Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2018) 26: 1833 – 1846
© TÜBİTAK
doi:10.3906/elk-1710-27

Reduction of PMUs via hybrid PMU-RTU communication changeover in the case of cyberattack on vulnerable power transmission lines

Noorollah FARDAD, Soodabeh SOLEYMANI*, Faramarz FAGHIHI
Department of Electrical Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran

Received: 03.10.2017 • **Accepted/Published Online:** 06.04.2018 • **Final Version:** 27.07.2018

Abstract: A power grid strictly depends on information and communication technology. The key role of real-time measurement and information control for the reliable operation of a power grid is the responsibility of the phase measurement units (PMUs). As smart power grids encounter a variety of unauthorized malicious accesses such as cyberattacks, PMU placement is an important problem. In this study, a new algorithm was proposed to specify the minimum number of PMUs in the case of cyberattacks on their communication lines and equipment. In order to analyze complete observability of the distribution system, a range of probable contingencies for the vulnerable lines of a typical power system was discussed. The proposed algorithm implementation shows that the number of required PMUs can be reduced by removing irrelevant information through cyberattack circumstance intervals by using communication equipment potential.

Key words: Smart grid, phase measurement unit, cyberattack, observability

1. Introduction

The conventional measurements by remote terminal units (RTUs) in substations mainly include active and reactive power together with the amplitude of voltage and current. The precise time-synchronized measurements of voltage and current with their phase, frequency, and rate of frequency variation are done using phase measurement units (PMUs). PMUs' time synchronization is carried out through the satellites' GPS signals.

PMUs are applied for various purposes such as fault detection and fault location in smart grids [1], steady-state performance analysis [2], state estimation of power system scenarios for real-time supervision, power system protection and control [3,4], and voltage stability investigation [5].

Since it is not affordable to install PMUs on each bus for full observability, specifying the optimum number of PMUs under normal operation of the system has always been an important concern. To achieve this purpose, various methods, such as direct numerical techniques like integer linear programming (ILP) [6–8], binary integer linear programming [9], and genetic algorithms [10,11], are used.

Even though PMUs are adequately accurate, they might not be accessible due to interruption of communication lines or cyberattacks. Since PMUs are dependent on GPS signals, their manipulation leads to the loss of partially transferred data even if false data occur [12].

The security analysis is fully reliant on the network modeling; consequently, fault analysis of the communication paths is of extreme importance [13].

*Correspondence: s.soleymani@srbiau.ac.ir

Like supervisory control and data acquisition (SCADA) systems' cyber vulnerabilities, a cyberattack may be carried out on the phasor network with the purpose of injecting false data. Moreover, the attackers may impose abnormal operation conditions on the power system through GPS signal spoofing or jamming [14,15].

With the increase in the information technology in SCADA systems, the threats of cyberattacks should be seriously considered [16].

In order to neutralize cyberattacks, in the work of [17], a new algorithm for PMU optimum placement was offered, and the system not only defended against data integrity attacks but also assured the system observability. The authors of [18] reported on integrity attacks in a wide area measurement system (WAMS). In the work of [19], secondary protection through PMUs for data acquisition and storage was introduced and was effective in overcoming the outages. The authors of [20] used a hybrid genetic simulated annealing procedure to obtain the optimum number of RTUs and PMUs for a power system.

This paper discusses the potential vulnerabilities of WAMS including its related tools like PMUs. Its focus is on cyberattacks on the communication networks between PMUs. Using the available communication equipment and the minimum investment, the optimum PMU placement is achieved. Cyberattack occurrence on communication equipment and data transmission lines leads to defective data and fault command transfer followed by delayed computation.

The effects of communication line interruptions and damages to the related communication equipment on the system observability were also analyzed. A new algorithm based on ILP was presented for optimal PMU placement during cyberattack occurrence via the MIP Solver of GAMS software. In order to illustrate the good result of the proposed algorithm, a typical network was studied. Numerical results indicated that the suggested method ensures full observability of the system in the case of contingencies caused by cyberattacks.

The paper is organized as follows: in Section 2, WAMS system cybersecurity is evaluated. PMU optimal placement techniques are suggested by presentation of a new algorithm in Section 3. In Section 4, the proposed algorithm is simulated and the obtained results are discussed. Brief conclusions and future works are presented in Section 5.

2. WAMS Cybersecurity

A power network is an essential infrastructure and any weakness in its flexibility and reliability may have negative effects on the national economy. A WAMS, which includes measurement equipment and communication infrastructures, can facilitate the continuous and simultaneous supervision of the power system.

2.1. WAMS structure and its communication routes

The main components of the WAMS are the substations with PMUs, the substations with phasor data concentrators (PDCs), super PDCs (SPDCs), and communication systems. PMUs are located at the lowest level of the WAMS and network data are transferred through them [21]. Thus, WAMS reliability in the upper levels depends on the precision of the installed PMUs in the substations. Figure 1 shows the WAMS hardware architecture and communication [22].

It is necessary to clarify that PMUs' communication with SPDCs is completed via PDCs. In the control center, data analysis and different studies such as state estimation are accomplished. The SPDC is at the highest level of WAMS architecture, which stores the received measured value at the lowest level. It is notable that all control decisions towards protection and monitoring procedures are performed by SPDCs.

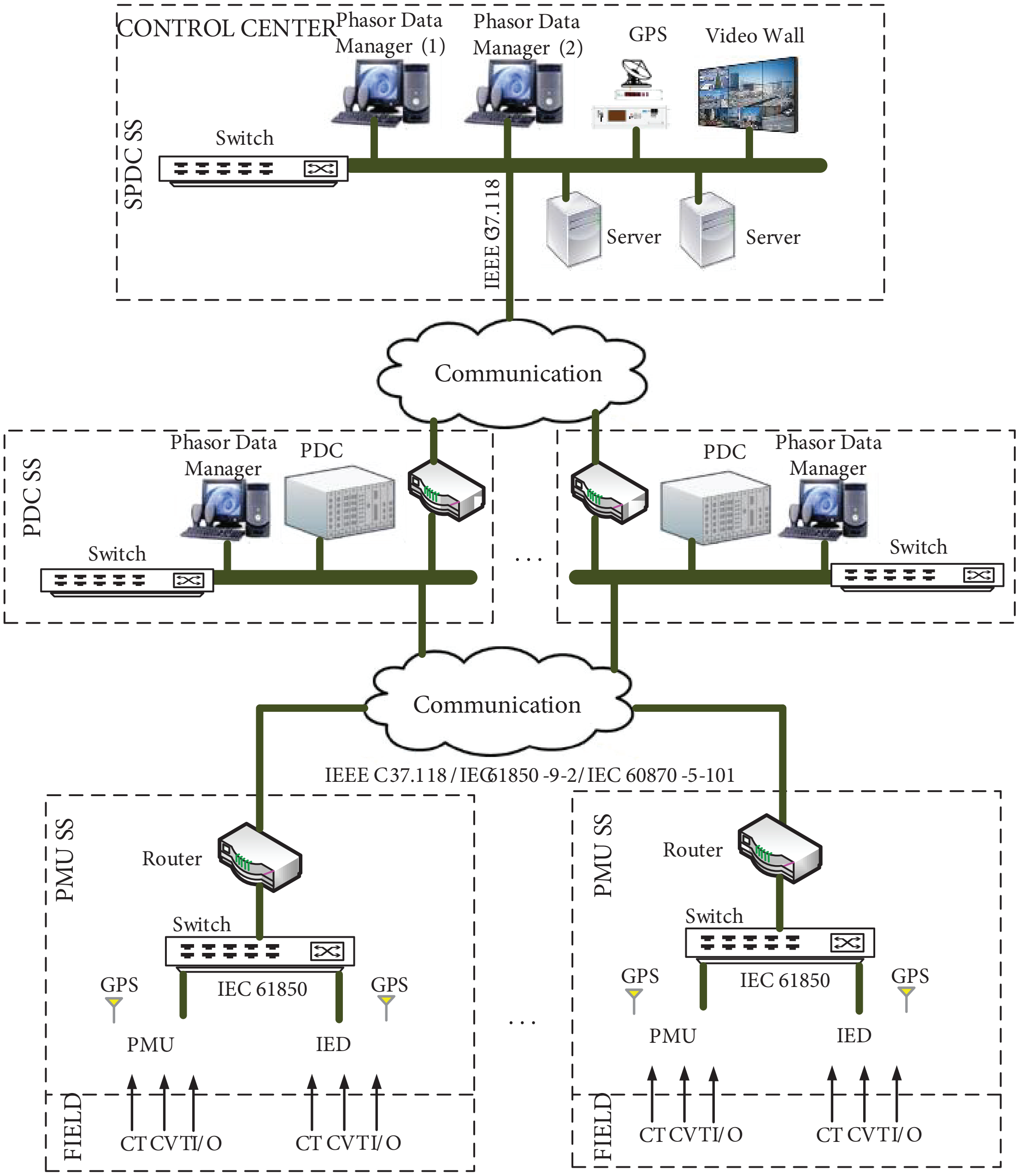

Figure 1. WAMS hardware architecture and communication.

An inclusive approach for understanding the security issues of the power system should incorporate the concept of physical cyberinfrastructures [23]. It indicates the relationship between the information communications and physical structures.

Fiber optic cables are the backbone of the network, but copper wires, radio waves, and microwaves together with a power line carrier (PLC) may also be applied [24].

Each attack on the information communication configuration can lead to an emergency situation for physical systems. Also, maloperation of a physical infrastructure device can cause a critical situation in part of a power system v25].

2.2. WAMS equipment cybersecurity

Regarding the importance of the transferred measured values in SCADA, attention to the WAMS cyberarrangement is significant and it must be equipped with adequate defense capabilities against cyberattacks. WAMS vulnerabilities are as follows [26–28].

2.2.1. PMU, PDC, and communication infrastructure cybersecurity

The aim of cyberattackers is to penetrate intelligent equipment such as PMUs and PDCs to identify the data transferred to the WAMS. The communication and the applied equipment such as switches and optical fiber terminals are among the important targets of the cyberattackers.

Different cyberattacks, such as man-in-the-middle attacks, threaten PMUs. The attackers intend to crack the data packages of the PMU network and replace them with false data. Also, they can carry out replay attacks, which lead to PMU data traffic penetration [29].

2.2.2. Access to transferred data

During attack occurrences such as false data injection to PMUs and PDCs, it is possible to send false commands to the equipment. Denial of service (DoS) attacks create interruption in data transfer to the control center. Any data manipulation by the attacker leads to deviations beyond expectations. If an attacker has access to PMUs of the network, that can change the measurements of all the PMUs [30].

2.2.3. GPS cybersecurity

Some cyberattacks can damage the GPS. Thus, they can disturb the synchronization, consequently changing the magnitude and phase angle [31].

3. Methods for optimum placement of secure PMUs

A PMU's optimum placement is applied to assure complete observability of the power system in normal operation situations as well as to consider the probable contingencies and the cyberattacks on the PMU's communication channels.

3.1. Secure PMU placement regarding the highest visibility

It is clear that, technically, the best state is achieved by installing a PMU on each bus, but economic constraints oblige the installation of an optimum number of PMUs, which may cover the technical requirements of network monitoring with acceptable probability. Furthermore, by allocating the PMUs on the designated buses, the system observability is obtained. Thus, state estimation through a couple of installed PMUs at the critical points is achieved. For installation of such equipment, the benefits, e.g., security, stability, redundancy increment, and reduced computation time, are considered [32].

System observability is closely related to the number of PMUs. Any unexpected power outage of the system or PMU will affect the system observability, which may cause a serious problem [33]. There are several algorithms for optimum placement of PMUs in the power system. An extensive review of these methods is suggested in the work of [34]. Due to saving the processor's calculation time, ILP is commonly used to obtain the optimum placement of PMUs. The ILP formula for PMU placement with the aim of full system observability is as follows [35]:

$$\min \sum_{m=1}^{n} Cx_m, \tag{1}$$

subject to:

$$AX \geq B_{PMU}, \tag{2}$$

$$C = [1\,,\,1,\ \ldots\,,\,1]_{\ 1\times n}, \tag{3}$$

$$X = [x_1,\, x_2,\, \ldots\,, x_m]^T\ \ ,\ x_m \in \{0, 1\}\,. \tag{4}$$

PMU placement x_m is stated by a binary variable. A, C, and n are the bus connectivity matrix, cost function, and number of system nodes, respectively.

$$x_m = \left\{ \begin{array}{ll} 1 & \text{if PMU is located at Bus m} \\ 0 & \text{Otherwise} \end{array} \right. \quad , \tag{5}$$

$$A_{i,j} = \left\{ \begin{array}{ll} 1 & \text{if node}\, i \text{ is connected to node}\, j \text{ or } i = j \\ 0 & \text{Otherwise} \end{array} \right. \quad , \tag{6}$$

where B_{pmu} is a matrix with n × 1 vertical vectors of which all components are one. The objective function of Eq. (1) is the minimum required number of PMUs for full system observability. The cost function is the same for all PMUs, which means that each PMU cost function is the same. The inequality constraint of Eq. (2) indicates that each system node should be observable by at least one PMU.

3.2. Secure PMU placement considering cyberattacks on data transferring equipment

Communication is an essential requirement for a PMU in the measuring system. It is clear that any failure of the communication routes increases the necessary number of PMUs in comparison with a normal situation. In relation to the probabilistic risk mitigation, the vulnerabilities and threat levels of PMUs in the case of cyberattacks can be reduced [36]. When PMUs are optimally placed in a power system, using branch and node theory, stochastic contingencies can be modeled. The interruption of line i-j in the case of a cyberattack will yield a new graph with one branch less than the main graph. Assuming the interruption of lines i and j, the constraint relations of the optimization equation are changed and the optimal final solution is achieved in a way that ensures complete observability under these conditions [37]. The algorithm shown in Figure 2 represents the occurrences of cyberattacks on the data transmission lines and their effects on PMU placement.

Based on this algorithm, the following points can be expressed.

1. The vulnerable lines in the network are identified via a decision-making method such as the fuzzy analytic hierarchy process.
2. Optimum placement of PMUs is determined in a healthy or intact network.
3. It is identified whether or not a cyberattack has been carried out on vulnerable lines.
4. In the case of cyberattacks, optimization problem solution constraints are updated. The cyberattacks on the vulnerable lines are identified by the intrusion detection systems or detection algorithms.
5. The optimal placement is calculated based on the restrictions of cyberattacks on communication lines.

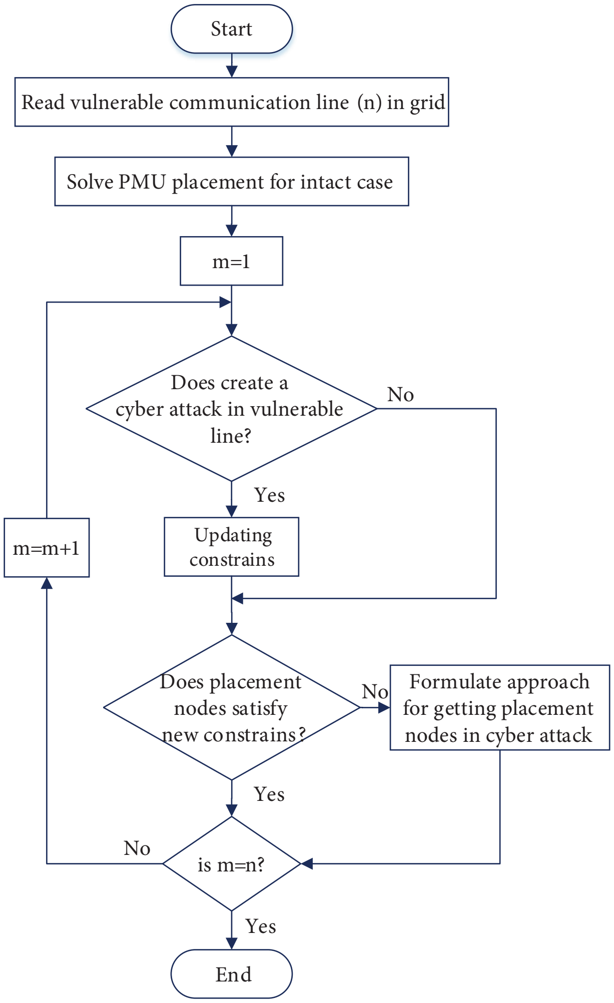
Start
Read vulnerable communication line (n) in grid
Solve PMU placement for intact case
m=1
Does create a cyber attack in vulnerable line?
No
Yes
Updating constrains
m=m+1
Does placement nodes satisfy new constrains?
No
Formulate approach for getting placement nodes in cyber attack
Yes
is m=n?
No
Yes
End

Figure 2. PMU optimal placement during cyberattack on data transmission lines.

3.3. Proposed algorithm

The applied method in Section 3.1 yields the system observability through secure PMU placement in an intact system. However, the method of Section 3.2 is implemented for allocation of PMUs in the case of cyberattacks on the communication line equipment. In this condition, more PMUs for system observability are needed. In the case of cyberattacks on data transmission lines, an approach is proposed based on the power network communication system, which can save the expenditure of PMU applications. During cyberattack occurrences on PMUs' communication network, with negligible accuracy of the measured values, alternative telecommunication equipment can be used. In this regard, measured RTU values are transferred through transmission channels that are not shared with PMUs' communication lines (like PLCs). Therefore, the proposed algorithm can be introduced in accordance with Figure 3 and according to the following points:

1. The vulnerable lines of the network are determined.
2. Based on the ILP method, PMU placement on the complete system is performed.
3. It is surveyed whether a cyberattack has occurred on the communication equipment in the data transmission line or not.

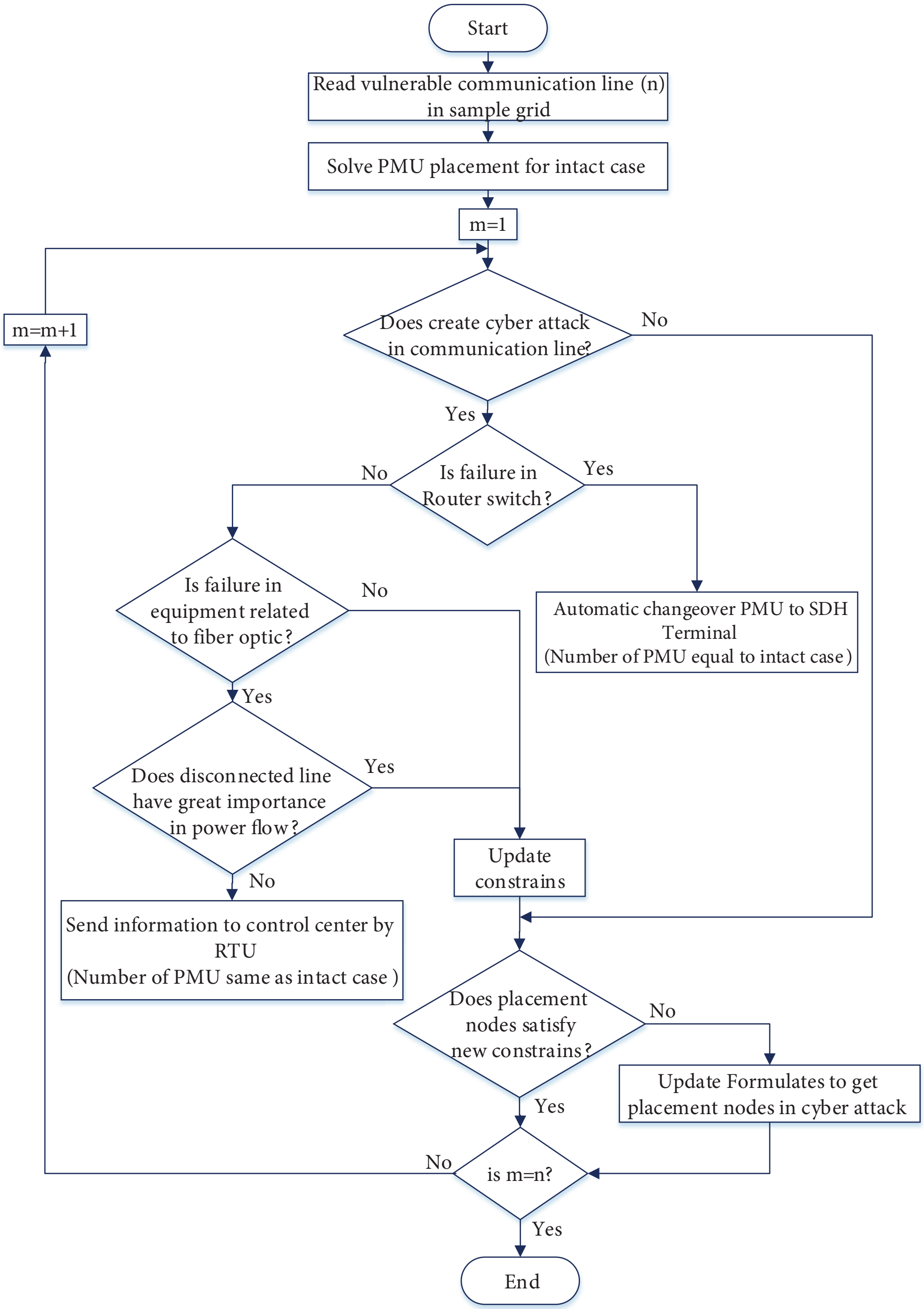
Start
Read vulnerable communication line (n) in sample grid
Solve PMU placement for intact case
m=1
m=m+1
Does create cyber attack in communication line?
No
Yes
Is failure in Router switch?
No
Yes
Is failure in equipment related to fiber optic?
No
Automatic changeover PMU to SDH Terminal (Number of PMU equal to intact case)
Yes
Does disconnected line have great importance in power flow?
Yes
Update constrains
No
Send information to control center by RTU (Number of PMU same as intact case)
Does placement nodes satisfy new constrains?
No
Update Formulates to get placement nodes in cyber attack
Yes
No
is m=n?
Yes
End

Figure 3. Proposed algorithm for PMU placement.

4. If a cyberattack occurs on the router that connects a PMU to the communication network, a failure signal from the router is received. In this state, the PMU is automatically connected to the current fiber optic terminal units such as the synchronous digital hierarchy (SDH). The number of PMUs will be the same as in the intact system (Figure 4).

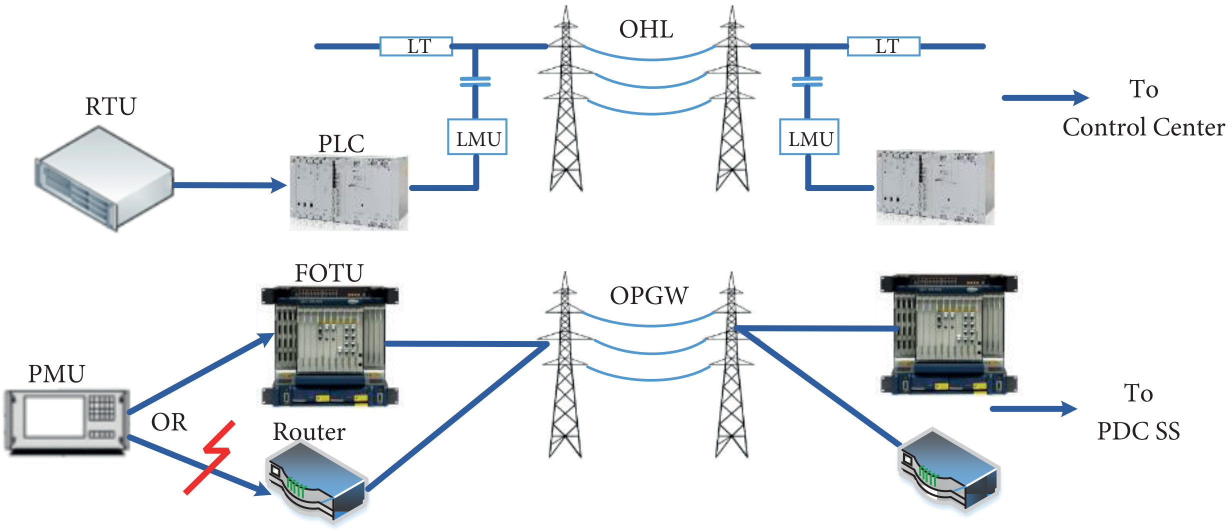

Figure 4. Data communication paths through PMU and RTU.

5. If a cyberattack leads to the total disconnection of the data transmission lines through optical fiber media, the line is investigated from the viewpoint of power flow and the amount of transition power.
6. If significant power is not transferred from the attacked line, by a little neglect of accuracy of the measured values, it is possible to use the data transferred by the RTU (Figure 4). In this case, the PMUs' values are the same as in the intact system.
7. Otherwise, and based on the algorithm presented in Figure 2, the PMUs' optimal placement is performed through the changes in network constraints of the intact mode.

4. Implementation of the proposed algorithm, analysis, and simulation

Figure 5 illustrates a single-line diagram of a sample network for implementing the proposed algorithm. This network includes a power plant with 3 units, a local SCADA, and 9 HV substations for supplying industrial plants. All lines have the same specifications and electrical parameters. The results of the power flow study are also demonstrated in the single-line diagram. Substations of this network are geographically and geostrategically specific.

Figure 6 shows the communication paths of data transfer for the sample network as a case study. There is the possibility of cyberattack and vulnerability for data transmission paths. Consequently, the cyberattacker always seeks to attack intelligent devices, including communication paths. In this paper, the cyberattacks on the communication routes are analyzed. The cybersystem includes ICT networks, intelligent equipment, and intelligent electronic devices. In the communication network, SDH fiber terminals and router switches are used for the communication infrastructure. In each substation, the measured values by RTUs are transferred to the SCADA center.

PMU placement for a case study network, considering different scenarios including the intact network and cyberattacks on the communication line equipment, is applied. ILP calculation via GAMS software is used for maximum observability. In real networks with numerous buses, it may use methods such as Strassen's algorithm and the divide and conquer method [38,39]. In order to decrease the degree of calculating complexity, an improved ILP method can also be applied to decrease the degree of complexity [40].

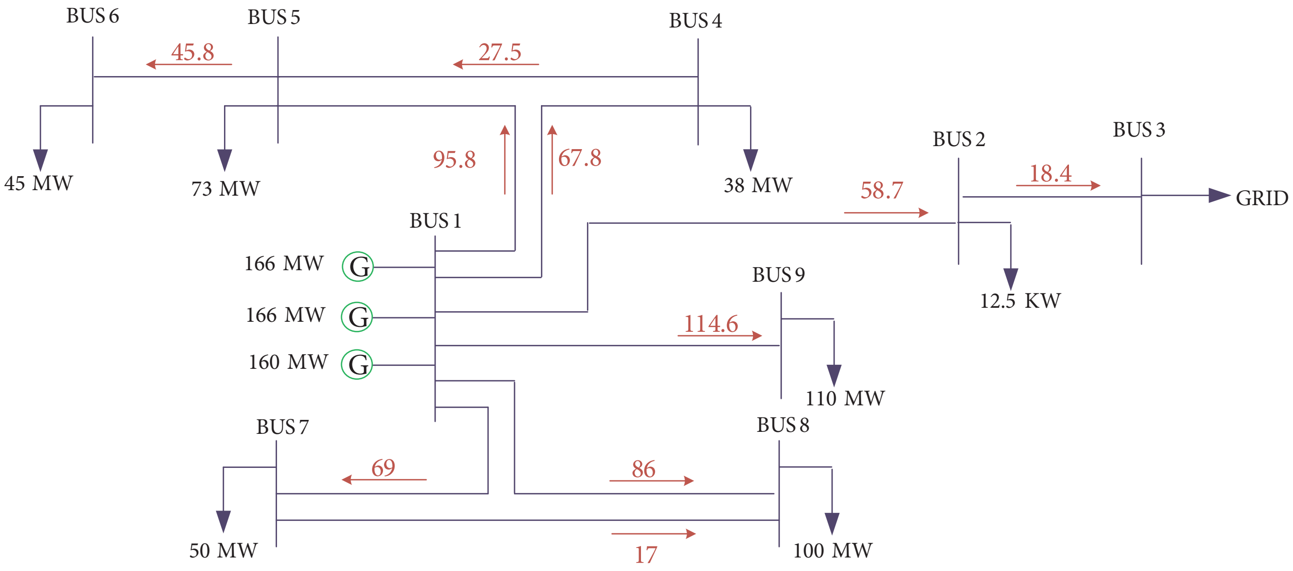

Figure 5. Single-line diagram with power flow values.

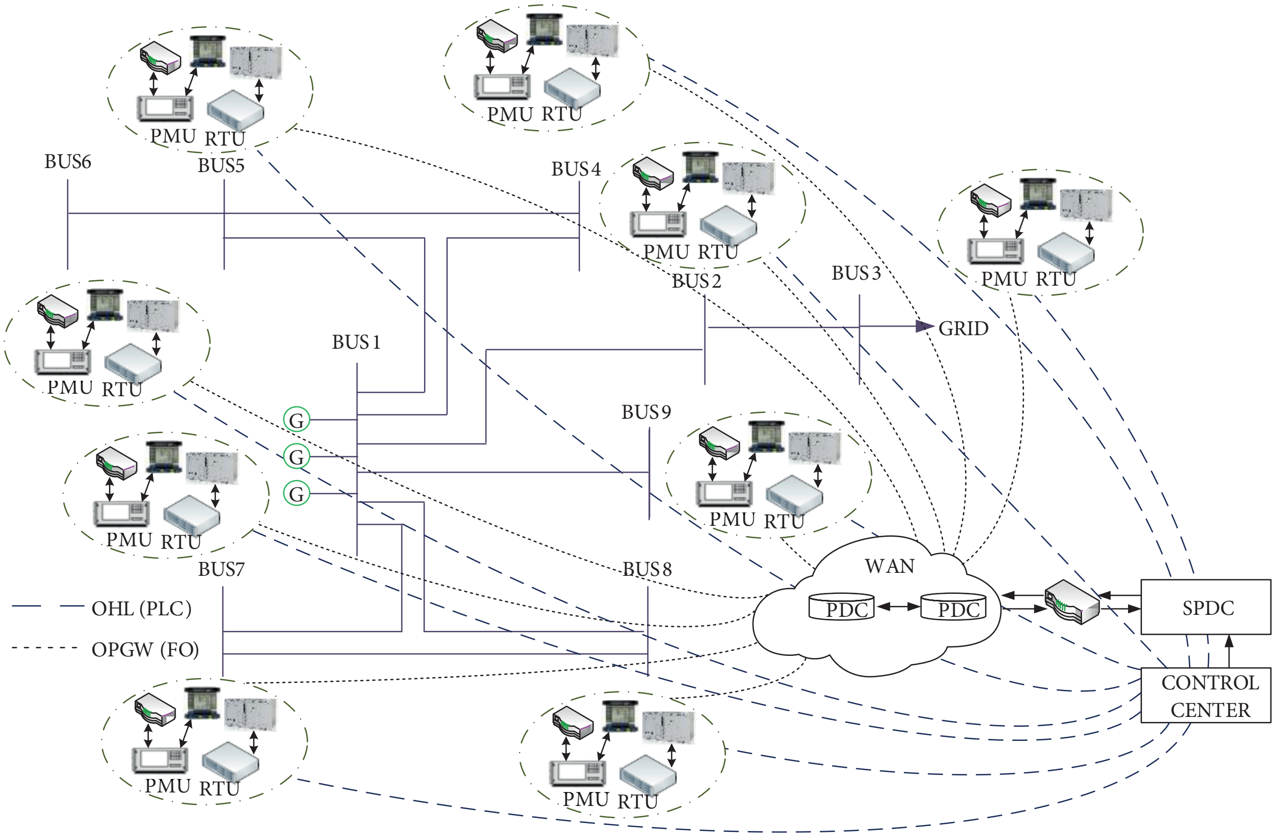

Figure 6. Communication paths between PMU, RTU, and control center.

4.1. Maximum observability without any cyberattack on the communication network equipment

The observability of the case study network is calculated. In this system, X includes 9 binary decision variables. Each constraint is formulated as each bus is topologically observable. The ILP problem is formulated as:

$$\min \sum_{m=1}^{n} Cx_m \,, \tag{7}$$

$$\text{subject to:} \quad \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \end{bmatrix} \geq \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} . \tag{8}$$

By solving the above mentioned ILP, the optimal placement of PMUs is $\{1, 2, 5\}$.

4.2. Maximum observability of the sample network with a cyberattack on the communication network equipment

Cyberattacks on the intelligent equipment of the vulnerable lines are investigated for 2 situations: attacks on the intelligent equipment of the vulnerable lines in an independent (individual) manner and sequential mode.

4.2.1. Case I: Attack on the vulnerable lines in independent mode

Based on the analysis of the sample network, 3 vulnerable lines (1–7, 1–8, and 1–9) were specified. According to Eq. (8), constraints in comparison with the perfect state are changed as shown in Table 1.

Table 1. ILP constraints for vulnerable lines (Case I).

Constraint	Line 1–7	Line 1–8	Line 1–9
g_1	$x_1 + x_2 + x_4 +$ $x_5 + x_8 + x_9 \geq 1$	$x_1 + x_2 + x_4 +$ $x_5 + x_7 + x_9 \geq 1$	$x_1 + x_2 + x_4 +$ $x_5 + x_7 + x_8 \geq 1$
g_2	$x_2 + x_1 + x_3 \geq 1$	$x_2 + x_1 + x_3 \geq 1$	$x_2 + x_1 + x_3 \geq 1$
g_3	$x_3 + x_2 \geq 1$	$x_3 + x_2 \geq 1$	$x_3 + x_2 \geq 1$
g_4	$x_4 + x_1 + x_5 \geq 1$	$x_4 + x_1 + x_5 \geq 1$	$x_4 + x_1 + x_5 \geq 1$
g_5	$x_5 + x_1 + x_4 + x_6 \geq 1$	$x_5 + x_1 + x_4 + x_6 \geq 1$	$x_5 + x_1 + x_4 + x_6 \geq 1$
g_6	$x_6 + x_5 \geq 1$	$x_6 + x_5 \geq 1$	$x_6 + x_5 \geq 1$
g_7	$x_7 + x_8 \geq 1$	$x_7 + x_1 + x_8 \geq 1$	$x_7 + x_1 + x_8 \geq 1$
g_8	$x_8 + x_1 + x_7 \geq 1$	$x_8 + x_7 \geq 1$	$x_8 + x_1 + x_7 \geq 1$
g_9	$x_9 + x_1 \geq 1$	$x_9 + x_1 \geq 1$	$x_9 \geq 1$

In the case of the loss of line 1–7 due to a cyberattack on the communication equipment, it is realized that the mentioned line's current measured phasor value provided by the PMU on bus 1 is lost. Therefore, PMUs are not able to observe bus 7. With disconnection of line 1–7, using PMUs of the normal states, it is seen that the g_7 constraint in column 1 of Table 1 is not satisfied and thus node 7 is not observable. Solving the objective function regarding the above-mentioned constraints, the result of the ILP is given as shown in Table 2.

Table 2. Optimal PMU placement during cyberattack (Case I).

Case	Optimal locations	No. of locations
Intact lines	1, 2, 5	3
Cyberattack to line 1–7	1, 2, 5, 7	4
Cyberattack to line 1–8	1, 2, 5, 7	4
Cyberattack to line 1–9	1, 2, 5, 9	4

4.2.2. Case II: Sequential attacks on the intelligent equipment of the vulnerable lines

Cyberattacks occurred sequentially in the intelligent equipment of the vulnerable lines. The constraints of the ILP problem were changed as stated in Table 3.

By solving the optimal ILP, the results shown in Table 4 can be obtained.

Table 3. ILP constraints to vulnerable lines (Case II).

Constraint	Line 1–7	Line 1–8	Line 1–9
g_1	$x_1 + x_2 + x_4 +$ $x_5 + x_8 + x_9 \geq 1$	$x_1 + x_2 + x_4 +$ $x_5 + x_9 \geq 1$	$x_1 + x_2 + x_4 +$ $x_5 \geq 1$
g_2	$x_2 + x_1 + x_3 \geq 1$	$x_2 + x_1 + x_3 \geq 1$	$x_2 + x_1 + x_3 \geq 1$
g_3	$x_3 + x_2 \geq 1$	$x_3 + x_2 \geq 1$	$x_3 + x_2 \geq 1$
g_4	$x_4 + x_1 + x_5 \geq 1$	$x_4 + x_1 + x_5 \geq 1$	$x_4 + x_1 + x_5 \geq 1$
g_5	$x_5 + x_1 + x_4 + x_6 \geq 1$	$x_5 + x_1 + x_4 + x_6 \geq 1$	$x_5 + x_1 + x_4 + x_6 \geq 1$
g_6	$x_6 + x_5 \geq 1$	$x_6 + x_5 \geq 1$	$x_6 + x_5 \geq 1$
g_7	$x_7 + x_8 \geq 1$	$x_7 + x_8 \geq 1$	$x_7 + x_8 \geq 1$
g_8	$x_8 + x_1 + x_7 \geq 1$	$x_8 + x_7 \geq 1$	$x_8 + x_7 \geq 1$
g_9	$x_9 + x_1 \geq 1$	$x_9 + x_1 \geq 1$	$x_9 \geq 1$

Table 4. Optimal PMU placement during cyberattack (Case II).

Case	Optimal locations	No. of locations
Intact lines	1, 2, 5	3
Cyberattack to line 1–7	1, 2, 5, 7	4
Cyberattack to lines 1–7, 1–8	1, 2, 5, 7	4
Cyberattack to lines 1–7, 1–8, 1–9	2, 5, 7, 9	4

4.3. Implementation of the proposed algorithm for the network's PMU placement with maximum observability

In this regard, cyberattacks on the vulnerable lines of the previous system were considered, but the situation of the proposed algorithm was evaluated for both states of Section 4.2. Table 5 depicts the results of the cyberattacks on the communication equipment based on the proposed approach.

Table 5. Optimal PMU placement during cyberattack.

Case	Outage	Attack to router switch		Attack to a whole line	
		Optimal	No. of	Optimal	No. of
	lines	locations	locations	locations	locations
I	1–7	1, 2, 5	3	1, 2, 5	3
	1–8	1, 2, 5	3	1, 2, 5, 7	4
	1–9	1, 2, 5	3	1, 2, 5, 9	4
II	1–7	1, 2, 5	3	1, 2, 5	3
	1–7–8	1, 2, 5	3	1, 2, 5, 7	4
	1–7–8–9	1, 2, 5	3	2, 5, 7, 9	4

- According to the proposed algorithm, in the case of cyberattacks on the router switch, the PMU is automatically displaced to the current optical terminal of the bus, and in this way data transfer will continue and the number of PMUs will be in the normal state. These conditions are specified in the third column of Table 5.
- When the occurred failure is not related to the router and only a communication fiber with a low amount of transition power is disconnected, the available RTU of the bus can be applied. This scenario took place with less certainty in comparison with the PMU data. Thus, during this period, RTU data can be used.
- Based on the power flow analysis, since the transferring power of line 1–7 is 69 MW, with slight neglect, RTU data can be used. Therefore, as shown in column 5 of Table 5, the number of PMUs did not change in comparison with the normal state of the network.
- When the emerged failure is not related to the router but this line transfers a high amount of power, the mentioned constraints should be modified and the observability can be obtained by increasing the number of PMUs.

5. Conclusion

In order to obtain power system observability, a variety of probable contingencies such as loss of measurement and disconnection of the communication lines are considered. In this paper, a new algorithm was proposed where, using the available communication equipment and facilities such as RTUs, observability was obtained by the minimum number of PMUs. The obtained results illustrate that in the case of cyberattacks on PMU peripheral equipment and the communication network, the number of PMUs did not significantly increase. In this paper, the application of the proposed algorithm was analyzed on a small sample network, but it is simple to apply it on large-scale networks, which will lead to a high amount of cost savings. In future works, hybrid systems including WAMS and SCADA during cyberattacks on the communication lines can be analyzed. Also, in real large networks, it can utilize the algorithm by a considerably reduced ILP model to decrease the degree of calculating complexity in further research.

References

[1] Gopakumar P, Reddy MJB, Mohanta DK. Fault detection and localization methodology for self-healing in smart power grids incorporating phasor measurement units. Electr Pow Compo Sys 2015; 43: 695-710.

[2] Fan D, Centeno V. Phasor-based synchronized frequency measurement in power systems. IEEE T Power Deliver 2007; 22: 2010-2016.

[3] Abbasy NH, Ismail HM. A unified approach for the optimal PMU location for power system state estimation. IEEE T Power Syst 2009; 24: 806-813.

[4] Yang Q, Chang L, Yu W. On false data injection attacks against Kalman filtering in power system dynamic state estimation. Secur Commun Netw 2016; 9: 833-849.

[5] Deepika K, Rao GK, Kumar JV, Sankar RR. Fast and real-time algorithm to detect impending voltage instability. International Journal of Control Theory and Applications 2017; 10: 407-412.

[6] Billakanti S, Venkaiah C. An effective binary integer linear programmed approach for optimal placement of PMUs in power systems. In: IEEE 2014 International Conference on Smart Electric Grids; 19–20 September 2014; Guntur, India. New York, NY, USA: IEEE. pp. 1-8.

[7] Esmaili M, Gharani K, Shayanfar HA. Redundant observability PMU placement in the presence of flow measurements considering contingencies. IEEE T Power Syst 2013; 28: 3765-3773.

[8] Khare G, Sahu N, Sunitha R. Optimal PMU placement using matrix modification based integer linear programming. In: IEEE 2014 International Conference on Power and Computing Technologies; 20–21 March 2014; Nagercoil, India. New York, NY, USA: IEEE. pp. 632-636.

[9] Aminifar F, Khodaei A, Fotuhi-Firuzabad M, Shahidehpour M. Contingency-constrained PMU placement in power networks. IEEE T Power Syst 2010; 25: 516-523.

[10] Allagui B, Aribia HB, Abdallah HH. Optimal placement of phasor measurement units by genetic algorithm. In: IEEE International Conference on Renewable Energies and Vehicular Technology; 26–28 March 2012; Hammamet, Tunisia. New York, NY, USA: IEEE. pp. 434-439.

[11] Kumar S. Optimal placement of PMU using probabilistic approach. In: IEEE International Conference on Engineering and Computational Sciences; 6–8 March 2014; Chandigarh, India. New York, NY, USA: IEEE. pp. 1-6.

[12] Shepard DP, Humphreys TE, Fansler AA. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. Int J Crit Infr Prot 2012; 5: 146-153.

[13] Bhonsle J, Junghare A. Optimal placing of PMUs in a constrained grid: an approach. Turk J Electr Eng Co 2016; 24: 4508-4516.

[14] Fan Y, Zhang Z, Trinkle M, Dimitrovski AD, Song JB, Li H. A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids. IEEE T Smart Grid 2015; 6: 2659-2668.

[15] Jiang X, Zhang J, Harding BJ, Makela JJ, Domı AD. Spoofing GPS receiver clock offset of phasor measurement units. IEEE T Power Syst 2013; 28: 3253-3262.

[16] Watts D. Security and vulnerability in electric power systems. In: 35th North American Power Symposium; 20–21 October 2003; Rolla, MO, USA. pp. 559-566.

[17] Yang Q, An D, Min R, Yu W, Yang X, Zhao W. On optimal PMU placement-based defense against data integrity attacks in smart grid. IEEE T Inf Foren Sec 2017; 12: 1735-1750.

[18] Paudel S, Smith P, Zseby T. Data integrity attacks in smart grid wide area monitoring. In: Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research; 23-25 August 2016; Belfast, UK. pp. 1-10.

[19] Ivanković I, Kuzle I, Holjevac N. Wide area information-based transmission system centralized out-of-step protection scheme. Energies 2017; 10: 633.

[20] Kerdchuen T, Ongsakul W. Optimal placement of PMU and RTU by hybrid genetic algorithm and simulated annealing for multiarea power system state estimation. In: International Conference on Technical Cooperation of Rajamangala Institute of Technology; 16–18 January 2009; Nakhonratchasima, Thailand. pp. 51-55.

[21] Hadley M, McBride J, Edgar T, Neil LO, Johnson J. Securing Wide Area Measurement Systems. Washington, DC, USA: US Department of Energy, 2007.

[22] Deng Y, Lin H, Phadke AG, Shukla S, Thorp JS , Mili L. Communication network modeling and simulation for wide area measurement applications. In: IEEE Innovative Smart Grid Technologies; 16–20 January 2012; Washington, DC, USA. New York, NY, USA: IEEE. pp. 1-6.

[23] Sridhar S, Hahn A, Govindarasu M. Cyber–physical system security for the electric power grid. P IEEE 2012; 100: 210-224.

[24] Zhang Y, Larsson M, Pal B, Thornhill NF. Simulation approach to reliability analysis of WAMPAC system. In: IEEE Power & Energy Society Innovative Smart Grid Technologies Conference; 18–20 February 2015; Washington, DC, USA. New York, NY, USA: IEEE. pp. 1-5.

[25] Mo Y, Kim T, Brancik K. Cyber–physical security of a smart grid infrastructure. P IEEE 2012; 100: 195-209.

[26] Heng L, Makela JJ, Dominguez-Garcia AD, Bobba RB, Sanders WH, Gao GX. Reliable GPS-based timing for power systems: a multi-layered multi-receiver architecture. In: IEEE Power and Energy Conference at Illinois; 28 February–1 March 2014; Champaign, IL, USA. New York, NY, USA: IEEE. pp. 1-7.

[27] Morris TH, Pan S, Adhikari U. Cyber security recommendations for wide area monitoring, protection, and control systems. In: IEEE Power and Energy Society General Meeting; 22–26 July 2012; San Diego, CA, USA. New York, NY, USA: IEEE. pp. 1-6.

[28] Rihan M, Ahmad M, Beg MS. Vulnerability analysis of wide area measurement system in the smart grid. Smart Grid and Renewable Energy 2013; 4: 1-7.

[29] Lin H, Deng Y, Shukla S, Thorp J, Mili L. Cyber security impacts on all-PMU state estimator-a case study on co-simulation platform GECO. In: IEEE Third International Conference on Smart Grid Communications; 5–8 November 2012; Tainan, Taiwan. New York, NY, USA: IEEE. pp. 587-592.

[30] Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. ACM T Inform Syst Se 2011; 14: 1-33.

[31] Kim TT, Poor HV. Strategic protection against data injection attacks on power grids. IEEE T Smart Grid 2011; 2: 326-333.

[32] Baalbergen F, Gibescu M, Sluis L. Modern state estimation methods in power systems. In: IEEE Conference on Power Systems Conference and Exposition; 15–18 March 2009; Seattle, WA, USA. New York, NY, USA: IEEE. pp. 1-6.

[33] Gou B, Abur A. A direct numerical method for observability analysis. IEEE T Power Syst 2000; 15: 625-630.

[34] Manousakis NM, Korres GN, Georgilakis PS. Taxonomy of PMU placement methodologies. IEEE T Power Syst 2012; 27: 1070-1077.

[35] Gou B. Generalized integer linear programming formulation for optimal PMU placement. IEEE T Power Syst 2008; 23: 1099-11104.

[36] Mousavian S, Valenzuela J, Wang J. A probabilistic risk mitigation model for cyber-attacks to PMU networks. IEEE T Power Syst 2015; 30: 156-165.

[37] Sodhi R, Srivastava S, Singh S. Optimal PMU placement to ensure system observability under contingencies. In: IEEE Power & Energy Society General Meeting; 26–30 July 2009; Calgary, Canada. New York, NY, USA: IEEE. pp. 1-6.

[38] Cormen TH, Leiserson CE, Rivest RL, Stein C. Introduction to algorithms. 2nd ed. Cambridge, MA, USA: MIT Press, 2009.

[39] Kleinberg J, Tardos E. Algorithm Design. Boston, MA, USA: Pearson Education, 2006.

[40] Gou B, Kavasseri RG. Unified PMU placement for observability and bad data detection in state estimation. IEEE T Power Syst 2014; 29: 2573-2580.