attack Evaluation in a Practical Grid

In Section 7, different attack scenarios are demonstrated using a 140 W inverter in our testbed. However, in this section, an industry used software, the *Electrical Power System Analysis & Operation Software Etap 19.0.1,* is used to show the impacts and the consequences of the previously explained attack scenarios in the context of a large grid.

The IEEE 13 bus test grid is used to model a medium-sized isolated grid with 2.3 MW and 1.536 MVar distributed loads (typical size of a substation/micro-grid representing approx. $\sim$ 150 houses) to demonstrate the attack consequences (Fig. 14). The test grid has five distributed generators and a lumped solar inverter. The generators and the inverter have ranges of 1000 MW, 500 kW, and 100 kW generation rating. Let us assume that the attacker has chosen the comparatively small 100 kW inverter (Gen 5) to show how attacking a small generation could eventually collapse the entire grid. It is important to note that a single inverter can bring down the entire network if the grid is weak, the inverter size is large compared to other

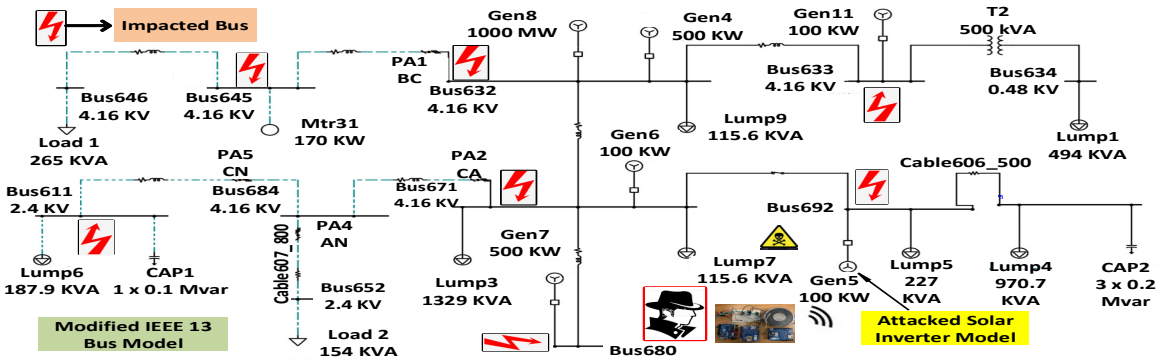

Figure 14: IEEE 13 bus model simulation in Etap to demonstrate the attack impacts in a large system.

generators, or the grid does not have the inertia to compensate for the sudden load change. Usually, residential inverters (0.1 kW-10 kW) are too small to bring down the entire network. Rather, in this section, we address the impact of compromising a larger inverter (e.g., 100 kW) in detail.

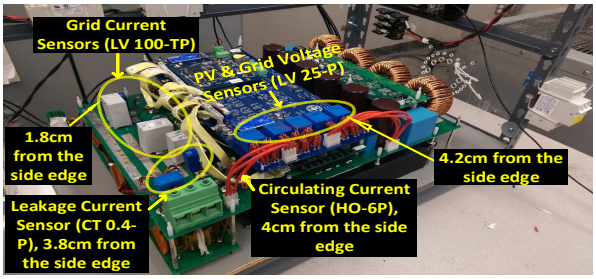

Figure 15: Feasibility analysis of using a 100 kW inverter.

Feasibility Analysis of using a 100 kW Inverter: Large inverters (e.g., 100 kW) normally exist as the central inverter in solar/industrial plants or shopping malls. To the best of our knowledge [58, 59, 60], the inverters have abc-to-dq transformation blocks, PI controllers, PLLs, MPPT, SVPWM in common, irrespective of their sizes (see Section 5.3). These high power central inverters are normally connected with high voltage DC (> 600V) and AC (∼480V) lines, and overall good efficiency (>98%) is a critical requirement of these inverters. To increase efficiency, they are designed as an iron-core transformerless system. However, this way of design increases the injection of DC voltage/current and circulating current into the grid. These injections of unwanted signals can cause overloading in the distribution transformer. Therefore, tight control is necessary to overcome these shortcomings, and accurate measurement is the key to obtaining this control. Thus, designers commonly use Hall sensors because of their lower measurement error, better linearity, higher efficiency, and better galvanic isolation. Hall sensors are used to find DC current injection and measure ground leakage current and circulating current in the inverter's power stage [58] [61]. Fig. 15 is a teardown of a 100 kW inverter, which is obtained by contacting the designers of the relevant inverter [58]. *This figure clearly shows the presence of Hall voltage and current sensors inside of it and gives a strong insight of using a 100 kW inverter in our simulation.* The PV and grid voltage sensors are LV 25-P, and the leakage current sensors are CT 0.4-P, the circulating current sensors are HO-6P, and the grid current sensors are LA 100-TP. These sensors are present within 4.2 cm from the edge, therefore, these sensors are within the attack range. The enclosures of these inverters are made of steel, aluminum, or non-metallic poly-carbonate. Metallic enclosures often get hot due to sunlight, and it is detrimental for the inverter. Therefore, manufacturers prefer non-metallic poly-carbonate [62] as an enclosure, which is heat-resistant but more fragile to our attack model. *As we can't access a high voltage inverter for safety reasons, our experiments use the miniature inverter having core functionalities similar to an industry-standard inverter. It is clear from Table 1 and the above discussion that highly efficient small, medium, and large grid-tied inverters have Hall sensors. This gives a strong intuition behind the generalization of our attack model.*

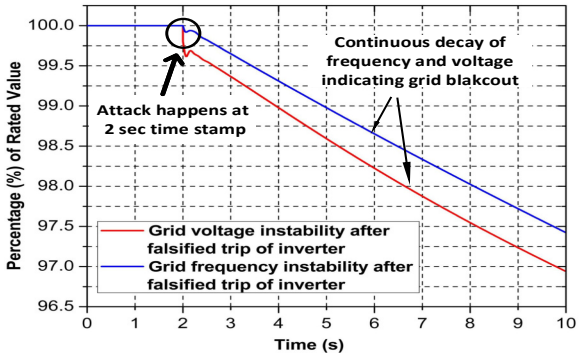

Figure 16: Grid voltage and frequency instability in IEEE 13 bus model after the grid synchronization attack.

8.1 Grid Synchronization Attack Evaluation

Inverters are typically connected with the power grid using protective relays at the point-of-interface (POI). These protective relays have under/over frequency, rate of change of frequency , under/over voltage detection schemes. If the frequency/voltage changes fast or goes beyond the threshold set by the standard (e.g., IEEE 1547, IEEE 2030), the relays trip out the corresponding inverters/loads from the POI.

The attacker can perturb output voltage, phase, and frequency of the 100 kW (Gen 5) target inverter by using our attack model (Scenario 1, 2, 3 of Section 7). This can lead to any of the following consequences: the inverter can be damaged, it can be shut down, or connected protective relays can

trip it out from the connected grid. Any of these consequences can result in a sudden loss of 100 kW power from the grid.

Explanation of Cascading Grid Collapse [63]: The grid power generation should be equal to the sum of power consumption and loss. This balance needs to be maintained for a stable grid health. As the 100 kW inverter stops working without *prior notice, anticipation, or preparation*, it will shift its 100 kW load to nearby generators. Those nearby generators will be overloaded and will shift their loads onto other generators in a cascading manner in a very short time, eventually causing grid collapse. This effect can be extreme during peak hours when the generators are already running at maximum capacity and may be unable to compensate for this 100 kW sudden mismatch between generation and demand. Moreover, when the 100 kW inverter stops working, the adjacent generator's *governor set point* is also changed to push kinetic energy into the grid to catch up with this power disparity. When generators adjust their governors, power system frequency falls and blackout is required in the affected part to preserve the power system. *Due to the grid weakening, this frequency fluctuation is an important issue, and the attacker can leverage this vulnerability by using our attack model.*

This is demonstrated in Fig. 16 by simulating in Etap 19.0.1. The simulation is run for a 10-second window. The attacker attacks the inverter at $t = 2$ second. After this point, the grid voltage and frequency start continuously decaying and fall to 97% of the rated values within 8 sec. IEEE 1547 standard [64] indicates that the grid will shut down as the grid frequency is out of this range: 59.3 Hz $<$ frequency $<$ 60.5 Hz. This may result in a blackout in the region.

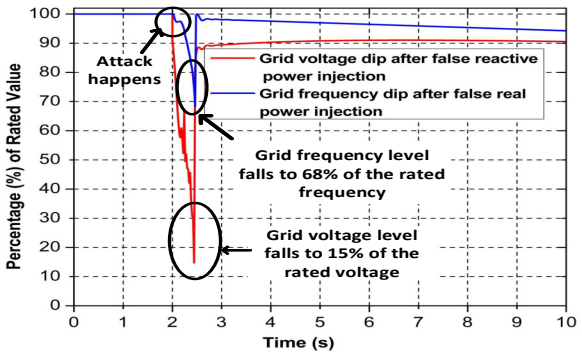

Figure 17: Impact of false real and reactive power injection.

8.2 Real and Reactive Power Injection Attack

Section 7.4 explains that the attacker can force the inverter to inject more or less real/reactive power into the grid by duty-cycle variation. Let us consider a scenario where the grid is balanced (i.e., generation = consumption) and the 100 kW inverter (Gen 5) is running in under-rated condition (i.e., sending less power into the grid than the rated maximum amount). Suddenly, the inverter (Gen 5) is compromised and pushes excess real/reactive power into the grid because of +MMF spoofing. This sudden push of power (i.e., adversarial control) forces the other nearby generators to regulate their own *governor* set-points to absorb the excess power. As frequency and voltage depend on the set-points of the governors, the sudden swing of the governors can cause temporary grid voltage and frequency dip. This scenario is shown in Fig. 17. The adversary attacks the inverter at $t = 2$ second by injecting real/reactive power. This injection causes frequency to fall to 68% and voltage to fall to 15% of the rated value. The attacker can also force the inverter to push less power than the inverter set-point by -MMF spoofing (Section 7). If the attacker keeps injecting more/less power into the grid in a periodic fashion (Scenario 5), the nearby generators will continuously change their *governor set-points* and this may create oscillations in grid voltage and frequency. This can cause transient instability and may result in a blackout in the region because of the reasons already described in Section 8.1.

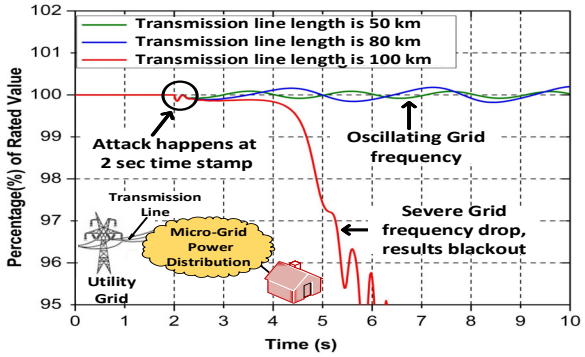

Figure 18: Frequency instability in a weak micro-grid.

8.3 Attacking Utility Connected Micro-Grid

Section 8.1 and Section 8.2 show the impacts of our attack on an isolated grid. Let us consider a scenario where this isolated grid is connected with the utility grid forming a medium-sized micro-grid. Normally, a utility grid having rotational generators is considered as a strong grid, and any grid (i.e., the micro-grid) connected with this strong grid is also considered as strong. A small amount of power and frequency fluctuation in the micro-grid can be absorbed by the connected strong utility grid. However, a micro-grid becomes weaker as its distance from the utility grid increases. A long transmission line acts as a large impedance between the micro-grid and the utility grid. Voltage/frequency fluctuation in the micro-grid cannot ride through to the utility grid because of this large impedance. As a result, disparities in the micro-grid may not be absorbed by the connected strong utility grid. In large countries like the U.S.A. or China, this far away micro-grid can be easily found (e.g., Borrego Springs, 90 miles east of San-Diego [65]; 6.8 GW Gansu province wind farm project, 1000 miles from the industrial east coast in China [66]; Blue Lake Rancheria, 300 miles north of San Francisco [67], etc.).

Etap 19.0.1 simulation in Fig. 18 shows that if the transmission line length between the utility and the micro-grid increases, the micro-grid becomes weaker. Scenario 1, 2, 3, 4 can cause the grid frequency to drop in our IEEE 13 Bus model if the transmission line length is *more* than 100 km

(i.e., micro-grid is 100 km away from the utility grid). If the distance is less, the micro-grid remains strong and a negligible frequency fluctuation can be present after the attack.

9 Defense and Limitations

9.1 Defense

The defense against this type of unconventional attack should consider the following four practices together:

Sensing Presence of External Magnetic Field: The first practice is to put a magnetic flux sensor as a guard near the Hall voltage/current sensor device to measure the presence of an external magnetic field. This idea is similar to the presence of a temperature sensor near a MOSFET to shut it down at a higher temperature. Most high power devices use this method to protect a MOSFET from over temperature. Sensing of a high external magnetic field by the guard magnetic sensor can be used to relay the information to the operator about the possible attack situation. It is noteworthy that this guard sensor has a very low chance of getting influenced by the external magnetic field generated by a nearby current-carrying conductor as this magnetic field is very low. For example, a 500 A current-carrying conductor in the power system can generate only 1 mT at 10 cm distance [68], and the attacker's external magnetic field is much greater (> 0.8 T) than this. Therefore, the additional magnetic sensor can safely separate the attacker's high spoofing magnetic field from the magnetic field usually present in the power grid.

Secured Surrounding Environment: The second practice is to prevent any visitor or unauthorized personnel from going near the grid-tied solar inverter. Any unauthorized object found near the inverter should be considered as a security breach. Furthermore, any authorized electronic device, which has magnetic capabilities placed near the inverter, should be carefully examined. However, this countermeasure *alone* may fail in a few scenarios that involve large countries where solar plants are usually found in an isolated place with less security. Staggs et al. [42] demonstrated how easily this countermeasure can be defeated and an attacker can access a wind plant in the middle of a remote field.

Shielding: Shields redirect the magnetic fields from sensitive devices. Presence of multiple lamination layers in the shield can increase the robustness against the strong magnetic field. High saturation magnetic flux density material (HB), non-magnetic material (NM) and amorphous alloy material (AM) can be used as lamination layers of the shield [69]. Aluminum and poly-carbonates are not good for shielding and should never be used. The thickness of the shields also matters. *We have increased the thickness of the shield from 2mm to 4 mm and the impact of the attack is reduced by approx. 40%.* The thickness of the shield can also increase the weight making it more inconvenient. Alloys, such as CO-NETIC-AA, NETIC S3-6, and MuMETAL, can be used as shields [70] but they are costlier. However, we must remember that having only a good shield is not enough, as any shield can be compromised with a stronger magnetic field.

Robust Sensors: Differential Hall effect sensors can be used because they are robust to external common-mode magnetic interference. The differential Hall effect sensor has two Hall elements, which are closely placed together to cancel out common-mode noises [71]. Sensor-shielding can be added to the Hall sensor to make it insensitive to a small external magnetic field ($< \sim 30$mT) [72]. Moreover, a field concentrator can be added to a Hall sensor to make it robust to an external magnetic field. However, a field concentrator causes magnetic hysteresis, which introduces an additional source of error in the measurement [72].

9.2 Limitations

In this paper, the introduced adversarial control does not offer fine-grained control compared to [24, 25]. The reason for this is that the direct feedback from the compromised Hall sensor to the attacker is absent. However, the attack is strong enough to perturb the connected power grid. Our adversarial attack offers limited control over the inverter voltage within a limited range (Section 7.4) and exceeding this range can result in a DoS attack as the inverter is very sensitive to output voltage variation. Moreover, close access near the inverter, short-attacking range, finding the weak grid scenario, and the prior knowledge on the timing of the attack (i.e., peak hours) are also the limitations. Furthermore, the attacker can not inject high frequency (>2Hz) pulsating MMF, because the inductive property of the electromagnet filters it out.

10 Conclusion

We have proposed and presented a noninvasive attack using the magnetic field on the grid-tied solar inverter. The presence of the Hall sensors in the inverters leaves them vulnerable to be spoofed from the outside. We have illustrated the integrity and availability risks of an inverter by proper mathematical modeling of the basic blocks of the inverter controller. This shows how the false data injection into a Hall sensor can compromise the inverter controller. We have identified five attack scenarios by which the attacker can compromise the inverter and also the connected grid. Moreover, we have introduced a duty-cycle variation approach for adversarial control that can alter the inverter voltage and real power noninvasively. We have tested the attack scenarios in our scaled-down testbed of the power grid and demonstrated our proof of concept. We discuss the feasibility of using a 100 kW inverter and this gives insights behind the generalization of our attack model. We have used industry-standard software Etap 19.0.1 to show the consequences of our attack in a large power grid. This attack can lead to a grid blackout in a weak grid. Our work is an example of a noninvasive attack that originates in the physical domain following some physical laws, compromises the cyber domain, and again finally impacts the physical domain. This can cause financial loss to the power companies. Hence,

this attack is novel in power CPSs and it can draw attention to the security community for further research.

Acknowledgments

The authors would like to thank the anonymous reviewers, our shepherd Prof. Xiali Hei and colleagues Nathan, Kelvin, Anthony, Arnav and Luke for their valuable comments that greatly helped to improve this paper. This paper is based upon work partially supported by the University of California, Office of the President under Grant No. LFR-18-548175 and the Broadcom Fellowship.

References

[1] Alvaro Cardenas, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, Shankar Sastry, et al. Challenges for securing cyber physical systems. In *Workshop on future directions in cyber-physical systems security*, volume 5. Citeseer, 2009.

[2] Suhail Qadir and SMK Quadri. Information availability: An insight into the most important attribute of information security. *Journal of Information Security*, 7(03): 185, 2016.

[3] Guangyu Wu et al. A survey on the security of cyber-physical systems. *Control Theory and Technology*, 14 (1):2–10, 2016.

[4] Ang Chee Kiong Gary and Utomo Nugroho Prananto. Cyber security in the energy world. In *2017 Asian Conference on Energy, Power and Transportation Electrification (ACEPT)*, pages 1–5. IEEE, 2017.

[5] Blake Sobczak. Experts assess damage after first cyberattack on U.S. grid, May 6, 2019. https://www.eenews.net/stories/1060281821. (Accessed: 05-14-2020).

[6] Kevin Poulsen. Slammer worm crashed Ohio nuke plant net. *The Register*, 20, 2003.

[7] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5(6):29, 2011.

[8] Kim Zetter. Inside the cunning, unprecedented hack of ukraine's power grid. *Wired*, 2016.

[9] Johannes Reichl, Michael Schmidthaler, and Friedrich Schneider. The value of supply security: The costs of power outages to Austrian households, firms and the public sector. *Energy Economics*, 36:256–261, 2013.

[10] Michaela D Platzer. US solar photovoltaic manufacturing: Industry trends, global competition, federal support. Library of Congress, Congressional Research Service, 2012.

[11] Phillip Brown. European Union wind and solar electricity policies: overview and considerations, 2013.

[12] Søren Lund Lorenzen, Alex Buus Nielsen, and Lorand Bede. Control of a grid connected converter during weak grid conditions. In *2016 IEEE 7th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, pages 1–6. IEEE, 2016.

[13] Robert H Lasseter and Paolo Piagi. Microgrid: A conceptual solution. In *IEEE Power Electronics Specialists Conference*, volume 6, pages 4285–4291. Citeseer, 2004.

[14] Mark Yampolskiy, Peter Horvath, Xenofon D Koutsoukos, Yuan Xue, and Janos Sztipanovits. Taxonomy for description of cross-domain attacks on CPS. In *Proceedings of the 2nd ACM international conference on High confidence networked systems*, pages 135–142. ACM, 2013.

[15] Denis Foo Kune, John Backes, Shane S Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. Ghost talk: Mitigating EMI signal injection attacks against analog sensors. In *2013 IEEE Symposium on Security and Privacy*, pages 145–159. IEEE, 2013.

[16] Youngseok Park, Yunmok Son, Hocheol Shin, Dohyun Kim, and Yongdae Kim. This ain't your dose: Sensor spoofing attack on medical infusion pump. In *10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16)*, 2016.

[17] Drew Davidson, Hao Wu, Rob Jellinek, Vikas Singh, and Thomas Ristenpart. Controlling UAVs with sensor input spoofing attacks. In *10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16)*, 2016.

[18] Chen Yan, Wenyuan Xu, and Jianhao Liu. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *DEF CON*, 24(8):109, 2016.

[19] Hocheol Shin, Dohyun Kim, Yujin Kwon, and Yongdae Kim. Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications. In *International Conference on Cryptographic Hardware and Embedded Systems*, pages 445–467. Springer, 2017.

[20] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 103–117, 2017.

[21] Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. Non-invasive spoofing attacks for anti-lock

braking systems. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 55–72. Springer, 2013.

[22] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. Rocking drones with intentional sound noise on gyroscopic sensors. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pages 881–896, 2015.

[23] Zhengbo Wang et al. Sonic gun to smart devices: Your devices lose control under ultrasound/sound. *BlackHat USA*, 2017.

[24] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 3–18. IEEE, 2017.

[25] Yazhou Tu, Zhiqiang Lin, Insup Lee, and Xiali Hei. Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pages 1545–1562, 2018.

[26] Oliver Kosut, Liyan Jia, Robert J Thomas, and Lang Tong. Malicious data attacks on the smart grid. *IEEE Transactions on Smart Grid*, 2(4):645–658, 2011.

[27] Elias Bou-Harb, Claude Fachkha, Makan Pourzandi, Mourad Debbabi, and Chadi Assi. Communication security for smart grid distribution networks. *IEEE Communications Magazine*, 51(1):42–49, 2013.

[28] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2011.

[29] Arman Sargolzaei, Kang K Yen, and Mohamed N Abdelghani. Preventing time-delay switch attack on load frequency control in distributed power systems. *IEEE Transactions on Smart Grid*, 7(2):1176–1185, 2015.

[30] Amir-Hamed Mohsenian-Rad and Alberto Leon-Garcia. Distributed internet-based load altering attacks against smart power grids. *IEEE Transactions on Smart Grid*, 2 (4):667–674, 2011.

[31] Ilge Akkaya, Edward A Lee, and Patricia Derler. Model-based evaluation of GPS spoofing attacks on power grid sensors. In *2013 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, pages 1–6. IEEE, 2013.

[32] Eduard Muljadi, CP Butterfield, Brian Parsons, and Abraham Ellis. Effect of variable speed wind turbine generator on stability of a weak grid. *IEEE Transactions on Energy Conversion*, 22(1):29–36, 2007.

[33] Stephen J Chapman et al. *Electric machinery and power system fundamentals*. 2002.

[34] Harold Kirkham. Current measurement methods for the smart grid. In *2009 IEEE Power & Energy Society General Meeting*, pages 1–7. IEEE, 2009.

[35] Grid-tied Solar Micro Inverter with MPPT Schematic (Rev. A). page 4, . http://www.ti.com/lit/df/tidr767a/tidr767a.pdf. (Accessed: 05-12-2020).

[36] 10kW 3-Level 3-Phase Grid Tie Inverter Reference Design for Solar String Inverts (Rev. A). page 1, . http://www.ti.com/lit/pdf/tidue53. (Accessed: 05-12-2020).

[37] AN4070: 250 W grid connected microinverter. page 6. https://www.st.com/content/ccc/resource/technical/document/application_note/fa/f1/fe/3d/81/1e/47/45/DM00050692.pdf/files/DM00050692.pdf/jcr:content/translations/en.DM00050692.pdf. (Accessed: 05-12-2020).

[38] AN1444: Grid-Connected Solar Microinverter Reference Design. page 15. http://ww1.microchip.com/downloads/en/appnotes/01444a.pdf. (Accessed: 05-12-2020).

[39] Steve Taranovich. Teardown: The power inverter – from sunlight to power grid. https://www.edn.com/teardown-the-power-inverter-from-sunlight-to-power-grid/. (Accessed: 05-12-2020).

[40] Solar Inverter. https://solarpv4u.co.nz/solar-inverters. (Accessed: 05-12-2020).

[41] Jonathan Stidham. Can hackers turn your lights off: The vulnerability of the US power grid to electronic attack. *SANS Institute InfoSec Reading Room*, 2001.

[42] Jason Staggs. Breaking wind: Adventures in hacking wind farm control networks. *Black Hat*, 2017.

[43] J.R. Appelbaum, L. Poitras, M. Rosenbach, C. Stöcker, J. Schindler, and H. Stark. Inside TAO : documents reveal top NSA hacking unit. *Der Spiegel*, 12 2013. ISSN 0038-7452.

[44] Lonneke Van der Velden. Leaky apps and data shots: Technologies of leakage and insertion in NSA-surveillance. *Surveillance & Society*, 13(2):182–196, 2015.

[45] Bill Snyder. Snowden: The NSA planted backdoors in cisco products. *InfoWorld*, 15, 2014.

[46] Sujit Rokka Chhetri et al. Tool of spies: Leaking your ip by altering the 3d printer compiler. *IEEE Transactions on Dependable and Secure Computing*, 2019.

[47] Pawel Swierczynski, Marc Fyrbiak, Philipp Koppe, Amir Moradi, and Christof Paar. Interdiction in practice—Hardware Trojan against a high-security USB flash drive. *Journal of Cryptographic Engineering*, 7(3): 199–211, 2017.

[48] Benjamin Sprecher, Rene Kleijn, and Gert Jan Kramer. Recycling potential of neodymium: the case of computer hard disk drives. *Environmental science & technology*, 48(16):9506–9513, 2014.

[49] J David Irwin. *Control in power electronics: selected problems*. Elsevier, 2002.

[50] Junjian Qi et al. Cybersecurity for distributed energy resources and smart inverters. *IET Cyber-Physical Systems: Theory & Applications*, 1(1):28–39, 2016.

[51] Vikram Kaura and Vladimir Blasko. Operation of a phase locked loop system under distorted utility conditions. *IEEE Transactions on Industry applications*, 33 (1):58–63, 1997.

[52] Laurent Chiesi, Karim Haroud, John A Flanagan, and Rade S Popovic. Chopping of a weak magnetic field by a saturable magnetic shield. *Sensors and Actuators A: Physical*, 60(1-3):5–9, 1997.

[53] Charles Steinmetz. *Theory and Calculation of Electric Circuits*. The McGraw-Hill Companies, 1.00 edition, 1917. https://books.google.com/books?id=z0IOAAAAYAAJ&pg=PA84#v=onepage&q&f=false. (Accessed: 05-11-2020).

[54] INDUCTORS AND TRANSFORMERS. https://www.ece.k-state.edu/people/faculty/gjohnson/files/tcchap4.pdf. (Accessed: 05-11-2020).

[55] The Tesla Radio Conspiracy. http://teslaradioconspiracy.blogspot.com/. (Accessed: 05-11-2020).

[56] Loudspeaker Power Handling Vs. Efficiency. https://sound-au.com/articles/pwr-vs-eff.htm. (Accessed: 05-11-2020).

[57] DP Hohm and M E_ Ropp. Comparative study of maximum power point tracking algorithms. *Progress in photovoltaics: Research and Applications*, 11(1):47–62, 2003.

[58] Yanjun Shi, Lu Wang, Ren Xie, and Hui Li. Design and implementation of a 100 kW SiC filter-less PV inverter with 5 kW/kg power density and 99.2% CEC efficiency. In *2018 IEEE Applied Power Electronics Conference and Exposition (APEC)*, pages 393–398. IEEE, 2018.

[59] Frede Blaabjerg, Remus Teodorescu, Marco Liserre, and Adrian V Timbus. Overview of control and grid synchronization for distributed power generation systems. *IEEE Transactions on industrial electronics*, 53(5):1398–1409, 2006.

[60] Mihai Ciobotaru, Remus Teodorescu, and Frede Blaabjerg. Control of single-stage single-phase PV inverter. *EPE Journal*, 16(3):20–26, 2006.

[61] Yanjun Shi, Lu Wang, Ren Xie, Yuxiang Shi, and Hui Li. A 60-kW 3-kW/kg five-level T-type SiC PV inverter with 99.2% peak efficiency. *IEEE Transactions on Industrial Electronics*, 64(11):9144–9154, 2017.

[62] Enclosures for the Solar Industry. https://fiboxusa.com/enclosures-for-solar-power/. (Accessed: 05-11-2020).

[63] William Edwards and Scott Manson. Using protective relays for microgrid controls. In *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*, pages 1–7. IEEE, 2018.

[64] Distributed Generation Photovoltaics and Energy Storage. IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces. *IEEE Std*, pages 1547–2018, 2018.

[65] James Glanz and Brad Plumer. In a High-Tech State, Blackouts Are a Low-Tech Way to Prevent Fires. https://www.nytimes.com/2019/10/12/business/power-blackouts-california-microgrids.html (Accessed: 05-11-2020).

[66] Amjad Ali, Wuhua Li, Rashid Hussain, Xiangning He, Barry W Williams, and Abdul Hameed Memon. Overview of current microgrid policies, incentives and barriers in the European Union, United States and China. *Sustainability*, 9(7):1146, 2017.

[67] Schatz Energy Research Center. Blue Lake Rancheria microgrid. http://schatzcenter.org/blrmicrogrid/. (Accessed: 05-11-2020).

[68] Magnetic Field of Current. http://hyperphysics.phy-astr.gsu.edu/hbase/magnetic/magcur.html. (Accessed: 05-11-2020).

[69] Takashi Sato, Toshio Yamada, and Masami Kobayashi. Magnetic shielding material, September 3 1991. US Patent 5,045,637.

[70] Warren R Osborn and Bryan P Dunford. Protective container for readable cards, January 16 2007. US Patent 7,163,152.

[71] https://www.allegromicro.com/~/media/Files/Datasheets/ACS724-Datasheet.ashx. (Accessed: 05-14-2020).

[72] Managing External Magnetic Field Interference When Using ACS71x Current Sensor ICs. https://www.allegromicro.com/en/Insights-and-Innovations/Technical-Documents/Hall-Effect-Sensor-IC-Publications/Managing-External-Magnetic-Field-Interference-ACS71x-Current-Sensor-ICs.aspx. (Accessed: 05-11-2020.

[73] Yong Yang, Yi Ruan, Huan-qing Shen, Yan-yan Tang, and Ying Yang. Grid-connected inverter for wind power generation system. *Journal of Shanghai University (English Edition)*, 13(1):51–56, 2009.

11 Appendix

11.1 Grid Synchronization

Grid-tied solar inverters need to synchronize itself with the power grid to work in unison. Therefore, The inverter output frequency should be equal to the connected grid frequency (e.g., 60 Hz). Moreover, the inverter voltage should have the same phase angle and slightly higher magnitude than the grid voltage to push power into the grid. There are a few methods for the grid synchronization. The most common synchronization method is *Phase-Locked-Loop* (PLL). Any wrong synchronization of frequency, voltage, and phase angle may bring the grid down. Moreover, the damage could get worse for large inverters like the central one, because these inverters have a higher influence on the connected power grid.

11.2 Real Power and Reactive Power

The concept of real and reactive power is important in a power grid. Real power is the energy required to rotate a motor, illuminate a house, heat a room, etc. The real power generation should be equal to the power demand. If the power generation surpasses the demand, it will increase the grid frequency that may damage the connected loads. If the power generation is less than the demand, this scenario will reduce the grid frequency and may cause blackout. Therefore, the frequency variation is critical for the grid health and this should be within the acceptable limit (e.g., IEEE 1547 standard: $59.3\,Hz < frequency < 60.5\,Hz$) for stable grid operation.

On the other hand, reactive power is used to regulate grid voltage. It is used to control the voltage level and this is essential for the active power to do real work. If the reactive power generation is less than the demand, the voltage level will drop and if the generation is higher, the voltage level will rise compared to the nominal value. This variation should be within 1% of the nominal voltage for healthy grid operation. Nowadays, the *distributed energy resources* (DERs) like solar/wind inverters can push real and reactive power into the grid and facility's energy management system control this amount depending upon the actual demand.

11.3 Generators in a Strong and a Weak Grid

A strong grid consists of rotational generators because the rotational generators provide inertia that can compensate for any sudden change of loads in the power system. The rotational generator has a governor-control mechanism that controls the prime-mover of the generator during load variation. In a strong grid, the majority of the power comes from the centralized rotational generators. On the other hand, in a weak grid, the majority of the power may not come from the centralized rotational generators, but comes from many distributed energy sources, such as solar/wind turbines, battery energy storage. Due to the continuous integration of distributed energy sources, the modern grid is experiencing poor control and lack of inertia causing grid weakening over time.

11.4 Presence of Hall Sensors in Inverters

Fig. 19 is a teardown [39] of *Sunny Boy* series inverter from SMA Solar Technology. This figure indicates the presence of Hall sensors. Fig. 20 is a block diagram [36] of a three-phase grid-tied inverter from Texas Instruments Inc. This figure also clearly indicates the presence of Hall sensors. **Both inverters also require >800 V DC source and that is why they are not safe to test in the lab set-up.** Page 6 of [37] also indicates the presence of Hall sensors in the inverter made by STMicroelectronics. Page 15 of [38] indicates the presence of Hall sensors in the inverter made by Microchip.

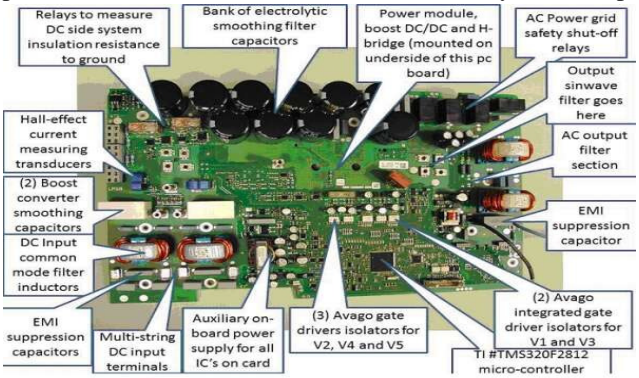

Figure 19: SMA Solar Technology Sunny Boy inverter [39].

11.5 $\vec{S}_{abc}$ to $\vec{S}_{dq}$ Transformation

The *Clarke Matrix* (CM) and the *Park Matrix* (PM) are expressed as follows [73]:

$$Clarke\ Matrix,\ CM = \sqrt{\frac{2}{3}} \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} \end{bmatrix} \tag{22}$$

$$Park\ Matrix,\ PM = \begin{bmatrix} \cos\omega t & \sin\omega t \\ -\sin\omega t & \cos\omega t \end{bmatrix} \tag{23}$$

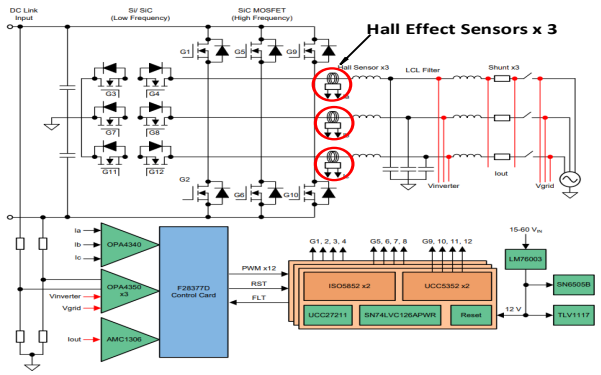

Figure 20: 10 kW grid-tied inverter reference design [36].

From Eqn. 2, 22 and 23, vector $\vec{S}_{abc}$ to $\vec{S}_{\alpha\beta}$ transformation and vector $\vec{S}_{\alpha\beta}$ to $\vec{S}_{dq}$ transformation can be written as follows:

$$\vec{S}_{\alpha\beta}(t) = \begin{bmatrix} e_\alpha \\ e_\beta \end{bmatrix} = CM \times \vec{S}_{abc} = \begin{bmatrix} \sqrt{\frac{3}{2}} E \cos \omega t \\ \sqrt{\frac{3}{2}} E \sin \omega t \end{bmatrix} \tag{24}$$

$$\vec{S}_{dq} = \begin{bmatrix} e_d \\ e_q \end{bmatrix} = PM \times \vec{S}_{\alpha\beta}(t) = \begin{bmatrix} \sqrt{\frac{3}{2}} E \\ 0 \end{bmatrix} \tag{25}$$

Where both e_d and e_q are non varying quantities and $e_q = 0$ for balanced grid voltage. Here, ωt is unknown in Park Matrix, PM (Eqn. 23) and for $\alpha\beta$-*to*-dq transformation (Eqn. 25), ωt is required. This $\theta = \omega t$ is supplied by *Phase Locked Loop* (PLL) (Fig. 5, Eqn. 10).

11.6 Relation Between $\vec{S}_{abc}$ and $\vec{U}_{abc}$

A loop filter is present to smooth the inverter output voltage. If the inverter output voltages $[u_a, u_b, u_c]$ are expressed as a vector $\vec{U}_{abc}$ and ouput currents $[i_a, i_b, i_c]$ as $\vec{I}_{abc}$ and the phase inductance of the three phase loop filter is L (Fig. 5), the relation between $\vec{S}_{abc}$ and $\vec{U}_{abc}$ is (neglecting filter's coil resistance R):

$$\vec{S}_{abc} = \begin{bmatrix} e_a \\ e_b \\ e_c \end{bmatrix} = \begin{bmatrix} u_a \\ u_b \\ u_c \end{bmatrix} - L \begin{bmatrix} \frac{di_a}{dt} \\ \frac{di_b}{dt} \\ \frac{di_c}{dt} \end{bmatrix} = \begin{bmatrix} u_a - L\frac{di_a}{dt} \\ u_b - L\frac{di_b}{dt} \\ u_c - L\frac{di_c}{dt} \end{bmatrix} \tag{26}$$

After placing eqn. 26 into eqn. 24 and from 3, we can obtain the following equation:

$$\vec{S}_{dq} = \begin{bmatrix} e_d \\ e_q \end{bmatrix} = PM \times CM \times \begin{bmatrix} u_a - L\frac{di_a}{dt} \\ u_b - L\frac{di_b}{dt} \\ u_c - L\frac{di_c}{dt} \end{bmatrix} = PM \times \begin{bmatrix} u_\alpha - L\frac{di_\alpha}{dt} \\ u_\beta - L\frac{di_\beta}{dt} \end{bmatrix}$$
$$= \begin{bmatrix} u_d \\ u_q \end{bmatrix} - \begin{bmatrix} L\frac{di_d}{dt} \\ L\frac{di_q}{dt} \end{bmatrix} + \omega L \begin{bmatrix} i_q \\ -i_d \end{bmatrix} \tag{27}$$

Using $e_q = 0$ (from eqn. 3) in eqn. 27, the inverter's output voltage u_d, u_q can be obtained and written by:

$$u_d = e_d + L\frac{di_d}{dt} - \omega L i_q \tag{28}$$

$$u_q = L\frac{di_q}{dt} + \omega L i_d \tag{29}$$

11.7 Attack Scenario 3

After injecting $\Delta E_a(t)$, $\Delta E_b(t)$, $\Delta E_c(t)$ measurement errors into $\vec{S}_{abc}$, Eqn. 2 changes as follows:

$$\vec{S}^{false}_{abc}(t) = \begin{bmatrix} e_a \\ e_b \\ e_c \end{bmatrix} + \begin{bmatrix} \Delta E_a(t) \\ \Delta E_b(t) \\ \Delta E_c(t) \end{bmatrix}$$
$$= \begin{bmatrix} E\cos\omega t \\ E\cos(\omega t - 120^0) \\ E\cos(\omega t + 120^0) \end{bmatrix} + \begin{bmatrix} E^f_a \cos(\omega^f t) \\ E^f_b \cos(\omega^f t) \\ E^f_c \cos(\omega^f t) \end{bmatrix} \tag{30}$$

Where E^f is the magnitude and ω^f is the frequency of the injected error voltage. If we assume that the injected error frequency ω^f is equal to ω, the R.H.S of Eqn. 30 may be simplified as:

$$\vec{S}^{false}_{abc}(t) = \begin{bmatrix} e_a + \Delta E_a(t) \\ e_b + \Delta E_b(t) \\ e_c + \Delta E_c(t \end{bmatrix} = \begin{bmatrix} E^f_{1a}\cos(\omega t + \theta^f_a) \\ E^f_{2a}\cos(\omega t + \theta^f_b) \\ E^f_{3a}\cos(\omega t + \theta^f_c) \end{bmatrix} \tag{31}$$

where E^f_{1a},E^f_{2a},E^f_{3a} and θ^f_a, θ^f_b, θ^f_c are the false magnitudes and phase angles, respectively.

11.8 Attack Scenario 5

Let us assume the attacker uses pulsating square ($\sqcap$) MMF (as square wave generation is easier than the sine wave generation) for spoofing $\vec{I}_{abc}$ sensors. It creates pulsating perturbation $\Delta I_\sqcap(t)$ with frequency $\omega_\sqcap$. This may be expressed as: $\Delta I_\sqcap(t) = sgn(\sin(\omega_\sqcap t))$ where sgn is the signum function. This $\Delta I_\sqcap(t)$ may cause pulsating $V^{f\sqcap}_{Hall}(t)$ (Eqn. 12). This false $V^{f\sqcap}_{Hall}(t)$ results injection of pulsating $\Delta I_{a\sqcap}(t), \Delta I_{b\sqcap}(t), \Delta I_{c\sqcap}(t)$ measurement error into $\vec{I}_{abc}$ as follows:

$$\vec{I}^{false}_{abc}(t) = \begin{bmatrix} I_a \\ I_b \\ I_c \end{bmatrix} + \begin{bmatrix} \Delta I_{a\sqcap}(t) \\ \Delta I_{b\sqcap}(t) \\ \Delta I_{c\sqcap}(t) \end{bmatrix}$$
$$= \begin{bmatrix} I\cos\omega t + sgn(\sin(\omega_\sqcap t)) \\ I\cos(\omega t - 120^0) + sgn(\sin(\omega_\sqcap t)) \\ I\cos(\omega t + 120^0) + sgn(\sin(\omega_\sqcap t)) \end{bmatrix} \tag{32}$$