Closed-Form Solution for Synchrophasor Data Correction under GPS Spoofing Attack

Xiaoyuan Fan, Seemita Pal
Electricity Infrastructure Group
Electricity Infrastructure & Buildings Division
Pacific Northwest National Laboratory
Richland, WA, 99352

Dongliang Duan
Department of Electrical
and Computer Engineering
University of Wyoming
Laramie, WY 82071

Liang Du
Department of Electrical
and Computer Engineering
Temple University
Philadelphia, PA 19122

***Abstract*—Phasor Measurement Units (PMUs) are increasingly being deployed to augment monitoring, protection and control applications in the power grid. PMUs rely on the Global Positioning System (GPS) for generation of time-synchronized and accurate measurements. However, civilian GPS signals, being unencrypted, are susceptible to GPS spoofing attacks (GSA). Hence ensuring the integrity of GPS-timing dependent synchrophasor data has become critical. In this paper, a closed-form analytical solution for estimating the GSA phase shift has been proposed and integrated to the spoofing detection & correction framework. Extensive simulations have been performed in order to verify the accuracy of the solution in determining the location and the phase shift of the compromised PMU. Time domain dynamic simulations presented in this paper demonstrate the applicability of the proposed solution for near-real-time detection of GSA, and this will enable faster detection and correction of phase angles of compromised synchrophasor data.**

***Index Terms*—Synchrophasor, PMUs, GPS, Spoofing, Data Correction, Synchronization.**

I. Introduction

Global Positioning System (GPS)-timing dependent applications are widely being utilized in our everyday lives. In 2014, 3.6 billion Global Navigation Satellite System (GNSS) devices were in use around the world, and by 2019, the number is forecasted to nearly double [1].

GPS signals coming from the satellites are very weak, the signal strength measured at the surface of the earth being about -160 dBW. This is roughly equivalent to viewing a 25 Watt light bulb from a distance of 10,000 miles [2]. Hence these weak broadcasted signals can be overridden by signals in the same frequency band, and they need not be strong. Furthermore, since the signal structure is available in the public domain, the transparency and predictability of GPS signals make them easy to imitate and counterfeit [3].

The GPS system is a frequent target of jamming and spoofing attacks. Among those two, GSA is considered to pose a greater threat since the GPS receiver continues to receive fake signals and is completely unaware of any issues. In 2013, a professor from the University of Texas at Austin successfully spoofed the navigation system on an $80 million super yacht in the Ionian Sea with a $2,000, custom-made device [4].

A PMU is a powerful tool which can measure voltage and current phasors, typically at a reporting rate of 30 or 60 samples per second. It is equipped with GPS receiver which provides timestamping with 1 μs or better accuracy using a Coordinated Universal Time (UTC) time reference [5]. Presently PMUs are increasingly being used for applications such as forensic event analysis, phasor-based linear state estimation, and oscillation monitoring.

PMUs are vulnerable to GSA, due to their reliance on GPS signals. GSA can cause the GPS receiver to compute an erroneous clock offset value, resulting in wrong time-stamp calculation and injection of error in the phase angle measurements [5]. It could introduce an error in the phase angle at a rate of 1.73 degrees per minute, which is above the allowable maximum phase error [6], [7].

GSA on a single PMU can lead to erroneous estimates of power system states, and therefore trigger false alarms of power instability [5]. It has been demonstrated that a time synchronization attack which shifts the time estimate by as little as 2.8 ms can lead to a fault location error as large as 180 km [8].

In this paper, a closed-form analytical solution has been proposed to fight against single GSA. In Section II, a brief overview of the existing methods used for detecting and mitigating spoofing attacks is provided. Section III introduces the synchrophasor use case, where the proposed closed-form analytical solution is derived and validated, the simulation-based results are discussed in Section IV. Section V concludes the paper.

II. Related Work

A number of countermeasures for detecting GSA have been proposed. A comprehensive review of the various anti-spoofing techniques and their performances has been provided in [9]. But most of them are not practical to be applied in the power industry practices. For example, one of the existing techniques propose that the GPS receivers be programmed to monitor the carrier-to-noise C/N_0 ratios so that users may be alerted by blip in the ratio when GPS signal is spoofed. Another method proposes to track the absolute power of the received GPS signal and alert any deviation from the expected value. Both the above methods, however, require more signal-processing channels and hardware in each receiver [10].

In [11] a cross-layer defense mechanism which utilizes a patch-monopole hybrid antenna connected to two GPS re-

978-1-5386-7703-2/18/$31.00 ©2018 IEEE

ceivers computes the difference between the standard deviation of each receiver's C/N_0 ratio to detect the compromised PMU. This technique requires specific kind of antenna and two GPS receivers per PMU.

In another spoofing-detection technique, the Directions of Arrival (DoA) of the GPS signals are monitored, since spoofing signals can be typically identified by their similar DoA. However, this method requires considerable off-line data processing [12].

In [13], a multi-receiver GPS-based direct time estimation (MRDTE) algorithm is proposed for GSA detection and mitigation, but it requires multiple (typically four) receivers and the computation time is relatively high. It should be noted that most of the existing methods require additional hardware and/or software at each of the PMUs, thereby making the solutions expensive. None of them utilize synchrophasor measurements from grid-wide PMUs or the system model information to detect and mitigate GSA.

III. Synchrophasor Use Case

In this section, we introduce the synchrophasor use case which has been used for the development and validation of the proposed closed-form analytical solution, within the GPS spoofing detection & correction framework [14]. PMUs across the power grid utilize the GPS reference source to synchronize measurements. Regional PMUs send measurements to the local Phasor Data Concentrators (PDCs), where the measurements are aggregated, time-aligned and sent to the Super PDCs and/or the control center.

The impact of GSA on the synchrophasor measurements will be on the phase angle θ [6], [14], [15]. Mathematically, for any single snap shot, the spoofed voltage and current synchrophasor data are affected by the GSA as follows:

$$\begin{aligned} V_{\text{spf}} &= V_{\text{true}} \times e^{j\theta_{\text{spf}}} \\ I_{\text{spf}} &= I_{\text{true}} \times e^{j\theta_{\text{spf}}} \ , \end{aligned} \tag{1}$$

where θ_{spf} denotes the phase shift introduced by the GSA to the true measurements at the current time instance.

Generally, a GPS spoofing attack can be denoted by its location k and phase shift θ_{spf} as GSA(k, θ_{spf}). Hence, the correction of GPS-spoofed synchrophasor data can be tackled by estimating those two parameters, or equivalently estimating the corresponding $\boldsymbol{G}$ matrix. Once the GSA location was detected and the GSA phase shift was estimated, the synchrophasor measurement can be corrected as follows:

$$\hat{\boldsymbol{m}}_{\text{true}} = \hat{\boldsymbol{G}}^{\mathcal{H}} \boldsymbol{m}_{\text{spf}} \tag{2}$$

In our previous work [14], a general spoofing detection & correction framework has been proposed to fight against GPS spoofing attack, the corresponding flow diagram is given in Fig. 1. In this paper, a closed-form analytical solution has been provided for accomplishing Step 2 of Fig. 1 (where the GSA phase shift of the victim PMU is estimated).

The cost function for GSA is represented by the root mean square error (RMSE) of estimation residual.

$$J(k, \theta_{\text{spf}}) = \|\boldsymbol{r}(k, \theta_{\text{spf}})\|_2 \ , \tag{3}$$

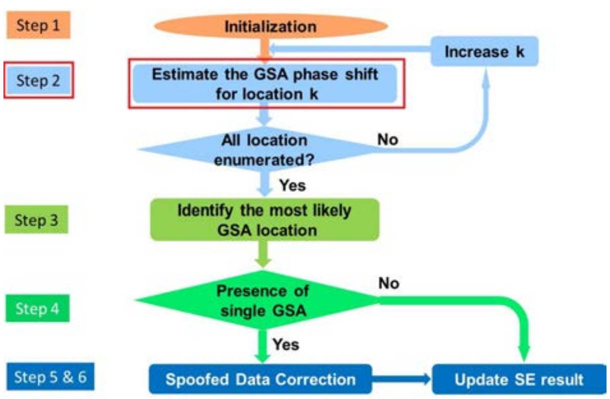

Fig. 1. The flow diagram describing the spoofing detection & correction framework, where the red box indicates the proposed close-form analytical solution.

where $\|\cdot\|_2$ denotes the L$_2$-norm. The system model formulation and mathematical defefinitions could be found in [14].

Since both the variable k, θ_{spf} and the objective function $J(k, \theta_{\text{spf}})$ are scalars, the first-order derivative test may be applied. By calculating the first-order derivative of the cost function with respect to θ_{spf}, a closed-form expression is given as follows:

$$\begin{aligned} &\hat{\theta}_{\text{spf}} = \arctan\left(-\frac{t_2}{t_1}\right) \quad \text{where } \hat{\theta}_{\text{spf}} \in \left(\text{-}\frac{\pi}{2}, \frac{\pi}{2}\right), \text{ and} \\ &t_1 = \Re\left\{ \boldsymbol{m}_k^H \left(\sum_{i=1, i\neq k}^{p} \boldsymbol{Z}_{k,i} \boldsymbol{m}_i \right) \right\} \\ &t_2 = \Im\left\{ \boldsymbol{m}_k^H \left(\sum_{i=1, i\neq k}^{p} \boldsymbol{Z}_{k,i} \boldsymbol{m}_i \right) \right\} \end{aligned} \tag{4}$$

where t_1, t_2 are scalars, p is the total number of PMUs installed, $\boldsymbol{m}_k$ is the measurement vector provided by the k-th PMU, $\boldsymbol{Z}_{k,i}$ is the (k-th,i-th) block of matrix $\boldsymbol{Z}$ given in (6) and $\boldsymbol{X}^{\mathcal{H}}$ denotes the Hermitian (conjugate transpose) of $\boldsymbol{X}$.

To derive the first order derivative of $J(k, \theta_{\text{spf}})$ by θ_{spf}, let the GSA location k be fixed, and the mathematical deduction process is given as follows:

$$\begin{aligned} \frac{\partial J}{\partial \theta_{\text{spf}}} &= \frac{1}{2(\boldsymbol{r}^{\mathcal{H}}\boldsymbol{r})^{\frac{1}{2}}} \times \frac{\partial(\boldsymbol{r}^{\mathcal{H}}\boldsymbol{r})}{\partial \theta_{\text{spf}}} \\ &= \frac{1}{2(\boldsymbol{r}^{\mathcal{H}}\boldsymbol{r})^{\frac{1}{2}}} \times \frac{\partial(\hat{\boldsymbol{m}}_{\text{true}}^{\mathcal{H}} \boldsymbol{Y}^{\mathcal{H}} \boldsymbol{Y} \hat{\boldsymbol{m}}_{\text{true}})}{\partial \theta_{\text{spf}}}. \end{aligned} \tag{5}$$

Let $\boldsymbol{Z} = \boldsymbol{Y}^{\mathcal{H}}\boldsymbol{Y}$, so $\boldsymbol{Z}^{\mathcal{H}} = \boldsymbol{Z}$, then

$$\begin{aligned} \frac{\partial(\hat{\boldsymbol{m}}_{\text{true}}^{\mathcal{H}} \boldsymbol{Z} \hat{\boldsymbol{m}}_{\text{true}})}{\partial \theta_{\text{spf}}} &= \frac{\partial(\hat{\boldsymbol{m}}_{\text{true}}^{\mathcal{H}})}{\partial \theta_{\text{spf}}} \boldsymbol{Z} \hat{\boldsymbol{m}}_{\text{true}} + \hat{\boldsymbol{m}}_{\text{true}}^{\mathcal{H}} \boldsymbol{Z} \frac{\partial(\hat{\boldsymbol{m}}_{\text{true}})}{\partial \theta_{\text{spf}}} \\ &= \boldsymbol{m}_{\text{spf}}^{\mathcal{H}} \left(\frac{\partial \hat{\boldsymbol{G}}}{\partial \theta_{\text{spf}}} \boldsymbol{Z} \hat{\boldsymbol{G}}^{\mathcal{H}} + \hat{\boldsymbol{G}} \boldsymbol{Z} \frac{\partial \hat{\boldsymbol{G}}^{\mathcal{H}}}{\partial \theta_{\text{spf}}} \right) \boldsymbol{m}_{\text{spf}}. \end{aligned} \tag{6}$$

By partitioning the matrices $\hat{\boldsymbol{G}}$, $\boldsymbol{Z}$ into $p \times p$ blocks and partitioning the vector $\boldsymbol{m}_{\text{spf}}$ into p vectors,

$$\begin{aligned}\frac{\partial(\hat{\boldsymbol{m}}_{\text{true}}^{\mathcal{H}}\boldsymbol{Z}\hat{\boldsymbol{m}}_{\text{true}})}{\partial\theta_{\text{spf}}} &= \left\{-je^{-j\theta_{\text{spf}}}\left(\sum_{j=1,j\neq k}^{p}\boldsymbol{m}_j^H\boldsymbol{Z}_{j,k}\right)\boldsymbol{m}_k\right\}\\ &+\left\{je^{j\theta_{\text{spf}}}\boldsymbol{m}_k^H\left(\sum_{i=1,i\neq k}^{p}\boldsymbol{Z}_{k,i}\boldsymbol{m}_i\right)\right\}\\ &= 2\Re\left\{je^{j\theta_{\text{spf}}}\boldsymbol{m}_k^H\left(\sum_{i=1,i\neq k}^{p}\boldsymbol{Z}_{k,i}\boldsymbol{m}_i\right)\right\}\end{aligned} \tag{7}$$

Let $t_1 = \Re\left\{\boldsymbol{m}_k^H\left(\sum_{i=1,i\neq k}^{p}\boldsymbol{Z}_{k,i}\boldsymbol{m}_i\right)\right\}$ and $t_2 = \Im\left\{\boldsymbol{m}_k^H\left(\sum_{i=1,i\neq k}^{p}\boldsymbol{Z}_{k,i}\boldsymbol{m}_i\right)\right\}$. Therefore, by the Euler's formula, we have,

$$\frac{\partial J}{\partial\theta_{\text{spf}}} = \frac{-2(t_2\cos\theta_{\text{spf}} + t_1\sin\theta_{\text{spf}})}{2(\boldsymbol{r}^{\mathcal{H}}\boldsymbol{r})^{\frac{1}{2}}} \tag{8}$$

Then by the first order derivative test, we obtain the following:

$$\hat{\theta}_{\text{spf}} = \arctan\left(-\frac{t_2}{t_1}\right) \quad \text{where } \hat{\theta}_{\text{spf}} \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \tag{9}$$

when $t_1 \neq 0$.

The first-order derivative test can be adopted as an alternative solution for Step 2 in the spoofing detection & correction framework. Comparing to the Golden Section search algorithm that employed in our previous research, this provides a better estimation of the θ, and it is in closed-form to provide the direct mathematical solution. It should be noted that $arctan$ function maps the estimated GSA phase angle into the range of $\{-\frac{\pi}{2}, \frac{\pi}{2}\}$, while the GSA phase shift is defined within the range of $[0, 2\pi\}$. As a result, the estimated GSA phase shift could be unwrapped based on the nature of $arctan$ function.

IV. Numerical Simulations

Extensive simulations have been carried out to illustrate the effectiveness of the proposed closed-form analytical solution for GPS-spoofed synchrophasor data correction. The effect of the location of GSA, the value of GSA phase shift will be examined and analyzed by the following case studies. In this section, the Monte Carlo simulation results from IEEE 14-, 30-, 57- and 118-bus testing caes have been analyzed, along with a time sequence simulation results from the modified IEEE 14-bus testing case considering power system dynamic models.

A. Monte Carlo Simulations with IEEE Test Cases

The standard IEEE 14-, 30-, 57-, 118-bus test cases provided in [16] have been adopted for our simulation setup. Eight different scenarios represent different PMU placement profiles, and the details are given in Table I [14]. In scenario 1, 3, 5, 7, the minimum number of PMUs that satisfying the system observability are considered, while in scenario 2, 4, 6, 8, some randomly selected redundant PMUs are selected in addition to scenario 1, 3, 5, 7 correspondingly. Both the GSA location and GSA phase shift are randomly selected. Gaussian noise with zero mean, standard deviation 1×10^{-2} is added to the voltage and current phasors to simulate realistic PMU measurements. For each testing scenario, 200 Monte Carlo simulations are conducted for each scenario and the analysis on the simulation results is given as follows.

TABLE I
PMU PROFILE UNDER DIFFERENT TEST SCENARIOS.

# of Buses	Scenario	Total # of PMUs
14	1	4
	2	6
30	3	10
	4	16
57	5	17
	6	28
118	7	32
	8	45

In Scenario 1, a GSA is launched on the 3rd PMU (installed on bus 7) with one randomly selected phase shift (denoted as GSA(3, θ_{spf})) in IEEE 14-bus system. The detection results shown in Fig. 2 indicate that the GSA location is identified correctly for all 200 iterations, and the estimated GSA phase shifts are centralized around the true one.

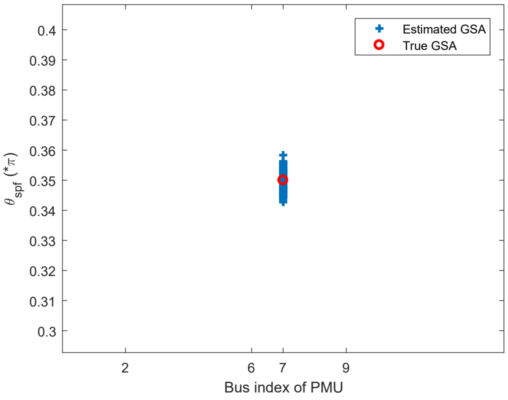

Fig. 2. Numerical result for detecting GSA(3, θ_{spf}) in Scenario 1.

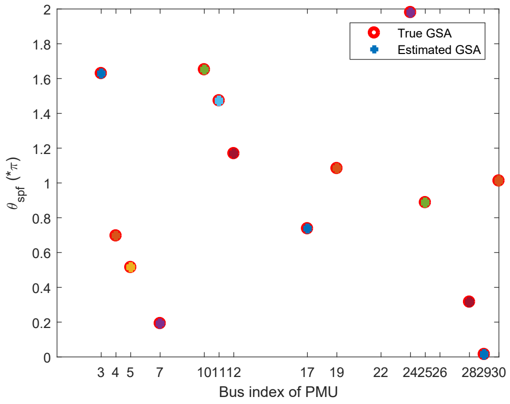

Fig. 3. Combined results for detecting GSA on each PMU in Generalized Scenario 4.

Moreover, to show the proposed algorithm is insensitive to the location of GSA, Scenario 4 has been generalized by

TABLE II
GSA DETECTION PERFORMANCE UNDER SINGLE GSA

Scenario	1	2	3	4	5	6	7	8
$p_{\text{CDT}}(\%)$	100	100	100	100	100	100	100	100
$p_{\text{MDT}}(\%)$	0	0	0	0	0	0	0	0
$\text{Bias}(\hat{\theta}_{\text{spf}})$	0.0020	0.0017	0.0019	0.0017	0.0027	0.0018	0.0019	0.0022
$\text{RMSE}(\hat{\theta}_{\text{spf}})$	0.0024	0.0021	0.0025	0.0021	0.0034	0.0022	0.0023	0.0027

simulating a GSA on one PMU in each simulation run, then their results are combined in Fig. 3. Clearly the GSA can be correctly detected no matter where the GSA are located or what the GSA phase shift is

Numerical simulations have been implemented for all eight scenarios, and the probability of correct detection (p_{CDT}) and the probability of miss detection (p_{MDT}) are adopted as system performance metrics. Moreover, the statistical analysis including the bias and root mean square error (RMSE) is performed to evaluate the accuracy of the estimated GSA phase shift $\hat{\theta}_{\text{spf}}$. Details of numerical results for all scenarios are given in Table II.

Once the GSA location was detected and the GSA phase shift was estimated, synchrophasor data correction could be applied to provide more reliable inputs for the power system state estimation (SE). Here the synchrophasor-based linear model is adopted for comparisons among different algorithms. We compare the SE performance with and without the synchrophasor data correction through the traditional weighted least square (WLS) algorithm. The true GSA information is also included in all comparisons for reference to the "perfect" solution.

The numerical simulations for the linear SE algorithm have been implemented for all 8 scenarios, and the details of results are given in Table III. It is observed that when GSA is present, SE with synchrophasor data correction has superior performance compared to SE without correction, and the errors from the proposed solution are comparable to the impact from the true GSA. An additional performance metric has also been calculated to indicate the improvement regarding to SE performance with and without synchrophasor data correction. It is denoted as $(1 - \frac{\text{RMSE}_{\text{w}}}{\text{RMSE}_{\text{w/o}}}) \times 100\%$ and calculated for magnitude and phase separately. The results showed that SE with synchrophasor data correction has a consistently better performance.

B. Time Domain Simulation for Modified IEEE 14-Bus System

Comparing to the previous simulations given in Section IV-A, the time domain synchrophasor data is also a great validation for the proposed closed-form analytical solution. More specifically, power system dynamic simulations have been performed for Scenario 1 described in Table I, namely the modified IEEE 14-bus system where the detailed generator dynamic models were included. A 10-second time sequence of voltage and current phasor data has been generated and the sample speed of PMU measurements is 30 samples/s. Detailed implementations of this dynamic simulation are given as follows:

- The total simulation length is 10 seconds;
- Dynamic models for 5 generator are included;
- 1 system load model is included;
- 1 normal grid operation event is included, Load Ramping starts at 2s and ends at 8s;
- The synthesized GPS spoofing attack is launched on PMU on bus 7, starts at 3s and ends at 10s;
- The measurement noise is added to the final synthesized synchrophasor data.

With the above simulation setup, a synthesized GPS spoofing attack is applied to further generate the ”compromised” synchrophasor data. Fig. 4 and Fig. 5 present the voltage/current magnitudes and phase angles of those synchrophasor data.

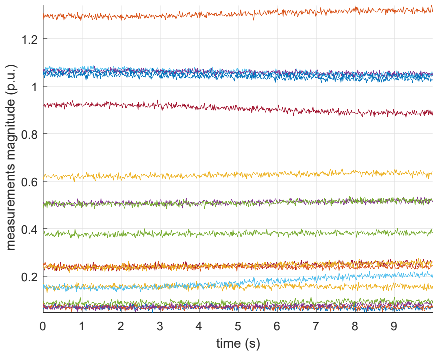

Fig. 4. The synthesized synchrophasor measurements magnitude (p.u.) under GSA.

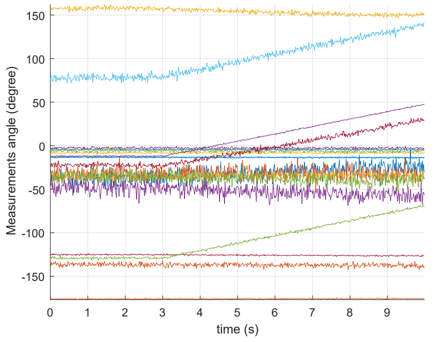

Fig. 5. The synthesized synchrophasor measurements phase angle (degree) under GSA.

Fig. 6 illustrates the noise-free synthesized GSA phase shift in the 10 second simulation, which linearly increases from 0 to 60 degrees over 7 seconds. The estimated GSA phase shifts are presented in Fig. 7, they are small random values (due to the injected noise) during the initial three seconds; but once the GSA started, the proposed close-form analytical solution has identified this attack at the very early stage, then followed through this GSA from 3s to 10s. There is no doubt that the

TABLE III
RMSE OF STATE ESTIMATION WITH AND WITHOUT SPOOFING DETECTION & CORRECTION UNDER DIFFERENT SCENARIOS

Sce.	SE with GSA Correction		SE without GSA Correction		SE with True GSA		Improvement	
	Mag.(p.u.)	Pha.(π)	Mag.(p.u.)	Pha.(π)	Mag.(p.u.)	Pha.(π)	Mag.(%)	Pha.(%)
1	0.0039	0.0012	0.1109	0.0770	0.0039	0.0012	96.52	98.38
2	0.0031	0.0011	0.0778	0.0585	0.0031	0.0010	95.97	98.18
3	0.0041	0.0013	0.0442	0.0277	0.0041	0.0013	90.72	95.26
4	0.0024	0.0008	0.0298	0.0173	0.0024	0.0007	92.09	95.55
5	0.0054	0.0019	0.0283	0.0250	0.0054	0.0018	81.02	92.47
6	0.0021	0.0007	0.0162	0.0100	0.0021	0.0007	86.86	93.09
7	0.0029	0.0010	0.0155	0.0074	0.0029	0.0010	81.59	86.83
8	0.0019	0.0006	0.0093	0.0045	0.0019	0.0006	78.47	86.36

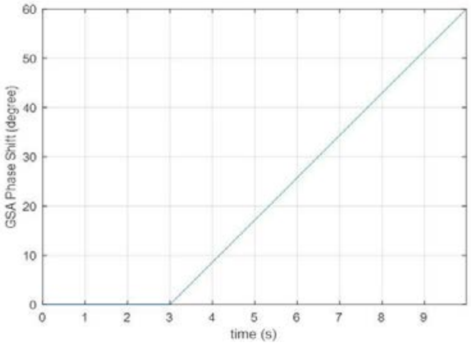

Fig. 6. The noise-less synthesized GSA.

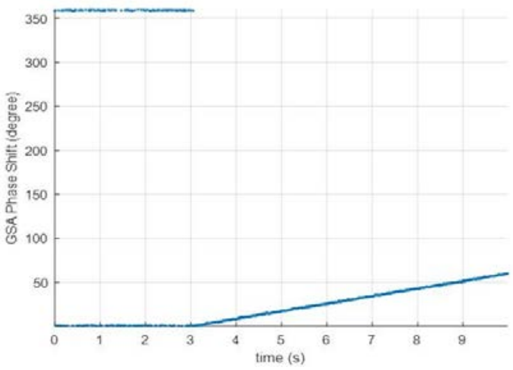

Fig. 7. The estimated GSA phase shift from the closed-form analytical solution.

proposed spoofing detection & correction framework can be transformed into a potential near-real-time application, which can be deployed at the grid control center to enhance the power grid resilience regarding to GSA.

V. CONCLUSION

In this paper, a closed-form analytical solution to estimate the potential GSA phase shift has been proposed and integrated into the spoofing detection & correction framework. The Monte Carlo simulations and the time domain dynamic simulations demonstrated the effectiveness of the proposed solution. It is potential to enhance the power grid resilience regarding to GSA by integrating the proposed spoofing detection & correction framework into the control room near-real-time applications.

ACKNOWLEDGMENT

The authors gratefully acknowledge the support and guidance from the Pacific Northwest National Laboratory staff Paul Skare and David Manz.

REFERENCES

[1] "GNSS market report," European Global Navigation Satellite Systems Agency, Tech. Rep. Issue 4, 2015.

[2] *Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System.* John A. Volpe National Transportation Systems Center Technical Report, August 2001.

[3] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, September 2012.

[4] L. Kugler, "Why GPS spoofing is a threat to companies, countries," *Commun. ACM*, vol. 60, no. 9, pp. 18–19, August 2017.

[5] X. Jiang, J. Zhang, B. Harding, J. Makela, and A. Dominguez-Garcia, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. on Power Systems*, vol. 28, no. 3, pp. 3253–3262, August 2013.

[6] IEEE Std, *IEEE Standard for Synchrophasor Measurements for Power Systems, C37.118.1-2011 (Revision of IEEE Std C37.118-2005)*, December 2011.

[7] D. P. Shepard and T. E. Humphreys, "Characterization of receiver response to a spoofing attacks," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, Portland, OR, September 2011.

[8] Z. Zhang, S. Gong, A. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. on Smart Grid*, vol. 4, no. 1, pp. 87–98, March 2013.

[9] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012.

[10] A. Jafarnia Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements," *International Journal of Satellite Communications and Networking*, vol. 30, no. 4, pp. 181–191, 2012. [Online]. Available: http://dx.doi.org/10.1002/sat.1012

[11] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2659–2668, Nov 2015.

[12] J. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing," *Journal of Applied Research and Technology*, vol. 13, no. 1, pp. 45 – 57, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1665642315300043

[13] S. Bhamidipati, Y. Ng, and G. X. Gao, "Multi-receiver GPS-based direct time estimation for PMUs," in *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2016)*, September 2016.

[14] X. Fan, L. Du, and D. Duan, "Synchrophasor data correction under GPS spoofing attack: A state estimation based approach," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[15] I. Akkaya, E. Lee, and P. Derler, "Model-based evaluation of GPS spoofing attacks on power grid sensors," in *2013 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Berkeley, CA, May 20, 2013, pp. 1–6.

[16] University of Washington, *Power System Test Case Archive*. [Online]. Available: http://www.ee.washington.edu/research/pstca/.