IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 July 2023, accepted 18 August 2023, date of publication 23 August 2023, date of current version 30 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3308052

APPLIED RESEARCH

Smart PV Inverter Cyberattack Detection Using Hardware-in-the-Loop Test Facility

THUNCHANOK KAEWNUKULTORN[1,2], (Graduate Student Member, IEEE),
SERGIO B. SEPÚLVEDA-MORA[1,3], (Member, IEEE),
ROBERT BROADWATER[4], (Senior Member, IEEE), DAN ZHU[4],
NEKTARIOS G. TSOUTSOS[2], (Member, IEEE),
AND STEVEN HEGEDUS[1,2], (Senior Member, IEEE)
[1]Institute of Energy Conversion, University of Delaware, Newark, DE 19716, USA
[2]Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716, USA
[3]Departamento de Electricidad and Electrónica, Universidad Francisco de Paula Santander, Cúcuta, Norte de Santander 540006, Colombia
[4]Electrical Distribution Design (EDD), Blacksburg, VA 24060, USA

Corresponding author: Thunchanok Kaewnukultorn (thuncha@udel.edu)

This work was supported in part by the U.S. Department of Energy under Award DE-0008768, and in part by the University of Delaware Graduate College through the University Dissertation Fellowship.

ABSTRACT This paper evaluates residential smart photovoltaic (PV) inverters' responses to cyberattacks and assesses the performance of an intrusion detection strategy for smart grid devices by comparing time-series power flow results from a simulation application called Faster Than Real-Time (FTRT) Simulator to measurements from a Power Hardware-in-the-Loop (P-HIL) laboratory as a testbed. Twenty different cyberattacks from three classes - Denial of Service (DoS), Intermittent attack, and Modification - were designed and tested with grid-tied smart inverters in order to study the inverters' responses to malicious activities. The intrusion detection strategy was developed using a comparison between the predicted PV power output from FTRT and the power flows measured from P-HIL laboratory through the API interface. Real and reactive power thresholds were assigned based on a number of repeated experiments to ensure the applicability of the thresholds. The results showed that inverters from different manufacturers have their own unique responses which could be detected by the power flow measurements. Our detection method could identify over 94% of actual malicious actions and 7.4% of no-attack hours are detected as false positives. Out of 38 under-attack hours, 2 undetected hours are due to the intermittent attacks. Different attacks can be detected based on the targeted components of the complex power that attackers are aiming to cause disturbances. Our findings additionally show that DoS can be noticed immediately after the devices have been sabotaged, and they can be detected from the active power analysis. However, modification attack detection will depend more on the reactive power measurements, while intermittent attacks remain the most challenging for the proposed detection method since the objective of intermittent attacks is to create an oscillation of the complex power components which need a relatively high time resolution for the measurement.

INDEX TERMS Smart inverters, cyberattacks, hardware-in-the-loop laboratory, grid supporting function, cyberattack detection.

I. INTRODUCTION

The penetration of renewable energy systems into the centralized electric grid has been increasing during the last decade [1]. Smart inverters and energy storage have been introduced to mitigate the impact of such high penetration of renewable energy, as well as to support grid functionality by improving voltage and frequency stability and serving residential loads during grid failures [2]. Network communications for the smart devices in the power grid

The associate editor coordinating the review of this manuscript and approving it for publication was Zhilei Yao.

offer substantial benefits to users and system operators by enabling real-time monitoring, control, and dispatch remotely. Nevertheless, synchronization control protocols utilized by smart inverters exchange local information with edge devices in the same network, causing them to be vulnerable to infiltration and cyberattacks. In order to support and stabilize the utility grid, modern smart inverters are embedded with modes of grid-supporting operation [3] where the control settings are commanded by a centralized grid controller, rendering these functions vulnerable to cyberattacks as their smart functionalities provide direct access to their internal control settings and external data [4], [5]. Without an awareness of malicious attacks from the control side, the grid system could continuously respond to the false inputs and the adversaries can generate system abnormalities which lead to both technical and economical disadvantages [6].

Security awareness has been raised in the smart grid community and a number of studies have been conducted attempting to analyze the impact of cyberattacks in smart grid systems in order to develop detection models and strategies [7], [8], [9], [10], [11], [12]. The authors of [7] and [13] have shown that preventive strategies are effective mitigation actions against threats on the inverter-based resources (IBRs) which completely avoid experiencing fluctuations in the distribution grid. To harden a target system against cyberattacks, a thorough study of the impact of cyberattacks on smart inverters and the grid is crucial to develop reference data and modeling solutions to potential attacks [9], [14], [15]. In [7] and [8], a simulation platform was developed to evaluate potential impacts of different attack scenarios on DERs and electric grid and mitigation strategies for each scenario were introduced. Olowu et al. investigated the impacts of the false data injection attack (FDIA) on smart inverter function settings such as volt-var and volt-watt [10]. Liu et al. observed intense adverse effects on power system dynamic performance from DoS on load frequency control [11]. Additionally, the reliability of distribution systems under large scale DoS on AMIs was studied in [12].

According to our observations, it is possible to predict the behavior of the inverter and grid during the attacks and create an intrusion detection system (IDS) for the smart grid through a combination of simulation and a Power Hardware-in-the-Loop (P-HIL) test facility. A cyber-physical system in P-HIL configuration has drawn significant interest as a cyberattack detection/mitigation testbed [16], [17], [18], [19]. In power grid security, Kollmer et al. have employed HIL test environment for observing and evaluating DoS cyberattack on a three-bus electrical network microgrid system [20]. In [21], a co-simulation platform with HIL laboratory was proposed for cyberattack analysis based on RT-laboratory and OPNET software to evaluate case studies of DoS. A recent study by Choi et al. utilized a real-time HIL cybersecurity testbed to capture cyber-physical impacts of power electronics under cyberattack events using Simulink and OPAL-RT interface for modeling PV systems and inverters [22]. Additionally, Naderi et al. studied impacts of FDIA on a lab-scale microgrid using hardware-in-the-loop as a testbed where a programmable load, 160 W PV arrays, and lab-scale power controllers were involved [23].

These approaches are similar to the study here, which employs HIL to investigate impacts of malicious attacks on smart inverters. However, instead of power electronic simulations as reported in previous works, the HIL described here utilizes physical inverters embedded in the FTRT simulation, which encompasses from transmission through secondary distribution of a real-power system. The physical inverters were placed on a secondary in the FTRT simulation, where the FTRT simulation provided voltages to the physical inverters and the physical inverters provided power flows back to the FTRT simulation. Unlike previous research efforts, the research here focuses heavily on evaluating the proposed intrusion detection strategy and identifying impacts of different cyber-attacks using actual residential-scale hardware which are deployed in the field. The FTRT approach can accurately model power flow for transmission and distribution systems much faster than previous methods [24], [25]. This has demonstrated the scalability of the detection system for integrating communication and controls for utility-scale grid.

We previously found that different inverters meeting the same IEEE standards can still have very different operating responses and control limitations depending on the manufacturers, leading to different level of vulnerability. Consequently, a validation of inverter responses to cyberattacks is essential and can be useful for the grid utility to understand the inverter behaviors to malicious actions and address possible solutions before the centralized control is applied to the field. In this work, we are evaluating the performance of the cyberthreat detection strategy using an electric distribution network simulator and a P-HIL laboratory as a test facility. 20 cyberattack scenarios were proposed based on their high efficacy to cause severe disturbance to the grid system including collapsing inverter operations, retarding the grid, and causing output oscillations.

The attacks in this work are classified into three categories based on their consequences, namely Denial of Service (DoS), intermittent attack, and modification. An imitative system of the utility grid was simulated using the measurements from the P-HIL laboratory to calculate the expected power flow; cyberattacks were triggered and the actual responses were compared for intrusion detection. A variety of cyberattacks targeting active/reactive power components were successfully simulated and the ability to detect the attacks analyzed. Our work highlights the significance of validating the intrusion detection method, as well as valuable lessons towards the inverters' responses, cyberattack prevention and preparation on the grid control authority side to protect the system from online threats. Our key contributions are summarized as follows.

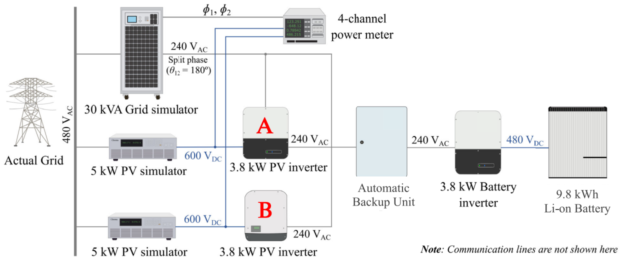
- Design and hardware simulation of 20 possible cyberattacks scenarios for a grid-tied PV system in a P-HIL environment to evaluate cyberattack responses of smart PV inverters from a laboratory setup;
- Assessment of intrusion detection methodologies for the smart grid.

The rest of this article is organized as follows: Section II presents the P-HIL configuration and elaborate description of the methodology for collecting data of 20 proposed cyberattacks. Section III presents our experimental results along with a discussion about the response of the system under attack. Lastly, our concluding remarks are presented in Section IV.

II. METHODOLOGY

A. POWER HARDWARE-IN-THE-LOOP (P-HIL) TESTBED SETUP

A P-HIL setup involves the actual power hardware connected to the simulated network in a closed loop. Our P-HIL test facility has been installed at the Institute of Energy Conversion, located at the University of Delaware, Newark, DE, USA. We have optimized the P-HIL laboratory infrastructure for investigating security attacks that can be launched by malicious actors and cause service disruption as a post-exploitation step. Two inverters from different manufacturers were installed and connected each to a PV simulator to study the inverters' behavior under different settings. The inverter brands are labeled as Inverter A and B to avoid sensitive cyberattack information disclosure. Fig. 1 offers an overview of the P-HIL environment and shows the power connections of P-HIL equipment with the voltage levels. Inverter B represents a residential grid-tied PV system. Inverter A is part of an AC-coupled PV system with battery backup where a regular PV grid-tied inverter and a battery-based inverter are required. The Automatic Backup Unit (ABU) has the role of switching Inverter A subsystem operation between grid-tied and backup mode depending on the grid condition. The additional equipment details of the P-P-HIL laboratory are described in [26]. As our objective is to analyze the impact of cyberattacks on smart PV inverters, we excluded the battery, ABU unit, and the battery inverter from this study.



Note: Communication lines are not shown here

FIGURE 1. P-HIL power connections diagram with nominal AC and maximum DC operating voltages.

B. SMART COMMUNICATION AND CONTROLS

Over the past years, advanced power electronics such as smart inverters, intelligent electronic devices (IEDs) and advanced metering infrastructure (AMI) are integrated into DER systems to support control and communication needed to balance generation and load [27]. At the same time, the inclusion of smart functionalities eventually increases vulnerability of the system to cyberthreats. Two fundamental layers, namely power and communication/control, play a key role in connecting DERs and the electric grid by enabling bidirectional energy and communication flows [10]. In general, the power conversion of DERs is controlled by individual energy management systems (EMS), allowing users to have access to operating controls remotely. Notably, the communications with smart inverters via remote access interfaces can be interfered by a malicious entity, and each such attack can cause abnormality in the power and communication/control layers of the system, which could escalate to equipment damage, voltage-frequency violations, and/or false tripping.

Many smart inverters are capable of providing additional grid supporting functionalities to solve some grid instability issues as defined by IEEE 1547-2020 [28]. Some examples of grid supporting functions are volt-var control, volt-watt control, constant power factor, grid feed-in control, and voltage and frequency ride-through. Volt-var control is the most promising reactive power control mode for grid voltage regulation due to the ability to inject and absorb reactive power in real-time depending on the grid operating voltage [29]. A simulation study which evaluated grid reliability of volt-var and volt-watt modes under data attack was proposed in [10]. By injecting false setpoints to each mode, the results show that the smart inverter settings can yield different impacts to the grid. Consequently, cyberattacks on the inverters under volt-watt mode could lead to serious increases in the overall real power losses of the system, while the attack on the volt-var mode may cause higher voltage instability.

C. CYBERATTACK CLASSIFICATION

From our methodology, three classes of cyberattacks were identified, namely a Denial of service (DoS) attack, an intermittent attack, and an integrity modification attack, which can be applied on the inverters of the P-HIL infrastructure. We remark that each inverter in the P-HIL environment is from a different manufacturer, and we discovered that they respond differently to the attacks. In all cases, a potential attacker was assumed that they have already established Modbus TCP/IP access to the inverters (e.g., by leveraging open-source intelligence [30]) as Modbus communication is applied in most commercially available inverters for remote controls due to its accessibility and cost savings, yet increases vulnerability to malicious attacks by external actors due to its lack of authentication [31], [32]; moreover, for the case of Inverter A, we assumed that the potential attacker is able to enter the grid guard code to unlock the advanced control functions of the inverter. We remark that the various attack types described hereafter are applicable regardless of the current control mode of the inverter.

Denial of service (DoS) is a two-step attack of preventing the inverter from communicating with other clients or devices. The first step is *inverter disconnection attack*, while the second step entails changing grid voltage or frequency operation ranges to obstruct the inverter reconnection attempts when the grid is operating in nominal conditions. A blocking attack can be classified as DoS where the attacker's target is to create a failure of the attempted reconnection, preventing power delivery from the inverter to the load or the grid. In this work, we will combine blocking and DoS as one category. Preventing the inverter from operating in a normal range can have a significant impact on the grid and the system owner because it effectively causes the inverter to shut off [33]. On one hand, if multiple inverters are simultaneously shut down, it will create a significant drop in power generation, and the load/generation unbalance can cause voltage and/or frequency instabilities, leading to a severe power grid failure. On the other hand, the system owner will also be affected because their PV system will not produce power and their revenue will be reduced.

Intermittent attacks consist of repeatedly changing the active or reactive power level of the inverter in short intervals (e.g., 1-5 seconds) from a high to a low value to create an oscillation in the output of the inverter. This oscillation can cause malfunctions in the inverter conversion system, as it forces the inverter to produce the maximum active power output and to suddenly reduce it to a significantly lower level. This attack was designed to avoid showing any alert messages at an inverter's front display. The lowest power level was selected as 5% to prevent the inverter from shutting down due to having zero AC power. The consequence of this attack is a significant instability in real power, causing a grid failure and PV owners losing revenues. In case of intermittent power factor attack, an attacker can change the power factor excitation from under-excitation to over-excitation or vice versa. The inverter will inject a certain level of reactive power and instantaneously absorb the same reactive power level which could lead to a significant oscillation in the grid voltage and the inverter operating system due to excessive ramping.

Modification attacks refer to disturbing the grid stability by modifying the characteristic curves for reactive power control (e.g. volt-var), or real power control (e.g. volt-watt). According to the IEEE 1547-2020 standard, the volt-var curve is implemented to regulate the grid operating voltage by injecting and absorbing the reactive power up to 44% of the rated active power of the inverter. Technical issues and economical losses potentially occur when unwanted reactive power is flowing in the system which leads to under or over voltages. These issues could increase the possibility of circuit equipment failures. For inverters which are set to have reactive power priority based on the IEEE 1547 standard, modification attacks leading to injecting or absorbing excessive reactive power could cause active power curtailment which causes active power revenue losses to the system owner [34].

The ultimate goal of this work is to detect cyberattacks and provide guidance to the electric utilities, installers, and solar customers to have a better preparation for a wide range of possible attacks, thus we present possibility of some attacks which are relatively unique and might require a skillful hacker with a technical knowledge of power electronics to do so. Some attacks we investigate are already recognized in the field (e.g. DoS attacks) while others (e.g. intermittent oscillations) are more speculative but still possible for a dedicated hacker. With the current solar penetration on the grid being so low, so they are not yet a high-value targets for most attackers. However, our proposed cyberattacks will be more likely when the scale of residential solar installations in the field increase and thus become more inviting targets.

D. CYBERATTACK SIMULATIONS

All cyberattacks were simulated using the Modbus protocol and the P-HIL equipment. In this case, we assume that the victim devices have network connectivity and are accessible remotely; indeed, this is a realistic assumption, as thousands of devices with open port 502 (modbus) are currently available online, according to the Shodan search engine [35]. Our analysis reveals that a well-motivated attacker who exploits an existing vulnerability of an existing Modbus interface of the targeted P-HIL devices (e.g. lack of robust firewall controls) might be able to undermine the integrity of grid operations. Prior research has demonstrated that adversaries can use open-source intelligence to reverse engineer critical parts of the grid, while existing search engines for connected devices, such as Shodan, enable anyone to find potential targets with openly accessible Modbus interfaces [27], [32], [36].

In the P-HIL laboratory, the main local computer communicates with all the Chroma devices using Standard Commands for Programmable Instruments (SCPI) commands through the General-Purpose Interface Bus (GPIB) interface to control the parameters such as grid voltage, DC power output, and phase angle. Inverter B and Inverter A are connected to the local University of Delaware computer network that can be accessed through Modbus from the main P-HIL computer with the inverter's IP address. To launch the cyberattacks remotely, malicious control instructions are sent from the main computer to the inverters through Modbus TCP port 502 with different unit IDs for each inverter. Python is implemented for Modbus communication of the inverters, the GPIB and SCPI commands for synchronization of all Chroma equipment.

Our detection method is potentially applied to a feeder with multiple PV inverters in communication with the substation, and where there is a hierarchical control on the feeder that communicates with the PV inverters. We assumed that cyberattacks are performed by the potential attackers accessing the control center and attacking the inverters on the feeder. Our main objectives are analyzing cyberattack responses of smart inverters and evaluating intrusion detection methodologies. We emphasized *lessons learned* from the inverter responses while providing high-level details of the cybersecurity layers to maintain the focus of the paper.

In our evaluation, we were able to demonstrate laboratory experiments designed to test the limits for control settings under simulated cyber security breaches. The 20 cyberattacks are performed under normal and abnormal grid operating conditions which are shown in Table 1. All the cases were tested to verify the consequences of inverter control changes. A number of repeated experiments were performed to assure that the inverter responses can be considered as the abnormal behaviors triggered by malicious control or setpoint modifications. The proposed attack scenarios were designed to be in opposition to the recommendations in IEEE1547-2018 standard and we assumed that any control modifications resulting in responses that are dramatically different from the standard or any other recommendations from electric grid reliability experts will be considered as cyberattack scenarios.

In this work, we studied the impact of modification attacks only on Inverter A due to an unavailability of the grid-supporting functions via Modbus for Inverter B. Additionally, the intermittent attacks were simulated only on the Inverter B, as Inverter A has an inherent hardware limitation on Modbus register changes (namely, it supports up to 1000 times during its lifetime by default to avoid damaging its internal chipset). Our simulation schedule was distributed across multiple days and totaled about 200 simulation hours (from about 8:00 to 17:00 on each day); within this frame, we launched multiple cyberattacks for a total of 38 hours (complemented with 162 hours of normal operation time), and all attacks were triggered within a time window from 11:00 to 15:00 when the simulated daytime PV power was highest. For our analysis, we simulated a P-HIL environment under attack hours for 12 hours of DoS, 7 hours of intermittent attacks, and 19 hours of modification attacks.

E. DATA ACQUISITION

A Faster Than Real-Time (FTRT) simulator is developed on the DEW (Distributed Engineering Workstation) platform [37]. The FTRT uses two forecasts for PV generation and load, a one-minute step size, 30-minute forecast, and a one-hour step size, 24-hour forecast. During each measurement/control interval, either or both of the forecasts may be employed in time-series analysis. Types of time-series analysis that are performed by the FTRT include: power flow; optimal power flow for control calculations; voltage stability analysis; and abnormality detection, which is of primary interest here. Inputs to the FTRT come from three-independent measurement systems: Advanced Metering Infrastructure (AMI), Supervisory Control And Data Acquisition (SCADA), and cloud-based, inverter measurements. The FTRT simulation employs Graph Trace Analysis (GTA). GTA is a matrix-free approach to analysis where system equations (i.e., Kirchhoff's voltage and current laws) are evaluated dynamically as traces are performed [38]. During each measurement/control interval the FTRT abnormality detection compares the historical statistical performance of errors between power flow calculations and field measurements with time-series errors currently being recorded. If errors are persistent and large with respect to the statistical experience, then an abnormality is flagged. In addition to cyber-attacks, the abnormality detection is also valuable in detecting physical attacks, failed instrumentation, and failed controllers.

Fig. 2 shows the communication between the P-HIL laboratory and the Measurement and Model Integrator for Ensuring Grid Security (M2IEGS) system which has FTRT implemented as a part of it. The M2IEGS incorporates real-time voltage stability monitoring, large and small PV generation, and coordination between transmission system needs and primary/secondary distribution system controls. For our experiments, we developed a specialized API that receives a set of grid control parameters from external inquiries and responds to the measurement requests to test the FTRT simulator with the actual P-HIL hardware. Two separate endpoints were implemented to the web interface: The first one is a GET request which retrieves voltage, active and reactive power from each individual inverter. The second endpoint is a POST request that allows external users to change the control (voltage, phase angle, and simulation time) of each inverter.

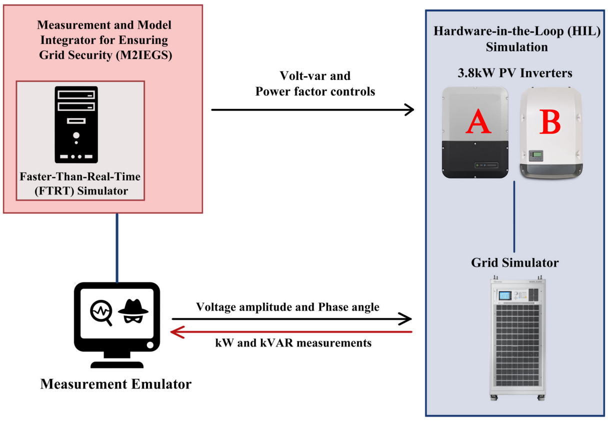

Measurement and Model Integrator for Ensuring Grid Security (M2IEGS)
Faster-Than-Real-Time (FTRT) Simulator
Volt-var and Power factor controls
Hardware-in-the-Loop (HIL) Simulation
3.8kW PV Inverters
A
B
Grid Simulator
Voltage amplitude and Phase angle
kW and kVAR measurements
Measurement Emulator

FIGURE 2. Communication diagram between laboratory setup and software simulator.

Our process of initiating new cyberattack simulations and subsequent data collection can be summarized as follows: an external user sends grid conditions, the local server changes the grid simulator parameters, changes the output power of the PV simulators according to the simulation time, awaits briefly for the inverters to react, and finally responds with the total active and reactive power measured from each inverter in a JSON format. Additionally, the Python language was used to develop a program that can directly change the corresponding Modbus registers for monitoring (GET) and altering

TABLE 1. Description of our proposed cyberattack scenarios.

Classification	Case #	Experimental description	Inverter
DoS/Blocking	1	Inverter voltage operating range is limited at 120.0 V from both lower and upper thresholds to immediately disconnect the inverter from the grid. After the inverter has been disconnected, it will be out of the network until the operating range is reset.	A
	2	Inverter voltage operating range is limited from 120.0 V to 121.0 V to create an extremely narrow voltage threshold for the inverter. After the inverter has been disconnected, it will be out of the grid network until the operating range is reset.	A
	3	Inverter frequency operating range is limited from 59.9 Hz to 60.1 Hz to create an extremely narrow frequency threshold for the inverter. After the inverter has been disconnected, it will be out of the grid network until the operating range is reset.	A
	4	Inverter frequency operating range is limited from 55.0 Hz to 58.0 Hz to immediately disconnect the inverter from the grid. After the inverter has been disconnected, it will be out of the grid network until the operating range is reset.	A
	5	Inverter advanced control access is remotely deactivated to prevent any corrective changes on the grid-supporting controls.	A
	6	Inverter is forced to disconnect from the grid and operate in its standby mode and will not be automatically reconnect to the network until the issue has been solved by the operator.	B
	7	The grid feed-in operating mode of the inverter is interfered to prevent exporting PV power to the grid. Feed-in control is used to set a level of grid export in a normal operation scenario.	A
Intermittent attack	8	Inverter active power output is changed rapidly from 100% – 5% – 100% of the inverter maximum power output in every 5 seconds to create an aggressive oscillation. The duration of this attack is 3 min (18 cycles).	B
	9	Inverter active power output is changed rapidly from 100% – 5% – 100% of the inverter maximum power output every second to create an aggressive oscillation. The duration of this attack is 1 min (60 cycles).	B
	10	Inverter active power output is changed rapidly from 100% – 0% – 100% of the inverter maximum power output every 3 seconds to create an aggressive oscillation. The duration of this attack is 3 min (30 cycles).	B
	11	Inverter power factor is changed rapidly from under-over-under excitation every 3 seconds to create an aggressive oscillation in the inverter reactive power. The duration of this attack is 3 min (30 cycles).	B
Modification	12	Inverter reactive power setpoints in volt-var control mode are modified to its maximum (60% of P_{rated}) injection/absorption values.	A
	13	Inverter volt-var control curve is modified from the IEEE1547 standard to create two infinite slopes at 117.6 V (0.98 p.u.) and 122.4 V (1.02 p.u.) grid operating voltage.	A
	14	Inverter volt-var control curve is modified to eliminate a dead-band to create an infinite slope at 120 V grid operating voltage.	A
	15	Inverter volt-var control curve is modified reversely compared to the from the IEEE1547 standard.	A
	16	Inverter volt-var control curve is modified from the IEEE1547 standard to eliminate a dead-band and replaced with a linear slope from 117.6 V (0.98 p.u.) to 122.4 V (1.02 p.u.) grid operating voltage.	A
	17	Reactive power mode of the inverter is switched from constant PF of 1 to dynamic volt-var control which affects the reactive power at the inverter and the grid.	A
	18	Reactive power mode of the inverter is switched from dynamic volt-var control to constant PF of 1 which affects the ability of voltage control of the inverter and the voltage oscillation at the grid.	A
	19	Inverter volt-var control is interrupted by limiting active power output to zero to prevent the inverter from injecting/absorbing the reactive power.	A
	20	Inverter volt-watt control curve is modified to create an infinite slope at 126 V (1.05 p.u.) grid operating voltage, resulting in a severe oscillation in active power at the desired voltage.	A

(POST) the different parameters of the PV inverters at the P-HIL laboratory. In order to make the process automated and systematic, the cyberattacks are triggered from the API and saved as records in a data log.

F. DATA ANALYSIS

As our detection system is targeting the cyberattacks in distributed energy resources (DERs) that are communicating via a hierarchical utility control, our detection method was developed to detect inverter abnormalities in terms of values of P and Q that were beyond their expected values (the baseline or forecasted value). These lead to interpretation in terms of inverter operating failures, loss of production, and disconnection from the grid. While the inverter voltage, frequency, and current can also be considered for an attack detection, there are still some cyberattack scenarios that do not have an impact on those parameters, leading to a lower accuracy in the detection method. After a number of repeated experiments with a variety of possible attack scenarios, we have concluded that the power components play the critical role in electric network stability and can be detected if unexpected control has been assigned to the inverter in a timely manner. The two thresholds used in the detection method are obtained based on repeatability and applicability of the detection threshold. Different thresholds were also evaluated with the most appropriate one resulting in the highest overall accuracy of the detection system is 50% of the maximum active power and 5% of the maximum available reactive power depending on the inverter capacity.

For our experimental evaluation, we simulated all 20 cyberattacks and developed an intrusion detection method to determine whether the inverter is under attack or not based on the power flow. The flowchart of the proposed detection method is depicted in Fig. 3. Moreover, the three equations shown below are used for the power flow analysis:

$$\Delta\text{Meas}(\text{kW}) = \text{FTRT}(\text{kW}) - \text{HIL}(\text{kW}) \tag{1}$$

$$\Delta\text{Meas}(\text{kVAR}) = \text{FTRT}(\text{kVAR}) - \text{HIL}(\text{kVAR}) \tag{2}$$

$$\Delta\text{Base}(\text{kW}) = \text{PV}_{base}(\text{kW}) - \text{FTRT}(\text{kW}) \tag{3}$$

where FTRT(kW) and FTRT(kVAR) are forecasted active and reactive power from FTRT simulators, and HIL(kW) and HIL(kVAR) are the active and reactive power measured hourly from the inverters. PV_{base}(kW) in (3) refers to the PV output profile from 8:00 - 17:00 used to setup the PV simulators. All parameters in (1) - (3) are determined hourly hence there are 10 values per simulated day.

In Fig. 3, the differences between the expected and measured data are initially calculated for active and reactive power which is shown in (1) and (2), respectively. Our assumption is that remote attackers will exploit network vulnerabilities (e.g., lack of firewall rules) and manipulate the victim devices over modbus. This method would allow the system to discriminate the cyberattacks targeting active power from the ones impacting reactive power. To obtain more realistic simulation results, we ran the hardware simulation in the P-HIL laboratory using only one PV generation profile for all simulation days, while using 20 different PV forecasted profiles to simulate 20 days of the experiment. Therefore, a data distortion from the PV prediction can be observed and will be taken into account during a first data filtering procedure. First, we calculate the differences of the specific power profile assigned to the PV simulator vs. the active power forecasted by the FTRT simulator using (3), and average them to compute the baseline. Then ΔMeas(kW) was calculated and compared to ΔBase(kW). The threshold was assigned based on a number of repeated experiments of cyberattack launches to identify the minimum difference between the expected and actual power flows that should be considered as an abnormality of power flows due to malicious attacks. We found that the appropriate threshold of active power abnormality detection was determined at 50% of the maximum active power to detect malicious activities that impact active power controls. If the condition is fulfilled, it is considered as a detected attack from an active power abnormality, while the data below the threshold will be screened through the second filtering process. Depending on the reactive power discrepancy, if the value of ΔMeas(kVAR) is within the threshold (below 5% of the maximum reactive power), those datapoints will be considered as no-attack hours. If they are higher than this range, they will be labeled as detected attack hours due to reactive power abnormalities.

We used case 10 as an example scenario shown in Fig. 4 to demonstrate our detection strategy. During 10 hours of a simulation day, the intermittent active power attack had been triggered for 2 hours from 13:00 - 15:00. In the first data screening process, the difference between PV profile (blue dots) and the forecasted data (red triangle) will be calculated and compared to the measured data. After calculating ΔMeas(kW), the malicious activity will be detected due to large discrepancy of ΔMeas(kW) as under-attack hours.

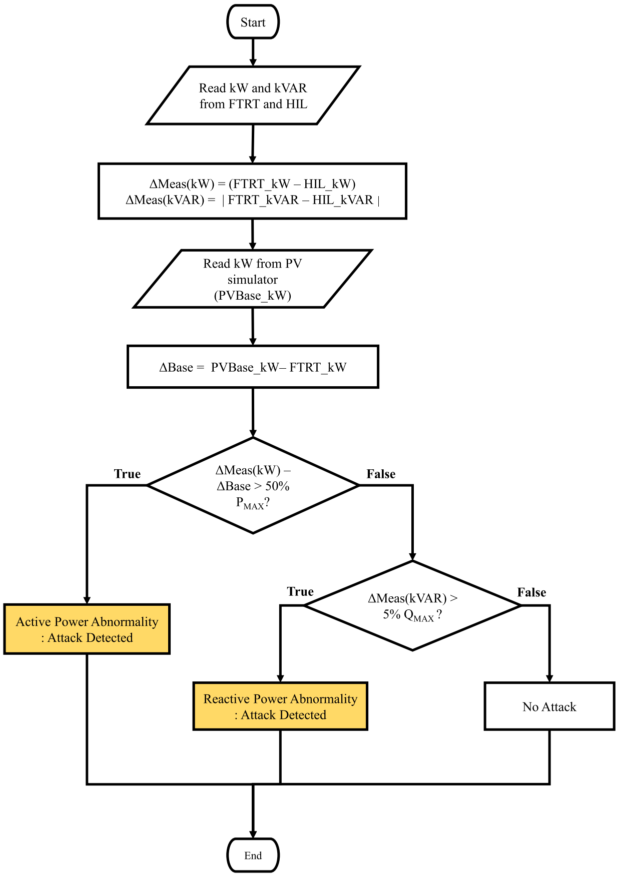

Start
Read kW and kVAR from FTRT and HIL
ΔMeas(kW) = (FTRT_kW – HIL_kW)
ΔMeas(kVAR) = | FTRT_kVAR – HIL_kVAR |
Read kW from PV simulator (PVBase_kW)
ΔBase = PVBase_kW– FTRT_kW
ΔMeas(kW) – ΔBase > 50% P_MAX?
True
False
ΔMeas(kVAR) > 5% Q_MAX ?
True
False
Active Power Abnormality : Attack Detected
Reactive Power Abnormality : Attack Detected
No Attack
End

FIGURE 3. Flowchart of the cyberattacks detection process.

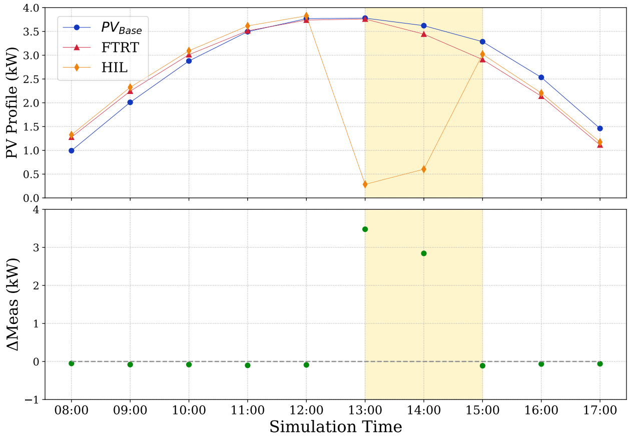


FIGURE 4. An intrusion detection strategy using the PV profile, FTRT forecasted, and HIL data with (1) and (2) to detect under-attack hours.

III. RESULTS AND DISCUSSION

A. DENIAL-OF-SERVICE (DoS)

1) OUT-OF-RANGE VOLTAGE AND/OR FREQUENCY (CASES 1–4)

For case 1, the attack was launched by altering the inverter voltage range to be impossibly limited from 120.0 - 120.0 V.

As expected, after the attack was created, Inverter A immediately went to a fault mode and disconnected itself from the grid as it cannot tolerate a fluctuation in the grid voltage greater than 0.1 V. Additionally, as the grid voltage was usually fluctuating more than 1 V, we observed the same result for case 2. The frequency range attacks in cases 3 and 4 delivered the same results where the inverter immediately disconnected from the grid and could not reconnect itself back unless those ranges were changed back to the normal range. Thus, all of these attacks were detectable since the output went to zero.

2) BLOCKED CORRECTIVE COMMANDS FROM AN AUTHORITY (CASE 5)

Instead of attacking the inverter control modes, case 5 attacked the permission of controls to prevent recovering the system after any attacks have been launched. This attack could be the second step of a coordinated cyberattack where the goal is to freeze the abnormal settings that an attacker creates, resulting in system abnormality which will be intensified with a longer attack period. The result from the P-HIL simulation indicates that the attack did delay and block any further corrective controls being sent to the inverter and the previous attack was still running, which can potentially cause technical and economic problems to the PV system owner. This attack cannot be cleared via Modbus due to the unavailability of a specific register to reverse this attack.

3) FORCED GRID DISCONNECTION BY A LIMITED ACTIVE POWER (CASES 6–7)

Cases 6 and 7 are similar in terms of blocking the inverter from transferring the produced power to the grid. For case 6, the malicious disconnection was performed by forcing the inverter to operate under the standby mode. Every attempt of the attack was successful, and the result showed that Inverter B took approximately 3 minutes to reconnect and recover itself to full power. If the attack occurs multiple times during the high PV output period, customers could lose their revenue as they are unable to export the PV power to the grid. This attack could also create an under-grid-voltage issue when the PV penetration is expected to be high. Additionally, if a large number of inverters were turned off simultaneously this could introduce significant transient power issues. Similarly, the forced grid disconnection attack on Inverter A was simulated using the function called "*feed-in management*", which showed similar results to a standby mode on Inverter B. This type of attack is detectable and neither Inverter B nor Inverter A was able to dispatch the PV power to the electric grid during the attacks.

B. INTERMITTENT ATTACKS

1) ACTIVE POWER OSCILLATIONS (CASES 8–10)

We simulated the active power oscillation by changing the active power limitation from 100% maximum power (P_{MAX}) down to a very low level, then back up to 100% again to observe the behavior of Inverter B under attack. As expected, the oscillation in the active power was detected at the inverter. Fig. 5 and 6 show Inverter B reaction to the intermittent active power attack with different time intervals. Overall, both different power levels and duration of each cycle can have an impact on the inverter response patterns which would be more predictable when the interval is larger since the inverter has longer time to adjust the power levels and to reach the desired power setpoint. However, the results summarized in Table 2 indicate that forcing the inverter repeatedly to output zero active power significantly affects the inverter capability to ramp up the power output to its maximum, and the effect from lowering the power level is more critical than narrowing the time intervals.

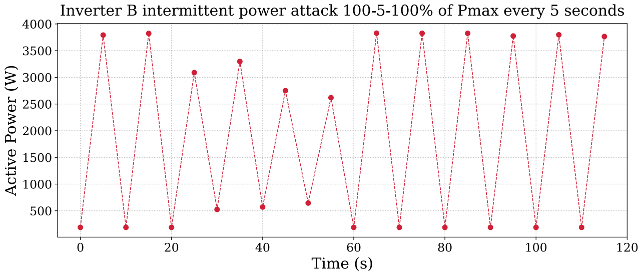


FIGURE 5. Intermittent active power attack from 100-5-100 % of the inverter maximum AC power every 5 seconds on Inverter B.

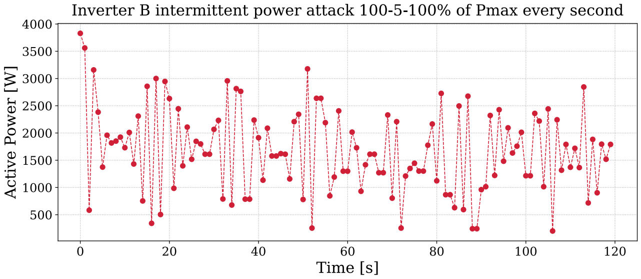


FIGURE 6. Intermittent active power attack from 100-5-100 % of the inverter maximum AC power every second on Inverter B.

TABLE 2. Intermittent active power attacks results.

Case #	High Power (%)	Low Power (%)	Time Interval (s)	Average Output Power (W)	Power Loss (%)
8	100	5	5	1,904	49.9
9	100	5	1	1,860	55.8
10	100	0	3	1,451	61.8

2) REACTIVE POWER OSCILLATION (CASE 11)

Another intermittent attack was evaluated on Inverter A, and the goal is to create an oscillation of reactive power by changing the excitation of the power factor, while keeping a power factor of 0.98 during the simulation. The result showed that Inverter B responded to the changes of PF excitation continuously, and it was able to inject and absorb reactive power at least 50% of the maximum reactive power for every cycle. This attack is expected to have a serious impact on the electric grid since transient reactive power could result in exacerbating the grid voltage instability issue. The ability to detect this type of attack depends on the sampling rate being faster than the oscillation.

C. MODIFICATION ATTACKS

1) VOLT-VAR CHARACTERISTIC MODIFICATIONS (CASES 12–16)

Cases 12 - 16 were tested under the same concept of disturbing the grid stability by modifying the volt-var characteristics from IEEE 1547-2020 to have different shapes. Fig. 7 shows the result of case 14 where the volt-var curve was modified to eliminate a deadband and replace it with an infinite slope at 120 V of the grid voltage. At the attacked point of the volt-var curve, instead of creating a large oscillation at 120 V, Inverter A follows only one commanded setpoint to avoid the oscillation during the attack. As a result, the reactive power is absorbed by the inverter at 45% (∼1739 VAR) of the inverter nominal power (3800 W), which is the maximum absorbed reactive power that was set for this experiment. This is considered a significant threat for the grid voltage stability, and becomes worse when multiple inverters are under attack. The result of cyberattack case 13 is relatively similar to the case 14 in terms of the inverter's response. However, it is detectable when the grid voltage is out of the deadband zone which is different from case 14 where the attack is detectable immediately during normal grid operation.

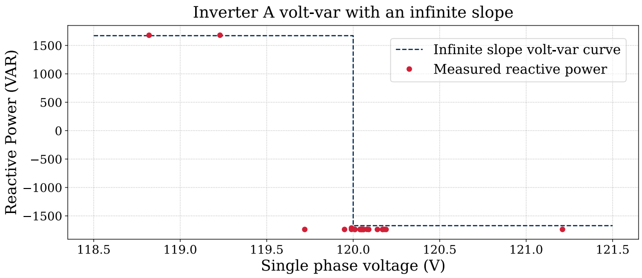


FIGURE 7. Volt-var curve with an infinite slope at 120 V grid operating voltage on Inverter A with a 3800 W active power output.

Case 15 refers to reversing the volt-var control where we reversed the voltage and reactive power setpoints of the IEEE 1547 volt-var curve to inject or absorb unwanted reactive power, leading to an exacerbation rather than moderation of voltage instability. In this experiment, we let the inverter inject reactive power at 22 % of P_{rated} to intensify the negative impact of the attack. Overall, Inverter A behaved as expected by following the control setpoints and injecting high reactive power during a low grid voltage period, and undesirably absorbed high reactive power when the grid voltage is higher than 115 V. With the reactive power priority being assigned to Inverter A by default, we observed an active power curtailment of ∼700 W_{AC} when absorbing high reactive power, and ∼400 W_{AC} when injecting the same amount of VAR. As a result, this attack clearly shows its unique signature in both active and reactive power measurements. When the reverse control attack is launched by an attacker, the undesired reactive power can be detected at any grid voltage, especially at extremely high voltage. Admittedly, implementing this type of attack would require someone with advanced knowledge of Volt-VAR controls and register mapping of control curve parameters.

2) VOLT-VAR CONTROL INTERRUPTION (CASES 17–19)

Instant reactive power mode switching is yet another cyberattack on volt-var control which causes grid disturbance when the grid operating voltage is greater than 1.0 pu. In case 17, the IEEE volt-var control was disrupted with the unity power factor and triggered the attack at 123 V where the reactive power starts to be absorbed for voltage regulation. According to the result, active power is normally curtailed when Inverter A injects high reactive power as expected due to its reactive power priority. However, after the attack has been triggered, the reactive power immediately goes to zero due to the unity power factor control mode caused by the attack. This type of inverter response is distinctive and detectable by measuring reactive power. Additionally, activating the volt-var control while having the maximum active power at high grid voltage could also be an indication of this attack since no power curtailment is performed, meaning that the inverter does not absorb reactive power at its supposed level (∼ −1672 VAR).

As we observed a specific behavior of volt-var control on Inverter A when there is no active power, we tested the attack case 19 based on that response of Inverter A. The result of case 19 is shown in Fig. 9 and it showcases that when the active power is restricted to zero, Inverter A is not able to inject or absorb any reactive power compared to the ability of outputting reactive power when having active power (See Fig. 8). The result also indicates the danger of zero active power limitation to the electric grid when volt-var control is needed for grid voltage stabilization. Nevertheless, our findings confirmed this type of attack did not impact Inverter B and concluded that this malicious attack is not applicable to every inverter, but only the ones whose reactive power control cannot be operating when active power is zero.

3) VOLT-WATT CHARACTERISTIC MODIFICATIONS (CASE 20)

We modified two volt-watt setpoints of Inverter A to have a vertical slope at 126 V (1.05 p.u.) which was the original voltage setpoint where the inverter started to take action and reduced active power. The response of this attack is shown in Fig. 10. This modified volt-watt curve has its own signature which comprises the unpredictable fluctuation of the active power between 1000 - 2500 W around the designated threshold of 126 V. With the response being observed, this volt-watt attack is expected to cause a significant oscillation in active power which could be worse when multiple inverters are under attack at the same time. To cause more severe grid instability issue, a hacker could also move the threshold

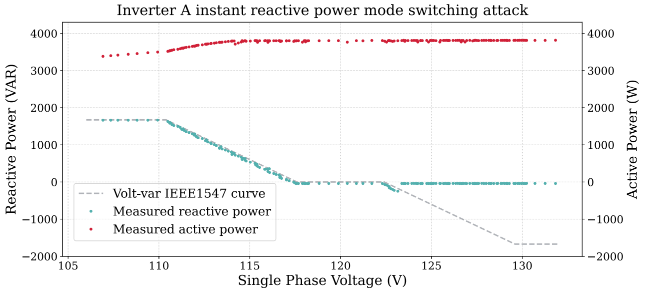


FIGURE 8. Volt-var IEEE1547-2020 control interruption by the reactive power mode switching from volt-var to the unity PF on Inverter A with a 3800 W active power output.

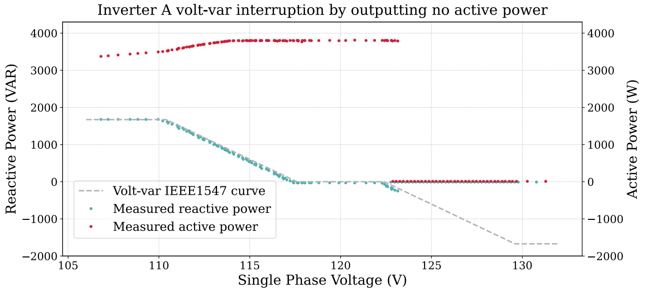


FIGURE 9. Volt-var IEEE1547-2020 control interruption by zero active power output to the grid at 123 V grid voltage.

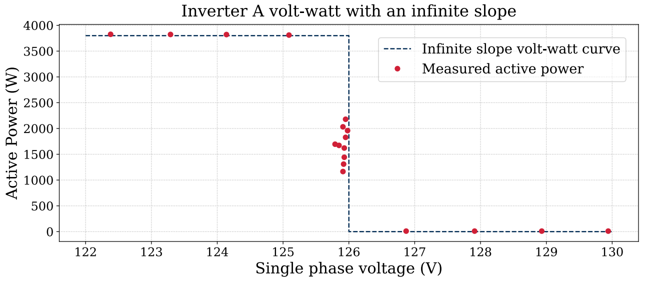


FIGURE 10. Volt-watt IEEE1547 curve modification from IEEE curve to a volt-watt curve with an infinite slope at 126V (1.05 p.u.) grid operating voltage on Inverter A with 3800 W active power output.

to 120 V to create massive oscillations around the normal operating voltage.

D. INTRUSION DETECTION SYSTEM EVALUATION

We evaluated our intrusion detection system using the methodology proposed in Section III. The results of cyberattack detection system are summarized in Table 3. Overall, the detection system achieved 93.0 % accuracy of all datapoints, 92.6 % normal condition detection, and 94.7 % cyberattack detection. We investigated the 2 undetectable cyberattacks and found that the ability of cyberattack detection actually depends on the resolution of data collection. The 2 undetectable attack hours correspond to the intermittent active power attacks which will be undetectable when the power flow is being measured at a random timestamp during high power output periods. Additionally, intermittent power attacks essentially depend on the power components they are targeting, and the responses of these power components will be completely independent of each other.

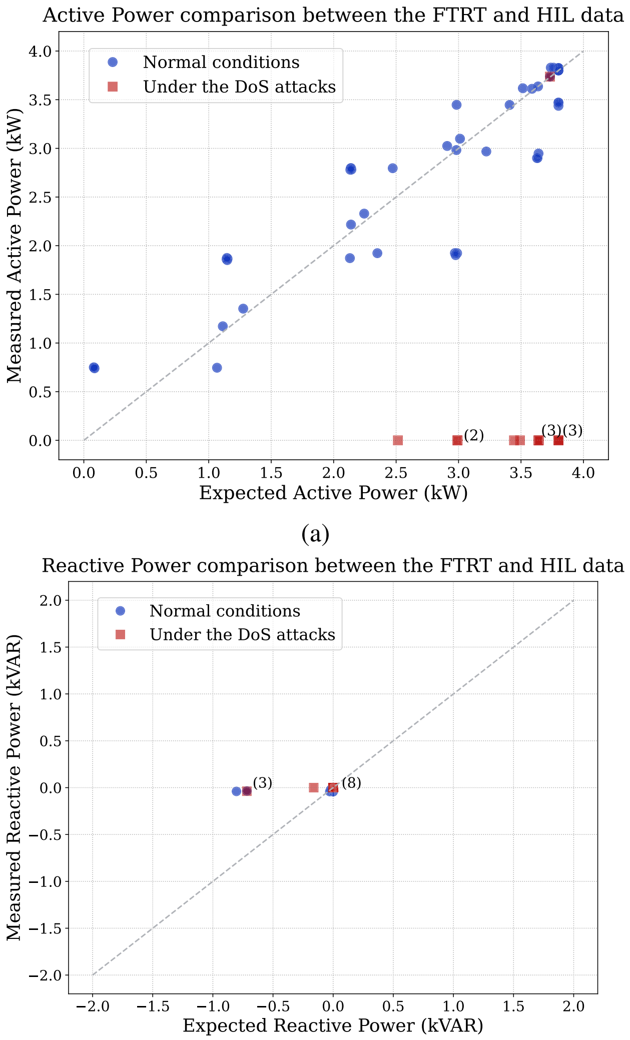
TABLE 3. Cyberattack detection assessment results.

Class	Case #	No attack	FP	Undetected	Detected
DoS	1	8	0	0	2
	2	5	1	0	4
	3	7	1	0	2
	4	6	2	0	2
	5	6	3	0	1
	6	9	0	0	1
	7	9	0	0	1
Intermittent	8	8	0	2	0
	9	9	0	0	1
	10	8	0	0	2
	11	8	0	0	2
Modification	12	8	0	0	2
	13	8	0	0	2
	14	8	0	0	2
	15	8	0	0	2
	16	6	2	0	2
	17	8	0	0	2
	18	8	0	0	2
	19	5	3	0	2
	20	8	0	0	2
Total		150	12	2	36

In Fig. 12, the 2 hours with unexpected reactive power of more than −400 VAR are the intermittent PF attacks which directly affect the reactive power injection or absorption, yet this does not have any impact on the active power, so that we have a perfect alignment of approximately 3.7 kW of expected and actual active power.

Another detection error (referred to as a *false positive or FP*) is generated during the time frame flagged as a cyberattack, when in fact there are no malicious activities during those periods [39]. In this work, 12 out of 162 no-attack hours (7.4%) are detected as false positives due to large discrepancies in active and/or reactive power as a result of PV forecasting, as well as unexpected reactive power controls that are activated instantaneously for grid stability purposes.

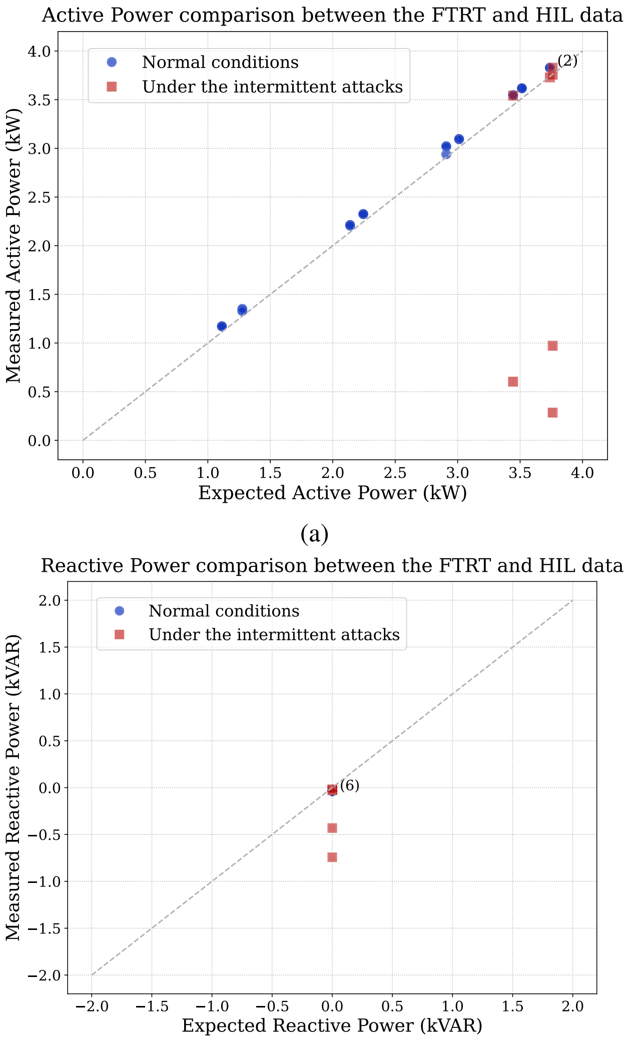
We compared the actual power flows to the expected active and reactive power to demonstrate that different malicious activities have unique signatures which could be detected from different parameters. Some of our results of expected and measured data are shown in Fig. 11 and and 13. When the inverter is attacked with DoS, over 90 % of those under-attack hours are noticeable by measuring only active power as the inverter immediately disconnects from the electric grid and stops producing the power output. As shown in Fig. 11, active power abnormality will be much more observable than reactive power when the inverter is under DoS attacks. Nonetheless, intermittent and modification attacks indicate the significance of reactive power monitoring compared to DoS, since both attack classes could be launched targeting reactive power (especially modification attacks). Fig. 13 compares active and reactive power abnormalities during modification attacks, which demonstrates that we were able



(a)

(b)

FIGURE 11. Active (a) and reactive (b) power comparison between calculated power flows from the FTRT simulator and P-HIL lab. The results were collected on each day when the DoS had been launched for a specific duration. The total data points are 70 for each plot and the numeric indications refer to the number of overlapping datapoints in the plot.



(a)

(b)

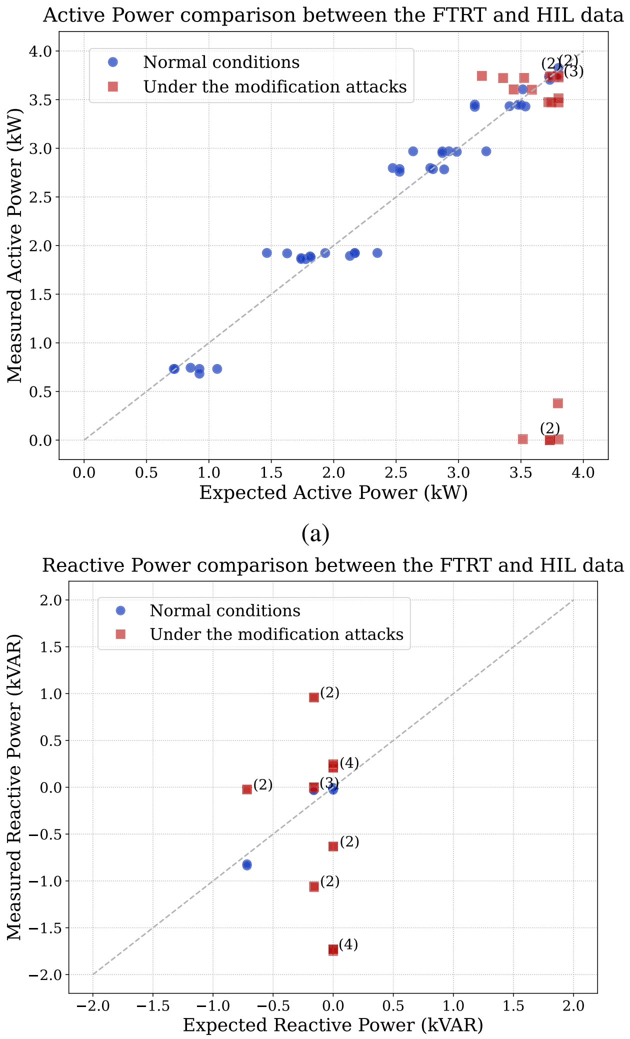
FIGURE 12. Active (a) and reactive (b) power comparison between calculated power flows from the FTRT simulator and P-HIL lab. The results were collected on each day when the intermittent attacks had been launched for a specific duration. The total data points are 40 for each plot and the numeric indications refer to the number of overlapping datapoints in the plot.

to detect all 17 hours of malicious activities and 12 of them are identified based on abnormal reactive power. This evidently shows that our detection system can distinguish different classes of cyberattacks based on their signatures.

The introduced detection method will mainly detect inverter abnormalities caused by changes of the inverter controls leading to inverter operating failure, production issues, and/or disconnection from the grid. As the detection system is expected to be applied to a feeder with multiple PV inverters, the malicious attacks can be distinguished in a high level when more than two inverters show the same abnormal behavior after the responses have been confirmed by repeated measurements.

The most common non-cyberattack failure is a total loss of power while maintaining communication [40], [41]. Many of the inverter responses to our cyberattacks result in a different but still abnormal responses. Although the changes of inverter controls can be modified by a number of methods, a possibility of inverter setpoints and/or control modes being changed by the inverter itself due to a malfunction appear to be relatively small. Additionally, the changes caused by human error from nonspecialists are not likely to happen as most commercially available inverters require permission and an access code from the manufacturers in order to have the same access level as installers. Consequently, we believe that our detection system is adequately effective to be deployed in the field despite the system not having a clear distinction between causes of issues.

While an analysis of remedial actions are beyond the scope of our detection framework, there are several mitigation



(a)

(b)

FIGURE 13. Active (a) and reactive (b) power comparison between calculated power flows from the FTRT simulator and P-HIL lab. The results were collected on each day when the modification attacks had been launched for a specific duration. The total data points are 80 for each plot and the numeric indications refer to the number of overlapping datapoints in the plot.

options possible. A prominent example is the use of device diversity as *hot backups*. In this scenario, the victim device is paired with a similar device (of similar/identical functionality) from a different vendor. Here the assumption is that devices from different vendors cannot be exploited in exactly the same way. Therefore, as soon as an attack is detected on the victim device, a potential mitigation is to disconnect the victim from the network and switch to the hot backup device. Given that the network offers some degree of inertia, this switch is not expected to cause any further instabilities. However, this approach results in additional cost and installation complexity from having a second inverter and a remote activated 240 VAC transfer switch.

IV. CONCLUSION

This work evaluates an intrusion detection methodology for smart grid devices by analyzing responses of grid-tied smart inverters to the malicious attacks targeting their power components. Using a P-HIL laboratory as a test environment paired with the FTRT simulations for power flow prediction, we simulated three different classes of cyberattacks and measured the inverters' responses during the periods under attack for a total of 20 different scenarios. Our findings show that inverters from different manufacturers have different vulnerability levels to cyberattacks. Most of their responses to the cyberattacks can be captured by measuring the power flow locally and externally by the grid operator and comparing the actual real-time power flow to the predicted grid power flow. In terms of performance, our detection method identifies over 94% of actual malicious activities using the proposed two-step screening process. Different cyberattacks can be identified depending on which complex power components they are aiming to cause disturbances. Our results further show that DoS attacks can be noticed immediately after the attacks are launched, and they can be detected from the active power analysis. Conversely, modification attacks are detectable by the reactive power measurements, while intermittent attacks remain the most challenging for our detection system since the objective of intermittent attacks is to create an oscillation of the complex power components. Therefore, such attacks could be invisible when high power levels are assigned to the inverters. Our research has highlighted similarities and differences between responses of different inverter brands depending on the type of attack. Our future work will investigate the differences in inverters' behavior under abnormal controls, as well as improving the accuracy of our intrusion detection methodology by further reducing false positives.

ACKNOWLEDGMENT

The views expressed herein do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

REFERENCES

[1] Renewable Energy World. (2013). *Breakdown: Penetration of Renewable Energy in Selected Markets*. [Online]. Available: https://www.renewableenergyworld.com/baseload/penetration-of-renewable-energy-in-selected-markets/

[2] B. Mirafzal and A. Adib, "On grid-interactive smart inverters: Features and advancements," *IEEE Access*, vol. 8, pp. 160526–160536, 2020.

[3] J. H. Braslavsky, L. D. Collins, and J. K. Ward, "Voltage stability in a grid-connected inverter with automatic volt-watt and volt-VAR functions," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 84–94, Jan. 2019.

[4] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient networked AC microgrids under unbounded cyber attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3785–3794, Sep. 2020.

[5] A. Majumdar, Y. P. Agalgaonkar, B. C. Pal, and R. Gottschalg, "Centralized volt–var optimization strategy considering malicious attack on distributed energy resources control," *IEEE Trans. Sustain. Energy*, vol. 9, no. 1, pp. 148–156, Jan. 2018.

[6] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623–634, Jan. 2021.

[7] N. Duan, N. Yee, B. Salazar, J.-Y. Joo, E. Stewart, and E. Cortez, "Cybersecurity analysis of distribution grid operation with distributed energy resources via co-simulation," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2020, pp. 1–5.

[8] N. Duan, N. Yee, A. Otis, J.-Y. Joo, E. Stewart, A. Bayles, N. Spiers, and E. Cortez, "Mitigation strategies against cyberattacks on distributed energy resources," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2021, pp. 1–5.

[9] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[10] T. O. Olowu, S. Dharmasena, H. Jafari, and A. Sarwat, "Investigation of false data injection attacks on smart inverter settings," in *Proc. IEEE CyberPELS*, Oct. 2020, pp. 1–6.

[11] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-service (dos) attacks on load frequency control in smart grids," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2013, pp. 1–6.

[12] S. Asri and B. Pranggono, "Impact of distributed denial-of-service attack on advanced metering infrastructure," *Wireless Pers. Commun.*, vol. 83, no. 3, pp. 2211–2223, Aug. 2015.

[13] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 3153–3158.

[14] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.

[15] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[16] G. F. Lauss, M. O. Faruque, K. Schoder, C. Dufour, A. Viehweider, and J. Langston, "Characteristics and design of power hardware-in-the-loop simulations for electrical power systems," *IEEE Trans. Ind. Electron.*, vol. 63, no. 1, pp. 406–417, Jan. 2016.

[17] V. H. Nguyen, Y. Besanger, Q. T. Tran, C. Boudinnet, T. L. Nguyen, R. Brandl, and T. I. Strasser, "Using power-hardware-in-the-loop experiments together with co-simulation for the holistic validation of cyber-physical energy systems," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT-Europe)*. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers, Sep. 2017, pp. 1–6.

[18] T. Reinikka, H. Alenius, T. Roinila, and T. Messo, "Power hardware-in-the-loop setup for stability studies of grid-connected power converters," in *Proc. Int. Power Electron. Conf. (IPEC-Niigata -ECCE Asia)*. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers, May 2018, pp. 1704–1710.

[19] J.-H. Jung, "Power hardware-in-the-loop simulation (PHILS) of photovoltaic power generation using real-time simulation techniques and power interfaces," *J. Power Sources*, vol. 285, pp. 137–145, Jul. 2015.

[20] J. Kollmer, S. Biswas, L. Bai, A. Sarwat, and W. Saad, "A hardware-in-the-loop experimental platform for power grid security," in *Proc. ASEE Annu. Conf. Expo.*, 2018, pp. 1–6.

[21] Z. Liu, Q. Wang, and Y. Tang, "Design of a cosimulation platform with hardware-in-the-loop for cyber-attacks on cyber-physical power systems," *IEEE Access*, vol. 8, pp. 95997–96005, 2020.

[22] J. Choi, D. Narayanasamy, B. Ahn, S. Ahmad, J. Zeng, and T. Kim, "A real-time hardware-in-the-loop (HIL) cybersecurity testbed for power electronics devices and systems in cyber-physical environments," in *Proc. IEEE 12th Int. Symp. Power Electron. Distrib. Gener. Syst. (PEDG)*. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers, Jun. 2021, pp. 1–5.

[23] E. Naderi and A. Asrari, "Hardware-in-the-Loop experimental validation for a lab-scale microgrid targeted by cyberattacks," in *Proc. 9th Int. Conf. Smart Grid (icSmartGrid)*, Jun. 2021.

[24] B. A. Bhatti, R. Broadwater, and M. Delik, "Integrated T&D modeling vs. co-simulation—Comparing two approaches to study smart grid," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Atlanta, GA, USA, Aug. 2019, pp. 1–5.

[25] H. Jain, B. A. Bhatti, T. Wu, B. Mather, and R. Broadwater, "Integrated transmission-and-distribution system modeling of power systems: State-of-the-art and future research directions," *Energies*, vol. 14, no. 1, p. 12, Dec. 2020.

[26] T. Kaewnukultorn, S. B. Sepúlveda-Mora, and S. Hegedus, "Characterization of voltage stabilization functions of residential PV inverters in a power hardware-in-the-loop environment," *IEEE Access*, vol. 10, pp. 114802–114813, 2022.

[27] C. Konstantinou, M. Sazos, and M. Maniatakos, "Attacking the smart grid using public information," in *Proc. 17th Latin-Amer. Test Symp. (LATS)*, Apr. 2016, pp. 105–110.

[28] *IEEE Standard Conformance Test Procedures for Equipment Interconnecting Distributed Energy Resources With Electric Power Systems and Associated Interfaces*, IEEE Standard 1547.1-2020, IEEE, 2020.

[29] D. Almeida, J. Pasupuleti, and J. Ekanayake, "Comparison of reactive power control techniques for solar PV inverters to mitigate voltage rise in low-voltage grids," *Electronics*, vol. 10, no. 13, p. 1569, Jun. 2021.

[30] M. Robinson, "The SCADA threat landscape," in *Proc. 1st Int. Symp. ICS SCADA Cyber Secur. Res.*, 2013, pp. 30–41. [Online]. Available: https://www.eads.com

[31] C. Parian, T. Guldimann, and S. Bhatia, "Fooling the master: Exploiting weaknesses in the modbus protocol," in *Proc. 3rd Int. Conf. Comput. Netw. Commun.*, 2020, pp. 2453–2458.

[32] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Electr. Eng.*, vol. 67, pp. 469–482, Apr. 2018.

[33] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal, and M. J. Reno, "Power system effects and mitigation recommendations for DER cyberattacks," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 4, no. 3, pp. 240–249, Sep. 2019.

[34] T. Armin, M.-S. Ali, and L. Chen-Ching, "Cyber security risk assessment of solar PV units with reactive power capability," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2018, pp. 2872–2877.

[35] J. Matherly, "Complete guide to Shodan," Shodan, LLC, 2015, vol. 1.

[36] Y. Chen, X. Lian, D. Yu, S. Lv, S. Hao, and Y. Ma, "Exploring Shodan from the perspective of industrial control systems," *IEEE Access*, vol. 8, pp. 75359–75369, 2020.

[37] H. Shaalan, J. Thompson, R. Broadwater, M. Ellis, and H. Ng, "Distribution engineering tool features a flexible framework," *IEEE Comput. Appl. Power*, vol. 8, no. 3, pp. 21–24, Jul. 1995.

[38] Electrical Distribution Design. (2019). *Building a Better Grid Through Innovation*. [Online]. Available: https://www.edd-us.com/m2iegs/

[39] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology," Nat. Inst. Standards Technol., Tech. Rep., 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[40] T. Gunda, "Inverter faults & failures: Common modes & patterns," in *Proc. Photovolt. Rel. Workshop*. U.S. Department of Energy Office of Scientific and Technical Information, 2020. [Online]. Available: https://www.osti.gov/servlets/purl/1767382

[41] A. Nagarajan, R. Thiagarajan, I. Repins, and P. Hacke, "Photovoltaic inverter reliability assessment," Nat. Renew. Energy Lab., Tech. Rep., Oct. 2019. [Online]. Available: https://www.nrel.gov/docs/fy20osti/74462.pdf

THUNCHANOK KAEWNUKULTORN (Graduate Student Member, IEEE) received the B.S. degree in electrical engineering from Chulalongkorn University, Thailand, in 2018. She is currently pursuing the Ph.D. degree in electrical and computer engineering with the University of Delaware (UD), Newark, DE, USA. Since 2021, she has been a Research Assistant with the Institute of Energy Conversion, UD. She has also been a Teaching Assistant in solar electric technology and the design and operation of renewable microgrids. Her research interests include renewable energy integration, smart inverters, microgrid technology, and energy storage systems.

SERGIO B. SEPÚLVEDA-MORA (Member, IEEE) received the B.S. degree in electronics engineering from Universidad Francisco de Paula Santander, Cúcuta, Colombia, in 2007, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Delaware (UD), Newark, DE, USA, in 2012 and 2022, respectively.

Since 2016, he has been an Assistant Professor with the Department of Electricity and Electronics, Universidad Francisco de Paula Santander. He is currently the Program Director of electronics engineering with Universidad Francisco de Paula Santander. His research interests include modeling and simulation of microgrids, renewable energy integration, power energy systems, data science, and machine learning applications.

ROBERT BROADWATER (Senior Member, IEEE) is currently the Chief Technical Officer with Electrical Distribution Design and a Professor Emeritus of electrical power and computer engineering with Virginia Tech. His research interests include object-oriented analysis and design and computer-aided engineering. He is also interested in developing software for the analysis, design, operation, and real-time control of physical systems.

DAN ZHU received the bachelor's degree in communication engineering from South China Normal University, China, and the M.S. and Ph.D. degrees in electrical engineering from Virginia Tech. She is currently with Electrical Distribution Design. Her research interests include power distribution system reliability improvement and voltage control design.

NEKTARIOS G. TSOUTSOS (Member, IEEE) received the M.Sc. degree in computer engineering from Columbia University and the Ph.D. degree in computer science from New York University. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Delaware (UD), with a joint appointment in the Department of Computer and Information Sciences. He is also the Faculty Organizer of the International Embedded Security Challenge (ESC) Competition that is held annually during the Cyber Security Awareness Worldwide (CSAW) Event. He has authored multiple articles in the IEEE Transactions and conference proceedings. His research interests include cybersecurity and applied cryptography, with a special focus on hardware security, trustworthy computing, and smart grid security. He serves on the program committee for several international conferences.

STEVEN HEGEDUS (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Delaware (UD), in 1990.

In 1982, he joined the Institute of Energy Conversion (IEC), UD, as a Research Staff. Since 2018, he has been a split appointment as a Professor of electrical and computer engineering (ECE) and a Senior Scientist with the IEC. During his 40 years with the IEC, his research has encompassed all of the commercially active solar cell technologies, both thin film and crystalline Si, supported by the Department of Energy and Industry Funding. This included studies of device processing, device characterization, performance optimization, and accelerated stability studies. He has been involved in solar cell and renewable electricity research for 40 years. He is the author of more than 120 articles with one of them having more than 1000 citations. He teaches classes on photovoltaic technology and microgrids and has advised more than 15 ECE graduate students. His current research interests include exploring the application of smart inverters with storage, microgrids, and electric vehicles to enhance solar grid integration. He co-edited the first and second editions of the *Handbook of Photovoltaic Science and Engineering* (Wiley and Sons 2003, 2011). He has taught numerous tutorials at the IEEE Photovoltaics Conference. He serves on the Delaware State Renewable Energy Task Force and advises several state agencies on the intersection of renewable energy technology and policy.