OPTIMAL PMU PLACEMENT TO MITIGATE FALSE DATA INJECTION VULNERABILITY

Ketchiozo Wandji, PhD
Morgan State University
Electrical Engineering Dept.
Baltimore, MD 21251
Ketchiozo.Wandji@morgan.edu

Ali Aliwi
Morgan State University
Electrical Engineering Dept.
Baltimore, MD 21251
Alali2@morgan.edu

Abstract

The false data injection attack is one of the most cyber security challenging in the last decades. Phasor measurement units (PMUs) deploy on power system using different approach and strategy and it is possible for an intruder to manipulate them which makes them one of the vulnerable targets for causing power system operations to be disrupted. Previous research publications proposed different method to deploy these PMUs to improve voltage profile and power transfer capabilities, then power system security is the final goal. PMUs have a high installation cost, which prevents them from being installed throughout the network. In this study used topological spanning trees method to deploy PMUs along a network in optimum locations to ensures the grid's critical observability. The primary goal of this effort is to strategically install PMUs to reduce the grid's vulnerability to a prospective false data injection attack while also increasing grid observability via PMUs. Using power system analysis toolbox (PSAT) within MATLAB platform is performed, and the results are compared to prove the system improvement. Testing of the proposed scheme's effectiveness on the IEEE 30 bus test system has confirmed its efficacy.

1. Introduction

There is a wealth of information available on PMU placement optimization. Complete observability is a crucial quality from an information-theoretic standpoint, as it indicates that no bus is left unnoticed by the installed PMUs [1]. The PMU placement design was addressed by binary linear programming (BLP) [1]. [2] under complete observability and its generalizations. Under the complete observability constraint and additional operating conditions such as a single branch outage and the availability of zero injection buses, an exhaustive binary search was presented in [3]. [4] suggested a binary particle swarm optimization approach to maintain complete observability criteria in the event of PMU loss or branch outage. In [5] and [6], binary quadratic programming and BLP were used to investigate the impact of ZIBs and power flow measurements (PFMs) on complete observability.

PMU placement for the purpose of optimizing the so-called gain matrix in the maximum likelihood estimate of the grid state [7] was considered in [8], which formulated it as an optimization problem for a convex objective function subject to a simple linear constraint on binary variables. A convex relaxation with the binary constraint 0, 1 for binary variables relaxed to the box constraint [0, 1], as used in [8], not only fails to provide a local optimal solution in general but is also not scalable in the grid dimension due to the addition of a large-size semi-definite matrix variable. Additionally, [9] solved the problem of PMU placement to maximize the mutual information (MI) between the measurement output and grid state very efficiently using a greedy algorithm for submodular function optimization with a very low computational complexity [10]. Both computational methods described in [8] and [9] are incapable of dealing with observability constraints. [9] argued that its proposed mutual information criterion includes complete observability, which is obviously incorrect, because the latter, as demonstrated later in the paper, distinguishes the state estimate from its unconditional mean, which is the trivial estimate, whereas the former does not.

2. System Overview

At the voltage stability limit, the Jacobian matrix of power flow equations are singular. Ensuring a continuous power flow resolves this problem. Based on a load scenario, the continuous power flow provides solutions for load flow. Notably, it comprises the correction and prediction stages. The tangent predictor estimates the next solution for a specific pattern of load increase from a known base solution. In the correction stage, the Newton-Raphson technique aids in determining the exact solution. The conventional power flow employees this technique. Consequently, a new prediction comes up to provide a specific load increase through the new tangent vector. The corrector stage follows, and the process is continuous up to the critical point. At the critical point, the tangent vector is

0. The insertion of a load parameter reformulates the first power flow in continuation load flow.
Injected powers can be written for the k bus of an n-bus system as follows:

$$P_k = \sum_{l=1}^{N} |V_k||V_l|\,|Y_{kl}| cos(\delta_k - \delta_l - \theta_{kl})$$

$$Q_k = \sum_{l=1}^{N} |V_k||V_l|\,|Y_{kl}|\, sin(\delta_k - \delta_l - \theta_{kl})$$

$$P_k = PG_k + PD_k$$
$$Q_k = QG_k + QD_k$$

D and G subscripts indicate load and generation demand, respectively. A load parameter $\boldsymbol{\lambda}$ is inserted into demand powers $\boldsymbol{PDk_k}$ and $\boldsymbol{QD_k}$ simulate a load change.

$$PD_k = PG\ (1 + \lambda\ )$$
$$QD_k = QG(1 + \lambda\ )$$

3. Power Flow Solutions

Power flow refers to the energy transportation rate in transmission lines. The analytic solving of the power flow problem is a challenge. Therefore, iterative solutions on computer systems prove effective. Henceforth, this section reviews two solution methods, namely the Newton-Raphson and the Gauss iteration (Gauss-Seidel iterative) methods.
Studying power flow provides an understanding of the magnitude of information for every power system bus and the voltage angle. Thus, this sheds light on voltage conditions and generator and load power. In this process, one can analytically determine the generator reactive power output and the reactive and real power flow. Experts apply a range of numerical methods to come up with a solution because this problem is nonlinear.

Solutions to power flow issues start by determining the unknown and known variables. Significantly, these variables rely on the form of the bus. A Load Bus is that which has no connected generators. Conversely, a Generator Bus is that which has at least one connected generator. One selected arbitrary bus with a generator, called the Stack Bus, was the exception.
In resolving power flow problems, there is the basic assumption that at every Load Bus, the reactive power demand, and the real power demand (PD) at every Load Bus (QD). That is why "Load Buses" are termed as "PQ-Buses." Additionally, there is the assumption that the "voltage magnitude |V|" and the power generated (PG) are known for generator buses. Furthermore, the assumption for the "Slack Bus" is that the "voltage phase (θ)" and "voltage magnitude |V|" are familiar. Although it is possible to contrive a solvable system in which the Slack Bus has fixed vars (Q) and fixed angle (θ), selecting the biggest generator to function as the Slack Bus enhances the regulation of V and θ. Significantly, the reference phase angle is also integral in setting the system frequency (F). The fact is that Theta is the "constant" aspect of the time-varying quantity. Therefore, the Slack Machine plays a fundamental part in the regulation of system frequency. The process occurs in real-time while providing power flow calculations. Thus, the "voltage angle and magnitude" are known for each Load Bus and should be solved. Regarding the Slack Bus, no variables should be solved. There are unknowns in a system comprising R generators and N buses. Resolving this requires an equation that does not incorporate new unknown variables. The power balance equation is one of the possible equations to use in this case. The equation can be provided for reactive and real power for every bus. Hence, this equation is as follows:

$$P_k = \sum_{l=1}^{N} |V_k||V_l|\,|Y_{kl}| cos(\delta_k - \delta_l - \theta_{kl})$$

A breakdown of this equation is as follows

P_k -net power injected at bus k ,
$|V_l|$ –Voltage magnitude
δ_l - Angle of ith bus
$|Y_{kl}|$ -Magnitude of the bus admittance matrix ($YBUS$).
θ_{kl} -angle of YBUS corresponding to the kth row and lth column

The following is the power balance equation

$$Q_k = \sum_{l=1}^{N} |V_k||V_l|\,|Y_{kl}|\, sin(\delta_k - \delta_l - \theta_{kl})$$

Q_k - Net reactive power injected at bus k.

Vol $\begin{bmatrix} \Delta\theta \\ \Delta|V| \end{bmatrix} = -J^{-1} \begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix}$

and J is a matrix of partial derivatives known as a Jacobian

$$J = \begin{bmatrix} \frac{\partial P}{\partial \theta} & \frac{\partial P}{\partial |V|} \\ \frac{\partial Q}{\partial \theta} & \frac{\partial Q}{\partial |V|} \end{bmatrix}$$

The linearized system of equations is solved to determine the next guess (m + 1) of voltage magnitude and angles based on:

$$\theta^{m+1} = \theta^m + \Delta\theta$$

$|V|^{m+1} = |V|^m + \Delta|V|$

The process is continuous until it meets the stopping condition. The role of root finding routines is to evaluate every step to determine whether the current outcome is good. The tests conducted in this process are termed as stopping tests or termination conditions. The tests are represented as follows:

Residual size $|f(x)| < \epsilon$
Increment size $|x_{new} - x_{old}| < \epsilon$

Number of iterations: $ITCount > ITMAX$; IT is the iteration

The residual size is a vital choice because at the solution, the residual is zero. Nonetheless, this is a bad choice since the residual can be minutes despite iterate being far from the actual solution. The increment size is an excellent choice due to quadratic convergence nature of Newton's model. In this process, the increment excellently approximates the true error. The third stopping criterion is applied after the iteration numbers surpass the maximum. Hence, this is a safety indicator to determine the iteration's capacity to terminate infinitely. The following is an outline of the power flow problem solutions include an attack.

- Guess all the unknown angles and magnitudes. In most cases, scholars begin with a "flat start" by setting all voltage magnitudes at 1.0 p.u., and voltage angles at 0. Practically, utilizing the biggest generator as the Slack Bus promotes the regulation of θ and V.
- The most recent voltage magnitude and angle values should be used to resolve the power balance.
- The system should be linearized around recent voltage magnitude and angel values.
- Calculate changes in voltage magnitude and angle
- Provide an update of the voltage angle and magnitude
- Monitor stopping conditions and terminate when met.

4. PMU placement approach

The critical observability of the grid is ensured in the initial step of PMU placement in this project. The next step is to raise the PMU redundancy as much as possible, hence raising the grid's level of observability. As a result of this development, the grid will be less vulnera7. ble to attacks from outside sources. the possible false data injection attack while simultaneously using PMUs to improve grid observability The central notion counter cyber-attack PMU placement approach involves the use of provide excellent attack feasibility security for the nodes, lowering the vulnerable to cyber-attacks of the grid The issue of determining the order in which PMUs should be placed inside a stage can be dealt with by determining the attack feasibility of the PMU buses and then ranking them.

5. False Data Injection Attacks

In the linear model, the attacker fools the control center mainly by keeping the measurement residual unchanged, although the attacker has injected bad data into meters [1]. This is the targeted "false data injection attack," where the attacker focuses on finding an attack vector with the capacity to input a precise error into specific state variables. On the other hand, the "random false data injection attacks" involve the hacker aiming to locate attack vectors as far as the outcome is a wrong estimate of the state variables. Both attacks have the capacity to damage the power systems significantly. Nonetheless, random false data injection is more comfortable to execute. Regarding the "false data injection attacks," a possible attack scenario has been developed to enhance the understanding of ways in which the attacker can develop attack vectors to penetrate the existing poor measurement detection strategies.
Denoting a as the vector of malicious data, which is injected into the original measurement data z, therefore, the measurement vector is polluted as $z_{bad} = z + a$ after attack.
Denoting c as the deviation vector of the estimated state variable before and after the attack, the estimated state variable vector after attack can be represented as

$$\boldsymbol{x_{bad} = x + c}$$

$$\boldsymbol{\hat{x}_{bad} = (H^T WH)^{-1} H^T H_{zbad} = (H^T WH)^{-1} H^T H(z + a)}$$

$$\boldsymbol{\hat{x}_{bad} = \hat{x} + (H^T WH)^{-1} H^T Wa = \hat{x} + c}$$

The target of the attacker is to find the vector of malicious data which keeps the measurement residual unchanged before and after attack.$\hat{x}_{bad} = \hat{x} + c$, then:

$$\boldsymbol{\|z_{bad} - H\hat{x}_{bad}\| = \|z + a - H(\hat{x} + H^T WH)^{-1} H^T Wa\|}$$

6. Voltage-Loading Parameter (V-λ) Curve

The (V-λ) curve proves useful in analysis processes involving power flow solutions to monitor the impacts of the system voltage on the system due to an increase in power transfer. A range of load flow solutions produces this curve for various load levels that are distributed uniformly. In this process, the power factor remains constant. Moreover, the generator rating increases the generated active power proportionally. It is fundamental to determine the given load's critical point. The fact is that it can contribute to the system's voltage collapse. Different researchers have utilized various load flow analysis to propose voltage stability indexes. The objective of these

scholars is to assess the voltage stability limits. Nonetheless, when applying the Jacobian model alongside the Newton-Raphson method, the outcome is singular at the critical point. Additionally, a divergence is evident for load flow solutions near the critical limit. Thus, the continuous load flow eliminates these disadvantages.
The load bus makes it easy to draw the P-V curve as shown in figure (1), permitting the calculation of maximum transmissible power. Every transfer power value is corresponding to the voltage value at the bus until V-Vcrit. Any further decline in power at this point contributes to the bus voltage deterioration. The uppermost section of the curve reveals acceptable operations, while the lower side indicates unstable operations. Ensuring that the bus voltage is away from the critical voltage by an upper value decreases the voltage collapse risk. Therefore, the (V-λ) curve is fundamental in determining the collapse margin, contingencies, and the system's critical operating voltage.

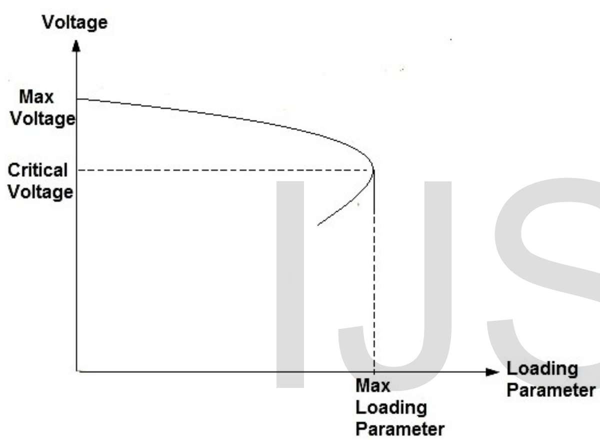

Figure 1: P-V Curve

7. Optimal PMU Placement to Mitigate False Data Injection Vulnerability

Optimal PMUs Placement is another term for minimal PMU placement (OPP). OPP refers to the smallest number of PMUs that can be placed in a network while still extracting all of the necessary data for a given application. In this context, OPP is a combinatorial problem, which means that N must be equipped with PMUs out of a total set of K system substations (or buses). N can be any number between 1 and K, so the number of possible combinations is given by:

$$\text{Number of combination} = \sum_{i=1}^{k} \binom{k}{i} = \sum_{i=1}^{k} \left(\frac{K!}{(K-i)!.\,i!}\right)$$

- State Estimation Methods: The following methods for optimal placement of PMUs are based on the concept of static state estimation, formulated as a nonlinear set of equations, as follows:

$$\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}) + \epsilon \quad [2]$$

Where:
z (z ∈ Rm): Measurement vector
x (x ∈ Rn): State vector
∈ (E ∈ Rm): Measurement vector error
h (h: Rm → Rm): Relationship between measurement vector and state vector

The Newton-Raphson method is commonly used to solve Equation (2). The use of devices capable of providing voltage and current phasors, such as PMU, results in a linear relationship between the state variables and the variables' measurements, as shown below:

$$\boldsymbol{z} = \boldsymbol{H}(\boldsymbol{x}) + \epsilon \quad [3]$$

Where H (H ∈ Rm X n) is the matrix of "state" of the system. Typically, m > n, and the solution of equation (3) is obtained by the least square's method.

State estimation methods are intended to monitor the entire system with the minimum number of measuring devices, applying the concepts of linear state estimation, and using the following placement general rules:

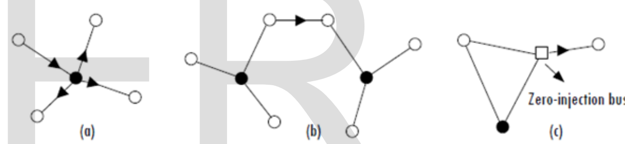

Figure (2)

- Rule 1: Assign the measurement to a bus where the PMU has been placed, including the measurement of current in each branch connected to that bus, see Figure 2a.
- Rule 2: Assign a pseudo-measurement of voltage at each bus seen by a PMU.
- Rule 3: Assign a pseudo-measurement of current to each branch bus connected to two voltage known buses seen in Figure 2b.
- Rule 4: Assign a pseudo-current measurement to each branch where the current can be calculated indirectly using Kirchhoff's current law. This rule applies when the current balance in a bus is known. If the current N-1 bus incidents are known, the last current can be calculated by difference, Figure 2c.

8. Experimental Results and Discussion

ISSN 2229-5518

Numerical simulation was performed on standard IEEE 9-bus, 14-bus, and 24-bus and 30-bus test systems to determine strategic locations for PMU placement under various observability levels in order to reduce node cyber vulnerability. In this work, state estimation method used to create multi-stage PMU deployment plans. This work also discusses the role of lowering the PMU requirement for different observability levels. The simulation results for the IEEE systems are discussed in detail, test systems are summarized in Tables 1.

a) Limited Observability of Each Bus with a Single PMU

The proposed method is intended to keep the system completely observable even if any one of the PMUs fails. In general, a bus is observed by a single PMU using a direct or a pseudo measurement. With the exception of double lines or more between buses, where a bus may be observed by the same PMU more than once. In general, a minimum redundancy level of one ensures complete system observability for any single PMU or single interconnection between bus outages. Each bus should be observed by at least two PMUs to increase the reliability of system observability. This ensures that a PMU outage or an interconnection failure between two buses will not result in a loss of observability. Table 1 shows different system result.

b) Robust Observability of Each Bus with at least Double PMU

In this case, each bus bar can be seen at least twice from the PMU, either directly or indirectly. To determine the ideal PMU numbers and locations for systems, we used the PSAT program with Dir (N-1) Spanning Trees and MATLAB optimization with state estimation programming.

The strategic selection of the minimum number of PMUs and their optimal location in order to ensure complete observability to determine the minimum number of PMUs in accordance with the constraints, which determined the optimal location of the PMUs in accordance with the maximum branches of the bus bar within these constraints, and then ensuring maximum redundancy as in figure 2 for 30-bus system.

Whichever approach is used to locate the PMU, it can be retrieved by placing it at the busbar with the most branches and then checking the system's observability. If the system's Basbars are visible twice, the placement is complete. Unless this is the case, the placement must be continued.

TABLE I: OPTIMAL NUMBER AND PLACEMENT OF PMU (OBSERVABILITY EACH BUS ONCE) FOR STATE ESTIMATION METHODS			
System Network	**# PMU**	**Optimal Location**	**Redundancy**
IEEE 9	2	4,7	12
IEEE 14	5	1,4,6,10,14	18
IEEE 24	6	2,8,10,15,17,20	22
IEEE 30	7	2,7,9,10,16,21,23,24	36

Table II summarizes the test findings for the offered approaches; there are multiple solutions for determining the ideal number and placement of PMUs set in the absence of zero injection buses.

The simulation results for the IEEEs -bus system are summarized in Table II. Each bus may be seen by at least two PMU using the optimization methods.

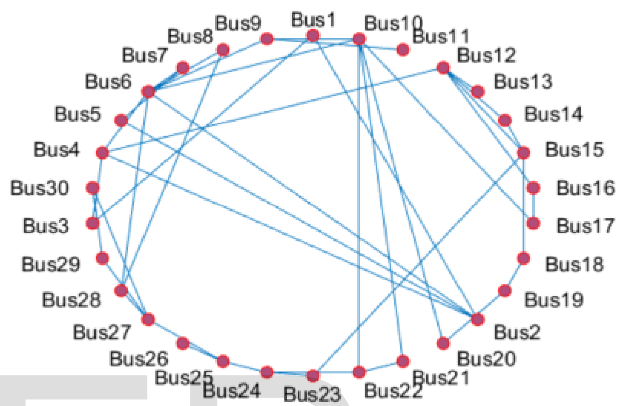

TABLE I: OPTIMAL NUMBER AND PLACEMENT OF PMU (OBSERVABILITY EACH BUS MULTIPLE) FOR STATE ESTIMATION METHODS			
System Network	**# PMU**	**Optimal Location**	**Redundancy**
IEEE 9	2	5,7	20
IEEE 14	5	1,3,7,10,12	32
IEEE 24	6	3,8,11,15,17, 23	47
IEEE 30	7	1,4,7,14,16,19,20,22	61

Figure (2) maximum redundancy 30-bus

9. Case study

The IEEEs -30 bus system simulation results are examined. We test the power transfer capacities vs voltage magnitude or the indicator of the static stability curve in three different conditions. The first scenario involves the deployment of PMUs with restricted observability and the placement of several PMUs on buses 2,7,9,10,16,21,23, and 24. From figure (3), The system can handle power up to 15.5 p.u. and an average voltage of 1.0 p.u., while the system's minimum knee point is 0.92 p.u.

Scenario 2 is the same as scenario 1, but with a false date injected into bus 7, 9, and 18, figure (4) shows that power transfer has been reduced to 9.5 p.u. and the maximum voltage has been reduced to 0.85 p.u., the reason being that the false date injected into the system via spoofing sensor brought the system closer to instability status.

Third Scenario is when we redeploy the PMUs based on robust observability approach and set them at 1,4,7,14,16, 19,20, and 22. We have now replicated the false date injection portion from the second scenario, injecting false dates into bus 7, 9, and 18. When we compare the second scenario to the third, we find that the result in figure (5) has been significantly improved, despite the fact that we used the same number of PMU with a different deployment strategy. This resulted in an improvement in the system security by increasing the buses' observability as proposed.

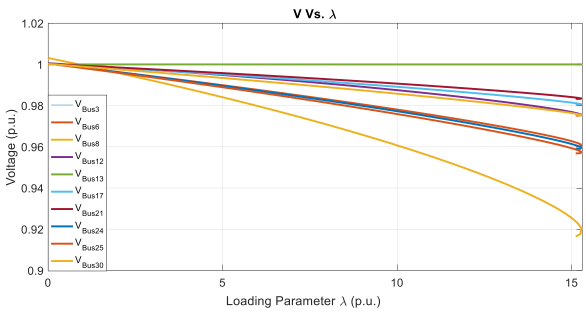

Figure (3)

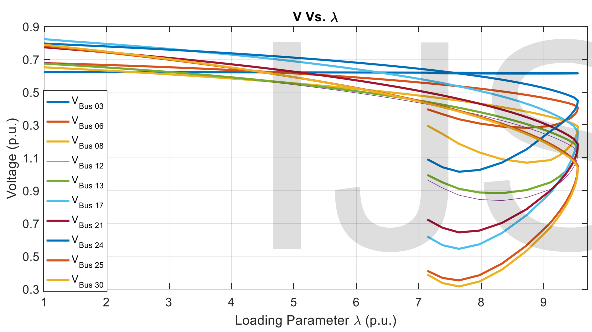

Figure (4)

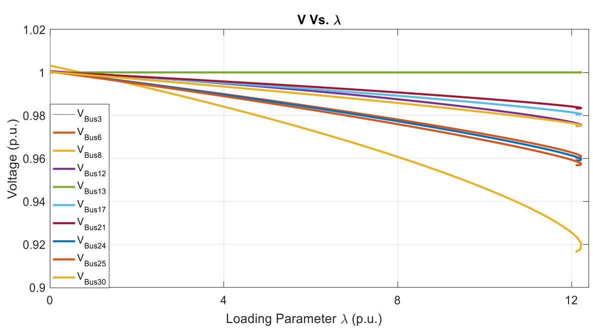

Figure (5)

10. Conclusion

In this paper we investigate full observable whole system measurements with maximum redundancy and minimum number of PMUs to mitigate false data injection vulnerability because each bus monitor by at least 2-3 PMUs, if the PMU injected with false measurement, then back up PMUs that observe similar bus indirectly identify that false data. Aside from the placement of PMUs, multiple location options are eliminated by selecting the combination of buses with the highest redundancy, with the possibility of losing one of the PMUs in the system considered. Simulation results IEEE-30 bus test systems with state estimation optimization method indicate satisfactorily provides full observable whole system measurements with maximum redundancy and minimum number of PMUs.

11. References

[1] R. F. Nuqui and A. G. Phadke, “Phasor measurement unit placement techniques for complete and incomplete observability,” IEEE Trans. Power Delivery, vol. 20, no. 4, pp. 2381–2388, 2005.

[2] J. Aghaei, A. Baharvandi, A. Rabiee, and M. Akbari, “Probabilistic PMU placement in electric power networks: An MILP-based multi objective model,” IEEE Trans. Indust. Informatics, vol. 11, pp. 332–341, April 2015.

[3] S. Chakrabarti and E. Kyriakides, “Optimal placement of phasor measurement units for power system observability,” IEEE Trans. Power Systems, vol. 23, no. 3, pp. 1433–1440, 2008.

[4] M. Hajian, A. M. Ranjbar, T. Amraee, and B. Mozafari, “Optimal placement of PMUs to maintain network observability using a modified BPSO algorithm,” Int. J. Elect. Power Energy Syst., vol. 33, no. 1, pp. 28–34, 2011.

[5] S. Chakrabarti, E. Kyriakides, and D. G. Eliades, “Placement of synchronized measurements for power system observability,” IEEE Trans. Power Delivery, vol. 24, no. 1, pp. 12–19, 2009.

[6] K. G. Khajeh, E. Bashar, A. M. Rad, and G. B. Gharehpetian, “Integrated model considering effects of zero injection buses and conventional measurements on optimal PMU placement,” IEEE Trans. Smart Grid, vol. 8, no. 2, pp. 1006–1013, 2017.

[7] A. Monticelli, “Electric power system state estimation,” Proc. IEEE, vol. 88, no. 2, pp. 262–282, 2000.

[8] V. Kekatos, G. B. Giannakis, and B. Wollenberg, “Optimal placement of phasor measurement units via convex relaxation,” IEEE Trans. Power Systems, vol. 27, no. 3, pp. 1521–1530, 2012.

[9] Q. Li, T. Cui, Y. Weng, R. Negi, F. Franchetti, and M. D. Ilic, “An information-theoretic approach to PMU placement in electric power systems,” IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 446–456, 2013.

[10] G. L. Nemhauser, L. A. Wolsley, and M. L. Fihser, “An analysis of approximations for maximizing submodular set functions-I,” Math. Programming, vol. 14, pp. 265–294, 1978.