Detection of Time Spoofing Attacks on GPS Synchronized Phasor Measurement Units

Andrew K. Mattei, *Member, IEEE,* W. Mack Grady, *Fellow, IEEE,* P. Jay Caspary, *Member, IEEE,* and Scott A. McBride, *Member, IEEE.*

***Abstract*—This paper builds a foundation for detecting spoofed GPS signals through multiple PMU comparison. Frequency measurements from PMUs in ERCOT and the Eastern Grid are used as the basis for calculations and simulated GPS signal time shifts. When PMUs in a single control area are compared, the difference between the individual PMU's frequency-based integrated time error and the average time error between PMUs is small, but when forced by a spoofed time-shifting signal, this difference becomes significant and detectable. Positive and negative phase angle shifts are considered, and an example of calculations during a significant power system transient is shown. The detection of fast or slow time-shifting events is possible by using a sliding averaging window with the frequency measurements.**

***Index Terms*-- global positioning system, phasor measurement units, power system protection, power system reliability, smart grids, substation automation, wide area measurements.**

I. Introduction

Global Positioning System-based time clocks have become standard equipment in most electric power substations. Their primary purpose is to synchronize internal clocks of microprocessor-controlled protective relays. Time synchronization of protective relays allows for accurate sequence-of-events analysis when multiple relays are being examined after an event.

Some of these protective relays are now being called upon to perform a second function: to act as a phasor measurement unit (PMU). As a PMU, the relay provides time-synchronized voltage magnitudes and phase angles, current magnitudes and phase angles, and frequency measurements to a secondary location such as a control center. This control center collects a constant stream of data from multiple PMUs, with each PMU sending 30 or more measurements per second.

This concentration of multiple high-speed streams of data allows for software in a control center to process or display power system data for utilization by programs or for observation and action by system operators. Of particular interest is the phase angle difference between PMU locations. The phase angle difference between two or more locations reflects the direction of power transfer between locations.

The PMU, or in many cases the protective relay at a substation, relies on its local GPS time source for the calculation of phase angles. When a system operator, software program, or another protective relay makes a decision to operate a device based on angular difference between two different PMUs, it is essential that the data being received are valid. The IEEE C37.118 Synchrophasor Measurement Standard specifies for performance and indicators for time quality [1], but this assumes the signals being received are from genuine GPS satellites. A problem arises if an attacker time-shifts the GPS signals at a substation. With this time-shift, the attacker would be able to change the phase angle calculation and potentially cause the execution of a decision based on an intentionally erroneous phase angle difference.

This paper introduces the theory behind a method that may be employed to detect a time-shifting attack on a GPS time source at a location where a phasor measurement unit is active. If such an attack is detected, the data can be marked as invalid and any control schemes based on this data can be disabled.

II. Reality Check: The GPS Spoofing Attack

GPS signal spoofing devices can be classified into three categories by [2]. The first is the "simplistic" type, which are commercial signal generators that can be purchased or rented for testing purposes. The second is "intermediate", which is capable of generating a false signal based on a slow shift away from a retransmitted actual signal. The third category is "sophisticated", which involves synchronizing signals with actual GPS signals and other nearby GPS spoofing devices.

The simplistic attack will fail in substation applications because it would not be synchronized with the existing network of satellites that the substation's GPS clock is also monitoring, so the signal would be ignored. The sophisticated attack requires significant time and effort to develop, and while possible, is highly improbable because it requires simultaneous spoofing at multiple locations. The most likely attack against GPS receivers would be the intermediate level. This level of development has been demonstrated in controlled tests by [3] and should be considered as a plausible scenario.

This work was supported in part by the Electric Power Research Institute (EPRI), the Southwest Power Pool (SPP), Idaho National Laboratories, Brazos Electric Power Cooperative, and Schweitzer Engineering Laboratories.

A. K. Mattei is a PhD student at Baylor University, Waco, TX 76777 USA (Andrew_Mattei@baylor.edu).

W. M. Grady is a professor in the Department of Electrical and Computer Engineering, Baylor University, Waco, TX 76777 USA (Mack_Grady@baylor.edu).

P. J. Caspary is the Director of Research, Development, & Special Studies at Southwest Power Pool, Little Rock, AR 72223 USA (JCaspary@spp.org).

S.A. McBride is the Director of The Department of National & Homeland Security, Critical Infrastructure Protection & Resilience Division at the U.S. Department of Energy's Idaho National Laboratory.

This paper is presented to the Texas A&M Conference for Protective Relay Engineers, College Station, TX, April 7, 2016.

GPS antennas that are used in electric utility substations require a clear line of sight to the sky and must be mounted outdoors, but not necessarily with significant elevation. Frequently the antenna is mounted on a piece of electrical conduit attached to an outside wall of the substation control house. Because of this lack of elevation and obvious placement, a spoofing antenna could be located nearby without exerting extraordinary effort.

The test attack scenario involving a GPS clock and PMU in [3] was performed inside an RF shielded tent, largely because of the legal difficulties involved with openly transmitting false GPS signals. It is unknown if the same attack would be as effective against an unshielded GPS receiver in an electric substation, but it is assumed that the system used in the test could be made portable and would likely be effective against a nearby receiver antenna.

Technical questions aside, perhaps the biggest defense mechanism of a synchrophasor network is that it exists as a network of devices. Seldom would a PMU be operated as a standalone device. Rather, the PMU serves as a node in a network of many devices. This network of devices contains a common element that can be monitored continuously and individual node deviation can be detected. The common element is the frequency of the grid itself.

III. Frequency and the US Electric Grid

The United States electric grid is divided into multiple regions, with each region having one or more Balancing Authorities [4]. Each Balancing Authority is required to maintain the frequency within their region in order to minimize frequency bias and estimated area control error (ACE) [5]. Within each of these control areas, measured frequency throughout the Balancing Authority's control area is very consistent when measured by multiple PMUs.

A. The ERCOT Region

The ERCOT region in Texas acts as a single control area. Three PMUs were monitored for eight days, at a data collection rate of 30 samples per second. These PMUs are located approximately 400 miles from each other in a triangular layout – one in Central Texas (Baylor University, Waco), one in South Texas (University of Texas - Pan America, Edinburgh), and one in West Texas (McDonald Observatory, Fort Davis). Each of these PMUs is connected to a 120 volt wall outlet for monitoring. Distribution voltage level does result in slightly more noise in the signal, but it has proven to be an effective location for grid frequency, per unit voltage, and phase angle measurement [6].

Overall, the one-minute average ERCOT grid frequency varies throughout the day, primarily between 59.97 and 60.03 Hz. An eight day graph of the one-minute average for a single ERCOT location is shown in Figure 1.

When graphed as an individual data point, the frequency measurement of a lone PMU appears dispersed and scattered. However, when considered as a network with other PMUs, the difference in measured frequency between the PMUs becomes very small. Figure 2 shows the same time period as Fig. 1, but with the one-minute average difference between three PMUs.

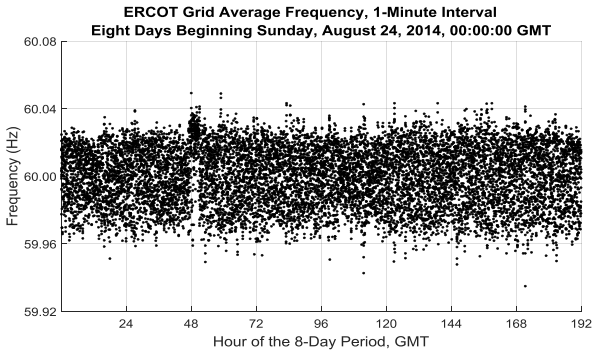

Fig. 1. ERCOT one-minute average frequency (Hz)

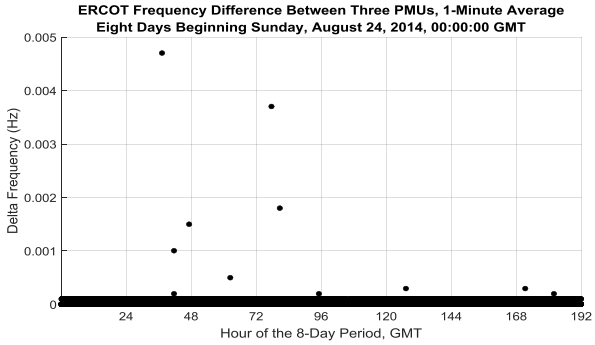

Fig. 2. ERCOT one-minute average difference between frequency measurements (Hz)

These results show that within a single control area the average difference between PMU frequency measurements is near zero. Only five minutes out of 11,520 were above 0.001 Hz in difference.

B. The Eastern Grid

Similar observations were performed using four PMUs in the Eastern Grid. The reference PMU for these measurements was located near Washington, D.C. Once again, the majority of the measurements were between 59.97 and 60.03 Hz. An eight day graph of the one-minute average for this Eastern Grid PMU is shown in Figure 3.

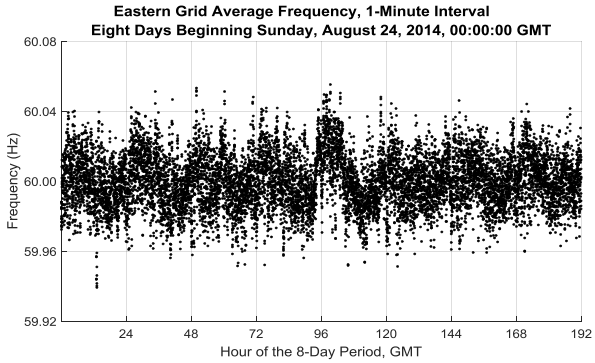

Fig. 3. Eastern Grid one-minute average frequency (Hz)

The Eastern Grid frequency is synchronized overall, but it is not a single control area like ERCOT and is much larger in scale, so slight variations due to frequency bias between Balancing Authority control areas are expected. The four PMUs under observation in this example are not in the same control area, so there is slightly more variation between their average frequency measurements. An eight day graph of the one-minute average difference for the Eastern Grid PMUs is shown in Figure 4.

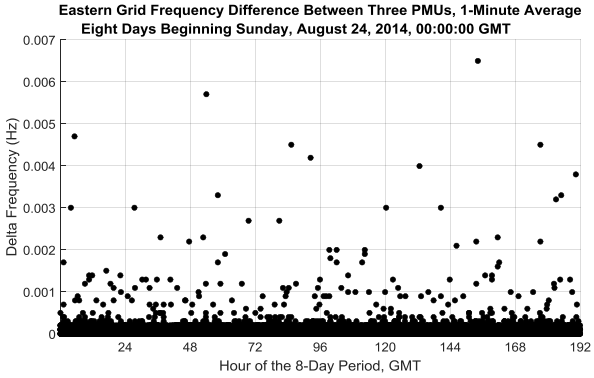

Fig. 4. Eastern Grid one-minute average difference between frequency measurements (Hz)

For the Eastern Grid, there were 83 minutes out of the 11,520 shown where the difference between one-minute average frequency measurements was greater than 0.001 Hz. The additional variations seen in Fig. 4 are the result of measurements across multiple control areas.

IV. Frequency and Time Error Correction

Time error in the electric grid is a result of the frequency deviating from 60 Hz. If the grid were capable of a constant 60.000 Hz, then a clock based on grid frequency would increment exactly one second every 60 cycles. However, because the electric grid is constantly balancing generation with load [5], the grid frequency is continuously moving slightly above or slightly below 60 Hz as shown in the previous section. This movement above and below 60 Hz introduces a concept called time error.

The National Electric Reliability Corporation (NERC) provides a formula relating time error to average grid frequency over a period of time [5].

$$TimeError = \frac{f - 60.000}{60} * time \qquad (1)$$

In (1), *time* is the elapsed time interval in seconds and *f* is the average frequency in Hz over the interval. This formula can be used to approximate time error across a short or long interval of time. For example, if the average frequency is 60.02 Hz over the duration of one hour, the time error would be 1.2 seconds.

V. Applying Synchrophasors to Time Error Correction

Common synchrophasor data streams are capable of providing time aligned frequency measurements at rates of up to 60 times per second. The time error equation from (1) can be rewritten as a set of *n* frequency measurements *f* being collected at S_{RATE} samples per second, as shown in (2).

$$TimeError = \frac{\frac{\sum_{i=1}^{n} f_i}{n} - 60.000}{60} * \frac{n}{S_{RATE}} \qquad (2)$$

A common measurement rate for synchrophasors is 30 samples per second. When applied to (2), the average time error across this single synchrophasor measurement is calculated with equation (3):

$$TimeError = \frac{f - 60.000}{60} * \frac{1}{30} \qquad (3)$$

The result of (3) is typically a very small number, representing a very small time error across 0.033 seconds. Time aligned PMU frequency measurements may have the appearance of varying slightly between PMUs and not being equal across a span of time, but when their time error values are integrated across some time period, that is a summation of individual values using (3). The resulting integrated time error (ITE) value is highly consistent across a set of PMUs that reside within a common control area.

VI. Single Control Area Time Error

Four phasor measurement units are chosen as representative samples within the ERCOT control area. Three of these were listed previously, with the fourth in Austin, Texas. The Austin PMU is connected to a voltage transformer on a high voltage bus at a substation. All PMUs transmit time-aligned frequency measurements at the rate of 30 measurements per second.

Table 1 contains the integrated time error measurements based on (3). The one minute and five minute integrated time errors are listed along with the differences between the average of the four PMU time errors and the individual measurement. The electric grid was at a normal steady state during these measurements (measurement date: 5/28/2015, 12:30 pm – 12:35 pm GMT).

TABLE I
Integrated Time Error (ITE) for ERCOT Single Control Area PMUs

Interval	Austin	Waco	S. Texas	W. Texas
1 Min. ITE	0.00909428	0.0090914	0.00909106	0.00909594
5 Min. ITE	-0.02076239	-0.0207712	-0.02077522	-0.02073206
1 Min. Diff	-0.0000011	0.0000017	0.00000216	-0.00000276
5 Min. Diff	0.00000217	0.000011	0.000015	-0.00002817

Table 2 contains similar time error measurements and

difference from the average based on equation (3) from four PMUs located in the Southwest Power Pool (SPP), which is in the Eastern Grid and operates as a single control area. Geographically, these PMUs are located hundreds of miles apart in the central United States. The electric grid was at a normal steady state during these measurements (measurement date: 5/28/2015, 12:30 pm – 12:35 pm GMT).

TABLE II
ITE for SPP Single Control Area PMUs

Interval	PMU1	PMU2	PMU3	PMU4
1 Min. ITE	-0.01461661	-0.0146087	-0.0146062	-0.0146171
5 Min. ITE	-0.01168711	-0.0117129	-0.0116756	-0.0117692
1 Min. Diff	0.00000447	-0.0000035	-0.0000059	0.0000049
5 Min. Diff	-0.0000241	0.0000017	-0.0000356	0.000058

Tables 1 and 2 show that the difference in time error within single control areas during steady state conditions results in very little time error between PMUs.

VII. GPS Spoofing and Time Error

The ultimate goal of a GPS spoofing attack is to have control of the clock that the PMU uses to calculate system frequency. Once the clock is under an attacker's control, the output of the one pulse-per-second IRIG-B clock signal may be modified to provide a pulse that is slightly longer or slightly shorter than one second. This change in the clock signal introduces a time error in calculated frequency, which then propagates to an error in the phase angle calculation for voltage and current phasors. Individual PMUs will not realize that their clocks have been compromised. However, three or more PMU time error corrections within a single control area can be compared and clock differences will become evident very quickly.

A. Characteristics of an Attack

Reference [3] published details of an experimental attack on the GPS clock source for a PMU. This involved seizing control of the GPS clock and then decreasing the interval for the one pulse-per-second clock signal. The voltage phase angle was monitored during the attack and as the attack occurred, the voltage phase angle was slowly shifted away from the reference phase angle at a constant rate of approximately -4.2 degrees per minute. If a system frequency of 60.000 Hz is assumed, a shift of -4.2 degrees per minute is the equivalent of 60.00019445 Hz – which appears as a very small frequency differential. This calculation is shown in (4).

$$f = \frac{60.000}{1 + \frac{-4.2}{60 * 60 * 360}} = 60.00019445 \qquad (4)$$

Applying equation (1) to this one-minute frequency average in (4) yields an estimated time error of 0.00019445 seconds. While this time error appears small, when compared to the one-minute time errors listed in Tables 1 and 2, this value is 37 times larger than the largest of the time errors in Table 2, and 33 times larger than the largest average one-minute time error shown in Table 1.

These frequency differentials are so small in magnitude they would likely be overlooked by human operators if basing decisions on frequency values alone. For example, Table 3 contains frequency differential values for several degree-per-minute change rates. These rates of change, while small, add up over time and can be detected.

TABLE III
Frequency Differential for Degrees per Minute Change

Degrees per Minute	Frequency Differential
1	0.0000462963
2	0.0000925927
4	0.000185186
5	0.000231482
8	0.000370373
10	0.000462967
20	0.00092594
50	0.002314904

B. Comparing the Data

The detection of an attack relies on being able to quickly and effectively compare measured time error values. For a time error correction measurement that measures close to the average, the value will be very small, and as the time error correction for an individual PMU measurement deviates farther from the average value, the deviation becomes very noticeable.

Figure 5 is a graph for one hour of data of the difference between the 30-second integrated time error and the average time error for four PMUs in ERCOT. The values are dispersed primarily below 0.00002 seconds.

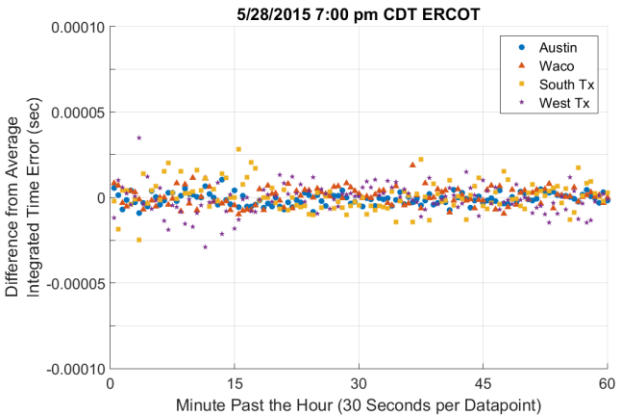

Fig. 5. 30-Second Difference from Average Integrated Time Error in ERCOT, one hour span.

Similarly, Figure 6 is a graph for the SPP region.

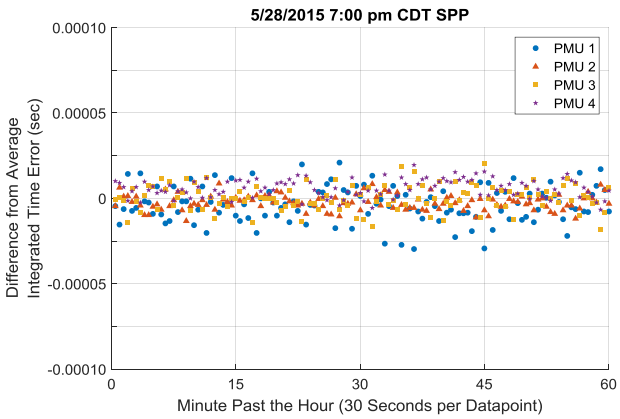

Fig. 6. 30-Second Difference from Average Integrated Time Error in SPP, one hour span.

C. Detecting an Attack

The frequency shift induced by a GPS attack will result in a measurable and observable change in both the average value for the set of PMU measurements and the individual PMU under attack. To simulate this, an attack based on [3], a shift of -4.2 degrees per minute, can be performed by scaling one PMU's frequency measurement by the value shown in (5).

$$Scaling = \frac{60.00019445}{60.000} * f = 1.000003241 f \qquad (5)$$

The value in (5) is a very small scaling factor. However, when applied to a series of frequency measurements, it produces enough change to be detectable. Figure 7 shows the same data as Fig. 5, but with a simulated 3-minute attack on the Austin PMU based on (5) occurring at the 30 minute (60th sample) mark.

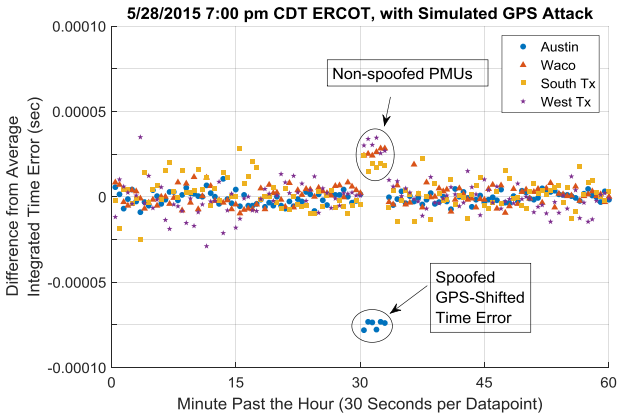

Fig. 7. 30-Second Difference from Average Integrated Time Error in ERCOT with simulated GPS attack, one hour span.

Likewise, a simulated GPS attack on the PMU1 PMU during the same time period is shown in Fig. 8.

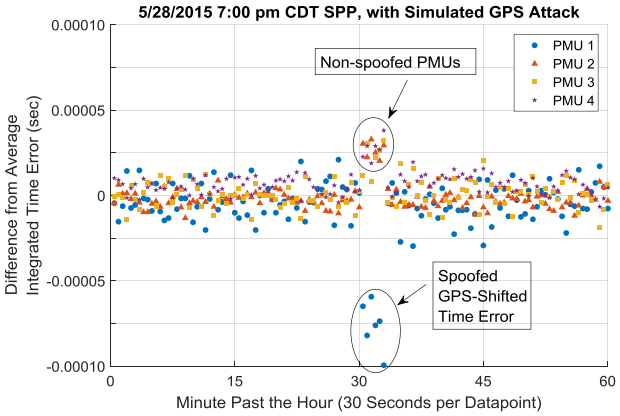

Fig. 8. 30-Second Difference from Average Integrated Time Error in SPP with simulated GPS attack, one hour span.

D. Observation Windows

For the previous example, an observation window of 30 seconds was chosen because of the slow rate of change for the given time shift. By their very nature, however, attacks are unpredictable, and may require different observation windows to capture different rates of change.

For example, a more aggressive -50 degree per minute (*Scaling*>1.0 in (5)) attack is detectable within a few seconds. Figure 9 shows a 15-second interval of GPS-Shifted time error with one minute of steady-state readings on either side of the simulated attack. If measured and averaged as part of a standalone 30-second window, this attack would appear as a single outlying data point.

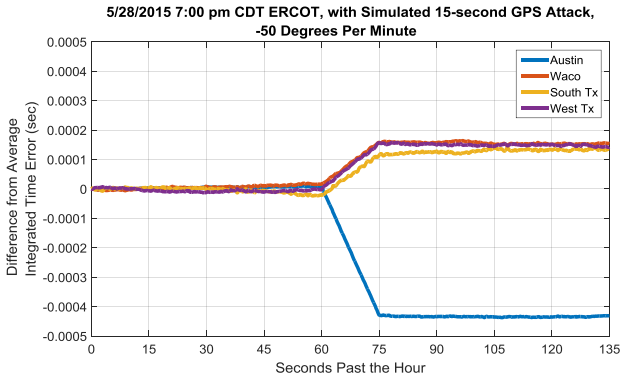

Fig. 9. Simulated -50 Degree Per Minute Aggressive Attack, 15-second Duration, Continuous Summation.

A +2 degree per minute (*Scaling*<1.0 in (5)) attack appears as a much more gradual slope. In Fig. 10, the GPS-Shift begins at the 60-second mark and continues for ninety seconds. A short sampling period would not be as effective in detecting this slow shift.

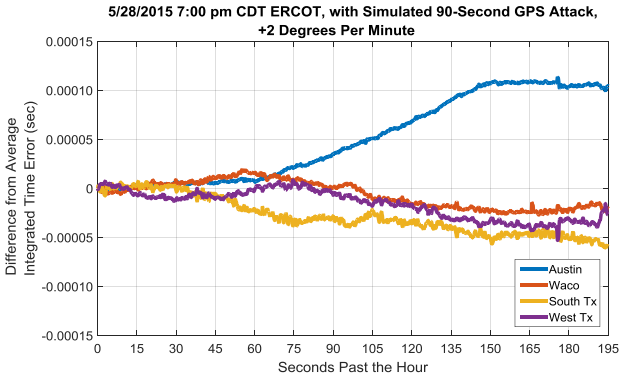

Figure 10. Simulated +2 Degree Per Minute Attack, 90-second Duration, Continuous Summation.

The values shown in Figures 9 and 10 are based on a continuous summation of the integrated time error.

Another way of monitoring the incoming data associated with Figures 9 and 10 is by utilizing a sliding window. When integrating time error, as in Figures 9 and 10, the shifted value remains offset from the other values. When using a 30-second sliding integration window, the shift becomes visible during the transition period, but is then removed as the forced shift is halted. Figures 11 and 12 use the data from Figures 9 and 10, but with a 30-second sliding window.

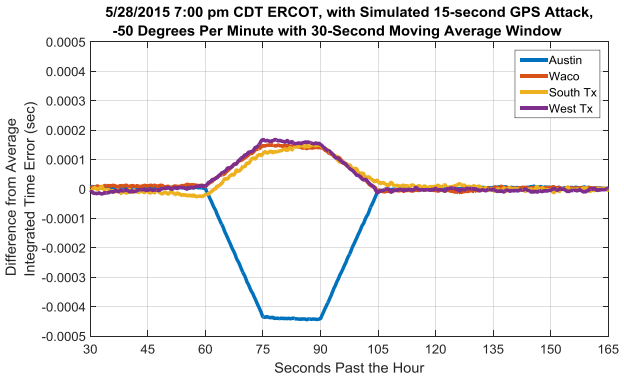

Fig. 11. Simulated -50 Degree Per Minute Aggressive Attack, 15-second Duration, 30-second Moving Average Window.

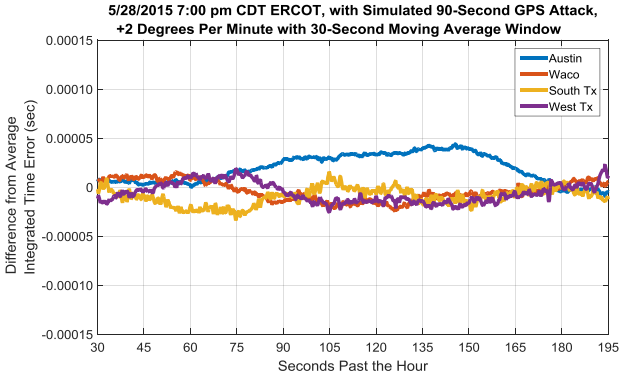

Fig. 12. Simulated +2 Degree Per Minute Attack, 90-second Duration, 30-second Moving Average Window.

VIII. Transient Period Response

Power system transients are the result of sudden changes in the operating characteristics of grid-connected devices. These changes often result in a change in frequency away from the 60 Hz center frequency for a period of time. Because the frequency changes can be rapid and dramatic, applying the previous frequency-based calculations to a faulted period is worthy of investigation.

The transient in this example occurred in ERCOT on May 27, 2015, at 8:32 PM, when 764 MW of generation tripped offline. The system frequency declined to 59.856 Hz, and recovery took several minutes. Figure 13 shows the frequency response recorded by the four ERCOT PMUs.

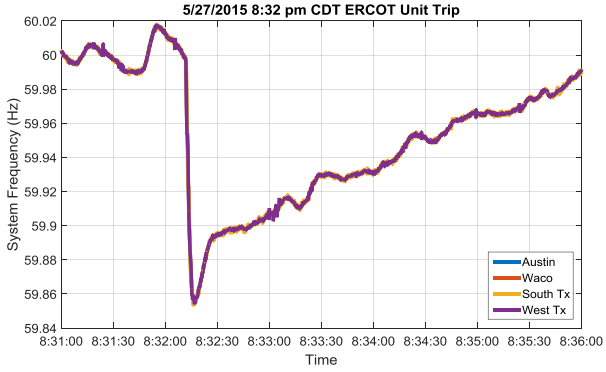

Fig. 13. ERCOT Unit Trip, 5/27/2015.

Applying the Integrated Time Error method to the four ERCOT PMUs, the transient results in time error values that appear different from the steady state. The resulting time error values spread above and below the zero error axis, as shown in Figure 14, and do not quickly trend back together.

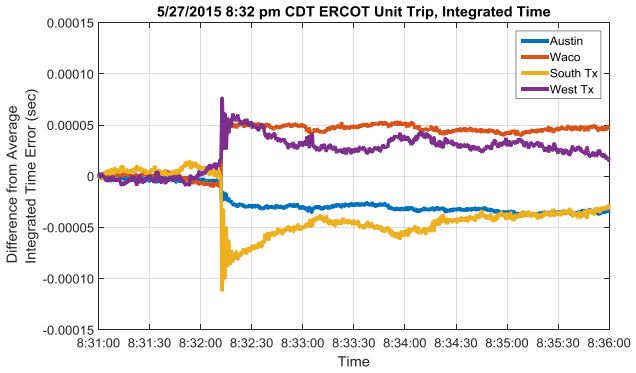

Fig. 14. PMU Difference from Integrated Time Error, ERCOT Grid Transient, 5/27/2015.

Finally, applying a sliding 30-second window to the fault results in the time error values returning to the zero error axis, as shown in Figure 15.

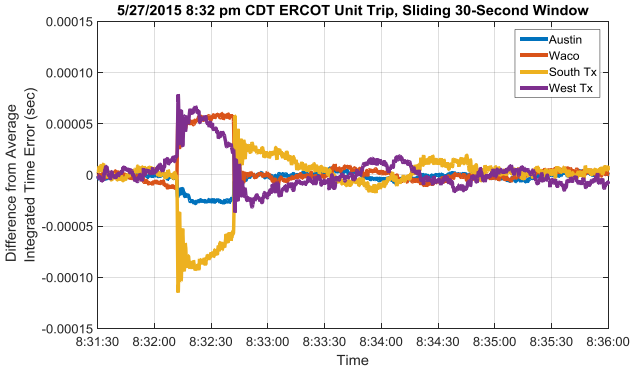

Fig. 15. PMU Difference from Average Integrated Time Error, 30-second Sliding Window, ERCOT Grid Transient, 5/27/2015.

During transient periods, the magnitude of the Integrated Time Errors equal or exceed the magnitude of the measurements associated with GPS-shifted signals. Because of this, detection based solely on specific target values is insufficient for detecting time-shifting.

IX. Discussion of Observations

A. Grouping of PMUs for Spoofing Detection

As mentioned previously, the PMUs being averaged together should reside in the same control area in order to minimize frequency variation between samples. Within an area like ERCOT this selection is simplified, but for the Eastern and Western grids, this makes PMU selection slightly more complicated. While the frequency of the overall grid is the same, the minor variations between control areas can impact the calculations used to detect clock drift.

An example of this is to add a fifth PMU to the Eastern Grid measurements. This PMU is within the same grid, but is operating in a different control area. This PMU is an outlier and its measurements are shown in Fig. 16. The frequency measurements provided by the node PMU5 vary slightly from the other example PMUs in the Eastern Grid. Nearly all of the integrated time difference exists as a positive difference from the average reflecting its exclusion from the control area that includes the other four PMUs.

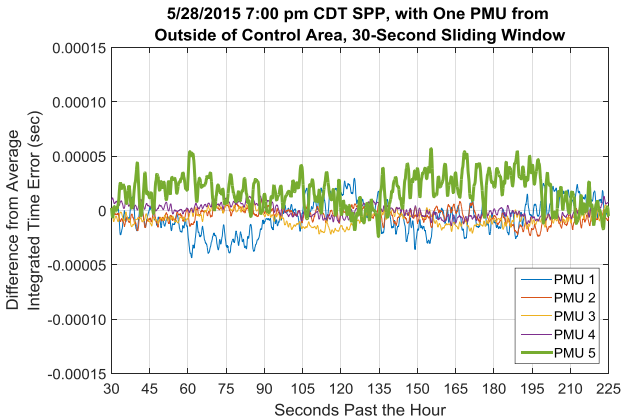

Fig. 16. PMU "PMU 5" from Outside of Control Area, 30-second Sliding Window

B. Data Visualization

Three different methods for visualizing time error have been presented:

1. Fixed 30-second window (Figures 5, 6, 7, & 8).
2. Selecting a beginning point in time and integrating all new values over time (Figures 9, 10, & 14).
3. A sliding 30-second window where values are integrated only within the previous 30 seconds (Figures 11, 12, 15, & 16).

Each of these calculations result in slightly different magnitudes, but they do have one common feature. In all cases, three of the four difference from average magnitudes move to one side of the zero time error axis, and the fourth, the signal being shifted, moves to the other side of the axis. When the frequency multiplier is greater than 1.0 (indicating a forced increase from the actual frequency), the shifted signal trends negative and the other signals trend positive. When the frequency multiplier is less than 1.0 (indicating a forced decrease from the actual frequency), the shifted signal trends positive and the other signals trend negative. This pattern did not occur during transient behavior, where two of the signals were positive and two were negative. This behavior was observed in other recorded transients as well.

The fixed 30-second window proved useful for detecting moderate rates of time shift. It would not be as useful for an aggressive rate of change such as 50 degrees per minute, because the signal would be shifted significantly before an alert would be raised.

Likewise, the continuous integration of differential time error over a longer period of time reflected time shift effectively, but it was observed that these values tend to drift away from each other. Thus, a 'reset to zero' would be needed occasionally.

The sliding window calculation offers the best opportunity to identify an anomalous time-shift event such as a spoofing attack. As the readings diverge, the PMU under attack separates itself from the others, and this allows the opportunity for an alert to be created. The system then automatically resets itself. Even this detection method could be defeated by intermittent time-shifts, but these would conceivably be occurring so slowly that this activity could be detected by other mechanisms, such as operators noticing that phase angles between the closely-coupled PMUs have begun to separate.

X. Conclusion

While GPS spoofing is technically challenging and unlikely to be successful, it has been demonstrated in a controlled environment thus detection of errant signals is worthy of investigation. By observing the consistency of the frequency across the ERCOT Grid and Eastern Grid, we determined that it was possible to detect GPS spoofing via calculations based on PMU frequency measurements.

By developing frequency scaling formulas and analyzing the time shifts involved with the controlled environment attack, we were able to create frequency shifts that simulated various rates of time-shifting attacks on PMUs. By averaging the frequency-based time error calculated with values from

multiple PMUs, and subtracting the individual PMU time error from the average error, we derived an integrated time error value that deviated from normal activity when under the influence of a spoofed signal.

These deviations were presented with several visualizations: fixed 30-second windows, continuous integration, and a sliding 30-second integration window. The sliding window is the most useful and flexible method of detecting time-shifting, as it allows for the detection of both fast and slow attacks.

This detection method can be considered a starting point for detecting time-shifting attacks, but it may also point out errors with GPS clocks themselves. Further research should be performed with the integration and implementation of time-shift detection algorithms in phasor data concentrator systems. The width of the sliding time window, presented as 30 seconds in this paper, may need to be expanded or contracted pending further analysis. It may be possible to perform these calculations at real-time speed, which would allow for the quick detection of signals that are experiencing errors or attacks.

These detection methods are relatively simple in concept and far less expensive than installing new spoof-resistant GPS clock infrastructure in substations. Until GPS technology offers additional security, mitigation techniques such as presented in this paper should be considered for power system clock protection.

XI. References

[1] *IEEE Standard for Synchrophasor Measurements for Power Systems*, IEEE Standard C37.118.1-2011, December 2011.

[2] T. H. Kim, C. S. Sin, and S. Lee, "Analysis of Effect of Spoofing Signal in GPS Receiver," *2012 12th International Conference on Control, Automation and Systems*, pp. 2083-2087, Oct. 2012.

[3] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol 5, pp. 146-153, September 2012.

[4] *NERC Regions and Balancing Authorities (as of June 30, 2014)*. [Online]. Available: http://www.nerc.com/comm/OC/RS Landing Page DL/Related Files/BA_Bubble_Map_20140630.jpg

[5] *Balancing and Frequency Control: A Technical Document Prepared by the NERC Resources Subcommittee – January 26, 2011*. [Online]. Available: http://www.nerc.com/comm/OC/Pages/RS/Resources-Subcommittee.aspx

[6] M. Kai, "Implementation and Lessons Learned from the Texas Synchrophasor Network," Ph.D. dissertation, Dept. Electrical Eng., University of Texas at Austin, 2012.

XII. Biographies

Andrew Mattei received his B.S.E.E. degree from Texas A&M University at College Station in 1993, and the M.S. Technology Management degree from Texas A&M University at Commerce in 2013. He is a Design and System Protection Engineer for Brazos Electric Cooperative and a Registered Professional Engineer in Texas. He is currently pursuing his Ph.D. degree in the Department of Electrical and Computer Engineering at Baylor University. His research interests include synchrophasor applications and transmission system protection.

W. Mack Grady (Fellow, 2000) received the B.S.E.E. degree from the University of Texas at Arlington in 1971, and the M.S.E.E. and Ph.D. degrees from Purdue University, West Lafayette, IN, in 1973 and 1983, respectively.
He is a Professor of Electrical & Computer Engineering at Baylor University in Waco, Texas. His research areas are electric power systems, power quality, and renewable energy. Dr. Grady was named Fellow of IEEE in 2000 "for contributions to the analysis and control of power system harmonics and electric power quality." He served as chairman of the IEEE-PES T&D Committee and is a Registered Professional Engineer in Texas.

P. Jay Caspary received his B.S.E.E. from the University of Illinois-Urbana in 1981 and has completed significant course requirements toward a Masters of Engineering Degree from Iowa State University. Jay is presently the Director of Research, Development & Special Studies at the Southwest Power Pool. Jay supports EPRI's Grid Planning, Operations and Renewable Integration program and serves on the Arkansas Alternative Energy Commission. Jay is a member of the Board of Directors for the Utility Variable-generation Integration Group (UVIG), and serves on Industry Advisory Boards for the Power Systems Engineering Research Center (PSERC), Grid-connected Advanced Power Electronics Systems (GRAPES), and the College of Engineering at Harding University.

Scott A. McBride received his B.S.E.E. from the University of Idaho and is the Director of The Department of National & Homeland Security, Critical Infrastructure Protection & Resilience Division at the U.S. Department of Energy's Idaho National Laboratory. Responsibilities include successful project/program execution from conception through completion including determining costs, budgets, schedules, scope and direction of research. Mr. McBride leads, directs and conducts research in state-of-the-art power engineering modeling simulation and testing for National and Homeland Security clients. He provides significant strategic involvement and leadership at the national level with external entities for business results. Mr. McBride is a Registered Professional Engineer in the State of Idaho.