Impact of GPS Spoofing on HVDC Modulation

Nathaniel Eastland and Vaithianathan “Mani” Venkatasubramanian
School of EECS, Washington State University, Pullman, WA
nathaniel.eastland@wsu.edu, mani@wsu.edu

Abstract

This paper investigates a variety of scenarios in which control signals utilized in high-voltage DC (HVDC) modulation are subjected to oscillatory error due to GPS spoofing of phasor measurement unit (PMU) time synchronization. The result of this spoofing is the presence of forced oscillations in a system through HVDC modulation due to cyclic erroneous measurements. These scenarios are tested in the Kundur two-area system with a supplementary HVDC line which utilizes various supplementary controllers for modulation. The simulation results are examined for system transient behavior as well as for the observable small-signal effects of the GPS spoofed control signals across the system. It is found that the harmonics of the spoofed control signal frequencies can interact with the inter-area modes of the system, resulting in resonant oscillations and the severity of the oscillations is dependent upon the magnitude of the time-error and the damping levels of the system modes.

1. Introduction

Most of the long-distance power transfer that occurs across the grid occurs over high-voltage AC (HVAC) transmission lines. The remaining power transmission infrastructure consists of HVDC transmission lines which may be utilized for purposes ranging from power transfer between two unsynchronized systems, to improving stability across a region due to its ability to modulate power flow between its endpoints. This modulation of the HVDC flow is typically achieved using a supplementary controller, which allows the HVDC link to provide improvements to damping of AC system oscillations, transient stability, and voltage support [1]. While early implementations of HVDC modulation can be found within the western interconnection as early as the 1970’s [2], the invention of phasor measurement units (PMUs) in the following decade could permit the usage of phase angle difference across remote HVDC terminals as a feasible control input for HVDC modulation. Such HVDC modulation methods have been proposed such as in [3]. Recently there has been a major effort to develop and implement phase angle difference based HVDC control modulation for the Pacific DC Intertie (PDCI) in [4] for small-signal stability benefits.

As new technologies proliferate throughout the industry and become more integrated into new control methods, the topics of grid security and reliability increasingly include questions about cybersecurity and reliability of the information upon which control actions are taken. The wide adoption of PMUs throughout the grid provides tremendous improvements in system visibility and facilitates operations and control methods which were impossible prior to their creation. A key piece of data which PMUs depend upon to serve their purpose, namely GPS time synchronization data, is something that has the potential to be compromised and can in turn cause deleterious effects. Of the possible types of possible GPS spoofing that may occur, spoofing that produces an oscillatory error is of particular interest in the context of oscillatory stability due to its potential for resonant interaction with system modes. The focus of this paper is the examination of the possible effects of GPS spoofing on oscillation monitoring and oscillation damping in a simulated case containing an HVDC line utilizing PMU acquired voltage angle measurements as control input.

2. GPS Spoofing Test Signals

Devices that utilize a GPS signal are susceptible to interference from jamming or spoofing attacks which may range in their complexity from simple to sophisticated. As the focus of this paper is the effect of spoofing, a fundamental description is detailed in [5] of how such interference can affect the time synchronization of a GPS device. From here, we proceed on the assumption that an attempt at spoofing a GPS signal used by a PMU has occurred successfully and is tailored to impact the target device on relevant time scales. In the context of power system stability our focus is on inter-area oscillations, therefore the

URI: https://hdl.handle.net/10125/64131
978-0-9981331-3-3

type of spoofing investigated here involve cyclic oscillatory signals.

As inter-area modes are known to typically be well below 1 Hz [2], the frequencies chosen for the test spoofed signals were 0.25 Hz, 0.33 Hz, and 0.50 Hz. An appropriate amplitude for the spoofed signals, meaning the amount of phase shift implied by the oscillatory spoofed signal, was determined using the following assumptions and information:

- Signal delay from a GPS satellite at an altitude of 20,000 km (directly overhead) is approximately 66.67 ms.
- For a 60 Hz grid, a measurement timing differential of 1 ms implies a differential in phase angle measurement of 21.6°.
- Time synchronization of the PMU occurs in 1 second intervals.

Desiring a spoofed amplitude corresponding to <1% deviation from our assumed satellite altitude which would also result in a phase angle differential much lower than 21.6°, an amplitude change of ±5° was chosen, which corresponds to a satellite signal delay of 0.2315 ms (or 0.347% altitude error). This error magnitude can be chosen to be sufficiently small to go undetected by the internal sanity checks within the GPS clocks and PMU devices depending on specific vendors and the value of ±5° is used in this paper for illustration. The magnitude of the resulting forced system oscillations will vary mostly linearly with the time-error magnitude as shown later in Section 4.3.

Since the timing error can only be introduced in one-second intervals during the GPS time synchronization stage, the spoofed waveforms in the timing error signal are modeled to undergo discrete changes every one second in our studies. Accordingly, approximations of sinusoidal oscillations by discrete waveforms that change every one second are plotted in Figure 1 along with the corresponding sinusoidal oscillations that they emulate. The simulated signals were generated by a user defined model [6] within the transient simulation software TSAT [7].

3. Simulation cases and methods

The simulation case for this paper extends work on a two-area system from [3], which has been modified from its original specifications in [1] to include a HVDC line between the two areas as illustrated in Figure 2. The net power transfer from Area 1 to Area 2 totals 400 MW, divided in half across the HVAC tie lines and HVDC line.

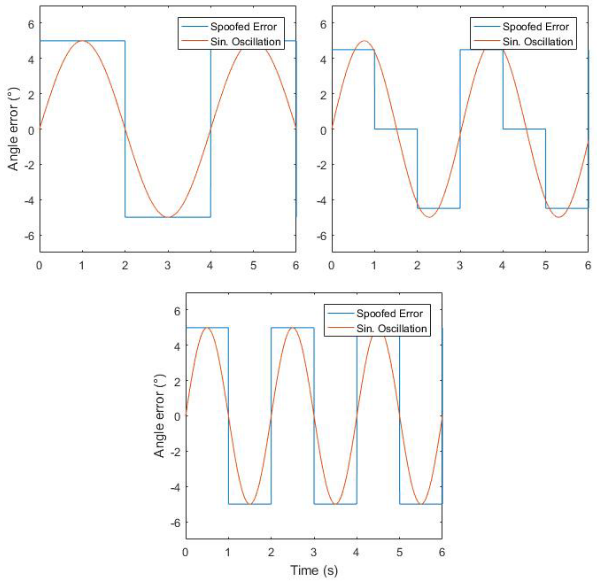

Figure 1. Waveforms of simulated spoofed signal errors and the sinusoidal oscillations they emulate: a) 0.25Hz error, b) 0.33 Hz error, c) 0.50 Hz error

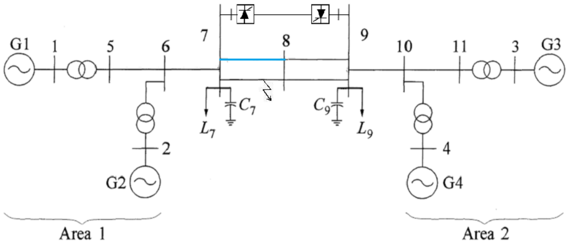

Figure 2. Kundur system with HVDC line

The effects on the system of GPS spoofing with various controllers are examined by simulation of a three-phase line fault between bus 7 and bus 8 on the green line shown in Figure 2. The fault in the transient simulation occurs at time t = 1 second and is cleared after 0.1 sec. The simulation continues with the line remaining out until t = 21 seconds at which point the line is restored and the simulation continues up to t = 40 seconds.

The input signal for the tested controllers is a phase angle difference between bus 7 and bus 9. The set of signal modifications made upon either measurement includes 0.25 Hz, 0.33 Hz, and 0.50 Hz. The set of HVDC modulation controllers tested includes a proportional controller as implemented in [8] and phase lead compensation of 30°, 60°, 90°, and 120°, as proposed in [3]. The suite of scenarios tested is comprised of the combination of those two sets where the spoofed signal is applied to the bus 7 measurement. Additional cases are also examined where spoofing is applied to measurements at both buses 7 and 9, referred to as combined cases. A diagram of the GPS spoofing affecting the measurement at either bus, as well as the controller block diagrams, are given in Figure 3.

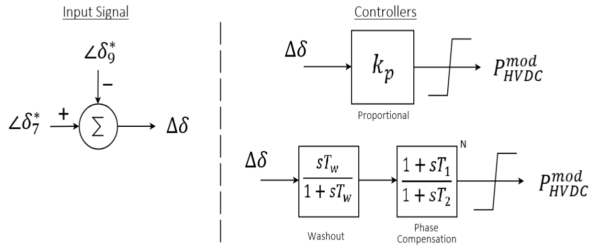

Figure 3. Control inputs (left) and block diagrams (right) for proportional and lead compensation controllers for HVDC modulation.

For phase lead compensation of 30°, 60°, 90°, and 120° the controller contains N = 1, 2, 3, or 4 stages of the phase compensation block with T1 = 0.5513 and T2 = 0.1838. The washout block time constant is Tw = 10 seconds and the output limits are ± 20% of the scheduled HVDC flow. Proportional gain kp is set to be 1.

To glean relevant insights of the system's behavior under the test scenarios laid out, an approach was taken to run transient simulations for each scenario and subsequently apply modal analysis methods to the data generated. The transient response of the system was simulated using TSAT [6], which provides various time series values across the system. Two main measures were chosen for examining the transient and modal properties of the system: real power-flow across the HVDC line and HVAC line between bus 7 and bus 8, and the voltage phase angle values at each bus in the system. The two simulated real power line flows are examined to gain some insight into the practical effects of each scenario on the system while the angle data was used for modal analysis, the results of both are detailed in the following section.

The time series data representing voltage phase angle across all buses in the system is used for modal analysis in Event Analysis Offline (EAO) software [9]. The data for each scenario is reconstructed using several modal analysis methods including Prony's method [10], Hankel Total Least Square (HTLS) [3], Matrix Pencil (MP) [11], and an eigensystem realization algorithm (ERA) [12]. The time series data from simulation spans the pre-fault, fault-on, and post-fault states of the system as well as the time after the line is restored. As the state of the system is not homogeneous for time windows containing any of these transitions the selection of different windows was necessary for the analysis methods to yield meaningful results. The accuracy of these different windows was verified by comparison of FFT of the input data to the reconstructions yielded from these methods and will be expanded upon in the following section.

4. Simulation Results and Analysis

The frequency and damping of the interarea mode of the two-area test system are both affected by the different controllers implemented, as well as changes in topology like the loss of a line in the simulation transient case. To provide context for the results in this section the frequency and damping ratio of the interarea mode with different controller implementations are given in Table 1, reflective of the steady state system. Only a select subset of numerical results is presented here.

Table 1. Effect of HVDC modulation controllers on inter-area mode.

Controller	**Frequency** (Hz)	**Damping** (%)	**Relative Energy** (%)
No control	0.623	1.284	100
Proportional	0.637	0.532	100
30° Lead	0.647	1.54	100
60° Lead	0.664	4.778	100
90° Lead	0.687	13.635	100
120° Lead	0.745	19.114	100

4.1. Transient simulation results

Data was collected on the real power flow across the HVDC line and HVAC line 7-8 as a starting point for assessing the oscillation damping performance of the system tested. The plots in Figure 4 show the oscillation of real power flow across the HVAC line 7-8 given different controllers in non-spoofed measurement cases.

The 90° and 120° phase lead compensators were found in [3] to provide the best oscillation damping in non-spoofed testing, using tie line flow and phase angle difference as respective control inputs (as confirmed with the bottom plot in Figure 4). As such, the effects of those two and the proportional controller on HVAC tie line flow oscillations are shown in Figure 5 for the various spoofed signals considered. The range of the real power swings across the HVAC line 7-8 as well as HVDC line for the cases shown are given in Table 2.

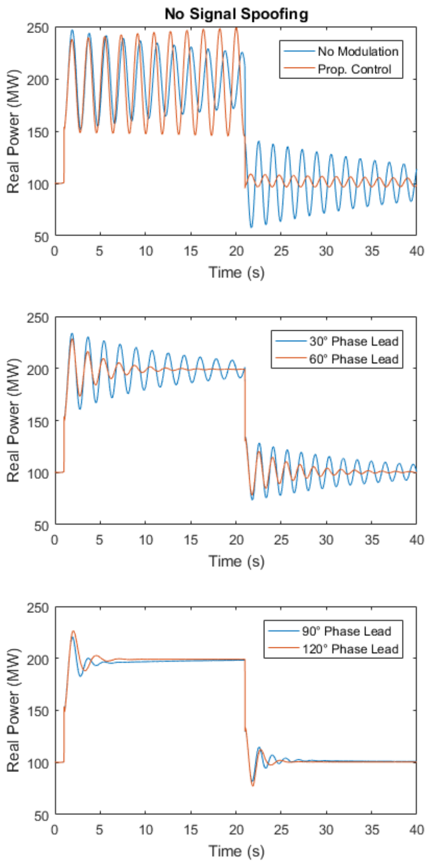

Figure 4. Transient inter-area real power flow with non-spoofed control signals.

Table 2. Magnitudes of real power flow dynamic range during post-fault period (from 1 to 21 seconds in simulation)

PMU Meas.	Line	Proportional	90˚ Lead	120˚ Lead
Unmodified	AC78 (MW)	103.5	37.7	38.2
	HVDC (MW)	13.7	26	38.9
0.25 Hz error	AC78 (MW)	112.1	34	48.6
	HVDC (MW)	24.3	38.6	38.4
0.33 Hz error	AC78 (MW)	111.2	43.4	59
	HVDC (MW)	21.3	33	38.4
0.50 Hz error	AC78 (MW)	147.2	57.5	140.3
	HVDC (MW)	28.2	29.2	43.3

It is clear from the data in Table 2 that there is a notable impact on real power flow due to the effect of GPS spoofing on the HVDC modulation. The values presented in the table show the range of the largest oscillation during the post-fault period prior to the line being restored. Additionally, it is worth noting that the case involving 0.50 Hz spoofed error and the 120° lead compensator exceeds the range of the HVDC power modulation output limits (± 20MW). The observation of this swing is likely the result of the interaction of the inter-area mode frequency and spoofed frequency being very close, in combination with the fact that the modulation output signal is a supplementary control signal for the HVDC system rather than a hard output limit. While the magnitude of the dynamic range of HVDC power flow is only slightly beyond the expected modulation range, this is an effect of the GPS spoofing in which a part of the system is caused to operate outside its expected range.

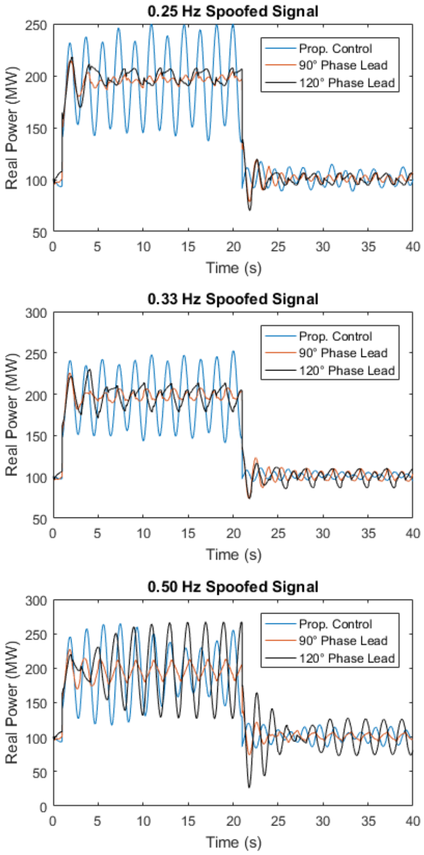

Figure 5. Transient inter-area real power flow with spoofed control signals.

Testing was done for spoofing of the angle measurement at bus 9 as well which yielded results that were generally consistent with those presented for the spoofing at bus 7. Two combined cases yielded significant real power dynamic swings across line 7-8 for combined scenarios involving a 0.50 Hz error at bus 7 and a 0.25 Hz error at bus 9. These two cases, which implemented either the 30° or 120° lead compensators, resulted in real power swings during the post-fault state of 140.29 MW and 100.72 MW respectively. Plots of these transient cases are shown in Figure 6.

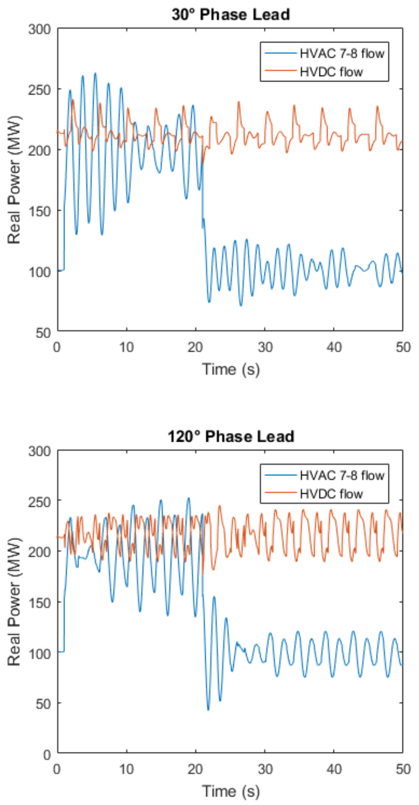

Figure 6. Transient inter-area power flow with spoofed control signal of 0.50 Hz at bus 7 and 0.25 Hz at bus 9

4.2. Analysis of system response

Modal analyses were conducted on each case tested to identify the characteristics of the system response to the spoofed control signals. Any modes identified with a relative energy (RE) of 5% or higher were recorded in set presented in Table 3. The data presented in the table is the result of Matrix Pencil analysis method specifically. The results from MP were checked for consistency with results from other engines such as HTLS and ERA.

The simulation data examined for the results in Table 3 were obtained using a window from t = 22 sec to t = 29 sec, however data in entries with an asterisk (*) were obtained with a 'two-window' method. The damping ratios given in the table which appear negative, but near zero, bear out to be a consequence of the analysis of the specific window selected and are not truly negatively damped. This is verified by two-window analysis as well as extended simulation of an additional 60 seconds beyond line restoration.

The entry denoted with {1} is for the substantial increase in interarea mode frequency over that of other controllers. Acceptance of the values for frequency and damping for this entry is supported by similar increases within the testing of [6] and verification of the soundness of the simulation case. The data for the entry denoted with {2} was obtained from a window of t = 25 to t = 35 seconds which reveals three modes, two of which appear to be caused by the spoofed signal error. One is identified with a frequency 0.652 Hz and 4.802% damping which is the interarea mode, while the other two have frequencies of 0.332 Hz (with RE < 5%, not listed in table) and 0.666 Hz, both with effectively 0% damping, which are the forced oscillations caused by spoofing. It appears that the second harmonic of the spoofed signal error contains the highest RE.

Table 3. Modal analysis results for system test cases

PMU status	**Controller**	**Freq.** (Hz)	**Damping** (%)	**Relative Energy** (%)
No error	Proportional	0.635	0.532	100
	30° Lead	0.647	1.540	100
	60° Lead	0.664	4.778	100
	90° Lead	0.687	13.635	100
	120° Lead {1}	0.745	19.114	100
0.25 Hz Error	Proportional	0.634	0.619	92.71
		0.250	-0.006	5.99
	30° Lead	0.647	1.155	98.78
	60° Lead	0.665	2.649	97.62
	90° Lead	0.672	8.796	91.46
		0.738	-0.063	8.54
	120° Lead *	0.791	13.764	100 (t=22-25)
		0.750	-0.086	57.69 (t=30-38)
0.33 Hz Error	Proportional	0.666	1.293	87.68
		0.334	0.804	9.34
	30° Lead	0.652	0.413	100
	60° Lead {2}	0.666	0.137	83.54
		0.652	4.805	14.88
	90° Lead {3}	0.662	12.589	91.27
		0.671	0.384	8.73
	120° Lead *	0.865	19.469	59.56 (t=22-25)
		0.666	-0.054	64.71 (t=30-38)
0.50 Hz Error	Proportional	0.635	0.526	84.98
		0.5	0.011	15.02
	30° Lead	0.647	1.41	94.84
		0.502	-0.723	5.160
	60° Lead	0.657	4.326	89.52
		0.500	-0.024	10.48
	90° Lead	0.679	12.413	85.72
		0.508	0.721	14.29
	120° Lead *	0.573	10.459	100 (t=22-25)
		0.500	0.061	100 (t=30-38)
Combined Error	Proportional	0.644	0.565	74.73
		0.493	-0.448	17.91
		0.247	-0.042	6.09
	90° Lead {4} *	0.647	15.993	97.33 (t=21-25)
		0.501	-0.224	67.61 (t=30-38)
		0.754	0.155	26.36 (t=30-38)
		0.247	-0.887	6.04 (t=30-38)

The entry {3} identifies a harmonic of the forced oscillation (spoofed signal) within the window from t =

22 to t = 29 seconds. A further window from t = 30 to t = 38 seconds identifies the forced oscillation of 0.333 Hz and its harmonic of 0.667 Hz, both with 0% damping, however the interarea mode fails to be identified distinctly from the harmonic. Finally, the entry {4} finds both forced oscillations of 0.247 Hz and 0.50 Hz, as well as the third harmonic of the 0.25 Hz signal, within a window from t = 30 to t = 38 seconds, all with 0% damping. The original simulation data and reconstructed signals are compared by FFT to assess the accuracy of the signal reconstructions and the modal analysis results. Figure 7 contains the plots of the FFTs for cases {2}, {3}, and {4}.

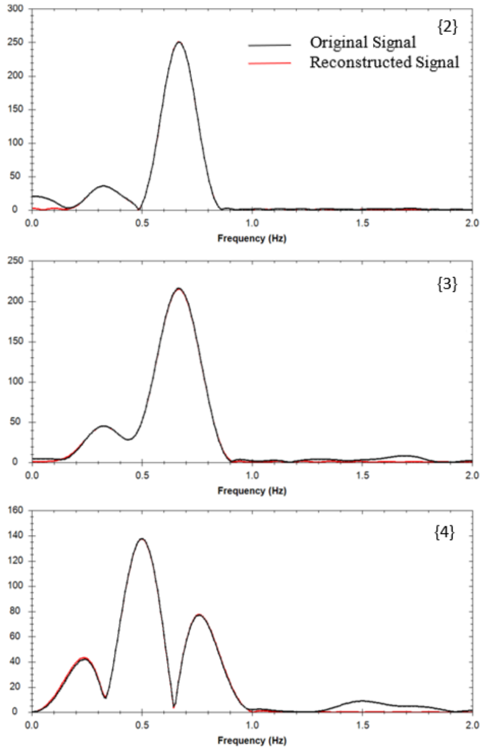

Figure 7. FFTs of original and reconstructed voltage angle at bus 7 for 0.33 Hz case with 60° lead comp. {2}, 90° lead comp. {3}, and combined case with 90° lead comp. {4}.

In the 0.25 Hz error cases, we see that the strongest component in the system response is a sustained oscillation of 0.75 Hz and 0.738 Hz for the 120° and 90° controllers, which corresponds to the third harmonic of the 0.25 Hz spoofed input. An interaction between the 0.75 Hz harmonic and the 0.67 Hz interarea mode causes a resonance effect that is seen in the system responses and is the cause of the 0.75 Hz oscillation having a higher amplitude (represented in RE in the modal analysis) than the 0.25 Hz forced oscillation [13]. Similarly, for the 0.33 Hz spoofed signal case, the second harmonic at 0.66 Hz excites the system mode and dominates the closed loop system responses in Table 3. As is the case for the second harmonic of the 0.25 Hz spoofed input, the 0.50 Hz spoofed case does not present a strong resonance effect, owing to it not being close to the 0.67 Hz system mode [13].

4.3. Sensitivity to time error magnitude

The initial assumption of a successful attack affecting the system with an oscillatory error of ±5° serves well as a basis for a severe case. However, the sensitivity of the system to subtler attacks should also be considered. A more detailed examination of system sensitivity could be conducted in future work, but within the scope of this paper a demonstration of the effects of increasing error amplitude were explored for a single case for illustrative purposes. The values presented in Table 4 are for a 30° lead compensator controller under the impact of a 0.33Hz spoofed oscillation. The real power fluctuations examined were from tie line 7-8 once the system reached a stable limit cycle (from 140 to 200 seconds).

Table 4. Real power fluctuation values for various spoofed error amplitudes

Error Amplitude (°±)	**Max Power** (MW)	**Min Power** (MW)	**Diff.** (MW)
0.10	100.935	100.124	0.811
0.25	101.537	99.507	2.03
0.50	102.526	98.485	4.041
1.00	104.505	96.444	8.061
2.00	108.457	92.345	16.112
4.00	116.473	83.954	32.519

As can be seen from the table, for the range of error amplitudes examined (near the amplitude of interest for this paper) there is mostly a linear relationship between the error amplitude and the amplitude of real power fluctuations in steady state. The increases in power fluctuation appear to increase in a roughly linear fashion with increases in the spoofed signal error amplitude which emphasizes the small-signal dynamic nature of the phenomenon.

Unlike drift attacks [5] where the time-error and the corresponding angle error gradually increase over time, the time-error varies within small ranges (back and forth) for the cyclic time-error of this paper as indicated in Figure 1. Therefore, time-error induced forced oscillations studied in this paper can possibly go undetected for long periods of time especially at small amplitudes causing potential damage to expensive power system equipment and possibly leading to unintentional tripping of system components.

5. Conclusions

In this paper the behavior of a power system in response to spoofed HVDC control signal during a transient event was investigated. Based upon several possible HVDC modulation control implementations, three spoofed GPS signal frequencies were simulated. The transient event simulation data revealed that the introduction of spoofed cyclic signals to HVDC control results in forced inter-area oscillations of varying amplitudes which were sensitive to inter-area mode damping ratio and the frequency of the spoofed signal. Some combinations of controller and spoofed signal frequency resulted in real power dynamic ranges in excess of ±35% of the scheduled line flow, as in the case of the 120° phase lead compensation controller and 0.50 Hz signal spoofing at bus 7. Combined cases were also examined in which control signals from both ends of the HVDC link were subject to spoofing.

The sustained oscillations caused by the cyclic time-error spoofing will persist as long as the spoofed signal is imposed. A possible consequence of such oscillations may be that an undesirable control action is taken by an operator to mitigate the oscillations which may lead to service disruptions. Alternatively, if such oscillations do not warrant direct intervention, their presence in the system over time may still adversely affect power quality or cause damage to equipment such as generator rotor shafts.

Various modal analyses were conducted on the data sets collected which revealed resonance phenomena due to the interaction of the spoofed signal with the inter-area mode frequency, as well as effects related to harmonics of the spoofed signal throughout the system. The resonance effect can be induced by any sufficiently high relative energy harmonic of the spoofed signal frequency, and not the fundamental frequency itself. This implies that for a given spoofed input signal there can be multiple inter-area modes which may be affected simultaneously by different harmonics of the spoofed input. A reduction in HVAC line flows or generator tripping are potential consequence of such sustained oscillations.

While the simulations conducted in this paper revealed that these undamped spoofed signals and harmonics resulted in stable limit cycles, further investigation is needed to determine more precisely how these effects impact other system components or if they result in unacceptable operational conditions beyond the transient and small signal stability properties examined here.

Several primary takeaways from the transient and small signal analyses are listed as follows:

- The spoofed cyclic timing error signals with any controller tested cause sustained, undamped oscillations in the system.
- The sustained oscillations may result in operator actions which disrupt service, or they may cause damage to synchronous generator equipment if they persist.
- A harmonic of the spoofed input signal can have resonant interactions with an inter-area mode, and consequently different harmonics may cause resonance with multiple interarea modes in large real systems.

While the system studied in this paper is quite simple, a similar study on a more complex system could yield useful insights for system operators. This further work could also include examination of possible ways to detect and mitigate the effects of such attacks upon the power system.

Acknowledgments

This research in this paper was supported by funding from the US Department of Homeland Security (DHS) and Lawrence Livermore National Laboratory (LLNL).

6. References

[1] P. Kundur, "Power System Stability and Control" in , New York:McGraw-Hill, Inc., 1994.

[2] R. Cresap, W. Mittelstadt, D. Scott, and C. Taylor, "Operating experience with modulation of the Pacific HVDC intertie", IEEE Trans. on Power Apparatus and Systems, vol. PAS-97, no. 4, pp. 1053-1059, 1978.

[3] Guoping Liu, J. Quintero and V. M. Venkatasubramanian, "Oscillation monitoring system based on wide area synchrophasors in power systems," 2007 iREP Symposium - Bulk Power System Dynamics and Control - VII. Revitalizing Operational Reliability, Charleston, SC, 2007, pp. 1-13.

[4] Brian J. Pierre, Felipe Wilches-Bernal, Ryan T. Elliott, David A. Schoenwald, Jason C. Neely, Raymond H. Byrne, and Daniel J. Trudnowski, "Simulation results for the pacific DC intertie wide area damping controller", Power & Energy Society General Meeting 2017 IEEE, pp. 1-5, 2017

[5] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," in Proceedings of the IEEE, vol. 104, no. 6, pp. 1258-1270, June 2016.

[6] User-Defined Model Manual for TSAT & SSAT, Model Manual, Powertech. Labs Inc., Surrey, BC, Canada, 2012.

[7] Transient Security Assessment Tool (TSAT), User's Manual, Powertech. Labs Inc., Surrey, BC, Canada, 2012.

[8] P. Bornard, “HVDC links in AC power system”, available at http://catedraendesa.us.es/documentos/jornadas_uimp_2015/2015%2003%2011%20Seville%20HVDC(p11).pdf

[9] Event Analysis Offline (EAO), Washington State University, Department of Electrical Engineering & Computer Science (EECS), Pullman, WA, 2019.

[10] J. F. Hauer, C. J. Demeure and L. L. Scharf, "Initial results in Prony analysis of power system response signals," in IEEE Transactions on Power Systems, vol. 5, no. 1, pp. 80-89, Feb. 1990.

[11] M. L. Crow and A. Singh, "The matrix pencil for power system modal extraction," in IEEE Transactions on Power Systems, vol. 20, no. 1, pp. 501-502, Feb. 2005.

[12] J. J. Sanchez-Gasca, "Computation of turbine-generator subsynchronous torsional modes from measured data using the eigensystem realization algorithm,", Proc. IEEE PES Winter Power Meeting, 2001.

[13] S. A. N. Sarmadi, and V. Venkatasubramanian, "Inter-area resonance in power systems from forced oscillations", IEEE Transactions on Power Systems, vol. 31, no. 1, pp. 378-386, 2016.