Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks

Daniel P. Shepard and Todd E. Humphreys
The University of Texas at Austin
Aaron A. Fansler
Northrop Grumman Information Systems

ABSTRACT

Results from Global Positioning System (GPS) spoofing tests against Phasor Measurement Units (PMUs) are presented, demonstrating that PMUs are vulnerable to spoofing attacks. A GPS spoofer can manipulate PMU time stamps by injecting a counterfeit ensemble of GPS signals into the antenna of the PMU's time reference receiver. A spoofer-induced timing error of only a few tens of microseconds causes a PMU to violate the maximum phase error allowed by the applicable standard. These and larger errors can give automated or human power grid controllers a false perception of the state of the grid, leading to unnecessary, and possibly destabilizing, remedial control actions. To emphasize this threat, it is shown that a particular PMU-based automatic control scheme currently implemented in Mexico, and whose control architecture and setpoints have been published in the open literature, could be induced by a GPS spoofing attack to trip a primary generator.

I. Introduction

Infrastructure supporting the generation and distribution of electric power, collectively known as the power grid, is regarded in the United States and other industrialized economies as critical national infrastructure. Past power disruptions and numerous government demonstrations have revealed that the power grid is vulnerable not only to natural disasters but also to malicious cyber activity, which, within the U.S., is on the rise. Past consequences of power disruption were annoyance and some economic loss; future disruptions resulting from intentional malicious activity could lead to crippling failures.

The power grid originally operated without an external time reference, but increased demand for reliability and capacity has spurred the introduction of grid sensors able to trace their timing accurately to universal coordinated time. In next-generation "smart grid" infrastructure, accurate timing signals will be broadly required, from the generation plant to the distribution substation to individual smart grid components [1].

The value of time synchronization is best understood by recognizing that the power grid is a complex, interconnected, and interdependent network. Thus, events in one part of the grid affect operation elsewhere, and extend beyond the grid to other systems reliant on stable power, much like what was observed in the 2003 Northeast Blackout [2]. Time-synchronized measurements such as the so-called synchrophasors produced by Phasor Measurement Units (PMUs) allow more accurate real-time estimation of the state of the power grid than do legacy sensors. The resulting reduced state uncertainty leads to (1) refined grid dynamical models for operations planning, which improves long-term grid reliability; and (2) increased grid capacity as utilities are enabled to operate with less conservative stability margins [1,3]. Ultimately, PMU-based energy management systems will be designed to anticipate failures, making it possible to take remedial actions before failures spread across the network [4].

PMUs rely on the Global Positioning System

Preprint of article published in the International Journal of Critical Infrastructure Protection, Vol. 5, December 2012

(GPS) for synchronization. This reliance creates a vulnerability to a particular type of malicious attack called GPS spoofing [5]. In 2001, the U.S. Department of Transportation (USDOT) evaluated the transportation infrastructure's GPS vulnerability and raised concern over the threat of GPS spoofers [6]. More recently, the North American Electric Reliability Corporation has recognized the vulnerability of the GPS-dependent U.S. power grid to GPS spoofing [7].

Spoofers generate counterfeit GPS signals that current civil GPS receivers are unable to distinguish from authentic GPS signals. The counterfeit signals can be used to commandeer a target receiver's tracking loops and induce spoofer-controlled time or position offsets. The USDOT report noted the absence of any off-the-shelf defense against civilian spoofing and recommended a study to characterize spoofing effects and observables. In 2008, researchers demonstrated that an inexpensive portable software-defined GPS spoofer could be built from off-the-shelf components, again highlighting the threat of spoofing [5].

In December, 2011, Northrop Grumman Information Systems and the University of Texas Radionavigation Laboratory jointly conducted a functional test and evaluation of the effects that spoofed GPS timing signals can have on synchrophasor measurements produced by PMUs. GPS spoofing attacks were performed, both through cable and over-the-air inside an RF shielded tent, against a GPS time reference receiver which sourced timing to a PMU. The goal of this exercise was to determine the extent of the adverse effects that spoofing can have on synchrophasor measurements and investigate the consequences of these effects on power grid management.

II. Background

A. Synchrophasors

As electric power grids continue to expand throughout the world and as transmission lines are pushed to their operating limits, the dynamic operation of the power system has become more of a concern and more difficult to accurately model. Moreover, effective real-time system control is now seen as a key to preventing wide-scale cascading outages like the 2003 Northeast Blackout [2,3].

For years, electric power control centers have inferred the state of the power system (the positive sequence voltage and angle at each network node) from indirect measurements, namely, power flows. But for improved accuracy in so-called power system state estimation, it will be necessary to feed existing estimators with a richer measurement ensemble or to measure the grid state directly [1, 3].

Alternating current (AC) quantities have been analyzed for over 100 years using the phasor construct developed by Steinmetz in 1893 [8]. A relatively new synchronization technique which allows referencing measured current or voltage phasors to absolute time was developed in the mid-1980s [9] and is currently being implemented throughout the world. The measurements produced by this technique are known as "synchronized phasor measurements" or "synchrophasors." Synchrophasors provide a real-time snapshot of current and voltage amplitudes and phases across a power system, and so, when drawn from a geographically dispersed set of nodes, can give a complete picture of the state of a power system at any instant in time. This makes synchrophasors useful for control, measurement, and analysis of the power system [1, 4].

In a typical deployment, synchrophasors are integrated in protective relays and are sampled from widely dispersed locations in the power system network. They are synchronized with respect to a common time source, Universal Coordinated Time (UTC), via GPS time reference receivers. In short, synchrophasors are basically measurements of AC voltage (or current) and absolute phase angle, made at a selected point and time in an electric transmission or distribution system.

B. GPS Spoofing

GPS spoofing is the act of producing a falsified version of the GPS signal ensemble with the goal of taking control of a GPS receiver's position-

velocity-time (PVT) solution. This is most effectively accomplished when the spoofer has knowledge of the GPS signal as seen by the target receiver so that the spoofer can produce a matched version of the signal [5, 6, 10–12]. In the case of military signals, this type of attack is nearly impossible because the military signal is encrypted and therefore unpredictable to a would-be spoofer [13]. On the other hand, the civil GPS signal is publicly-known and readily predictable.

In recent years, civil GPS spoofing is becoming recognized as a threat to critical infrastructure applications which rely heavily on the publicly-known civil GPS signal [14]. A number of promising methods are currently being developed to defend against civil GPS spoofing attacks [14–19], but it will be years before these technologies mature and see widespread implementation. Currently, there is a complete absence of any off-the-shelf defense against a GPS spoofing attack.

III. The Spoofer

The civil GPS spoofer used for the tests reported in this paper, shown in Fig. 1, is an advanced version of the spoofer first described in [5]. It is the only spoofer reported in open literature to date that is capable of precisely aligning the spreading codes and navigation data of its counterfeit signals with those of the authentic GPS signals. Such alignment capability allows the spoofer to carry out a sophisticated spoofing attack in which no obvious clues remain to suggest that an attack is underway. The spoofer is implemented on a portable software-defined radio platform with a digital signal processor (DSP) at its core. This platform comprises:

- A radio frequency (RF) front-end that down-mixes and digitizes a 2-MHz band around each of the GPS L1 and L2 frequencies.

- A DSP board that performs acquisition and tracking of GPS L1 C/A and L2C signals, calculates a navigation solution, performs real-time prediction of the the L1 C/A databits, and produces a consistent set of up to 14 spoofed GPS L1 C/A signals with a user-controlled fictitious implied navigation and timing solution.

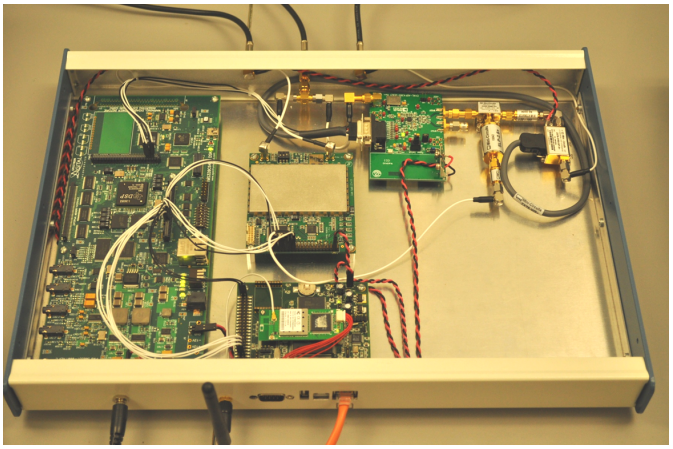

Fig. 1. The Civil GPS Spoofer.

- An RF back-end with a digital attenuator that up-converts the DSP-produced digital samples to analog output at the GPS L1 frequency with a user-controlled broadcast power.

- A single-board computer that handles communication between the spoofer and the user's control computer over the Internet.

The spoofer works by first acquiring and tracking GPS L1 C/A and L2C signals to obtain a navigation solution. It then enters a feedback mode in which it produces a counterfeit, data-free feedback GPS signal that is summed with its own RF input. The spoofer tracks the feedback signal and uses it to calibrate the delay between receipt of the authentic signals and production of the analog spoofed signals.

After feedback calibration is complete and enough time has elapsed to compile a navigation data bit library, the spoofer is ready to begin an attack. It produces signals that are initially nearly perfectly aligned with the authentic signals but with low enough power that they remain far below the target receiver's noise floor. The spoofer then raises the power of the spoofed signals slightly above that of the authentic signals. At this point, the spoofer has taken control of the target receiver's tracking loops and slowly leads the spoofed signals away from the authentic signals, carrying the receiver's tracking loops with it. Once the spoofed signals have moved more than 600 m in position or 2 μs in time away from the authentic signals, the target receiver can be considered completely

captured.

The spoofer and attack strategy have been tested against a wide variety of civil L1 C/A GPS receivers and has always been successful [20].

IV. Test Setup

The minimum threshold for success in the spoofing test exercise reported in this paper was to determine whether a GPS spoofer could force a PMU to violate the IEEE C37.118 Standard "Synchrophasors for Power Systems" [21]. This standard defines accuracy as the vector difference between the measured and expected value of the phasor for the measurement at a given instant of time, called the total vector error (TVE). TVE blends together three possible sources of error: magnitude, phase angle, and timing. A timing error appears identical to an error in phase angle. In the absence of timing and magnitude errors, a phase angle error of 0.573° corresponds to a 1% TVE, which is the maximum allowable TVE by the IEEE C37.118 Standard [22]. This phase angle error can be equivalently and indistinguishably induced by a timing error of 26.5 μs. This value was chosen as the threshold timing offset for a successful spoofing attack.

Figure 2 shows a schematic of the setup used for the over-the-air tests. Signals received via a rooftop antenna were routed to the spoofer for use in producing the counterfeit signals and separately to the RF shielded tent for retransmission. The counterfeit signals were also routed into the tent for transmission. In addition to the separate antennas transmitting the authentic and counterfeit signals, a third antenna was placed inside the tent to receive the combined authentic and spoofed signals. This setup is representative of an actual attack scenario in which the malefactor does not have physical access to the target receiver's antenna input but rather transmits the spoofed signals over-the-air from a remote location [23]. Figure 3 shows the tent's exterior; cables for the transmit and receive antennas are visible. Figures 4 and 5 show the transmit and receive antennas respectively as they were arranged at opposite ends of a support structure inside the tent.

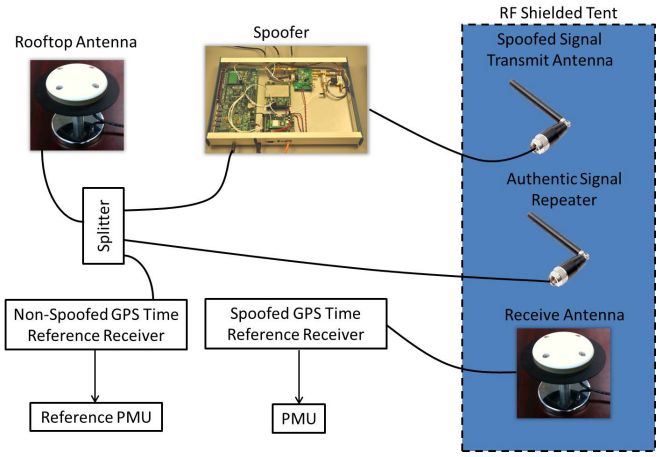

Fig. 2. Schematic of the test setup.

Fig. 3. RF shielded tent exterior with cables for the antennas.

In a second set of tests the authentic and spoofing signals were not transmitted over the air to the receive antenna; rather, in these cable-routed spoofing tests the setup inside the tent was replaced with a signal combiner that summed the authentic and spoofed signals.

The combined authentic and spoofed signals were fed to the target GPS time reference receiver. The output timing signal from the target receiver was used as the synchronization reference for one PMU, whereas a second PMU was given timing from a separate GPS time reference receiver that was tracking only authentic GPS signals. Since the PMUs were in the same room and measured the local voltage and carrier phasors, both PMUs would report approximately identical synchrophasors under normal circumstances. Thus, in the test any significant differences in the phase angle measurements between the two PMUs could be attributed to the effects of spoofing.

Fig. 4. Transmit antennas inside the RF shielded tent with one antenna for repeating the authentic signal and the other for broadcasting the spoofed signal.

Fig. 5. The receive antenna inside the RF shielded tent which was receiving both the authentic and spoofed signals to feed to the target receiver.

V. Test Results

Both the cable-routed and the over-the-air spoofing attacks were successful in forcing the synchrophasor measurements to diverge from their nominal values. Figure 6 shows the measured phase angle difference between the reference PMU, which was fed the true GPS signal, and the spoofed PMU throughout one entire test. This value would normally be less than a few degrees in the absence of spoofing, since the two PMUs are co-located. After the initial ten minute capture and carry-off, which proceeds slowly to avoid detection, the spoofer accelerates its timing carry-off and the reference and spoofed phase angles quickly diverge.

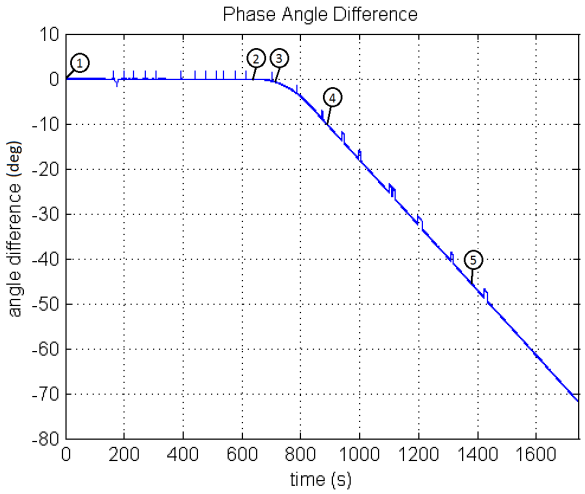

Fig. 6. A plot of the phase angle difference between the reference and the spoofed PMUs. Normally the phase angle difference would be nearly zero in the absence of a spoofing attack. Point 1 marks the start of the test. Point 2 marks the point at which the spoofer has completely captured the target receiver. Point 3 marks the point at which the IEEE C37.118 Standard has been broken. Point 4 marks the point at which the spoofer-induced velocity has reached its maximum value for the test. Point 5 marks the point at which the spoofed signal was removed.

Figure 7 shows pictures of an oscilloscope and the synchrophasor screen at the start of the test. The oscilloscope shows two pulse-per-second (PPS) signals, with the upper yellow pulse coming from a reference clock being fed true GPS and the lower blue pulse coming from the spoofed timing receiver. Both PPS signals are initially aligned with each other. The synchrophasor screen displays the PMU phase angle data in real-time as phasors with the nominal 60 Hz operating frequency subtracted from the phase angle. The red and green phasors show the phase data from the reference and spoofed PMUs respectively. These phasors are within a few degrees of each other at the beginning of the test.

Figure 8 shows pictures of the oscilloscope and the synchrophasor screen at about 620 seconds into the test. At this point, the spoofer has moved the target receiver 2 μs off in time and has completely captured the receiver. The delicate initial capture-and-carry-off is performed at a slow rate to suppress any evidence of the spoofer's presence. However, this process could be done quicker because the receiver was not looking for

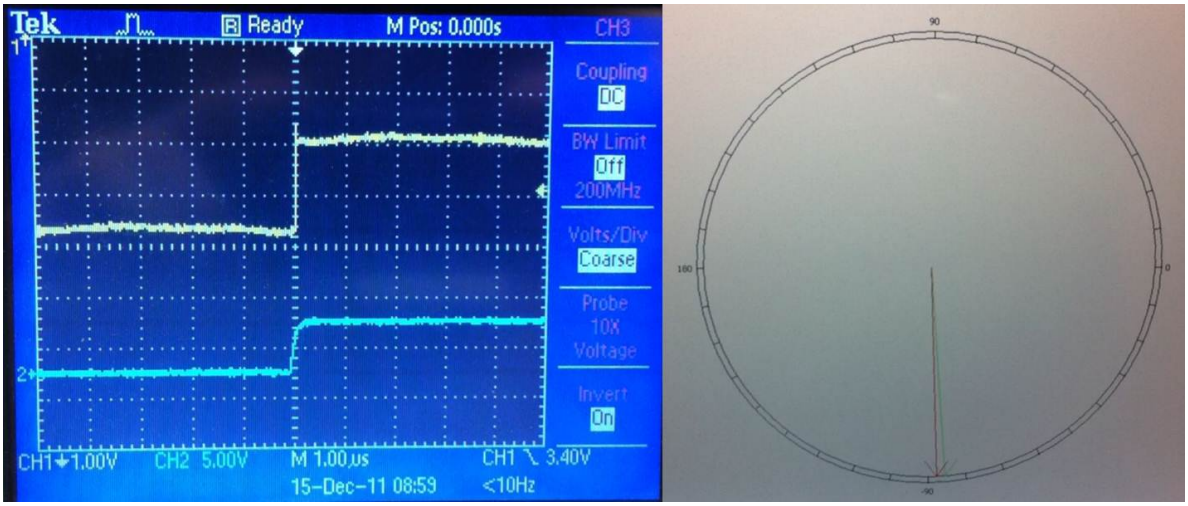

Fig. 7. Pictures of the oscilloscope (left) and synchrophasor (right) screen at the start of the test, which is marked as point 1 in Fig. 6.

such evidence of foul play. At this stage of the test, there is not yet any significant difference between the two phasors on the synchrophasor screen, since the spoofed time offset remains relatively small. The oscilloscope, however, reveals that the PPS output from the target receiver has moved by about 2 μs relative to the reference PPS. At this point, the spoofer begins to accelerate the target receiver's time solution at a distance-equivalent rate of 4 m/s^2 until it reaches a final distance-equivalent velocity of 1000 m/s. Distance-equivalent velocity can be converted into the actual time rate of change of time by dividing by the speed of light.

The acceleration segment of the attack must be tailored to the individual receiver's ability to track the spoofer-induced dynamics [20]. Otherwise, the spoofer risks loosing control of the target receiver's tracking loops by moving too quickly for the receiver to track or raising alarms. Alternatively, a malefactor could survey possible GPS time reference receiver's that might be used and tailor the spoofing attack such that any of the receivers would track and believe the spoofed signals. This would place severe limits on the spoofers ability to manipulate timing, but would not make the attack impossible or implausible.

Figure 9 shows pictures of the oscilloscope and the synchrophasor screen at about 680 seconds into the test. At this point, the spoofer has broken the IEEE C37.118 Standard for PMUs, which requires accuracy in the measured phase angle of 0.573° [22]. This demonstrates a significant vulnerability for PMU-based monitoring and control, since these applications leverage the accuracy supposedly guaranteed by the standard. There is yet no noticeable difference on the synchrophasor screen, but the oscilloscope clearly shows that the target receiver has now been offset in time by about 20 μs.

Figure 10 shows pictures of the oscilloscope and the synchrophasor screen at about 870 seconds into the test. At this point, the spoofer has reached its final velocity of 1000 m/s. A phase angle offset of 10° has also been introduced in a matter of minutes. As expected, there is a marked difference in the phasors on the synchrophasor screen. The oscilloscope also shows a time offset of 400 μs has been induced in the target receiver.

Figure 11 shows pictures of the oscilloscope and the synchrophasor screen at about 1370 seconds into the test. At this point, the spoofed signal was heavily attenuated and instantly realigned with the authentic signals. This was intended to be the end of the test, but when this particular receiver lost lock on the signal it continued to send out a valid time signal to the PMU while flywheeling off its internal clock. This caused an alarm to issue on the front panel of the time reference receiver indicating loss of GPS signal lock.

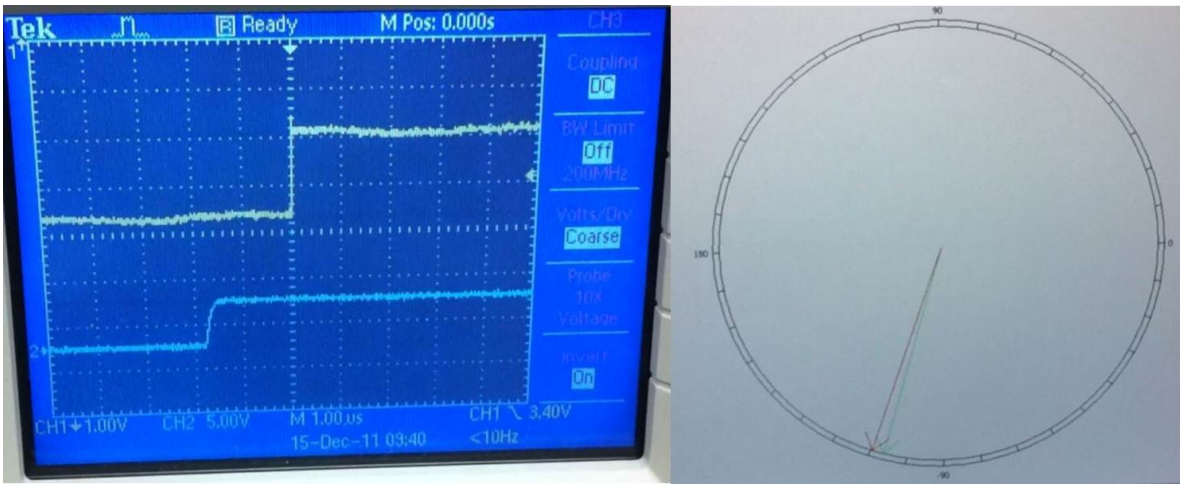

Fig. 8. Pictures of the oscilloscope (left) and synchrophasor (right) screen at about 620 seconds into the test, which is marked as point 2 in Fig. 6.

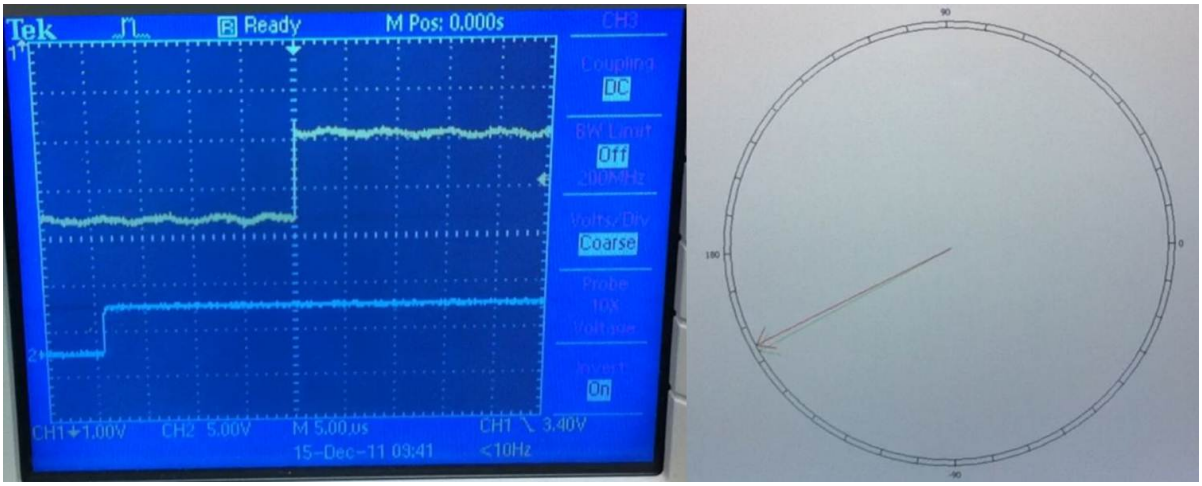

Fig. 9. Pictures of the oscilloscope (left) and synchrophasor (right) screen at about 680 seconds into the test, which is marked as point 3 in Fig. 6.

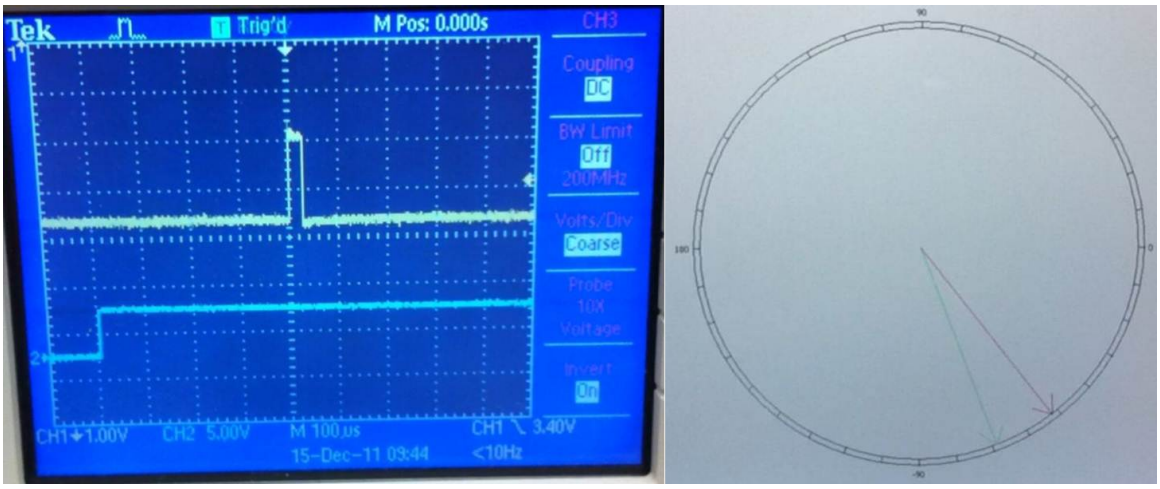

Fig. 10. Pictures of the oscilloscope (left) and synchrophasor (right) screen at about 870 seconds into the test, which is marked as point 4 in Fig. 6.

The downstream PMU, however, was oblivious to this loss of lock. This state persisted for about half an hour before the clock finally reacquired the authentic signal and instantly realigned its time output, which caused the phasors to realign. Figure 6 does not show the phase angle data for this entire period, but does show that the phase angle difference exceeds at least 70° before the time reference receiver reacquires the authentic signal.

VI. Implications for Synchrophasor-Based Control

Synchrophasor data provides a clear real-time picture of the state of the power system. As demands on power grids grow and stability margins are reduced to provide more distribution capacity, it will become desirable to use synchrophasors for control purposes [3]. PMU manufacturers are currently selling PMUs capable of implementing automated control schemes that offer response times less than 4 cycles. Such swift response times are seen as necessary to prevent grid instability or damage to equipment.

The simplest synchrophasor-based control scheme relies on phase angle differences between two PMUs as an indicator of a fault condition. Such a control scheme has been implemented on the Chicoasen-Angostura transmission link in Mexico [24]. This transmission line links large hydroelectric generators in Angostura to large loads in Chicoasen through two 400-kV transmission lines and one 115-kV transmission line. If a fault occurs in which both of the 400-kV lines are lost, then the hydroelectric generators may experience angular instability. To prevent this, two PMUs were deployed, one at each end of the transmission line, with a direct communications link between them. It was found that under nominal and single-fault (only one 400-kV line lost) conditions, the phase angle difference between the two locations was less than 7°, whereas a double-fault (both 400-kV lines lost) produced a phase angle difference of 14°. Based on this finding, the PMUs have been configured to automatically trip the hydroelectric generators when the phase angle difference exceeds 10°.

If a spoofer were to attack this system in Mexico or a similar implementation elsewhere, then the spoofer could cause a generator trip. In the test described in the previous section, a 10° offset, the threshold for the Chicoasen-Angostura link, was induced by the spoofer about 250 seconds after capturing the target receiver, as seen in Figs. 6 and 10. A malefactor could even lead the phase angle off in the opposite direction (say 7°) before cutting both 400-kV transmission lines. Instead of causing a generator to unnecessarily trip, this would prevent PMUs from tripping the generator when required and potentially cause damage to the generator or remaining transmission lines.

Beyond tripping a single generator, there is potential for the effects of the attack to propagate through the grid and cause cascading faults across the grid. One example of this type of cascading failure is the 2003 Northeast Blackout. Although this blackout did not involve PMUs nor a spoofing attack, it demonstrates how an appropriately targeted attack against PMUs used for control on the power grid could cause large scale blackouts that originate with a single generator or transmission line trip. On Aug. 14, 2003 at 3:05 p.m., a 345-kV transmission line in Ohio began to sag from increased flow of electric power. When the line sagged too close to a tree, it caused a short-to-ground and tripped offline. This is something that happens fairly frequently on the massive U.S. electrical grid and is usually easily dealt with. However, the tripping of that line in northern Ohio began a cascade of failures that, in a little more than an hour, led to a near total power loss for more than 50 million people in the northeastern U.S. and parts of Canada. The blackout is estimated to have cost approximately 6 billion U.S. dollars for only four days of power loss [2]. This led the Department of Energy and the North American Electric Reliability Corporation to fund and push for an improved "smart grid" with synchrophasor technology as a major component.

VII. Conclusions

Test results presented herein indicate that GPS spoofing poses a threat to the integrity of synchrophasor measurements. A spoofer can introduce a time error in a phasor measurement unit

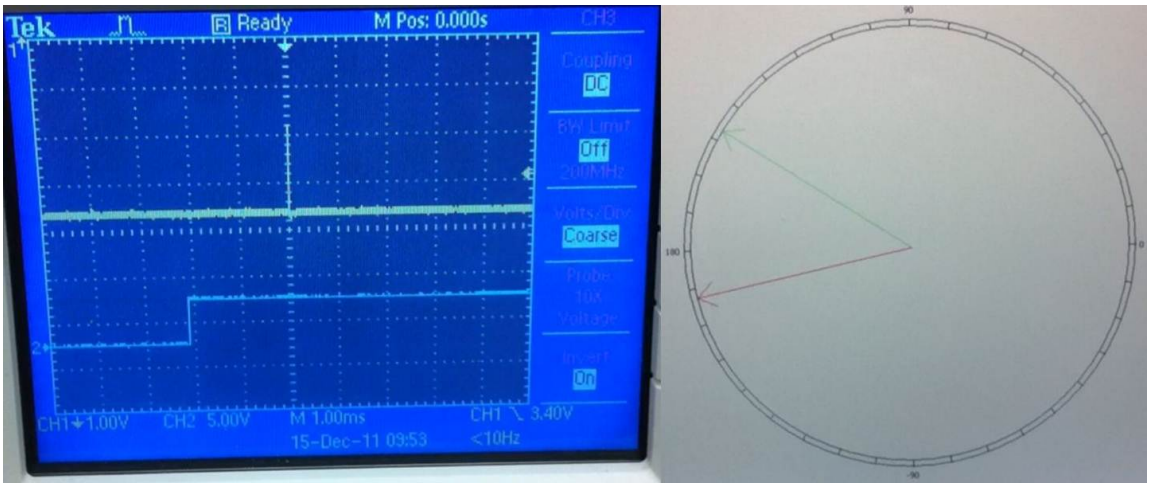

Fig. 11. Pictures of the oscilloscope (left) and synchrophasor (right) screen at about 1370 seconds into the test, which is marked as point 5 in Fig. 6.

(PMU) without having physical access to the PMU's GPS time reference receiver. This timing error produces a corresponding phase error in the synchrophasor data coming from that PMU. It was demonstrated that a PMU could be made to violate the IEEE C37.118 standard for synchrophasors in about 11 minutes from the start of a spoofing attack.

As PMU usage continues to grow throughout the world, PMUs will increasingly be used for automatic control purposes instead of just grid monitoring. An example of this is a currently operational system in Mexico which automatically trips a generator if the phase angle difference between PMUs at two particular locations exceeds 10°. The tests discussed in this paper demonstrate that a spoofer could cause control schemes such as the one in Mexico to falsely trip a generator. In the presence of other exacerbating factors, this could lead to a cascade of faults within the power grid.

References

[1] Authors, V., "Real-Time Application of Synchrophasors for Improving Reliability," Tech. rep., North American Electric Reliability Corporation, Oct. 2012.

[2] "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," Tech. rep., U.S.-Canada Power System Outage Task Force, April 2004.

[3] Giri, J., Sun, D., and Avila-Rosales, R., "Wanted: A more intelligent grid," *IEEE Power & Energy*, April 2009, pp. 34–40.

[4] Phadke, A. G. and Thorp, J. S., editors, *Synchronized Phasor Measurements and Their Applications*, Springer, New York, 2008.

[5] Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., and Kintner, Jr., P. M., "Assessing the spoofing threat: development of a portable GPS civilian spoofer," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Savannah, GA, 2008.

[6] Anon., "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," Tech. rep., John A. Volpe National Transportation Systems Center, 2001.

[7] Anon., "Extended loss of GPS Impact on Reliability," Tech. rep., North American Electric Reliability Corporation, July 2012.

[8] "Charles P. Steinmetz," http://www.britannica.com/EBchecked/topic/565056/Charles-Proteus-Steinmetz.

[9] Phadke, A., Pickett, B., Adamiak, M., Begovic, M., Benmouyal, G., Burnett Jr, R., Cease, T., Goossens, J., Hansen, D., Kezunovic, M., et al., "Synchronized sampling and phasor measurements for relaying and control," *IEEE Transactions on Power Delivery*, Vol. 9, No. 1, 1994, pp. 442–452.

[10] Scott, L., "Anti-spoofing and authenticated signal architectures for civil navigation systems," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Portland, Oregon, 2003, pp. 1542–1552.

[11] Wesson, K. D., Rothlisberger, M. P., and Humphreys, T. E., "A Proposed Navigation Message Authentication Implementation for Civil GPS Anti-Spoofing," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Portland, Oregon, 2011.

[12] Humphreys, T. E., Shepard, D., Bhatti, J., and Wesson, K., "A Testbed for Developing and Evaluating GNSS Signal Authentication Techniques," 2012, in preparation; available at `http://radionavlab.ae.utexas.edu/testbed`.

[13] Humphreys, T. E., "Detection Strategy for Cryptographic GNSS Anti-Spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, 2011, to be published; available at `http://radionavlab.ae.utexas.edu/detstrat`.

[14] Humphreys, T. E., "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," `http://homeland.house.gov/sites/`

homeland.house.gov/files/Testimony-Humphreys.pdf, July 2012.

[15] Wesson, K., Shepard, D., and Humphreys, T., "Straight Talk on Anti-Spoofing: Securing the Future of PNT," *Inside GNSS*, Jan. 2012.

[16] Wesson, K., Rothlisberger, M., and Humphreys, T. E., "Practical Cryptographic Civil GPS Signal Authentication," *NAVIGATION, Journal of the Institute of Navigation*, 2012, to be published; available at http://radionavlab.ae.utexas.edu/nma.

[17] Psiaki, M., O'Hanlon, B., Bhatti, J., Shepard, D., and Humphreys, T., "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals," *IEEE Transactions on Aerospace and Electronic Systems*, 2012, to be published; available at http://web.mae.cornell.edu/psiaki/.

[18] Montgomery, P. Y., Humphreys, T. E., and Ledvina, B. M., "A Multi-Antenna Defense: Receiver-Autonomous GPS Spoofing Detection," *Inside GNSS*, Vol. 4, No. 2, April 2009, pp. 40–46.

[19] Nielsen, J., Broumandan, A., and LaChapelle, G., "Method and system for detecting GNSS spoofing signals," May 31 2011, US Patent 7,952,519.

[20] Shepard, D. and Humphreys, T. E., "Characterization of Receiver Response to a Spoofing Attack," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Portland, Oregon, 2011.

[21] "IEEE Standard for Synchrophasors for Power Systems," 2005, IEEE Std. C37.118 Revision 1344–1995.

[22] Martin, K. E., Hamai, D., Adamiak, M. G., Anderson, S., Begovic, M., Benmouyal, G., Brunello, G., Burger, J., Cai, J. Y., Dickerson, B., Gharpure, V., Kennedy, B., Karlsson, D., Phadke, A. G., Salj, J., Skendzic, V., Sperr, J., Song, Y., Huntley, C., Kasztenny, B., and Price, E., "Exploring the IEEE Standard C37.118–2005 Synchrophasors for Power Systems," *IEEE Transactions on Power Delivery*, Vol. 23, No. 4, Oct. 2008, pp. 1805–1811.

[23] Shepard, D. P., Humphreys, T. E., and Fansler, A. A., "Going Up Against Time: The Power Grids Vulnerability to GPS Spoofing Attacks," *GPS World*, Aug. 2012.

[24] Schweitzer, E. O., Guzman, A., Altuve, H. J., and Tziouvaras, D. A., "Real-Time Synchrophasor Appliactions for Wide-Area Protection, Control, and Monitoring," Tech. rep., Schweitzer Eng. Laboratories, 2009.