Smart Grid and Renewable Energy, **2013, 4, 1-7**
http://dx.doi.org/10.4236/sgre.2013.46A001 Published Online September 2013 (http://www.scirp.org/journal/sgre)

Vulnerability Analysis of Wide Area Measurement System in the Smart Grid

Mohd Rihan[1], Mukhtar Ahmad[1], M. Salim Beg[2]

[1]Electrical Engineering Department, AMU, Aligarh, India; [2]Electronics Engineering Department, AMU, Aligarh, India.
Email: m.rihan.ee@amu.ac.in, doctormukhtar@gmail.com, mirzasalimbeg@yahoo.com

Received February 23rd, 2013; revised March 23rd, 2013; accepted April 8th, 2013

ABSTRACT

The smart grid will be a power grid more "aware" of its operating state and having the ability to self-heal. These features may be incorporated into the grid by implementing a phasor measurement units based wide area measurement system. Such a system will help in better real time monitoring and control of the grid. However, the wide area measurement system is subject to challenges with respect to its security. In this paper, a comprehensive analysis of security issues with a wide area measurement system is presented and the research efforts required to be taken are identified. Moreover, the effect of communication failure on a PMU installed system has been presented using integer linear programming.

Keywords: Wide Area Measurement Security; PMU; Smart Grid; Smart Grid Security

1. Introduction

Interconnected power systems span large geographical areas and virtually work as a single machine. The interconnected nature of the power system makes economical use of the power generated and improves the overall reliability. However, this increase in reliability comes at a price of increased risk associated with the possibility of a minor disturbance propagating and results in complete shutdown of the whole system [1]. Analysis has shown that most of the large scale blackouts shared a common thread and could have been prevented or at least these effects could have been mitigated. Leaving aside the natural causes of blackouts in a number of cases, the blackout condition was precipitated because of some controllable events. Some of these events are: lack of reactive power support, ageing equipment, lack of coordination in preventive measures, inadequate monitoring and communication equipments, and human error involved because of lacking automation [2]. With large interconnected power systems, blackouts are inevitable. The need is to develop a mechanism which should prevent the conditions leading to blackouts and even if one occurs the system should be able to recover very quickly. It requires a power grid which is more aware of its operating state and should be able to "self-heal" in case of a failure. Such a power grid was coined as "smart Grid".

Smart Grid will be characterized by a two-way flow of electricity and information to create an automated, widely distributed energy delivery network. It incorporates into the grid, the benefits of distributed computing and communications, to deliver real time information to balance power supply and demand [3]. Smart grid is the integration of power infrastructure with an information infrastructure, combining the maturity of the electric grid with the efficiency, connectivity, and cost gains brought about by Information Technology. Although there is no formal definition of a smart grid but based on its features proposed in the literature, the smart grid may be considered as a power grid in which modern sensors, communication links, and computational power are used to improve efficiency, stability, and flexibility of the system [4].

Fast and accurate real time monitoring throughout the grid is a fundamental requirement of the smart grid. Phasor measurement units may be deployed in the power grid to achieve this feature. Phasor Measurement Unit (PMU) is a device which measures both magnitude and angle of voltage and current. Moreover, these measurements are synchronized via the Global Positioning System (GPS). These measurements are highly accurate and sampled at a high rate sufficient to monitor the dynamic performance of the power grid in a much improved way. In fact, widely deployed PMUs in the power grid will

completely change the way that state estimation has been performed over the years. Due to all these factors, utilities are working towards installing PMU based Wide Area Measurement Systems (WAMS) in their networks. Such a network will facilitate accurate measurement of Synchrophasors at the network buses and their transmission to the control centre for contingency analysis and initiation of control actions. However, one of the key issues in the successful implementation and operation of such a system is the availability of a reliable communication system. In addition, there are other security issues with a WAMS like reliance on GPS and cyber security. In this paper, a comprehensive analysis of security issues with a WAMS is presented and the research efforts required to be taken are identified. Moreover, the effect of communication failure on a PMU installed system has been presented using integer linear programming. The structure and benefits of a WAMS are described in Section 2. Section 3 presents the security issues with WAMS and research directions to be pursued. Section 4 describes the optimal PMU placement problem while in Section 5 the effect of communication failure on optimal PMU placement has been analyzed. Section 6 presents the conclusions drawn from the present work.

2. Wide Area Measurement System

The smart grid influence all parts of a power system: generation, transmission and distribution. However the transmission system in a smart grid is set to be completely revolutionized with the help of synchrophasor measurements using Phasor Measurement Units (PMUs). The PMUs measurements are synchronized through Global Positioning system (GPS). With PMUs, advanced communications and computing techniques it will be possible to precisely measure the state of a power grid. It will be useful in preventing cascading blackouts. Today's power system operators take action in the multi-second to multi-minute time frame, but PMU based system can make and execute decisions in the100 millisecond time frame. A number of widely distributed PMUs in the power system may be utilized to implement a Wide Area Measurement System (WAMS) [5]. The architecture of a typical WAMS is shown in **Figure 1**. It consists of widely distributed PMUs in the power grid. These PMUs send the measurements to Phasor Data Concentrator (PDC). In general one PDC caters to a fixed number of PMUs. The PDC collects and sort the data based on the time tags. It keeps the data required for local applications and transmits the data for advanced applications to a super PDC through a dedicated communication network. These three layers of a WAMS may be categorized as: data acquisition, data management and applications layers [6].

The PMU based WAMS is one of the most important technologies expected to play a key role in the smart

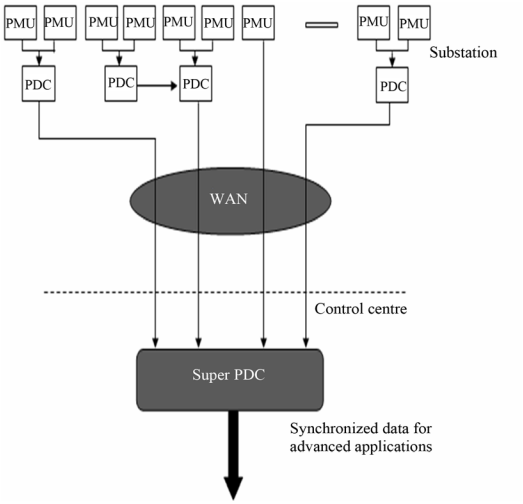

Figure 1. Wide area measurement system.

grid. The WAM technology may be utilized for the following [7,8].

2.1. Preventing Blackouts

PMU data provide information about the system at a common instant of time that can be used for real-time dynamic analysis. The real time information will be extremely useful in continuous monitoring and early detection of abnormalities. Timely initiation of corrective action will help in restricting the disturbance to a smaller area.

2.2. Improved State Estimation

The set of complex voltage phasors across its buses completely specifies the system; it is known as the system state. State estimator utilizes telemetered measurements from Remote Terminal Units (RTUs) to generate an optimal estimate of the system state. However these measurements do not contain the phase angles due to the difficulty associated with the synchronization of measurements. Consequently the phase angle has to be estimated with the slack bus as reference. However with the advent of Phasor Measurement Units (PMUs) this difficulty can be removed as the PMU measures voltage and current phasors synchronized through GPS. Due to technical and economical constraints it may not be feasible to install PMUs at every bus of the system. Therefore the existing SE can be improved by using data from a few PMUs installed at critical locations [9].

2.3. Transmission Line Congestion

The traditional approach to real-time line congestion management is based on the Nominal Transfer Capability, computed off-line using conservative hypothesis concerning thermal, voltage or stability limitations. However

the WAMS will allow computing the Real-time Transfer Capability for the actual operating conditions. Therefore it will result in better utilization of transmission line capacity. It is also expected that in future the PMU data will beintegrated with smart sensors measuring line temperature and sagetcthen the operational limit may further be increased.

2.5. Calibration of Instrument Transformers

2.4. The monitoring and control of a power grid depends heavily on the measurement of current and voltage signals derived from the secondary circuits of instrument transformers. The synchronized data available from WAMS may also be used to obtain accurate calibration of current and voltage transformers in a network.

2.6. Model Validation

For proper decision making during operation and control it is extremely important to have accurate models of synchronous machines of the system. PMUs can provide reliable information for validation of these models when located near or at the power plant.

3. Security Challenges to the WAMS

An essential feature of smart grid is the two way communication in order to monitor the 'health' of the system in a better way. However this two way communication feature presents new security challenges to protect data security and customer privacy. The smart grid as envisioned by the EPRI, should be resilient to the cyber/ physical attacks. As the WAM system is going to form an integral part of the smart grid, it is crucial to ensure the availability and integrity of the data it carries and the communication and computation infrastructure involved. As monitoring and control applications in the grid may rely on those data. The WAM systems are expected to operate over large geographical areas, which make the security aspect more complex. Some of the security vulnerability issues of WAMS are presented below [10,11].

3.1. Time Delay

The information from PMUs is time sensitive and it must reach the point of use within about two seconds. Late arriving data is either discarded or passed on to data store. Therefore any security measure adopted should not introduce a time delay.

3.2. Reliance on GPS

PMUs utilize the Global Positioning System for synchronization of the measurement. However the GPS signals may be jammed or spoofed by a hacker easily. If this happens then serious errors may be deliberately introduced in the time tags of the data. An invalid time stamp may result in a loss of data and visibility into the grid.

3.3. Configuration Management and Data Integrity

The crucial measurement data from the sensors should not be shared with anyone other than authorized data sharing partners. Not all PMUs deployed today support authentication for configuration. Moreover apart from the identity authentication, it is mandatory to preserve the integrity of data being shared between two authenticated entities.

3.4. Cyber Security

With the increased use of information and computation tools in the WAMS, its vulnerability to a cyber attack will increase. The ability of a phasor data concentrator or PMU to protect itself and recover from a cyber attack is not fully established and this area needs to be pursued rigorously.

3.5. Communication Infrastructure Vulnerabilities

To ensure availability of reliable data from PMUs it is necessary to ensure reliability of the communication infrastructure. The communication infrastructure being utilized at present for PMU communication contains vulnerabilities that may be exploited to interrupt communication or compromise integrity of data.

Based on the recommendations of various studies the requirements of security security measures for a WAMS are [11,12]:

- The security measures adopted should not in any way hamper the primary objective of the WAMS.
- The access to every PMU of a utility should be through an authentication procedure.
- The system should accept only authenticated and authorized changes in the configuration of the network.
- There should be proper mechanism to validate the integrity of data exchanged.
- The system should continue to perform essential functions in case of loss of synchronized measurements.
- The security mechanism should be able to minimize the impact of abnormalities on the performance of WAMS.

Considering the crucial role of synchronized measurements in order to achieve a smart grid, various groups/organizations are working on developing security

Table 1. Research initiatives on security challenges to WAMS.

Initiative	Research Direction
IEC 62351[13]	Describes recommended security profiles for various communications media and protocols
NERC CIP 002-009[14]	Deals with cyber-security standards
IEEE 1686-2007[15]	describes security measures from the perspective of an IED
IEEE C37.118[15]	the communications protocol for PMU communications
NISTIR[16]	guidelines for smart grid security

standards and recommendations for WAMS. **Table 1** provides a summary of these initiatives.

4. Optimal Placement of PMUs

Theapplication of state estimation (SE) for online power flow analysis was first proposed in [17] during the late 1960s. The estimation is done based on the measurement of real power injections and flows (P), reactive power injections and flows (Q) and voltage magnitudes V. The conventional SEs use the Intercontrol Center Communications Protocol (ICCP) for gathering the asynchronous data with a sampling rate of 1 sample per 4 - 10 seconds. The measurement model is given as:

$$Z = h(x) + e \tag{1}$$

Z: measurement data;
x: state of the system comprising of V and phase angle δ; except the phase angle at slack bus;
h: non linear power flow equations;
e: measurement noise.

The Weighted Least Squares Method (WLS) is most commonly used to generate an optimal estimate of the system state. The WLS minimizes the error between the measurements and the estimation of these measurements when using the state variables. The performance measure is given as:

$$J(x) = \left(z - h(x)\right)^T R^{-1} \left(z - h(x)\right) \tag{2}$$

This may be solved in terms of x to give:

$$x = \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} z \tag{3}$$

The jacobian matrix H may be calculated by determining the derivatives of each measurement with respect to the state variables.

The relationship between measurements and state variables is non linear and it has to be linearised and then the solution to WLS problem is obtained by using iterative technique. However if a PMU is placed at every bus of the system the relation between measurements and state variables is linear and a non-iterative least square solution may be used to determine the system state [18]. The PMU provides a synchronized measurement of the voltage phasor at a bus and the current phasors through the branches associated incident on it. The measurements are synchronized via the GPS signal with a frequency of about 30 samples per second. Due to technical and economical constraints it may not be feasible to install PMUs at every bus of the system. Moreover a system can still be made observable by placing PMUs only on few selected buses. Therefore the existing SE can be improved by using data from a few PMUs installed at critical locations. The data from these units may be utilized as pseudo measurement in the conventional SE. The result of such installations have reported benefits like increased accuracy, increased stability of estimator, less computation time, and increased redundancy etc. [19]. The observability of a system can be assessed in two ways; numerical and topological. Numerical observability is the ability of the system model to be solved for the state estimation. If the measurement jacobianmatrixis of full rank, then the system is considered to be numerically observable. Topological observability is defined as the existence of at least one spanning measurement tree of full rank in the network. A number of methods/algorithms have been reported for determining the optimal locations for PMUs in a system. An extensive review of these methods is given in [20].

Consider the IEEE 14 bus system shown in **Figure 2**. The objective is to find an optimal location set for PMUs which makes the system observable.

The optimal PMU placement problem can be defined as:

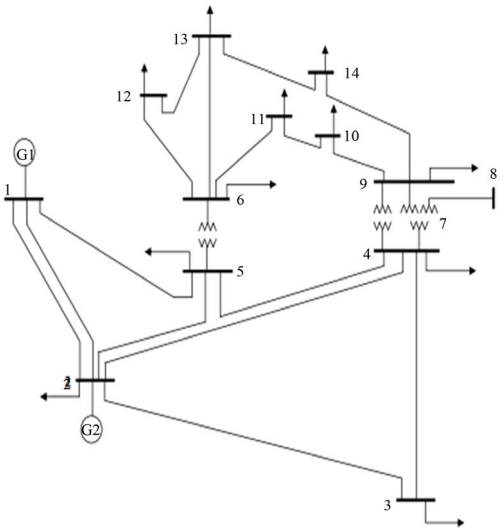

Figure 2. IEEE 14 bus system.

$$\min \sum_i^n w_i x_i \quad (4)$$

where

n is the number of buses in the system;

w_j is the cost of installation of a PMU on bus i;

x_i is a vector of dimension n and has binary values defined as:

$$x_i = \begin{cases} 1, & \text{if a } PMU \text{ is placed on bus } i \\ 0, & \text{if a } PMU \text{ is not placed on bus } i \end{cases} \quad (5)$$

Subjected to the following constraints:

$$x_1 + x_2 + x_5 \geq 1 \quad (6)$$

$$x_1 + x_2 + x_3 + x_4 + x_5 \geq 1 \quad (7)$$

$$x_2 + x_3 + x_4 \geq 1 \quad (8)$$

$$x_2 + x_3 + x_4 + x_5 + x_7 + x_9 \geq 1 \quad (9)$$

$$x_1 + x_2 + x_4 + x_5 \geq 1 \quad (10)$$

$$x_6 + x_{11} + x_{12} + x_{13} \geq 1 \quad (11)$$

$$x_4 + x_7 + x_8 + x_9 \geq 1 \quad (12)$$

$$x_7 + x_8 \geq 1 \quad (13)$$

$$x_4 + x_7 + x_9 + x_{10} + x_{14} \geq 1 \quad (14)$$

$$x_9 + x_{10} + x_{11} \geq 1 \quad (15)$$

$$x_6 + x_{10} + x_{11} \geq 1 \quad (16)$$

$$x_6 + x_{12} + x_{13} \geq 1 \quad (17)$$

$$x_6 + x_{12} + x_{13} + x_{14} \geq 1 \quad (18)$$

$$x_9 + x_{13} + x_{14} \geq 1 \quad (19)$$

The constraint equations (6)-(19) will ensure that the system is observable. These constraints may also be expressed as

$$A.X \geq [b]^T \quad (20)$$

A is called the bus to bus connectivity matrix defined as;

$$A_{ij} = \begin{cases} 1, & \text{if bus } j \text{ is incident to bus } i \\ 0, & \text{otherwise} \end{cases} \quad (21)$$

b is a vector having all its elements equal to 1.

Solving the optimal placement problem using Binary Integer Linear Programming (BILP), the buses for optimal location of PMUs for the IEEE 14 bus system are 2, 6, 7 and 9.

Here it may be noted that the number of PMUs required for complete observability of the system may reduce in the presence of conventional measurements and zero injection buses. However since in the present work the main objective is to show the effect of communication failure on optimal PMU placement, these measurements and zero injection buses have not been considered.

5. Placement of PMUs against Communication Failure

Availability of communication is an integral requirement for a PMU based measurement system. In the present work the effect of communication failure has been shown on the requirement of number of PMUs to maintain observability of the system. It is obvious that incorporation of this constraint in the PMU placement scheme will result into a greater number of PMUs than required under normal condition. Moreover this constraint may even limit the attainment of complete observability.

For studying the effect of communication failure on the observability of IEEE 14 bus system, it is assumed that there is failure of communication at buses 1 and 2. Under this condition, the constraints represented by (6) - (19) will be modified as follows:

$$x_5 \geq 1 \quad (22)$$

$$x_3 + x_4 + x_5 \geq 1 \quad (23)$$

$$x_3 + x_4 \geq 1 \quad (24)$$

$$x_3 + x_4 + x_5 + x_7 + x_9 \geq 1 \quad (25)$$

$$x_4 + x_5 \geq 1 \quad (26)$$

$$x_6 + x_{11} + x_{12} + x_{13} \geq 1 \quad (27)$$

$$x_4 + x_7 + x_8 + x_9 \geq 1 \quad (28)$$

$$x_7 + x_8 \geq 1 \quad (29)$$

$$x_4 + x_7 + x_9 + x_{10} + x_{14} \geq 1 \quad (30)$$

$$x_9 + x_{10} + x_{11} \geq 1 \quad (31)$$

$$x_6 + x_{10} + x_{11} \geq 1 \quad (32)$$

$$x_6 + x_{12} + x_{13} \geq 1 \quad (33)$$

$$x_6 + x_{12} + x_{13} + x_{14} \geq 1 \quad (34)$$

$$x_9 + x_{13} + x_{14} \geq 1 \quad (35)$$

Now again solving the optimal placement problem using BILP subjected to the constraints (22)-(35), it is found that the PMUs are required to be placed at five buses; 4, 5, 8, 11, 13. Which means a higher number of PMUs is required to maintain observability of the network in case of failure of communication at two buses of the system. Similarly failure of communication at larger number of buses was considered and the minimum number of PMUs required for each case was determined. The results are given in **Table 2**.

The results indicate that the number of PMUs required for maintaining observability of the network is increasing with the increase in the locations of communication fail

Table 2. PMUs required for observability of 14 bus system against communication failure.

noitacinummoC eruliaF	Number of PMUs Required	PMU Location
enoN	4	2, 6, 7, 9
1, 2	5	4, 5, 8, 11, 13
1, 2, 4	5	3, 5, 6, 7, 9
1, 2, 4, 6	5	3, 5, 7, 10, 13
1, 2, 4, 6, 13	6	3, 5, 7, 9, 11, 12
1, 2, 4, 6, 9, 10, 13	6	3, 5, 7, 11, 12, 14

ure. Although the system under consideration is a small system of 14 buses only but the increase in number of PMUs is significant. It may be inferred that for a large practical system, the difference in number of PMUs required under normal operating conditions and those required under communication failure will be considerably large.

These results are important as the utilities are planning to implement a PMU only linear state estimator in future. For this the network has to be observable with PMUs. However any such placement scheme should take into account the possibility of communication failure at the buses because otherwise the observability of the system may be lost and it will create serious problems in the monitoring of dynamic performance of the power network.

6. Conclusion

Wide area measurement systems based on phasor measurement units will form an integral part of the smart grid. However, there are various concerns related to the security of these systems which have been identified in the present work. Moreover, reliable communication is a fundamental requirement of a phasor measurement system. The effect of communication failure on a network installed with PMUs has been analyzed. It has been shown that the number of PMUs that are required to maintain observability increases significantly as the number of locations with communication failure increases and it may even restrict complete observability. Therefore availability of a robust communication infrastructure at the system buses should be an integral consideration of a PMU placement methodology.

REFERENCES

[1] W. T. Carson, "Improving Grid Behaviour," *IEEE Spectrum*, June 1999, pp. 40-45. doi:10.1109/6.769266

[2] D. Novosel, M. M. Begovic and V. Madani, "Shedding Light on Blackouts," *IEEE Power & Energy Magazine*, Vol. 2, No. 1, 2004, pp. 32-43. doi:10.1109/MPAE.2004.1263414

[3] V. K. Sood, D. Fischer, J. M. Eklund and T. Brown, "Developing a Communication Infrastructure for the Smart Grid," *IEEE Electrical Power & Energy Conference* (*EPEC*), Montreal, 22-23 October 2009, pp. 1-7. doi:10.1109/EPEC.2009.5420809

[4] M. Rihan, M. Ahmad and M. S. Beg, "Developing Smart Grid in India: Background and Progress," *IEEE International Conference on Innovative Smart Grid Technologies-Middle East*, Jeddah, 17-20 December 2011. doi:10.1109/ISGT-MidEast.2011.6220788

[5] J. S. Thorp, A. Abur, M. Bejovic, J. Giri and R. A. Roseles, "Gaining a Wider Perspective," *IEEE Power & Energy Magazine*, Vol. 6, No. 5, 2008, pp. 43-51. doi:10.1109/MPE.2008.927475

[6] M. Chenine, K. Zhu and L. Nordström, "Survey on Priorities and Communication Requirements for PMU-Based Applications in the Nordic Region," *IEEE Bucharest Power Tech Conference*, Bucharest, 28 June-2 July 2009. doi:10.1109/PTC.2009.5281956

[7] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, *et al*., "Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks," *Proceedings of the IEEE*, Vol. 99, No. 1, 2011, pp. 80-93. doi:10.1109/JPROC.2010.2060450

[8] M. Rihan, M. Ahmad and M. S. Beg, "Phasor Measurement Units in the Indian Smart Grid," *IEEE International Conference on Innovative Smart Grid Technologies-India*, Kerala, 1-3 December 2011. doi:10.1109/ISET-India.2011.6145392

[9] M. Rihan, M. Ahmad and M. Salim Beg, "Algorithms for Optimal Placement of PMUs in the Power Grid for Enhanced State Estimation," *Proceedings of International Conference on Roadmap for Smart Grid*, Central Power Research Institute, Bangalore, 3-4 August 2011.

[10] M. D. Hadley, J. B. McBride, T. W. Edgar, L. R. O'Neil and J. D. Johnson, "Securing Wide Area Measurement Systems," Prepared by Pacific Northwest National Laboratory for DOE, Washington, 2007.

[11] R. B. Bobba, *et al*., "Enhancing Grid Measurements: Wide Area Measurement Systems NASPInet and Security", *IEEE Power & Energy Magazine*, Vol. 10, No. 1, 2012, pp. 67-73. doi:10.1109/MPE.2011.943133

[12] H. Kenchington, *et al*., "Securing Tomorrow's Grid (Part I)," *Public Utility Fortnightly*, July 2011, pp. 29-42.

[13] http://www.iec.ch/smartgrid/standards/

[14] http://www.nerc.com

[15] http://www.ieee.org

[16] http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

[17] F. C. Schweppe and J. Wildes, "Power System Static State Estimation, Part I: Exact Model," *IEEE Transactions on Power Apparatus and Systems*, Vol. PAS-89, No. 1, 1970, pp. 120-125. doi:10.1109/TPAS.1970.292678

[18] L. Vanfretti, J. H. Chow, S. Sarawgi, D. Ellis and B. Fardanesh, "A Framework for Estimation of Power Systems

Based on Synchronized Phasor Measurement Data," *Proceedings of IEEE PES General Meeting*, Calgary, 26-30 July 2009. doi:10.1109/PES.2009.5275545

[19] F. Baalbergen, M. Gibescu and L. van der Sluis, "Modern State Estimation Methods in Power Systems," *Proceedings of IEEE PSCE*, Seattle, 15-18 March 2009. doi:10.1109/PSCE.2009.4840003

[20] M. N. Manousakis, G. N. Korres and P. S. Georgilakis, "Taxonomy of PMU Placement Methodologies," *IEEE Transactions on Power System*, Vol. 27, No. 2, 2012, pp. 1070-1077. doi:10.1109/TPWRS.2011.2179816

Nomenclature

PMU	Phasor Measurement Unit
GPS	Global Positioning System
OPP	Optimal PMU Placement
SMAW	Wide Area Management System
PDC	Phasor Data Concentrator
UTR	Remote Terminal Unit
IRPE	Electric Power Research Institute
SLW	Weighted Least Squares Method

