PMU Placement in Electric Transmission Networks for Reliable State Estimation against False Data Injection Attacks

Qiang Yang, *Member, IEEE*, Le Jiang, Weijie Hao, Bo Zhou, Po Yang and Zhihan Lv

***Abstract*— Currently the false data injection (FDI) attack bring direct challenges in synchronized phase measurement unit (PMU) based network state estimation in wide-area measurement system (WAMS), resulting in degraded system reliability and power supply security. This paper assesses the performance of state estimation in electric cyber-physical system (ECPS) paradigm considering the presence of FDI attacks. The adverse impact on network state estimation is evaluated through simulations for a range of FDI attack scenarios using IEEE 14-bus network model. In addition, an algorithmic solution is proposed to address the issue of additional PMU installation and placement with cyber security consideration and evaluated for a set of standard electric transmission networks (IEEE 14-bus, 30-bus and 57-bus network). The numerical result confirms that the FDI attack can significantly degrade the state estimation and the cyber security can be improved by an appropriate placement of a limited number of additional PMUs.**

***Index Terms*—Phase measurement units, state estimation, cyber attack, electric cyber-physical system**

NOMENCLATURE

$\mathbf{z}$	Measurement vector (i.e. active and reactive power flows, active and reactive power injections, voltage magnitudes and angles)
$\mathbf{x}$	System state variable vector (voltage magnitudes and angles)
$\mathbf{e}$	Measurement error vector (the error distribution is known)
$\mathbf{h(x)}$	Nonlinear function between measurement vector and the system state variable vector
$\mathbf{W}$	The weighting matrix
$\mathbf{J}_h$	Jacobian matrix derived from vector $\mathbf{h(x)}$
$\hat{\mathbf{x}}$	Estimated state vector
V_i	Voltage at bus i
θ_i	Phase angle at bus i
θ_{ij}	Bus phase angle difference ($\theta_i - \theta_j$)
$G_{ij} + jB_{ij}$	Line admittance between bus i and j
$g_{si} + jb_{si}$	Admittance of the shunt branch at bus i
Ω_i	A set of buses connected to bus i
X_0	State estimates under attack-free condition
X	State estimates under attack condition
E_0	The maximum state estimation deviation with available PMU placement
k	Attack impact coefficient
E	Estimation deviation metric

I. INTRODUCTION

IN recent decades, the advances of a number of enabling technologies (e.g., sensing, communication, intelligent control and decision-making) have driven the transition of the conventional electric power system to a smart grid. The existing supervisory control and data acquisition (SCADA) system can only obtain asynchronous snapshots of power system operation due to low sampling rate (with the poling cycle in minutes or even hours). Such statistical measurements can barely meet the stringent requirement of timely and accurate monitoring and control of smart transmission networks spanning over a large geographical area [1]. To this end, the WAMS is designed to continuously collect the network operational states through sophisticated digital devices, i.e. Phasor Measurement Units (PMUs), installed at specific locations in the transmission network. The PMUs can timely record and communicate GPS-synchronized dynamical state information with a high sampling rate (6-60 samples/second). The existing research effort, e.g., the North American Synchrophasor Initiative (NASPI) [2] and the Western Interconnection Synchrophasor Project (WISP) [3], have confirmed its benefit for dynamic health evaluation of large-scale power transmission grid. However, the complete replacement of SCADA legacy with WAMS is currently considered not impractical mainly due to the prohibitive reinforcement and maintenance cost. SCADA and WAMS

This work is supported in part by the National High Technology Research and Development Program (2015AA050202), National Science Foundation of China (51777183, U1509218) and Natural Science Foundation of Zhejiang Province (LZ15E070001).

Dr. Q. Yang, L. Jiang and W. Hao are with College of Electrical Engineering, Zhejiang University, Hangzhou, 310027, China (e-mail: qyang@zju.edu.cn). Dr. B. Zhou and Dr P. Yang are both with Department of Computer Science, Liverpool John Moores University, Liverpool, UK. Dr Z. Lv is with Department of Computer Science in University College London, London, WC1E 6EA, UK.

will coexist and complementarily support the wide-area monitoring and control in electric transmission networks.

The development of smart grid makes the electric power network and the underlying information and communications technology (ICT) system supporting its management functionalities highly coupled, which is considered as an integrated electric cyber-physical system (EPCS), as shown in Fig. 1. In fact, ECPS provides a novel analytical framework to investigate a number of key technical issues in electric power systems, including network modeling, topological and dynamical behavior characterization, cascading failure analysis and vulnerability assessment.

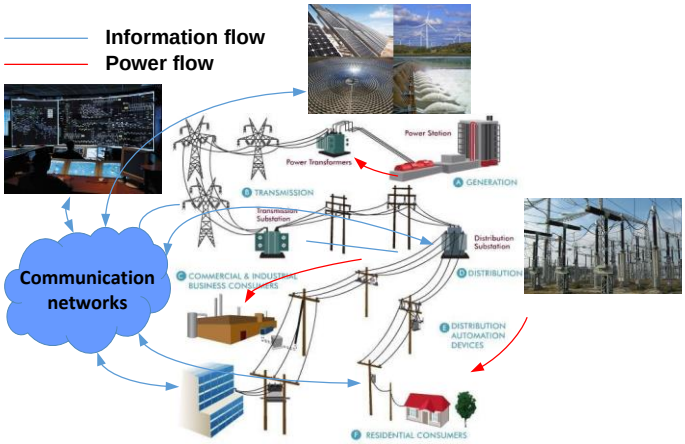


Fig 1. Cyber-physical system for electric power grid

II. Related Work

Existing studies have highlighted the importance of cyber security of ECPS against various forms of attacks from different aspects. In this paper, we look into the cyber-attacks in ECPS with a focus on the false data injection (FDI) attacks on PMU-based state estimation in power distribution networks. It is confirmed that the false data injection (FDI) attacks can circumvent bad data detection programs (e.g. [30], [31]) and inject bias into the values of the estimated state in power systems [4]. A number of recent studies have exploited the FDI attacks on power system state estimation and defense mechanisms, including detection-based methods (e.g. [5-7]) and protection-based methods (e.g. [8-16]).

The FDI attack detection approaches generally analyze the obtained measurements and detect the abnormal ones that cannot fit the expected distributions of historical measurements. A Kullback–Leibler distance (KLD) based method was proposed for FDI attack detection by tracking and calculating the distance between two probability distributions derived from measurement variations [7]. In [8], greedy algorithms were developed to strategically place secure PMUs at key buses in the power system to defend against data injection attacks with improved manageability and reduced cost. In [9], the authors exploited the graphical defending algorithms against false-data injection attacks through protecting the state variables with the minimum number of measurements. In [10], a risk mitigation model was presented for cyber-attacks to PMU networks through solving a mixed integer linear programming (MILP) problem to prevent cyber-attack propagation and maintain the observability of the power system. A detection and identification of cyber-attacks in PMU data based on the expectation-maximization algorithm was presented in [11]. The work in [12] designed the defense mechanism of FDI attacks on state estimation based on a least-budget strategy. In [13], an unobservable FDI attack on AC state estimation and its impacts on the physical system were studied. In [14], the authors exploited the optimal FDI attack strategy to cause the maximum damage and developed efficient algorithms to identify the optimal meter set for protection. In [15], the work proposed an efficient strategy for determining the optimal attacking region that requires reduced network information. Multiple robust estimators with different robustness properties to improve the overall cyber-security of power state estimation were investigated with the consideration of investment reduction [16].

In addition, solutions (e.g. [17-19]) are available to address the issue of optimal PMU placement with different objectives and deployment constraints. The optimal PMU placement can be obtained through minimizing the cost of overall WAMS (PMUs, phasor data concentrators and communication infrastructures (CIs)) [17]. An optimization formulation was proposed in [18] to improve the measurement redundancy with minimum number of PMUs while maintaining full system observability. The work in [19] focused on the minimization of total realistic cost with considering hidden but significant and integral part of PMU installation cost. The work in [27] developed a mixed integer programming model for optimal PMU deployment and optimal selection of existing PMUs to mitigate sparse unobservable attacks. A planning approach was developed in [28] for optimal PMU placement making the system more resilient to PMU failures. In particular, the authors in [29] enhanced the least-effort attack model to compute the minimum number of sensors that must be compromised to manipulate a given number of states, and developed an effective greedy algorithm for optimal PMU placement to defend against data integrity attacks.

Based on the aforementioned insights, this paper takes a different perspective to exploit the placement of additional PMUs considering the WAMS legacy to obtain different degrees of state estimation reliability against FDI attacks in the context of ECPS framework. The main technical contributions made in this work can be summarized as follows: (1) the adverse impact of FDI attacks on network state estimation is theoretically analyzed and assessed in a quantitative fashion for a range of attack scenarios (different attack levels, attack locations and measurement types) based on IEEE 14-bus network model; and (2) an algorithmic solution is proposed to identify additional placement of PMUs to obtain maximum cyber security against FDI attacks and validated for a range of standard electric transmission network models (IEEE 14-bus, 30-bus, 57-bus and 118-bus network).

The rest of this paper is organized as follows: the ECPS attacks are briefly overviewed in section III; Section IV presents the PMU-based state estimation under FDI attacks; Section V carries out the simulation experiments to assess the impact of FDI attack and PMU placement solution for different transmission network models; finally, the conclusive remarks are given in Section VI.

III. Overview of ECPS Attacks

The coupling of cyber and physical networks as well as the operational complexity and temporal-spatial characteristic make ECPS be vulnerable to cyber-attacks. Different forms of cyber-attacks, e.g. eavesdropping attacks, and malwares attacks, can significantly affect the operation of smart grid, from smart meters, transmission to distribution substations and control center. Theoretical models and tools are needed to obtain better insights in ECPS cyber-attacks and prevent, mitigate and tolerate cyber-attacks. For example, the authors in [20] presented a model of cyber-physical switching attacks and confirmed that a coordinated circuit breaker switching sequence can be designed to deliberately disrupt the network operation. In [21], an unobservable power injection attack evading the PMU measurement system was studied and its adverse impact on power system operation was analyzed. In [22], the authors proposed a sophisticated unique malware attack in the smart grid in a CPS framework. The replay attack that opponents records a sequence of sensor measurements and replays the sequence afterwards was studied in [23]. A holistic attack resilient framework is proposed in [24] to protect the integrated distributed energy resources (DER) and the critical power grid infrastructure from malicious cyber-attacks with improved grid reliability and stability.

In addition, the opponents may have the opportunities to inject false data or modify the available operational states at different parts of the ECPS, e.g. the real-time electricity pricing (RTP) data in advanced metering infrastructure (AMI), which can directly mislead the energy dispatch and power demand prediction. The cyber attacks on SCADA systems can also affect the decision-making process at the control center and result in issuing incorrect corrective control to the field control and protection devices, which may lead to large-scale network cascading failures. The opponents may hack the underlying communication infrastructure, including the communication protocols and communication devices or equipments (e.g. routers and switches). Currently power utilities tend to adopt the standard packet-switching based protocols (e.g. TCP/IP based protocols) and standard information models (e.g. IEC61850 in substations), which makes the power utility more vulnerable to the intentional attacks in comparison with the private or vendor's protocols. In summary, the cyber attacks can bring direct adverse or disastrous impacts on the operation of smart energy networks. This work focuses on the exploitation of FDI attack in PMU-based WAMS of electric transmission network.

IV. State Estimation and FDI Attacks

In WAMS, the PMUs are installed at the measurement points (buses) with the up-stream phasor data concentrators (PDCs), as shown in Fig. 2. The PMU measurements are rigorously synchronized through GPS satellite and made available to the remote electric transmission network control center to support network management functionalities, e.g. state estimation, dynamic model identification, model correction, transient stability prediction, low frequency oscillation analysis, fault location and protection.

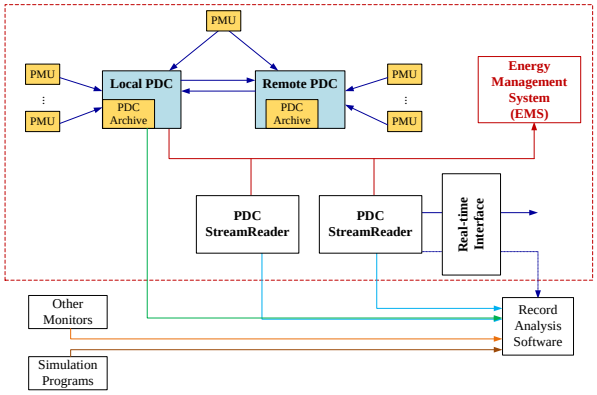


Fig 2. WAMS and synchronized PMUs in electric transmission network

A. PMU-based network state estimation

The state estimation of power system has been studied for years and the weighted least squire minimization is the most widely adopted method in state estimation programs to determine the state variable values [25]. The full non-linear power flow equations and a large amount of system data are needed to implement the state estimation. The power flows are nonlinearly dependent on the voltage magnitudes and angles, expressed mathematically as (1):

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

The state variables can be determined based on the weighted least square optimization problem given in (2):

$$\min F(\mathbf{x}) = (\mathbf{z} - \mathbf{h}(\mathbf{x}))^{\mathbf{T}} \cdot \mathbf{W} \cdot (\mathbf{z} - \mathbf{h}(\mathbf{x})) \tag{2}$$

where the elements of $\mathbf{W}$ correspond to the inverse of the accuracy of the individual measurements. The functions in the vector $\mathbf{h}$ depend on the type of measurements, i.e., active or reactive power flow on lines or as injections, voltage magnitudes and angles.

The iterative normal equation method can be adopted to solve (2). The first order optimality condition of this unconstrained optimization problem is formulated:

$$\frac{\partial F(\mathbf{x})}{\partial \mathbf{x}}\Big|_{\mathbf{x}=\hat{\mathbf{x}}} = -2\mathbf{J}_h^T(\hat{\mathbf{x}})\mathbf{W}(\mathbf{z} - \mathbf{h}(\hat{\mathbf{x}})) = 0 \tag{3}$$

The result is a nonlinear equation system which can be solved using an iterative process.

In fact, the faulty measurements can directly lead to significant errors in determining the state of a system, hence bad data detection schemes are used to detect them. Various forms of bad data detection algorithms are available and

mostly are based on the residual [25, 30] as follows.

$$\mathbf{r} = \mathbf{z} - \mathbf{h}(\hat{\mathrm{x}}) \tag{4}$$

This corresponds to the difference between the received measurement and the value for this measurement as a function of the estimated state. The FDI can be identified based on the largest normalized residual method if (5) is met, where τ is an appropriately predetermined threshold. The study in [25] indicated that, using the known error distributions and the theory of x^2 testing, the value of τ can be determined such that faulty measurements are identified if they exceed the expected probability distributions.

$$\|\mathbf{r}\| < \tau \tag{5}$$

B. Analysis of FDI on network state estimation

The FDI on WAMS can directly degrade the accuracy of the state estimation or make the network partially unobservable. It is indicated in [8] that the false data added to the measurement **a** can pass bad data detection if $\mathbf{a} = \mathbf{h}(\hat{\mathbf{x}} + \mathbf{c}) - \mathbf{h}(\hat{\mathbf{x}})$. Here, the FDI attack on network state estimation can either manipulate certain system state variables or manipulate certain measurements, which can be formulated and theoretically analyzed as follows:

Attack on system state variables: two types of system state variables are considered in state estimation, i.e. bus phase angle (θ) bus voltage magnitude (V). Once a specific state variable is tampered, the dependent measurements will also be affected based on the following equations.

(1) Real and reactive power injection at bus i

$$P_i = V_i \sum_{j \in \Omega_i} V_j (G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij}) \tag{6}$$

$$Q_i = V_i \sum_{j \in \Omega_i} V_j (G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij}) \tag{7}$$

(2) Real and reactive power flow from bus i to bus j

$$P_{ij} = V_i^2 (g_{si} + g_{ij}) - V_i V_j (g_{ij} \cos\theta_{ij} + b_{ij} \sin\theta_{ij}) \tag{8}$$

$$Q_{ij} = -V_i^2 (b_{si} + b_{ij}) - V_i V_j (g_{ij} \sin\theta_{ij} - b_{ij} \cos\theta_{ij}) \tag{9}$$

It can be observed from (6)–(9) that the attack on one state variable requires the manipulation of multiple measurements, e.g. the change of V_i needs a set of manipulations of P_i, Q_i, P_{ij} and Q_{ij} where $j \in \Omega_i$. If the FDI attack is carried out for multiple system state variables simultaneously, then the manipulation of more measurements needs to be implemented.

***Attack on certain measurements*:** a state measurment is determined by the system configuration and at least two system variables. Thus, to attack certain measurements, the change of least one state variable that controls the targeted measurement is required in FDI attacks.

C. PMU placement considering cyber attacks

Obviously, sufficient availability of PMUs in transmission networks can improve the performance of state estimation under FDI attacks due to data redundancy. With the available PMUs which obtain the system state observability, the proposed solution addresses the placement of additional PMUs to obtain the required accuracy of state estimation under attacks. The flowchart of the proposed algorithmic solution is illustrated in Fig. 3.

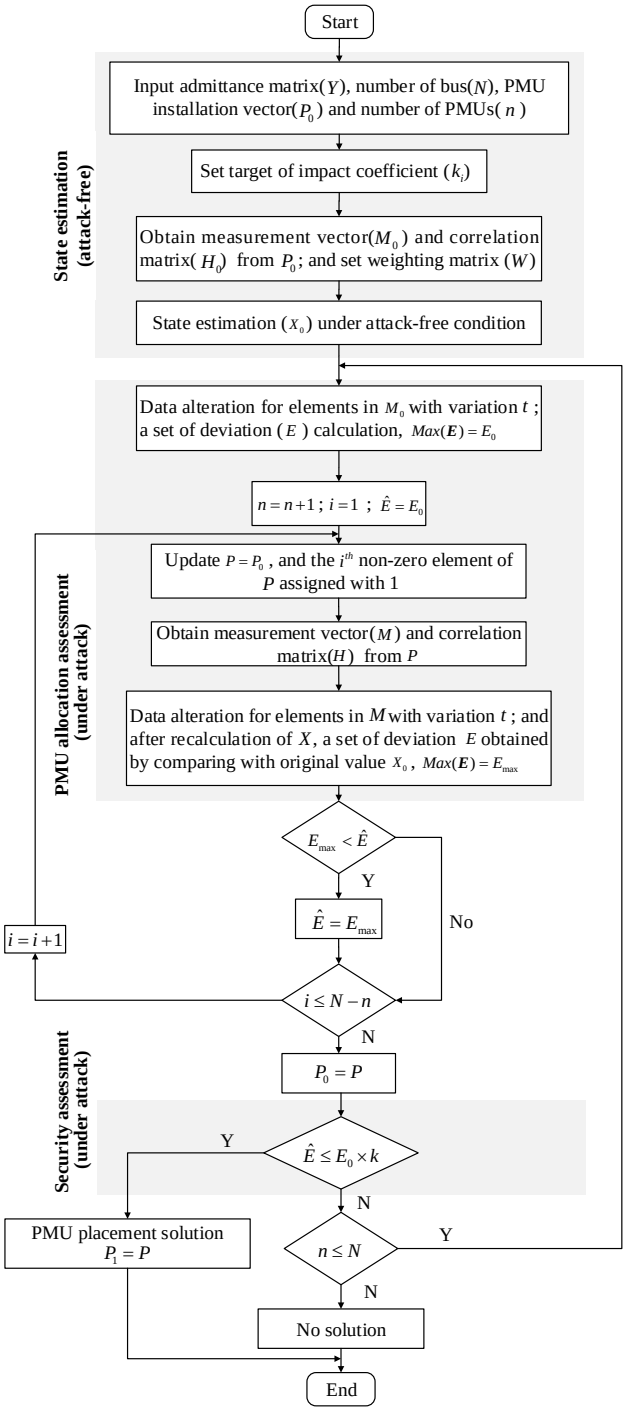


Fig.3 The flowchart of PMU placement considering FDI attacks

The key steps of the solution can be summarized as follows: (1) the most vulnerable buses which can impose the maximum adverse impact to the state estimation under FDI attacks are firstly identified; (2) the optimal placement of additional PMUs (number of PMUs and their locations) under FDI attack

is evaluated and determined through an iterative process; and finally, the obtained solution of PMU placement is further assessed to ensure the adverse impact on state estimation under FDI attack is managed to an acceptable range.

More specifically, an estimation deviation metric is defined to capture the inaccuracy of state estimation, as given in (10)

$$E=\frac{\sum_{i=1}^{N}\left|\frac{X(i)-X_0(i)}{X_0(i)}\right|}{N} \tag{10}$$

where N is the number of buses; X_0 and X are the estimated network states under attack-free and FDI attack conditions, respectively.

Here, the maximum deviation of state estimation from actual network states under same intensity of attack with the available PMU placement is denoted as base E_0, and the impact coefficient due to attacks is set as k, $k \in [0,1]$. In particular, the security assessment ensures the identified number of additional PMUs as well as the installation locations can guarantee the state estimation deviation within $E_0 \times k$ under FDI attacks (k can be pre-defined with different values to represent different state estimation accuracy requirements). Consequently, the system state observability and estimation accuracy under FDI attacks are simultaneously considered in the PMU placement.

V. Simulation Experiments and Numerical Result

A. PMU-based state estimation under FDI attacks

In this work, the impact of FDI attacks on network state estimation performance is quantified assuming that the state estimation is merely supported by the PMU-based WAMS. The performance is evaluated based on the IEEE 14-bus transmission network model [26] which requires at least 3 PMUs to obtain full network observation. Fig. 4 illustrates that in total 4 field PMUs are installed at the network buses with red circles (i.e. bus No. 2, 6, 8 and 9) to guarantee the system observability. Based on the given PMU placement in IEEE 14-bus network, the PMU measurements of both bus voltage and current can be obtained, respectively, as given in Table 1.

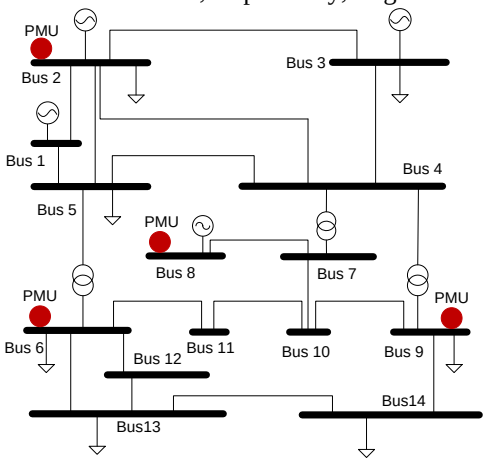


Fig 4. IEEE 14-bus transmission network with 4 PMUs

Table 1 Bus voltage and current measurements

Location	PMU measurements		Amplitude	Phase angle
Bus No.2	Voltage	Bus No. 2	1.046	-4.922 °
	Current	Bran. 2-1	1.496	-171.82 °
		Bran. 2-3	0.708	-9.583 °
		Bran. 2-4	0.546	-5.281 °
		Bran.2-5	0.398	-9.299 °
Bus No.6	Voltage	Bus No.6	1.064	-14.634 °
	Current	Bran. 6-5	0.432	-164.11 °
		Bran. 6-11	0.076	-40.338 °
		Bran. 6-12	0.077	-31.387 °
		Bran. 6-13	0.177	-36.220 °
Bus No.8	Voltage	Bus No. 8	1.093	-13.470 °
	Current	Bran. 8-7	0.163	-102.508 °
Bus No.9	Voltage	Bus No. 9	1.050	-15.145 °
	Current	Bran. 9-4	0.166	-165.422 °
		Bran. 9-7	0.274	155.797 °
		Bran. 9-10	0.062	-53.997 °
		Bran. 9-14	0.095	-35.906 °

This section presents a set of numerical result obtained from the simulation experiments through a comparative study. The network state estimation based on linear weighted least square approach is implemented and the network operational states can be estimated. Fig. 5 shows the network estimation and the exact network states (bus voltage amplitude and phase angle) under the attack-free condition, respectively. It can be seen that the state estimation algorithm based on the PMU measurements can well estimate the network states (the errors are within the acceptable range) without any cyber attacks. Here, the evaluation of FDI attacks on state estimation is carried out for three network scenarios considering the attack with different levels (case 1), at different locations (case 2) and on different measurement types (case 3), respectively. The FDI attacks are implemented through injection of randomly altered measurements with different degrees (e.g. 10%~30%), as adopted in existing studies (e.g. [7]).

Case 1: State estimation under different levels of FDI attacks

It is interesting to assess the adverse impact of data tampering at different levels on the network state estimation. Fig. 6 presents the estimated states of voltage amplitude and phase angle in the case that the PMUs installed at bus No. 2 is attacked with the voltage measurement values being randomly tampered at the level of 10%, 20%, and 30% compared with the exact PMU measurements, respectively. It is clearly demonstrated that that such attack can seriously affect the accuracy of the measurement of voltage amplitude, but with limited impact on the phase angle. With such tampered voltage measurement, the estimated network states are significantly deviated from the actual network operational states, which may eventually mislead the decision-making process and potentially the corrective control actions.

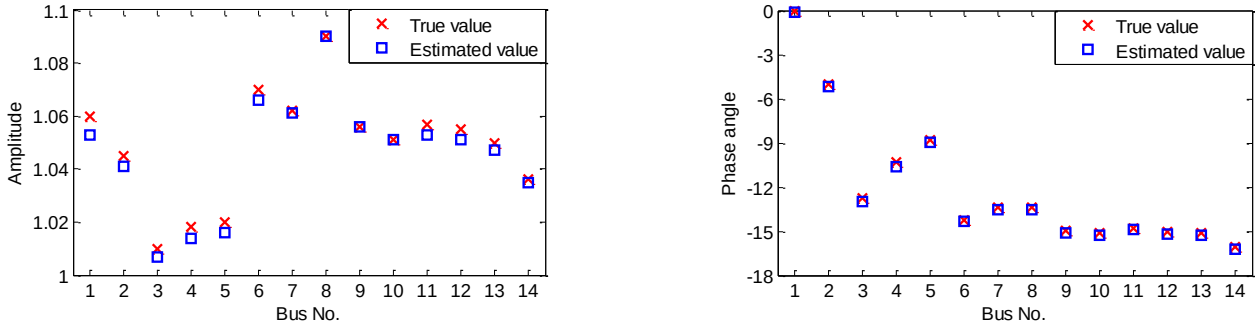
Case 2: State estimation under attacks at different locations

Due to the topological structure of power transmission network, the impact of attacks at different locations can vary. Thus, the simulation experiment for cyber-attacks at different locations are carried out to assess the impact on network state

estimation performance under FDI attacks at buses with PMU installations (No.2, 6, 8 and 9), respectively. Here, the PMU voltage measurements at the attacked buses are assumed to be altered with 10% in respect to their original values. The numerical result of state estimation of network states for different attack locations are presented against the scenario without attacks in Fig.7, respectively. It demonstrates that such attacks of information alteration can have great influence on the performance of state estimation, in particular the voltage amplitude. Further, we examined the estimation deviation of the attacks at different locations based on (12), and it shows that the most vulnerable location under attack is bus No.6, as the highest state estimation deviation ($E = 0.0276$) is observed.

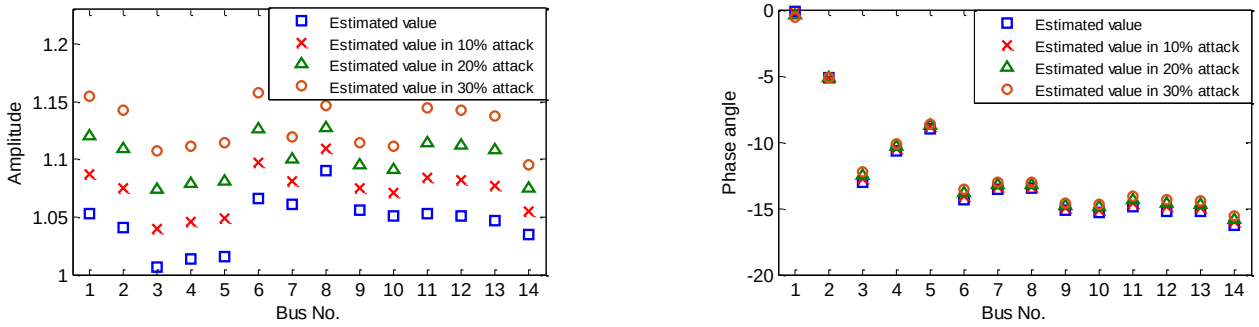
Case 3: State estimation under different measurement attacks

Here, the state estimation performance is assessed considering the attacks on specific types of PMU measurements, assuming that the attack location and intensity remain unchanged. The bus No. 2 is selected as the attack location with the PMU measurements are randomly tampered to be increased 10% in respect to the actual values, including the voltage at bus No.2 and current in branches 2-1, 2-4 and 2-5. The estimated states of voltage amplitude and phase angle are presented in Fig. 8, respectively. It confirms that the voltage amplitude changes significantly across the test network due to data tampering of measured voltage.



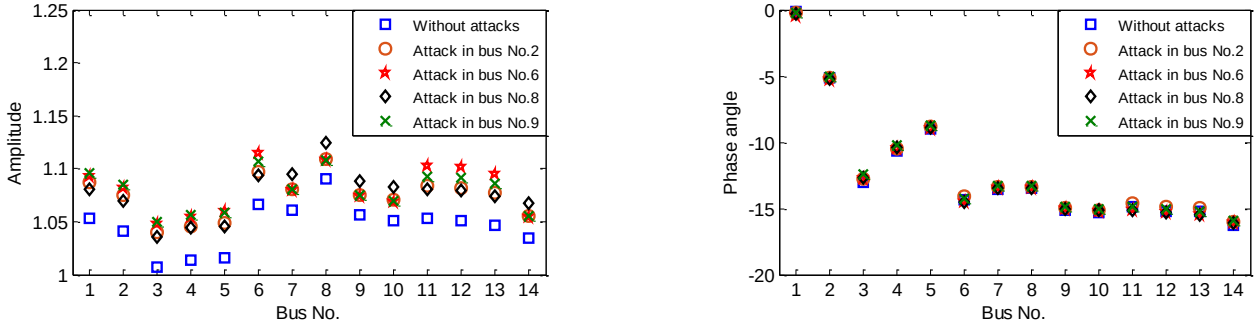
(a) *(b)*

Fig.5 State estimation using linear weighted least squares (without cyber-attacks) (a): voltage amplitude and (b) phase angle



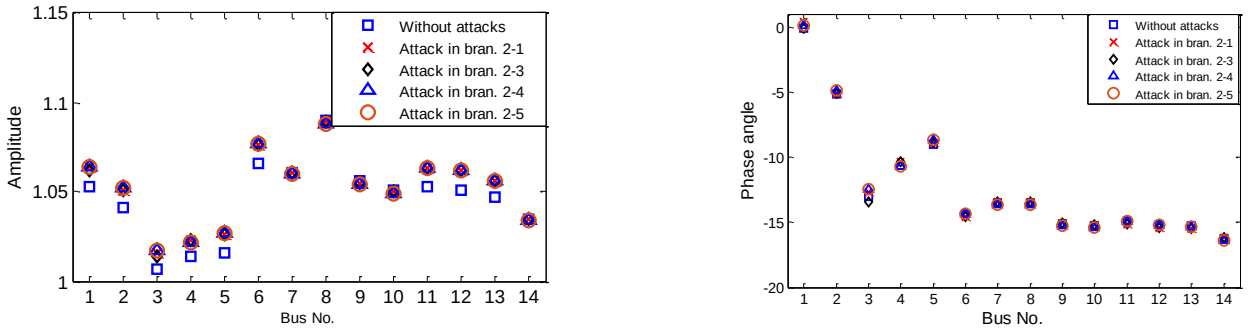
(a) *(b)*

Fig.6 Network state estimation under FDI attacks at bus No.2. (a): voltage amplitude and (b) phase angle



(a) *(b)*

Fig.7 State estimation with different FDI attack locations. (a): voltage amplitude and (b) phase angle

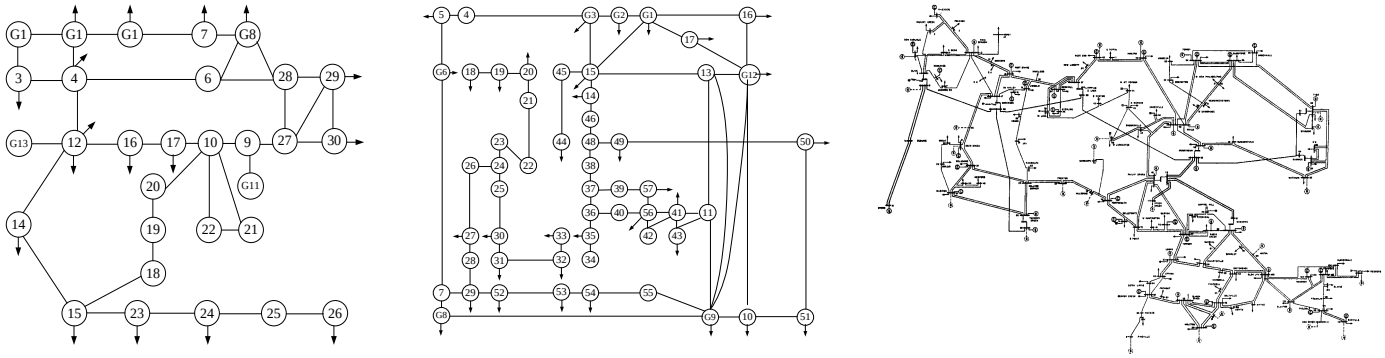


(a) *(b)*

Fig. 8 State estimation with FDI attacks on different types of measurements

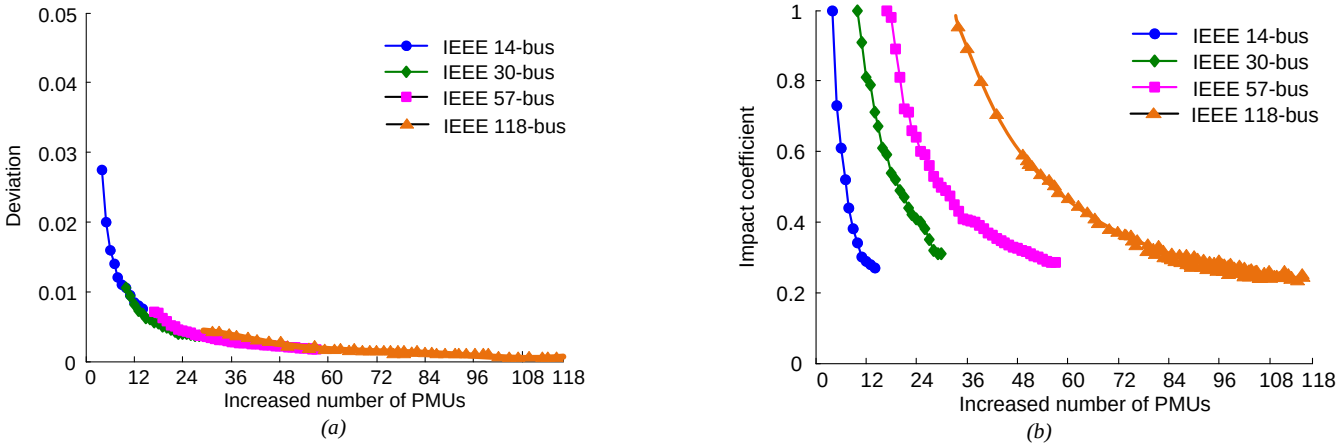
B. PMU placement considering FDI attack

Finally, the proposed algorithmic solution is further assessed for PMU placement considering cyber security improvement. The simulation experiments are carried out based on four standard test networks, i.e. IEEE 14-bus, 30-bus, 57-bus and 118-bus network [26], as illustrated in Fig. 9. Here, the same FDI attack implementations (Section IV-A) are used to these simulated test networks. The placement of additional PMUs (both number of locations) for these transmission networks for different security coefficient values ($k_1 = 2/3$, $k_2 = 1/2$ and $k_3 = 1/3$) are calculated based on the proposed solution (Section IV-C) and presented in details in Table 3. It implies that, given the security requirement in the presence of FDI attacks, the solution is able to cost-effectively identify the minimum number and optimal locations of additional PMU installations. Further, Fig. 10 presents the state estimation deviation (error) and the attack impact coefficient against the number of PMUs for the simulated test networks. It clearly shows that additional PMUs installed at appropriate buses can significantly improve the state estimation accuracy under FDI attacks. This result can effectively guide the power utilities for PMU deployment to prevent their assets from various forms of FDI attacks.



(a) *(b)* *(c)*

Fig.9 Three IEEE transmission test networks (a) 30-bus network; (b) 57-bus network; and (c) 118-bus network



(a) *(b)*

Fig. 10 The state estimation accuracy and impact coefficient vs. the increased number of PMUs

Table 3 PMU placement in IEEE 14-bus, 30-bus, 57-bus and 118-bus network considering FDI attacks

Test network		Impact coefficients		
		$k_1 = 2/3$	$k_2 = 1/2$	$k_3 = 1/3$
IEEE 14-bus	PMU location	{2,6,8,9,12}	{2,6,8,9,12,4,14}	{2,6,8,9,12,4,14,10,7,5,11}
	No. add. PMUs	1	3	7
IEEE 30-bus	PMU location	{2,4,6,9,10,12,15,18,25, 27,22,28,24,8,29}	{2,4,6,9,10,12,15,18,25, 27,22,28,24,8,29,17,3,16,7,21}	{2,4,6,9,10,12,15,18,25, 27,22,28,24,8,29,17,3,16,7,21,26,14,5,1,23, 30,19,20,11}
	No. add. PMUs	5	10	19
IEEE 57-bus	PMU location	{1,4,7,9,15,20,24,25,27,32,36,38 ,39,41,46,50,53,2,30,11,13,29}	{1,4,7,9,15,20,24,25,27,32,36,38,39, 41,46,50,53,2,30,11,13,29,21,34,14,3 ,16,51,56}	{1,4,7,9,15,20,24,25,27,32,36,38,39,41,46, 50,53,2,30,11,13,29,21,34,14,3,16,51,56,18 ,22,17,26,45,37,40,35,23,33,43,42,48,10,8}
	No. add. PMUs	5	12	27
IEEE 118-bus	PMU location	{5,56,57,34,52,28,1,72, 9,47,3, 110,42,118,30,48,18,22,17, 36, 4,108,58,100,15,68,31,106,98}	{5,56,57,34,52,28,1,72,9,47,3,110,42 ,118,30,48,18,22,17,36,4,108,58,100, 15,68,31,106,98,114,16,64,94,78, 103,39,87,54,41,84,44,10,27,46,112, 33}	{5,56,57,34,52,28,1,72,9,47,3,110,42, 118,30,48,18,22,17,36,4,108,58,100,15, 68,31,106,98,114,16,64,94,78,103,39,87, 54,41,84,44,10,27,46,112,33,51,20,92,113, 115,24,91,70,83,61,59,67,116,60,65,6,74}
	No. add. PMUs	16	35	52

VI. CONCLUSION AND REMARK

This paper exploited the cyber security problem of smart grid with the particular focus on the FDI attacks on state estimation of electric transmission networks. The impact of data tempering attacks of PMU measurements on state estimation is extensively evaluated through simulation experiments based on IEEE 14-bus transmission network model. The result clearly confirms our expectation that the cyber attacks on PMU measurement can bring significantly adverse impact on the state estimation which may result in degradation of network control and protection. Also, an algorithmic solution is proposed to address the issue of additional PMU installation and placement for cyber security improvement and analyzed for different standard electric transmission networks.

Two research directions are considered worth further research effort in the future work. The impact of different forms of cyber-attacks on the state estimation of PMU placement strategies in realistic transmission networks needs to be further studied and assessed. In addition, as the large-scale PMU deployment is often cost prohibitive, current wide-area measurement of electric transmission networks are often based on a hybrid infrastructure based on PMUs (operated in the time scale of millisecond) and SCADA legacy (operated in the time scale of seconds or minutes). The cyber security assessment needs to be carried out in such hybrid wide-area measurement infrastructures.

REFERENCES

[1] A. Chakrabortty and P. Khargonekar, Introduction to wide-area control of power systems, American Control Conference (ACC), Washington, DC, USA, June 17-19, 2013.

[2] North American Synchrophasor Initiative (NASPI), [Online] Available: https://www.naspi.org/.

[3] Western Interconnection Synchrophasor Project (WISP), [Online] Available: http://www.wecc.biz/.

[4] R. Deng, G. Xiao, R. Lu, H. Liang and A. V. Vasilakos, "False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey," in *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411-423, April 2017.

[5] O. Kosut, L. Jia, R. Thomas, and L. Tong, "On malicious data attacks on power system state estimation," in *Proc. 45th Int. Univ. Power Eng.Conf. (UPEC)*, Cardiff, U.K., 2010, pp. 1–6.

[6] L. Liu, M. Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.

[7] G. Chaojun, P. Jirutitijaroen and M. Motani, "Detecting False Data Injection Attacks in AC State Estimation," in *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476-2483, Sept. 2015.

[8] T. T. Kim and H. V. Poor, "Strategic Protection Against Data Injection Attacks on Power Grids," in *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326-333, June 2011.

[9] S. Bi and Y. J. Zhang, "Graphical Methods for Defense Against False-Data Injection Attacks on Power System State Estimation," in *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1216-1227, May 2014.

[10] S. Mousavian, J. Valenzuela and J. Wang, "A Probabilistic Risk Mitigation Model for Cyber-Attacks to PMU Networks," in *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 156-165, Jan. 2015.

[11] D. Lee and D. Kundur, "Cyber attack detection in PMU measurements via the expectation-maximization algorithm," *2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Atlanta, GA, 2014, pp. 223-227.

[12] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," *2011 IEEE GLOBECOM Workshops (GC Wkshps)*, Houston, TX, 2011, pp. 1162-1167.

[13] J. Liang, L. Sankar and O. Kosut, "Vulnerability Analysis and Consequences of False Data Injection Attack on Power System State Estimation," in *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3864-3872, Sept. 2016.

[14] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang and W. Zhao, "On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717-729, March 2014.

[15] X. Liu, Z. Bao, D. Lu and Z. Li, "Modeling of Local False Data Injection Attacks With Reduced Network Information," in *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1686-1696, July 2015.

[16] Y. Chakhchoukh and H. Ishii, "Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations," *IEEE Trans. Power Systems*, vol. 31, no. 6, pp. 4395-4405, Nov. 2016.

[17] M. Beg Mohammadi, R. A. Hooshmand and F. Haghighatdar Fesharaki, "A new approach for optimal placement of PMUs and their required communication infrastructure in order to minimize the cost of the WAMS," *IEEE Trans. on Smart Grid*, vol. 7, no. 1, pp. 84-93, Jan. 2016.

[18] J. G. Philip and T. Jain, "Optimal placement of PMUs for power system observability with increased redundancy," *2015 Conference on Power,*

Control, Communication and Computational Technologies for Sustainable Growth (PCCCTSG), Kurnool, 2015, pp. 1-5.

[19] Z. H. Rather, Z. Chen, P. Thøgersen, P. Lund and B. Kirby, "Realistic Approach for Phasor Measurement Unit Placement: Consideration of Practical Hidden Costs," in *IEEE Transactions on Power Delivery*, vol. 30, no. 1, pp. 3-15, Feb. 2015.

[20] J. Vijayan, Stuxnet renews power grid security concerns. Computerworld, Jul, 26, 2010.

[21] S. Liu, S. Mashayekh, et. al. A framework for modeling cyber-physical switching attacks in smart grid, IEEE Trans. Emerging Topics in Computing, vol. 1, no. 2, pp. 273-285, Dec. 2013.

[22] Y. Zhao, A. Goldsmith, and H. Poor, "Fundamental limits of cyber-physical security in smart power grids", In Proc. Decision and Control (CDC) annual conference, pp. 200-205, December, 2013.

[23] B. Min, and V. Varadharajan, "Design and analysis of security attacks against critical smart grid infrastructures," In Proc. Int. Conf. ICECCS, pp. 59-68, August, 2014.

[24] Mo, Y., Kim, T. H., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. Cyber–physical security of a smart grid infrastructure. Proc. of the IEEE, 100(1), 195-209, 2012.

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

[26] Power Systems Test Case Archive, [Online] Available: http://www.montefiore.ulg.ac.be/~weckesser/testcases.html

[27] A. Giani, R. Bent and F. Pan, "Phasor measurement unit selection for unobservable electric power data integrity attack detection", *International Journal of Critical Infrastructure Protection*, vol. 7, no. 3, pp. 155-164. 2014.

[28] J. Paudel, X. Xu, K. Balasubramaniam, et al., "A strategy for PMU placement considering the resiliency of measurement system", *Journal of Power and Energy Engineering*, vol. 3, no. 11, pp. 29-36, 2015.

[29] Q. Yang, D. An, R. Min, W. Yu, et al., "On optimal PMU placement-based defense against data integrity attacks in smart grid", *IEEE Trans. Information Forensics and Security*, vol. 12, no. 7, pp. 1735-1750, 2017.

[30] A. Abur and A. G. Expsito, *Power System State Estimation: Theory and Implementation*, 1st ed. New York, NY, USA: Marcel Dekker, Mar. 2004.