IET Cyber-Physical Systems: Theory & Applications

Research Article

IET Journals
The Institution of Engineering and Technology

ISSN 2398-3396
doi: 0000000000
www.ietdl.org

GPS Spoofing Effect on Phase Angle Monitoring and Control in an RTDS-based Hardware-In-The-Loop Environment

Charalambos Konstantinou[1], *Marios Sazos*[2], *Ahmed S. Musleh*[3], *Anastasis Keliris*[1], *Ahmed Al-Durra*[3], *Michail Maniatakos*[4]

[1] *Electrical and Computer Engineering, New York University Tandon School of Engineering, Brooklyn, New York, U.S.A.*
[2] *Center for Cyber Security, New York University Abu Dhabi, Abu Dhabi, U.A.E.*
[3] *Electrical and Computer Engineering, Khalifa University of Science and Technology, Petroleum Institute Campus, Abu Dhabi, U.A.E.*
[4] *Electrical and Computer Engineering, New York University Abu Dhabi, Abu Dhabi, U.A.E.*
✉ *E-mail: ckonstantinou@nyu.edu*

Abstract: In recent years, Cyber-Physical System (CPS) applications have been extensively utilized in the electric power grid to enable wide-area protection, control, and monitoring of power systems. Many of these applications in a smart grid CPS depend on reliable time synchronization. For example, synchrophasor data from geographically distributed Phasor Measurement Units (PMU) utilize Global Positioning System (GPS) for precise timing. However, these units are exposed to GPS time spoofing attacks that can lead to inaccurate monitoring and trigger unnecessary, and possibly destabilizing, remedial control actions. In this paper, we develop an end-to-end case study demonstrating the effect of GPS spoofing attacks on the phase angle monitoring and control functions of a PMU-based load shedding scheme. The evaluation of our attack strategy is performed in a Hardware-In-The-Loop Real Time Digital Simulator-enabled power system testbed.

1 Introduction

The upgrade of our electric power infrastructure into an intelligent Cyber-Physical System (CPS) has gradually led power systems and communication technologies to be closely interconnected. For instance, Wide Area Monitoring Systems (WAMS) highly rely on the communication network to gather system information from multiple sources and make proper control actions for local actuators. However, due to the interdependence of WAMS with power and communication applications, the operation and the performance of the entire system is anticipated to degrade during outage events.

The use of WAMS enables the real-time monitoring of power system dynamics, thus contributing towards smart grid reliability improvement. The requirement of rapid and accurate data acquisition has promoted Global Positioning System (GPS) as a trusted wireless clock synchronization mechanism for synchronized sensor monitoring equipment. As a consequence of GPS high precision and broad accessibility, Phasor Measurement Units (PMU) rely on GPS signals to provide time-stamped circuit quantities of power lines, i.e., synchrophasors. PMUs receive and decode the GPS data in order to estimate their clock position offset with respect to the GPS time measured by the on-board satellite clocks. Hence, PMUs leverage GPS clock synchronization to derive a Coordinated Universal Time (UTC) time-stamp reference for their measurements.

WAMS have PMUs installed across the grid infrastructure to measure voltage and current phasors [1], as presented in Fig. 1. The synchronized measurements from various geographic locations allow operators to be aware of the grid state in real-time. The IEEE C37.118 standard governing synchrophasor measurements for power systems states that the clock synchronization error between any two measurements from different PMUs should not exceed 31 or 26 μs for 50 or 60 Hz systems, respectively [2]. In comparison with traditional Supervisory Control And Data Acquisition (SCADA) systems which typically receive data every 2 to 5 seconds, WAMS data are captured at a much higher sub-second rate. PMUs can measure and transfer information at rates up to 120 samples per second. This provides an ideal way to increase situational awareness and take control countermeasures to mitigate the spread of disturbances.

PMUs with incorporated protective relaying functionalities provide unique advantages for wide area visibility. These units combine synchrophasor measurements and programmable logic control capabilities. As such, they can be used for a number of possible applications in power systems. Regarding wide-area protection, Remedial Action Schemes (RAS), also known as System Protection Schemes (SPS), utilize phasors to identify system conditions under which actions must be taken to avoid outages and maintain stability [3]. Examples of such protection schemes include *a)* Automatic Generation-Shedding schemes (AGSS) which shed generation resulting from the loss of transmission lines, buses, or loads as an action to maintain the load-generation balance, and *b)* Automatic Load-Shedding Schemes (ALSS), which take action if certain under-frequency and/or under-voltage conditions are met.

Although PMU technologies provide many benefits, the dependency on the communication infrastructure introduces security concerns. Measurement inaccuracies and errors may lead to wrong decisions which may further cause deterioration and damage to the system. For example, a spurious GPS signal can result in modified timestamp reference for PMU measurements [4]. The vulnerability of the GPS-dependent grid to GPS spoofing has been acknowledged by the North American Electric Reliability Corporation (NERC) [5]. According to NERC, each organization needs to ensure that reliability-critical applications are not affected by the disruption of GPS signals. However, studies have shown that erroneous timestamping of PMU data can affect algorithms related to stability monitoring, remedial action controllers, etc. [6, 7].

Due to the complexity and real-time requirements of grid applications, it is difficult to evaluate synchrophasor implementations on a real power system. The more feasible and efficient solution for testing individual grid modules, as well as the operation of the integrated system, is to use a Real Time Digital Simulator (RTDS) in a Hardware-In-The-Loop (HITL) testbed. The RTDS is a combination of specialized hardware and software designed to simulate power systems and test protection and control equipment. Actual hardware such as PMUs, relay controllers, and communication devices can be interfaced with the simulated power system model in the RTDS to enable realistic and accurate analysis of protection algorithms.

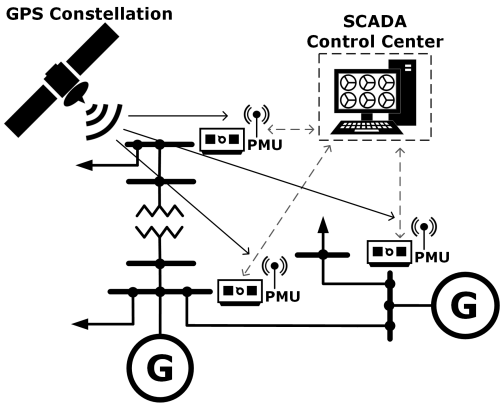

Fig. 1: Illustration of PMUs installed in substations across power grid to measure power lines.

Current research on RTDS implementations and PMU spoofing either performs only GPS spoofing on PMUs without modeling a real system [7–9] or it utilizes RTDS to study time-shift attacks without considering a real attack scenario [10, 11]. Bridging the gaps in existing literature, the contributions of this paper can be summarized as follows:

• We demonstrate, to the best of our knowledge, the first study that investigates *end-to-end* the effect of PMU-based GPS spoofed measurements on power system applications, using a real attack model in an RTDS-based HITL testbed with commercial field devices.

• We provide key insights to the feasibility and real-world impact of a GPS spoofing attack to the smart grid. We present how forged signals in the GPS receiver of PMUs can cause an increasing phase angle difference able to cause erroneous protection decisions by triggering the rapid shedding of loads.

• We utilize voltage phase angle differences in an under-voltage load shedding scheme to prevent system collapse. The phase angle difference between system buses is monitored closely as an indicator of grid stress that can lead to wide area outages. Specifically, the developed scheme uses an angle difference threshold able to detect a reduction in the system voltage due to imbalances between generation and load.

The structure of the paper is as follows: Preliminaries and related work are described in Section 2. The attack methodology and modeling, as well as the testbed setup, are presented in Section 3. Section 4 illustrates the impact of GPS spoofing on the ALSS algorithm. Concluding remarks are provided in Section 5.

2 Background and Related Work

2.1 Synchrophasor Monitoring and Control

Under steady state conditions, the current and voltage signals in the grid are ideal sinusoidal waveforms. A phasor is a quantity with magnitude and phase that represents a sinusoidal signal at a given frequency. The phasor magnitude is related to the magnitude of the sinusoidal and for a steady state signal it is constant. The phase angle, however, is a relative quantity as it represents the distance between the signal's sinusoidal peak and a specified reference. Phasor technology allows to sample voltage and current signals at different locations of the grid which all of them are in synchronism with a GPS clock. Fig. 2 depicts the synchronized sampling process of different waveforms at widely dispersed locations providing a common reference for the phasor calculations.

The availability of synchrophasors has contributed to the development of data-driven applications able to improve the grid reliability. Specifically, the angle difference between two sets of phasors measured at two different places could serve as an indicator of grid stress. A larger voltage phase angle difference between two buses

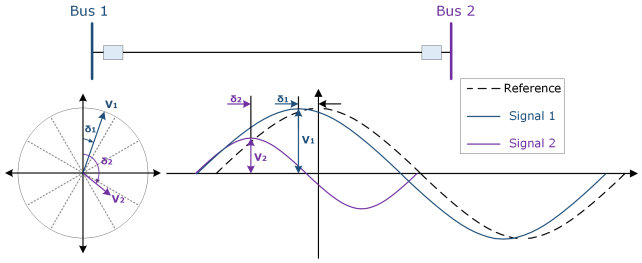

Fig. 2: Phasor representations at remote locations with common reference signal due to GPS synchronization.

could indicate, for instance, greater power flow between those points. As power flow increases, a larger stress is being exerted across the sending and the receiving bus terminal. Therefore, an increasing angle difference can be a serious problem; as the deviation from the nominal gets larger, closer the proximity of the system gets to instability.

To prevent the harmful effects of re-/closing transmission lines with a high angle difference, many utilities use synchrocheck relay schemes. The importance of such schemes has been emphasized in the investigation reports for the causes of the 2003 U.S. Northeast blackout and the 2011 Arizona - Southern California outages [12, 13]. Synchrocheck relay algorithms typically measure the voltage magnitude difference, frequency slip, and phase angle difference between buses and supervise against a predetermined setting prior to restoring a transmission line. Possible mitigation strategies against violations of predetermined limits could include generation shedding, use of phase-shifting transformers to reduce power flow, load curtailment, etc. For instance, a protection scheme intended to improve generation shedding in the transmission system of Mexico based on angle differences is presented in [14]: PMUs were configured to automatically trip the generators when the angle difference exceeds the detection threshold of 10° for double-line outages.

2.2 GPS Spoofing

GPS uses satellite transmitters equipped with a synchronized clock without any offset to the exact system time (UTC). These transmitters, which are located at known locations, broadcast a navigation signal that contains the satellites' deviation from the predicted trajectories as well as timestamp data [15]. The relative delays of a set of such satellite-transmitted signals are used from the GPS receiver to solve four equations which compute the time offset t_δ of the receiver and its 3-dimensional position.

The GPS time signal is of paramount importance for WAMS utilizing synchrophasors. In case of GPS offset errors due to spoofing attacks, the synchronization of PMUs would be affected and the provided data will be erroneous. A device that can transmit satellite signals can cause the GPS receiver of a PMU to latch onto the forged signal by gradually overpowering the authentic GPS signal, hence forcing the receiver to determine an incorrect clock offset. For an adversary, the goal is to maximize the difference of the receiver clock offset $\widetilde{t_\delta}$ (post-attack) with respect to its pre-attack value t_δ. For an f-Hz signal, the phase measurement error ϵ is related to the receiver offset error through the equation [7]:

$$\epsilon = [f \times (\widetilde{t_\delta} - t_\delta) \times 360^\circ] \,(\mathrm{mod}\, 360^\circ) \qquad (1)$$

For a successful attack, the spoofer requires exact information for the GPS signal as observed by the receiver of the target PMU. It is not necessary, however, to place the spoofing device inside the attacked substation. The spoofer must only be located in proximity to the satellite receiver [16].

While the time synchronization of PMUs depends on civilian GPS signals, there are also military GPS signals which are encrypted (authenticated) and nearly impossible to be spoofed. In our study, we consider only civilian GPS signals (as the ones utilized in PMUs operation). The susceptibility of civilian GPS signals to malicious

interference has been identified as early as 2001 in the VOLPE report [17]. Since then, several studies have been conducted that verify this vulnerability [18]. To the best of our knowledge, the only unclassified portable civilian GPS spoofer platform has been developed at the University of Texas at Austin [19].

In order to demonstrate the capability of an attacker transmitting falsified GPS signals, Kerns *et al.*. have investigated the feasibility to capture and control Unmanned Aerial Vehicles (UAVs) via GPS spoofing [20]. The effect of GPS spoofing has also been examined for grid applications. Results from live over-the-air GPS spoofing experiments and the de-synchronization of PMUs are presented in [8]. A simulation-based assessment of GPS spoofing is described in [21], where the authors present the vulnerability of grid sensors to erroneous time references. Timestamp attacks have also been demonstrated for applications such as transmission line fault detection, voltage stability monitoring, and event localization [9]. In addition, Jiang *et al.* have shown that spoofing of the GPS receiver clocks on PMUs can cause inaccurate estimates of the actual power load and trigger false alarms of power instability [7].

The requirements for successful GPS spoofing attacks are discussed in [15]. The study presents the timing requirements for transmitting valid and suitable spoofing signals, as well as the requirements regarding capturing a GPS receiver that is already locked to the legitimate GPS constellation. In comparison, this work demonstrates the impact of such attacks on grid monitoring and control algorithms implemented in an RTDS-based environment. The inclusion of hardware allows to validate the attack model of spurious synchrophasor measurements. Furthermore, Software Defined Radios (SDR) are utilized as they are less costly and more versatile in comparison to GPS simulators.

3 Attack Modeling and Setup

In this section, we introduce the theory and models of the study, as well as the experimental setup to assess the GPS spoofing effect on the phase angle monitoring and control algorithm.

3.1 Attacker Model

The attack model considered in this paper assumes a sophisticated adversary who is proficient in handling GPS signals and is familiar with PMU operational details. The adversary has a modest budget, sufficient to procure SDR and RF equipment capable of receiving, synthesizing, and transmitting GPS signals. In addition, we assume the attacker knows in advance the location of at least one substation equipped with a PMU used for monitoring and control purposes. This is a realistic assumption, as there exists public information on the location of PMUs [22]. For example, for the United States, the North American SynchroPhasor Initiative maintains a list of PMUs locations on its website. For delivering the GPS spoofing attack, the adversary is located in the physical proximity of such a substation. Since the attack is delivered over-the-air, the attacker is not required to bypass any physical security mechanisms present in the vicinity of substation or enter the substation.

3.2 System Model

Our system consists of a combination of generators, transformers, transmission lines, and loads described in Section 3.4.1. The monitoring and control of the system power flow, as well as the ALSS operation, is achieved through the use of PMUs (Fig. 1). We use an HITL PMU connected to an RTDS to assess the effect of de-synchronization via GPS spoofing attacks. The utilization of RTDS enables efficient real-time simulation of the entire power system model and the synchronization of the RTDS simulation time-step to an external GPS clock reference. At the same time, we demonstrate the practicality and applicability of de-synchronization attacks via an end-to-end experiment enabled by the inclusion of commercial hardware equipment in an HITL setup. We argue that this setup is the most accurate and efficient alternative to entire hardware replication or production system tests, which require significant budget and introduce dangers.

In practice, each PMU is equipped with a GPS receiver used for time synchronization. In our setup, we utilize one hardware PMU in HITL mode and one simulated PMU within the RTDS. Thus, two GPS receivers are required, one for the hardware PMU and one for providing time synchronization to the RTDS platform. Both GPS receivers are expected to receive signals from legitimate GPS satellites. Without loss of generality, due to inadequate live sky coverage at the location the experiments were conducted, we transmit a synthesized GPS signal to act as the legitimate GPS constellation.

The RTDS simulates the operation of the power grid as shown in Fig. 1. The HITL PMU corresponds to one of the system substations, which will be the target of our spoofer attacker. The adversary is in physical proximity to this target substation and knows the approximate coordinates of the PMU's GPS receiver in order to synthesize an almost identical time-shifted spoofing signal. A simulated PMU inside the RTDS corresponds to another substation of the system that the attacker is not aware of its location, and therefore it cannot be physically accessed. System monitoring and control is performed by a workstation operating as a SCADA center. The specifics of our experimental setup are explained in subsection 3.4.

3.3 Model of Phase Angle Separation Monitoring

Phase angle difference can serve as an effective indicator of the performance of a power system due to its relation to the system topology and power transfer capability. Consider the active power flow, P_{SR}, between two buses across a transmission line:

$$P_{SR} = \frac{V_S \times V_R}{X_L} \times \sin \delta_{SR} \tag{2}$$

where V_S and V_R are the sending-end and receiving-end bus voltage magnitudes, respectively, X_L is the line impedance between buses, and δ_{SR} is the phase angle difference between bus voltage phasors at each line terminal. The equation indicates that the angle difference depends on voltage magnitudes, line impedance, and active power flow. For example, a large angle difference can be a sign of topology changes, greater power flow between two buses, voltage drops, etc.

Load shedding at specific load buses is traditionally considered as the last but effective way in sustaining system stability and continuity after an angular, frequency, or voltage instability scenario [23]. In our phase angle monitoring algorithm, the disturbance detection is based on trigger-thresholds specified in NERC's disturbance monitoring standard [24]. The standard recommends the triggering criteria for disturbance detection in a Western Electricity Coordination Council (WECC) system, as either of the following: *i)* under-voltage trigger set no lower than 85% of the normal operating voltage for a duration of 5 seconds, *ii)* frequency < 59.55 Hz or > 61 Hz, *iii)* rate of change of frequency < -0.05625 Hz/s or > 0.124 Hz/s. However, utilities may use more stringent detection criteria as these values are too conservative and only a few disturbances can be detected. Regarding voltage deviation limits, for example, most utilities use a $\pm$ 5% or $\pm$ 10% criterion [25].

Typically, existing AGSSs and ALSSs monitor the topology and power flow capability of a system via open-line detectors which arm themselves and activate commands to shed load, trip generators, etc. To determine if a transmission line is open, shedding schemes utilize information from both ends of the line. Thus, for each line two open-line detectors are required [14]. For instance, a two-bus, four-transmission-line system requires eight open-line detectors and multiple communications channels. However, by monitoring the angle difference between the two buses the control scheme can detect reliably, for example, instantaneous changes in the transmission lines' impedance and thus contingency conditions. Such phasor-based shedding schemes have also fewer points of failure compared to the two-bus example system as they require only one communication channel to provide the buses angle information.

In our implemented ALSS, PMUs transfer synchrophasor data to a Phasor Data Concentrator (PDC) which acts as an automation

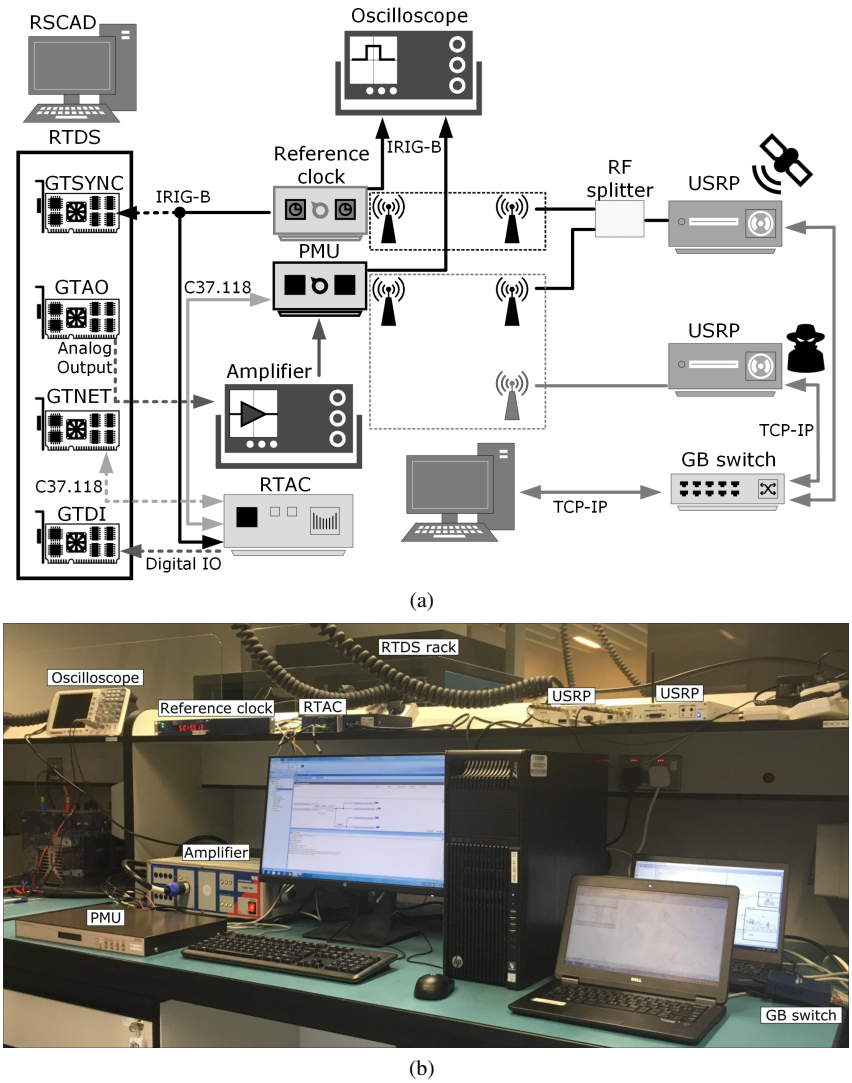

Fig. 3: HITL testbed platform with RTDS simulator: (a) schematic diagram, and (b) developed testbed, physically located at the Petroleum Institute, Abu Dhabi, UAE.

controller with incorporated protective relay functionalities. If the positive-sequence voltage angle difference between the local bus and a remote bus is greater than a threshold, the scheme sheds load for the system to remain within stability limits.

3.4 Experimental Setup and Modeling

The developed testbed platform includes an RTDS simulator, a physical PMU with GPS receiver, a Real-Time Automation Controller (RTAC), a GPS synchronized clock, GPS antennas, a network switch, an amplifier, a mixed-signal oscilloscope, Universal Software Radio Peripheral (USRP) embedded SDR platforms, and several workstations to run all the necessary software. In addition, several other components are used to support the connections between the aforementioned elements, such as RF splitters, external RF attenuators, and various types of cables and connectors. The arrangement of the testbed is depicted in Fig. 3.

3.4.1 RTDS and Power System Model: The RTDS technology facilitates efficient simulation and modeling of power systems. Also, RTDS allows efficient testing of field equipment using an HITL technique, enabling interaction with actual hardware in real-time. In our testbed, the hardware PMU is connected at one of the buses of the RTDS power system model. Similarly, a simulated PMU model is located at a different system bus. Both PMUs, gather synchronized real-time measurements and send the data to the RTAC at a rate of 60 frames per second. The RTAC, which servers as a central PDC with relay functionalities, processes the acquired information and sends the signals back to the RTDS-based controllers to open the corresponding breakers and shed the predefined load amount. The communication between the simulated PMU controller and the RTAC, as well as the communication between hardware PMU and the RTAC, is performed via the IEEE C37.118 protocol [2].

The power system used in this study is the IEEE 9-bus case which represents a simple approximation of the Western System Coordinating Council (WSCC) to an equivalent system with three generators and nine buses [26]. The system was slightly modified for simulation purposes: Circuit breakers are included at each line and after each generator before connected to the grid and PMUs are added to two of the system buses to monitor the real-time phasors of both voltages and currents. Specifically, the simulated PMU (PMU1) monitors the voltage and current phasors at bus 3 while the hardware PMU the corresponding phasors at bus 5 (PMU2). The single line diagram of the modified WSCC 9-bus system is presented in Fig. 4.

The HITL PMU-based WSCC 9-bus model implementation in RTDS software (RSCAD) is realized via the simulator interface cards [27]. The network interface GTNET card receives packets from the HITL Local Area Network (LAN) and transfer them as data to the processor card. The RTDS simulation data can be then sent from the processor card to the GTNET card which assembles them into packets. The packets are transferred to the LAN and picked up by the appropriate hardware devices. In our case, the GTNET

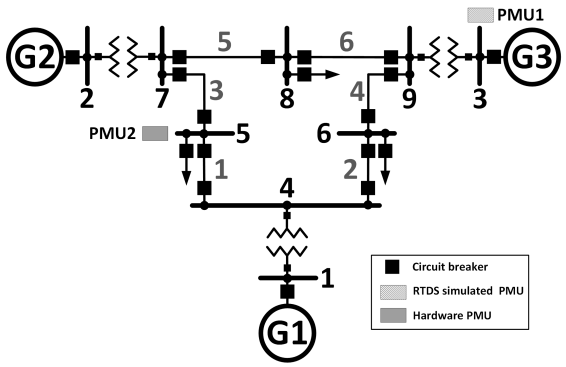

Fig. 4: Modified WSCC 9-bus system.

Table 1 Positive-sequence voltage phase angle difference between bus 3 and bus 5 of modified WSCC 9-bus system.

Scenario	Phase angle diff. PMU1-PMU2 (°)
Normal operation	8.73
System load increased by 50%	12.87
System load increased by 50%, Transmission line 3 out-of-service	20.62
System load increased by 50%, Transmission lines 3 and 5 out-of-service	21.68
System load increased by 50%, Transmission lines 3 and 5 out-of-service, Bus 5 load shed by 50%	16.42

card is utilized for the Ethernet-based phasor data communication according to the IEEE C37.118 protocol.

The GTSYNC card is used for synchronization of the simulated PMU (PMU1) in the RTDS. It ensures that the simulator clock remains locked to signal received from the GPS synchronized clock. In the experiment, the GTSYNC card uses the Inter-Range Instrumentation Group time code format B (IRIG-B) unmodulated signals as the synchronization source acquired from the external clock.

The digital signals of the RTDS simulation are transferred as analog waveforms to the hardware PMU via the GTAO card. The GTAO analog output card can produce a $\pm$ $10V$ peak maximum signal. However, the physical PMU of our testbed does not accept low level voltage signals. Thus, the GTAO analog output signals are properly scaled and transfer to the PMU via an amplifier. In this configuration, it is necessary to take into consideration the amplifier's voltage and current gain as well as the Current Transformer (CT) and Potential Transformer (PT) ratio and error phase of the physical PMU.

Similarly, the GTDI card is used to interface digital signals between the RTDS and external equipment. In the testbed setup, the GTDI card provides a digital input to the simulation from the RTAC which implements the ALSS. The output of the controller is triggered once the threshold of the phase difference between the bus 3 and 5 of WSCC 9-bus system exceeds a pre-defined value. The sampling rate of both GTAO and GTDI cards is specified by the time-step of the RTDS simulation. The time-step in our simulation model is 50 μs, hence the sampling rate is 20 kHz.

3.4.2 GPS Receiver Spoofing: For the implementation of the experiment, synthetic GPS signals are generated at the L1 GPS frequency based on satellites' Almanac and Ephemeris files [28] using the LabVIEW GPS toolkit [29] and USRP embedded SDR platforms [30]. The generated GPS signals are transferred via an industrial gigabit switch to the USRPs. The first USRP SDR generates and transmits the reference GPS signal (live sky), while the other USRP SDR generates and transmits a time-shifted version of the reference signal. Since GPS signals are sensitive to clock jitter and frequency offset, an improved frequency source is often necessary to control the radio transmitter frequency and to synchronize the USRPs. Thus, a board mounted GPS Disciplined Oscillator (GPSDO) is placed at the USRPs as the high precision frequency source.

The signals generated by both USRP SDR devices are routed inside two different Radio Frequency (RF) shielded and grounded boxes. The first box is used to re-transmit the reference GPS signal to the synchronized clock of the testbed used as the clock reference for the simulated PMU. The second RF shielded box acts as the GPS spoofer which receives both authentic (reference) and counterfeit signals for re-transmission. For transmitting the same reference signal at both RF shielded boxes an RF splitter is used. To ensure capture of the spoofed signal within the RF shielded box by the antenna of the physical PMU, we re-transmit the counterfeit GPS signal at higher dBm levels than the reference one. Initially, the two signals are transmitted at the same level. The strength of spoofed signal is then increased at steady steps until the GPS receiver of the PMU locks and tracks the spoofed set of satellites (6 dB gain).

Our initial experiments attempted to directly change the time on the GPS receivers by manipulating the time data of the spoofed GPS signal and injecting arbitrary time-shifts, ranging from $msec$ to hours. However, these efforts did not result in a satellite takeover and did not change the GPS receivers' reported time. This experimental finding is aligned with the observations in [15], where the requirements for achieving a seamless satellite takeover are discussed. Another possible explanation is the existence of GPS anti-spoofing mechanisms in the particular receiver models we use in our testbed [31, 32].

To overcome the above limitation while adhering to our attacker model, we force the receivers to lose GPS lock by transmitting Gaussian noise at the GPS frequency range, effectively jamming the legitimate GPS signals. Subsequently, we transmit spoofed signals at a slightly higher power level than legitimate signals to force the receivers to lock on the spoofed signals. For the takeover to be successful, we observed that the necessary duration of the jamming phase is receiver-dependent. In order to measure the time-shifts with μsec accuracy, we utilized an oscilloscope as shown in Fig. 3. We used the oscilloscope to compare the IRIG-B output signals between the reference signal at the clock output and the spoofed signal at the output of the hardware PMU.

The synchronized clock used to capture the reference GPS signal requires a minimum number of four satellites in order to lock and synchronize the GTSYNC card of RTDS. The hardware PMU requires at least one satellite to lock. In the case which the hardware PMU locks to the reference GPS signal, it provides the same phasor measurements with the RTDS model for bus 5 since the time-stamping of the IRIG-B signal for both PMU and RTDS will be the same. In the spoofing scenario, however, the hardware PMU receives and locks to the spoofed time-shifted GPS signal, thus the error in the phasor measurements changes based on the pre- and post-attack time-shift value (Eq. 1).

4 Results and Discussion

4.1 Phase Angle Monitoring on ALSS

Power systems are designed to handle a single contingency condition without violating system security and stability constraints [33]. Typical normal design contingencies are three-phase fault on any generator with normal fault clearing and reclosing, phase to ground faults on different phases, loss of any power system component without any fault, etc. Power systems should also sustain critical contingencies. Such contingencies include loss of major transmission lines and generators, permanent three-phase faults on generators, abnormal operation of control and protection devices, etc.

Regarding transmission line loss, there may be various triggering scenarios of such incident. For instance, a relay may trip the breaker open due to a fault condition [11] or even a cyber-attack scenario [34]. In addition, a common phenomenon is load variation, since load switching occurs throughout the day.

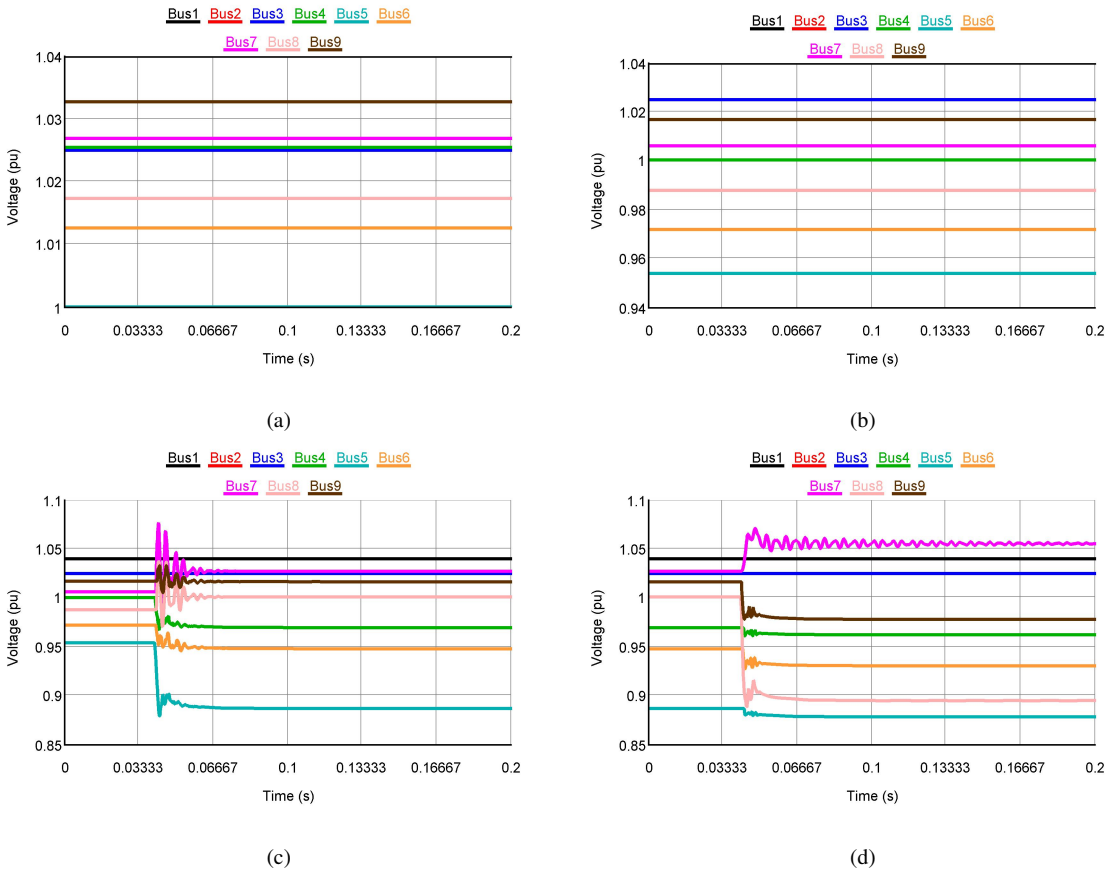

Fig. 5: Voltages of busbars for (a) normal operation, (b) when load increases by 50%, (c) with 50% of the load increased and line 3 out-of-service, and (d) with 50% of the load increased and both transmission lines 3 and 5 out-of-service.

4.1.1 Case Study: During normal operation, the generator at bus 2 of the WSCC 9-bus system can generate $417.16MVA$, while the other two generators can produce $1210.81MVA$. In such operating conditions, the total load of the system is $439.39MVA$. In order to test the functionality and performance of the angle-based load shedding scheme, an event is applied to the simulated system as follows: at $t = 0.04s$ the system load suddenly increases by 50% compared to the base case load. Fig. 5(a) and Fig. 5(b) present the busbars voltages of the system before and after this event, respectively. Voltage levels at all buses do not deviate outside stability limits. Also, the initial positive-sequence voltage phase angle difference of 8.73° between bus 3 and bus 5 is increased to 12.87° after the load change as shown in Table 1.

The above event follows a breaker opening on transmission line 3. As a result, the generated power at bus 2 flows to the rest of the system via the transmission line 5. In case the transmission line 5 is also lost, one of the system generators is isolated from the grid. Thus, the transfer impedance between the other two power plants is increased and the machines accelerate to meet load demand. The inability of the system to handle the loss of the lines is depicted in Fig. 5(c) and Fig. 5(d). In both cases, there exist bus voltages which exceed the 10% deviation limit. As shown in Table 1, the angle difference between bus 5 and bus 3 for single (loss of tie line 3) and double (loss of tie lines 3 and 5) contingencies if there are no protection or control actions taken are 20.62° and 21.68°, respectively.

Based on the results, an angle difference threshold of 7° can detect both single and double contingencies assuming a system load increase of 50%. This threshold is used in the ALSS to trip part of the least critical load. In the scenario which the load at bus 5 is shed by 50%, thus restored to its initial load level, the voltage of the system is restored and it becomes stable. Fig. 6 shows the voltages of busbars after the shedding of the load at bus 5. The simultaneous or sequential loss of two lines does not impact the stability of the system as the ALSS logic of 7° threshold between bus 3 and bus 5, provides reliable information to detect such network topology changes. After the load of bus 5 is restored to its initial value, the angle difference between the two PMUs becomes 16.42°, as shown in Table 1, and hence the protection logic is de-activated.

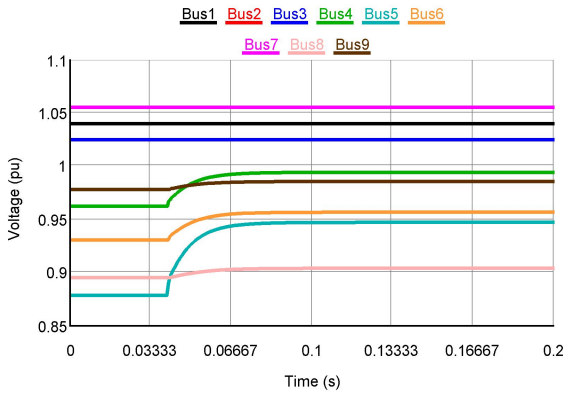

Fig. 6: Voltages of busbars after the load shedding scheme is applied.

4.2 *Impact of GPS Spoofing*

The GPS spoofing attack described in Section 3.4.2 is applied to the receiver of the hardware PMU located at bus 5 of the system (PMU2), successfully forcing the synchrophasor measurements to diverge from their nominal values. Fig. 7(a) and Fig. 7(b) present the phasor measurements of PMU2 before and after the spoofing

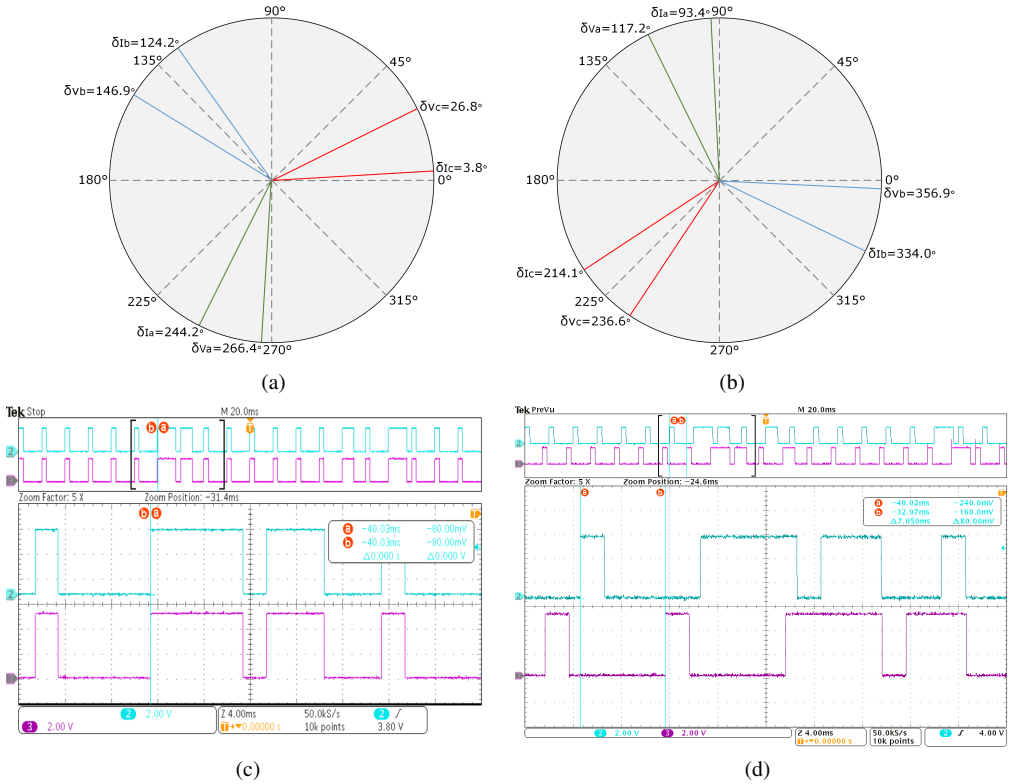

Fig. 7: Phasor measurements at bus 5 (a) before and (b) after the GPS spoofing attack. Before the attack, the GPS signals on the oscilloscope (IRIG-B format) received by the two PMUs are (c) initially aligned with each other while (d) after the spoofing there is a time-shift of $7.05ms$.

Table 2 Experimental results of GPS receiver clock offset error and the corresponding phase angle error.

A/A	GPS receiver clock offset error (ms)	Phase angle error ($^\circ$)
1	6.77	146.34
2	6.86	148.04
3	6.90	148.84
4	7.05	150.07
5	7.19	155.41

attack, respectively. While the PMU was initially fed with the reference (true) GPS signal (Fig. 7(c)), the GPS spoofing resulted in a receiver clock offset error of $7.05ms$ as shown in Fig. 7(d). This time offset difference between the counterfeit and authentic GPS signal caused the phasors to change according to Eq. 1 ($\approx 150^\circ$), thus verifying the validity of our experiments. This is large enough to induce misreadings in the grid monitoring and control algorithms.

Consider the case study of subsection 4.1.1 where the load-shedding scheme automatically triggers the corresponding relays to shed 50% of bus 5 in case transmission lines 3 and 5 are out-of-service (open breakers). A GPS spoofing attack on the hardware PMU of bus 5 able to cause a phase angle difference between bus 3 and bus 5 which exceeds 7° can activate the shedding algorithm and result in a falsified protection action. Table 2 lists several of the experimental results able to shift the phasor angles. All the GPS receiver clock offset error values shift the phasor angles by more than 7° and can induce false system alarms. In the scenario which the receiver clock offset error is shifted by $7.05ms$ with a corresponding angle error of $\approx 150^\circ$, the phase angle difference between bus 5 and bus 3 is greater than the defined 7° threshold causing a voltage increment and limiting the flow of current at bus 5. Fig. 8 shows the bus voltage and the load current at bus 5 for this case.

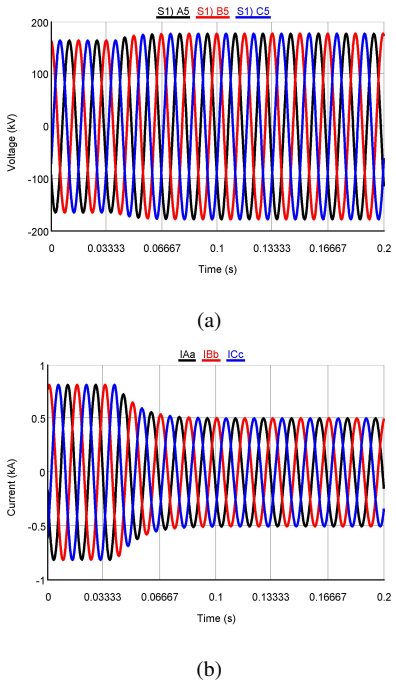

Fig. 8: (a) Bus voltage and (b) load current at bus 5 after GPS spoofing and the misleading triggering of the load shedding scheme.

5 Conclusions

In this paper, we presented the first study to examine the GPS spoofing effect on PMUs receiver clock in an HITL environment including RTDS. This end-to-end study demonstrated the threat to the integrity of synchrophasor measurements, providing key insights

related to the GPS spoofing effect, its feasibility, and implications to the smart grid. The presented spoofing attack can cause the GPS receiver of a PMU to compute an erroneous clock offset, which in turn introduces an error in the PMU's phase measurement. The utilization of RTDS enabled us to study the impact of attacks on a monitoring and control algorithm which automatically sheds load in case of contingency scenarios to preserve stability. The implemented load-shedding scheme is based on synchronized angle difference measurements which are utilized to detect topology changes. However, as shown in our work, an adversary located in the physical proximity of a substation can introduce a time error in PMUs by injecting a counterfeit ensemble of GPS signals into the antenna of the PMUs time reference receiver. As a result, the timing error can cause a corresponding phase error in the reported synchrophasor data, and therefore trigger control schemes unnecessarily.

Our study indicates that it is also important to employ robust protection schemes in smart grid implementations. Although substantial improvements in how PMU-enabled WAMS provide real-time monitoring of power systems, a number of drawbacks remain, most notably the timing challenges related with incorrect time-stamps able to cause a variety of problems for synchrophasor data analysis. Hence, PMUs should not be merely used for mission-critical schemes without additional data from WAMS and SCADA systems until timing issues have been resolved in a way that measurement and time integrity can be assured. Additional advancements in timing system provision, signal delivery, and the devices that use time signals are required before synchrophasor technology can become entirely reliable and resilient for increased dependence on automation in wide-area monitoring, protection, and control systems.

Acknowledgments

This work was supported by the Center for Cyber Security NYU Abu Dhabi, the NYU Abu Dhabi Global PhD Fellowship, and the ADNOC Research & Innovation Center. The authors would like to thank C. Pöpper and A. Bikos for their assistance with this project.

6 References

1 North American SynchroPhasor Initiative: 'PMUs and synchrophasor data flows in North America'. (NASPI, 2014)
2 IEEE: 'IEEE Standard for Synchrophasor Measurements for Power Systems', *IEEE Std C371181-2011*, 2011, pp. 1–61
3 O'Brien, J., et al. 'Use of synchrophasor measurements in protective relaying applications'. In: 67th Annual Conference for Protective Relay Engineers. (, 2014. pp. 23–29
4 Humphreys, T.: 'Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing', *University of Texas at Austin*, 2012,
5 NERC: 'Extended loss of GPS Impact on Reliability'. (NERC, 2012)
6 Jiang, J., et al.: 'An adaptive PMU based fault detection/location technique for transmission lines', *IEEE Transactions on Power Delivery*, 2000, **15**, (2), pp. 486–493
7 Jiang, X., et al.: 'Spoofing GPS receiver clock offset of phasor measurement units', *IEEE Transactions on Power Systems*, 2013, **28**, (3), pp. 3253–3262
8 Shepard, D., Humphreys, T., Fansler, A.: 'Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks', *International Journal of Critical Infrastructure Protection*, 2012, **5**, (3), pp. 146–153
9 Zhang, Z., et al.: 'Time synchronization attack in smart grid: Impact and analysis', *IEEE Transactions on Smart Grid*, 2013, **4**, (1), pp. 87–98
10 Almas, M., Vanfretti, L. 'Impact of time-synchronization signal loss on PMU-based WAMPAC applications'. In: Power and Energy Society General Meeting (PESGM). (, 2016. pp. 1–5
11 Adhikari, U., et al. 'Development of power system test bed for data mining of synchrophasors data, cyber-attack and relay testing in RTDS'. In: PESGM, IEEE. (, 2012. pp. 1–7
12 FERC, U. S. -Canada Power System Outage Task Force: 'Final Report on the August 14, 2003 Blackout in the U.S. and Canada: Causes and Recommendations'. (FERC, 2004)
13 FERC and NERC: 'Arizona-Southern California Outages on September 8, 2011: Causes and Recommendations'. (FERC, 2012)
14 Martínez, E., et al. 'Using synchronized phasor angle difference for wide-area protection and control'. In: Proceedings of the 33rd Annual Western Protective Relay Conference, Spokane, WA. (, 2006. pp. 1–11
15 Tippenhauer, N., et al. 'On the requirements for successful GPS spoofing attacks'. In: Proceedings of the 18th ACM conference on Computer and communications security. (, 2011. pp. 75–86
16 Yu, D., et al. 'Short paper: Detection of GPS spoofing attacks in power grids'. In: Proceedings of the 2014 ACM WiSec conference. (, 2014. pp. 99–104
17 John, A.: 'Volpe national transportation systems center vulnerability assessment of the transportation infrastructure relying on gps', *Volpe, Technical Report*, 2001,
18 Schmidt, D., et al.: 'A survey and analysis of the GNSS spoofing threat and countermeasures', *ACM Computing Surveys (CSUR)*, 2016, **48**, (4), pp. 64
19 Humphreys, T., et al. 'Assessing the spoofing threat: Development of a portable GPS civilian spoofer'. In: Proceedings of the ION GNSS international technical meeting of the satellite division. vol. 55. (, 2008. p. 56
20 Kerns, A., et al.: 'Unmanned aircraft capture and control via GPS spoofing', *Journal of Field Robotics*, 2014, **31**, (4), pp. 617–636
21 Akkaya, I., Lee, E., Derler, P. 'Model-based evaluation of GPS spoofing attacks on power grid sensors'. In: Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2013 Workshop on. (, 2013. pp. 1–6
22 North American SynchroPhasor Initiative: 'March 2015 PMU locations'. (NASPI, 2015)
23 Ghaleh, A., Sanaye.Pasand, M., Saffarian, A.: 'Power system stability enhancement using a new combinational load-shedding algorithm', *IET generation, transmission & distribution*, 2011, **5**, (5), pp. 551–560
24 NERC: 'PRC-002-2 disturbance monitoring and reporting requirements'. (NERC, 2014)
25 Russell, W., et al.: 'Restructuring vs. Reliability A Tale of Declining Standards'. (APPA, 2001)
26 Illinois Center for a Smarter Electric Grid (ICSEG): 'WSCC 9-Bus System'. (Information Trust Institute (ITI), 2017)
27 RTDS Technologies Inc. : 'RTDS and RSCAD technical information'. (RTDS, 2017)
28 NASA's Archive of Space Geodesy Data: 'Broadcast ephemeris data'. (NASA, 2017)
29 National Instruments: 'Manual for LabVIEW User'. (NI, 1998)
30 Ettus, M.: 'Usrp user's and developer's guide', *Ettus*, 2005,
31 North American SynchroPhasor Initiative: 'Time Synchronization in the Electric Power System'. (NASPI, 2017)
32 ICS-CERT: 'Improving the Operation and Development of GPS Equipment used by Critical Infrastructure'. (U.S. Department of Homeland Security, 2017)
33 NERC Standard TPL-001-4: 'Reliability Standards for the Bulk Electric Systems of North America'. (NERC, 2014)
34 Konstantinou, C., Maniatakos, M. 'Impact of firmware modification attacks on power systems field devices'. In: Smart Grid Communications (SmartGridComm), IEEE International Conference on. (, 2015. pp. 283–288