PMU Placement Protection Against Coordinated False Data Injection Attacks in Smart Grid

Chao Pei, Yang Xiao, *Fellow, IEEE*, Wei Liang, *Senior Member, IEEE*, and Xiaojia Han

***Abstract*—To maintain stable and reliable operations in smart grid, accurate state estimation is of paramount importance. However, synthesized false data injection attacks could wisely circumvent conventional bad data detection mechanisms by introducing arbitrary errors to state estimates to seriously affect the entire power system operation. To defend these attacks, phase measurement units (PMUs) are deployed in advance at various locations to reduce the chance of being attacked. However, when the budget of placement is not large enough so that the whole system cannot be covered by PMUs, the existing PMU placement algorithms based on greedy strategies are insufficient in some weak locations due to the nature of greedy strategies. In this article, we propose a new hybrid attack, which can be easily used by attackers to attack the buses with less connectivity and impose adverse impacts to state estimation with a low-attack cost so that existing defenses based on greedy strategies become invalid. We future propose a predeployment PMU greedy algorithm for this new attack in which the most vulnerable buses are first protected and, then, a greedy-based algorithm is used to deploy other PMUs until the whole system is observable. Experimental results on various IEEE standard systems demonstrate the effectiveness of our schemes.**

***Index Terms*—Cyber security, cyber-physical system, false data injection, phase measurement units (PMUs), state estimation, smart grid.**

Manuscript received August 11, 2019; revised November 8, 2019 and January 21, 2020; accepted March 5, 2020. Date of publication March 9, 2020; date of current version July 16, 2020. Paper 2019-SRPQ-1064.R2, approved for publication in the IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS by the Security, Reliability, Privacy, and Quality in Industrial Automation and Control Committee of the IEEE Industry Applications Society. The work of C. Pei and W. Liang was supported in part by the National Natural Science Foundation of China under Grant 61673371, in part by the International Partnership Program of Chinese Academy of Sciences under Grant 173321KYSB20180020, and in part by the Liaoning Provincial Natural Science Foundation of China under Grant 2019-YQ-09. The work of C. Pei at the Department of Computer Science, The University of Alabama, Tuscaloosa, USA was supported by the China Scholarship Council. *(Corresponding authors: Yang Xiao and Wei Liang.)*

Chao Pei is with the State Key Laboratory of Robotics Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China, and with the Key Laboratory of Networked Control Systems, Chinese Academy of Sciences, Shenyang 110016, China, and with the Institutes for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences, Shenyang 110169, China, and with the University of Chinese Academy of Sciences, Beijing 100049, China, and also with the Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487-0290 USA (e-mail: peichao275@gmail.com).

Yang Xiao is with the Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487-0290 USA (e-mail: yangxiao@ieee.org).

Wei Liang is with the State Key Laboratory of Robotics Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China, and with the Key Laboratory of Networked Control Systems, Chinese Academy of Sciences, Shenyang 110016, China, and also with the Institutes for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences, Shenyang 110169, China (e-mail: weiliang@sia.cn).

Xiaojia Han is with the Key Laboratory of Networked Control Systems, Chinese Academy of Sciences, Shenyang 110016, China, and with the Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China, and with the Institutes for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences, Shenyang 110169, China, and also with the University of Chinese Academy of Sciences, Beijing 100049, China (e-mail: hanxiaojia@sia.cn).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIA.2020.2979793

I. INTRODUCTION

ALTHOUGH the introduction and development of smart grid has brought many new and outstanding features to the power systems, the stronger coupling between cyber and physical operations make the smart grid more vulnerable to various malicious cyber-attacks [1], [2]. Generally, power system is one of a country's critical infrastructures, and its large fluctuation or destruction will have a devastating impact on the country's defense, economics, safety, and health fields.

To maintain normal operations, power systems are continuously monitored and controlled by supervisory control and data acquisition systems (SCADA) and energy management systems (EMSs) [3], [4]. It is usually not feasible to measure all possible states through various commonly used sensors, especially for voltage-phase angles of buses. Therefore, accurate states obtained from state estimation play an extremely important role to establish the basis for subsequent serious controls and analysis [5]. One main task of an estimator in a control center contains topology processing, observability analysis, state estimation, and bad data processing.

An important factor affecting the accuracy of state estimation is the introduction of bad data injection, which can be caused by nonmalicious accidents or malicious cyber attacks [6]. Nonmalicious accidents in actual situations are common: 1) dumped trees on streets break down transmission lines due to strong winds, leading sudden changes of some measurements of meters; and 2) sensors and meters may become faulty, affecting actual readings. Meanwhile, potential threats of malicious cyber-attacks can be launched by attackers [7]. Bad data injection can result in adverse impacts on the control and decision-making, and even lead to power outages. Actually, many conventional bad data detection (BDD) techniques proposed in the literature are all based on observations that the introduction of bad measurements will produce relatively large residuals of normalized measurements. However, to our knowledge, a coordinated false data injection attack (FDIA) in [6] shows that it can circumvent conventional normalized measurement residual-based BDD and can insert any bias into values of estimated states stealthily [8]. Such attacks are also named as stealthy attacks or data integrity attacks. Biased states could cause serious threats to the operation and control

of power grids, and it could directly lead to serious social and economic consequences [9].

In actual smart grids, the commonly used transmission protocols of measurements such as distributed network protocol 3 and MODBUS use clear text in the supervisory control and data acquisition system, and, then, the transmitted measurements can be easily sniffed in this case [3]. Even in the case where encrypted devices are deployed in smart grids, there are already many mature technologies involving computer and network security that can enable an attacker to eavesdrop and tamper with the transmitted information. Since the basic knowledge about the power grid is much available and public, attackers usually have lots of knowledge about operations and characteristics of the target systems, as well as some critical control and operation information. If an attacker has hacked the control center or if the attacker and the insider of the control center are colluding with each other, the Jacobian matrix of state estimation can be directly obtained [38], [39]. Even in the part of a grid, some measurements can be tampered easily by measuring the branch impedance associated with the attacked buses in the field through analyzing the topology of the power system. Usually, the changing topologies in smart grid caused by network reconfiguration strategies makes it more complicated to obtain an accurate Jacobian matrix for attackers. Although these conditions are critical and complicated for attackers, it is achievable from the analysis of Ukraine power outage [39].

After realizing the seriousness of this problem, a number of methods have been proposed recently in the literature to study the effective defense mechanisms toward FDIA. To solve this problem properly, from the perspective of protection-based defense, one efficient way is to improve the security of essential measurements by performing additional security mechanisms. Since phase measurement units (PMUs) are advance measurement units, they are equipped with many security measures, compared with traditional used voltage meters. PMUs can provide accurate and real-time synchronous phasor measurements with Global Positioning System (GPS) time and the PMU data are sampled from geographically dispersed buses in smart grid. The accurate measurements from different locations with real time stamps from PMUs possess inherent robustness against FDIAs. Moreover, the communication links between PMUs and data centers are usually secured and encrypted [10], [33], [37]. At the same time, instead of just using PMUs to improve the redundancy of received measurements, PMUs have the capability of verifying the state variables such as voltage phase angles independently and these advanced measurement units can improve the observability when they are deployed on specific buses. Therefore, we assume that the attacker cannot manipulate the measurements from PMUs and it implies that PMUs are robust against FDIAs. In [10], Yang *et al.* enhanced a least-effort attack model and, then, propose a reduced row echelon (RRE) form based method to compute the optimal attack vector; further, a greedy algorithm for the optimal PMU placement to defend against data integrity attacks is also developed. However, existing PMU placement algorithms based on greedy strategies may be insufficient when FDIA occurs during the device configuration process.

No matter how secure a method can be designed, during the configuration process of PMU placement and before the complete placement of PMUs, there is still a risk of being attacked by attackers even though this window of configuration is small. In this article, we target to reducing the chance of being attacked, attempting to close the window or at least reduce the window. When considering the security problem during the dynamic PMUs deployment process of attacker versus defender, the security toward FDIA is monitored by the observability analysis, which is achieved using PMUs deployment in smart grids. These secure PMUs can verify certain state variables independently since PMUs are advanced measurement units, which can provide accurate and real-time synchronous phasor measurements with GPS time and can directly measure voltage angles of the deployed bus in real time. Before all PMUs deployments are completed and the entire power grid is fully observable, there is always a risk of being attacked by attackers. But if the attacker wants to continue to launch the attack, the attacker needs to compromise more meter measurements during the small window of PMUs configuration. It means that attackers must increase the attack cost whereas the primary goal of a launched hybrid attack is to minimize the attack cost.

In this article, we first theoretically analyze adverse effects of FDIA targeted to state estimation considering generalized constraints and, then, we propose a new hybrid attack scheme (HAS) with lower computational complexity, which can easily attack buses with less connectivity during the device configuration process and impose adverse impacts with a low attack cost. We future propose a predeployment PMU-based greedy (PDPG) algorithm for this new attack in which the most vulnerable buses are first protected, and, then, a greedy-based algorithm is used to deploy other PMUs until the whole system is observable. The proposed mechanism has three advantages: covering some of weak locations first, forcing an attacker to increase its attack cost, and reducing the placement iterative process in terms of time. Experimental results on various IEEE standard systems demonstrate the effectiveness of our schemes.

The rest of the article is organized as follows. Section II presents related work about FDIA. In Section III, state estimation, BDD, FDIA, and characteristics of PMU are presented separately. Section IV presents the proposed new attack, and the proposed algorithm is described in Section V. Section VI provides experiments and performance evaluation results. Finally, we conclude this article in Section VII. We summarize all the symbols in this article in Table I for readers' convenience whereas the definitions of these symbols will be introduced later when needed.

II. Related Work

Defense mechanisms include protection (protecting a smart grid from attackers in advance), detection (detecting and identifying FDIA during the process of state estimation), and recovery [2], [11]. These defense methods can be broadly divided into three categories: 1) advanced signal processing-based defense, 2) data-driven-based defense, and 3) protection-based defense. As an advanced signal processing defense, the work

TABLE I
NOMENCLATURE

$\boldsymbol{z}$	Measurement vector
$\boldsymbol{h}(\boldsymbol{x})$	Nonlinear measurement function vector between $\boldsymbol{z}$ and $\boldsymbol{x}$
$\boldsymbol{x}$	State variables vector
$\boldsymbol{e}$	Measurement error vector
$\boldsymbol{R}$	Error covariance matrix of $\boldsymbol{e}$
$\boldsymbol{H}$	Jacobian matrix
$\boldsymbol{G}(\boldsymbol{x}^k)$	Gain matrix
ξ	Predefined threshold
$\hat{\boldsymbol{x}}$	Estimated state vector
$\hat{\boldsymbol{z}}$	Estimated measurement vector
$\boldsymbol{r}$	Measurement residual vector
τ	Detection threshold
$\boldsymbol{a}$	Nonzero attack vector
$\boldsymbol{z_a}$	Compromised measurement vector
$\boldsymbol{r_a}$	Measurement residual vector which is under attack
$\hat{\boldsymbol{x}}_{\boldsymbol{bad}}$	Estimated state vector which is under attack
$\boldsymbol{c}$	Introduced error to the correct state vector
$\boldsymbol{S}$	The set of indices of protected measurements
V_i	Voltage amplitude of bus i
θ_i	Phase angle of bus i
x_{ij}	The reactance of branch between bus i and bus j
P_{ij}	Real power flow from bus i to bus j
P_i	Real power flow injection of bus i
θ_i'	Phase angle of bus i after attack
P	Traceability matrix of elementary row transformation
Q	Traceability matrix of column exchange

in [12] introduced an adaptive scheme to self-adaptively detect both nonstealthy and stealthy injection attacks by taking power measurements of two sequential data collection slots into account in short-term sampling ranges and detecting FDIA by monitoring the measurements variations and state changes between two time slots. In [13], in order to avoid the deficiency of the traditional Chi-square detector based on measurement residuals, one cosine similarity matching metric is proposed to measure the deviation between estimated state values (via a Kalman Filter) and measured state values (via sensors). Huang *et al.* [16] presented an adaptive cumulative sum based approach by detecting residual vector mean changes of distributions under the occurrence of FDIA for the purpose of real-time detection. Also in reality, loads in smart grids vary due to influences of weather and temperature [17], [18], and show obvious time series characteristics. It means that there is a time correlation between states of different buses with system changes [19]. Thus, Zhao *et al.* [20] proposed a short-term state forecasting-aided method, which adopts autoregressive models to achieve one-step ahead state prediction, to detect FDIA, where the predicted states are regarded as accurate state variables. Furthermore, in [21] and [22], an FDIA detection problem can be formulated as a low rank matrix recovery and completion problem because of intrinsic low rank structure of erroneous-free measurements and sparse nature of malicious attacks.

For data-driven-based defense, Esmalifalak *et al.* [23] used a machine learning based method to detect FDIA using the following intuitive: whether there is an attack of data depends on whether constraints of the physical laws are met, such as the Kirchhoff's law. In [24], an optimized clustering algorithm combined with two parameters reflecting the physical property of smart grid is proposed to classify potential vulnerable nodes into several classes, and a state forecasting detection method is, then, used to detect attacks. Mohammadpourfard *et al.* [25] proposed detectors utilizing an unsupervised anomaly detection method through analyzing different statistical measures since FDIA can lead to a deviation in probability distribution of state vectors from normal trends.

For protection-based defense, Bobba *et al.* [27] proposed that FDIA can be defended either by securing basic measurements, which are selected strategically or by verifying state variables independently. Protection on meter measurements includes both physical and software methods [1]. In practice, it is usually infeasible to safely protect all of measurements in a power grid due to high cost. Nevertheless, FDIA can be defended through protecting a carefully selected set (called the minimum set) of essential measurements that meet the observable conditions of the power system, where the power system is said to be observable when the measurement set allows a unique solution of all state variables for state estimation problem; but the challenge is how to effectively identify these measurements. Bobba *et al.* [27] showed that it is necessary but not sufficient to protect at least n meters, which is the same as the number of state variables. Hao *et al.* [22] presented a greedy strategy-based approach to find the minimum measurement set that needs to be protected. A more practical background considering the insufficient number of encryption devices is presented in [26], and this problem is formulated as an objective optimization problem. From the perspective of game theory, a minimal cost defense strategy based on hybrid nonlinear integer programming and multiobjective optimization is discussed in [28].

As for verifying certain state variables independently, PMUs are usually used because these devices are typically robust against FDIA and can make the measurements secured [12]. By synchronizing to GPS, PMUs have the capability of providing accurate synchronous phasor measurements for geographically dispersed nodes in power grids. Early in the 2006, Chen and Abur [29] proposed to utilize deployment of PMUs to improve the ability of detecting bad data, and it is mainly by converting critical measurements into redundant measurements. Kim and Poor [30] proposed a less complex and secure PMU placement algorithm based on a fast greedy strategy. In [31], an optimal PMU placement is formulated as a semidefinite programming problem considering the impact of channel limits. A mixed integer programming model for optimal PMU placement is developed to defend FDIA in [32].

Overall, the aforementioned methods are aimed at either determining the optimal placement of PMUs to improve system observability, or considering multiobjective criteria such as observability, cost, security, and improving state estimation. These methods mentioned above do not consider the situation that the system is attacked by an FDIA during the device configuration process. Since aforementioned existing applications of PMU deployment in power systems are mainly focus on maximizing the measurement redundancy at the buses with a given number of PMUs or to ensure the completely observability about smart grid, these cases consider that the smart grid is secure when all PMUs are deployed. In this article, we further consider the interesting attacker-versus-defender dynamics. The reason is that if an attacker could have some knowledge about the

defender's corresponding defense measures, they could optimize their attack strategy. At the same time, the defender can also take measures to mitigate the influence of the worst-case scenario caused by the attacker. It means that the dynamics between the attacker and the defender need to be considered in practical applications. As described in this article, the buses with less connectivity can be easily attacked, and the attack can be occurred during the device configuration process; thus, there are some new problems that need to be solved.

III. Background

A. State Estimation and Conventional BDD

Operators in a control center are usually difficult to directly obtain state variables, such as phase angles, by sensors, and, thus, state estimation plays an important role to estimate or predict the system operating states. By using the redundant real-time measurements, error information caused by random interferences can be automatically eliminated. Here, we consider a steady-state and lossless power transmission system with n buses and m meters, and $m \gg n$. By taking measurement errors into account, the relationship between measurement vector $\boldsymbol{z}$ and state variables $\boldsymbol{x}$ can be described as follows:

$$\boldsymbol{z} = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix} = \begin{bmatrix} \boldsymbol{h_1}(x_1, x_2, \ldots, x_n) \\ \boldsymbol{h_2}(x_1, x_2, \ldots, x_n) \\ \vdots \\ \boldsymbol{h_m}(x_1, x_2, \ldots, x_n) \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e} \tag{1}$$

where $\boldsymbol{h}(\boldsymbol{x})$ is a nonlinear measurement function of state variables $\boldsymbol{x}$ in alternating current (ac) power system, $\boldsymbol{e}$ is the Gaussian error noise, which is assumed to have a normal distribution with zero mean and known error covariance matrix $\boldsymbol{R}$. $\boldsymbol{R}$ can be expressed as

$$\boldsymbol{R} = \begin{bmatrix} \sigma_1^2 & 0 & \cdots & 0 \\ 0 & \sigma_2^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_m^2 \end{bmatrix}_{m \times m} \tag{2}$$

where σ_i^2 $(1 \leq i \leq m)$ is the variance of the ith meter. Based on the weighted least square criterion, the state estimation problem can be formulated as the following objective function that minimizes the weighted least square error to obtain the estimated state variable $\hat{\boldsymbol{x}}$. The objective function is expressed as $J(\boldsymbol{x}) = [\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})]^T \boldsymbol{R}^{-1} [\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})]$ [36]. In order to obtain the minimum value, the first-order optimality condition must be satisfied, that is, $\boldsymbol{g}(\boldsymbol{x}) = \frac{\partial J(\boldsymbol{x})}{\partial \boldsymbol{x}} = -2\boldsymbol{H}^T(\boldsymbol{x})\boldsymbol{R}^{-1}[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})] = 0$, where $\boldsymbol{H}(\boldsymbol{x}) = \frac{\partial \boldsymbol{h}(\boldsymbol{x})}{\partial \boldsymbol{x}}$ is the so-called Jacobian matrix. Then, by using Taylor series around the state vector $\boldsymbol{x}_k$, which is typically a flat start, the nonlinear function $\boldsymbol{g}(\boldsymbol{x})$ can be expanded as $\boldsymbol{g}(\boldsymbol{x}) = \boldsymbol{g}(\boldsymbol{x}_k) + \boldsymbol{G}(\boldsymbol{x}_k)(\boldsymbol{x} - \boldsymbol{x}_k) + \cdots = 0$, where $\boldsymbol{G}(\boldsymbol{x}_k) = \frac{\partial \boldsymbol{g}(\boldsymbol{x}_k)}{\partial \boldsymbol{x}} = \boldsymbol{H}^T(\boldsymbol{x}_k)\boldsymbol{R}^{-1}\boldsymbol{H}(\boldsymbol{x}_k)$ is called the gain matrix, k is the iteration index, and $\boldsymbol{x}_k$ is the solution vector at iteration k. Neglecting the higher order terms leads to an iterative solution, which is known as the Gauss–Newton method, and, thus, we can get $\boldsymbol{x}_{k+1} - \boldsymbol{x}_k = \boldsymbol{G}(\boldsymbol{x}_k)^{-1}\boldsymbol{H}^T(\boldsymbol{x}_k)\boldsymbol{R}^{-1}[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})]$. That is $[\boldsymbol{G}(\boldsymbol{x}_k)]\Delta\boldsymbol{x}_{k+1} = \boldsymbol{H}^T(\boldsymbol{x}_k)\boldsymbol{R}^{-1}[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})]$, and $\Delta\boldsymbol{x}_{k+1} = \boldsymbol{x}_{k+1} - \boldsymbol{x}_k$. Then, the $\boldsymbol{x}_{k+1}$ is calculated iteratively until the maximum $\Delta\boldsymbol{x}_{k+1} < \xi$, where the parameter ξ is the predefined threshold.

However, since the nonlinear functions of the ac power model are computationally expensive, the convergence to the global optimal value cannot be guaranteed and, thus, a linearized direct current (dc) power flow model is widely adopted in power systems. The dc model is less accurate, but simpler and more robust than the ac model [8]. Therefore, the measurement vector $\boldsymbol{z}$ and state vector $\boldsymbol{x}$ can be associated by linear equations $\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e}$.

Normally, the state variables in the dc model are actually the bus-phase angles, and one arbitrary bus is chosen as the reference bus whose phase angle is set to be zero. The number of meters is far more than the number of state variables. Based on the widely used weighted least square method [8], the optimal solution of estimated state variables can be obtained as $\hat{\boldsymbol{x}} = (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{z}$. Naturally, the estimated measurement vector can be derived, that is, $\hat{\boldsymbol{z}} = \boldsymbol{H}\hat{\boldsymbol{x}} = \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{z} = \boldsymbol{K}\boldsymbol{z}$, and the parameter $\boldsymbol{K}$ is the so-called hat matrix.

Intuitively, measurements from normal meters usually produce state variables that are close to the actual values, and there are inconsistence between normal measurements and bad measurements. Bad measurements can be caused by meter failures, faults, or malicious cyber-attacks. Traditional BDD mechanisms are usually based on residual-based detectors, and normally residuals between observed measurements $\boldsymbol{z}$ and estimated measurements $\hat{\boldsymbol{z}}$ are compared with a predetermined detection threshold τ. Generally, the residual is defined as $\boldsymbol{r} = \boldsymbol{z} - \hat{\boldsymbol{z}} = \boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}} = (\boldsymbol{I} - \boldsymbol{K})\boldsymbol{z}$. In order to carry out the detection process, if the ℓ_2 norm of the residual is large than the predetermined threshold, i.e., $||\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}||_2 > \tau$, it indicates that there are bad measurements. On the contrary, if $||\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}||_2 \leq \tau$, the measurement vector $\boldsymbol{z}$ is regarded as a normal one.

B. False Data Injection Attacks

A compromised measurement $\boldsymbol{z_a}$ can be described as $\boldsymbol{z_a} = \boldsymbol{z} + \boldsymbol{a}$, where $\boldsymbol{a}$ denotes a nonzero attack vector, which is injected by attackers to the original measurements. $\hat{\boldsymbol{x}}_{\text{bad}}$ denotes an estimated state variable vector under the attack and is obtained as follows:

$$\begin{aligned} \hat{\boldsymbol{x}}_{\text{bad}} &= (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}(\boldsymbol{z} + \boldsymbol{a}) \\ &= \hat{\boldsymbol{x}} + (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{a} = \hat{\boldsymbol{x}} + \boldsymbol{c} \end{aligned} \tag{3}$$

where $\boldsymbol{c}$ is the introduced error to the correct state variables. The measurement residual under the attack is expressed as follows:

$$\begin{aligned} \boldsymbol{r_a} &= ||\boldsymbol{z_a} - \boldsymbol{H}\hat{\boldsymbol{x}}_{\text{bad}}||_2 = ||\boldsymbol{z} + \boldsymbol{a} - \boldsymbol{H}(\hat{\boldsymbol{x}} + \boldsymbol{c})||_2 \\ &\leq ||\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}||_2 + ||\boldsymbol{a} - \boldsymbol{H}\boldsymbol{c}||_2. \end{aligned} \tag{4}$$

If the original measurement vector $\boldsymbol{z}$ appears normal, $||\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}||_2 \leq \tau$ is satisfied in the measurement residual-based

bad data detector. Therefore, if $\kappa = ||\boldsymbol{a} - \boldsymbol{Hc}||_2 \leq \tau - ||\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}||_2$ holds, $\boldsymbol{r_a} = ||\boldsymbol{z_a} - \boldsymbol{H}\hat{\boldsymbol{x}}_{\text{bad}}||_2 \leq \tau$ holds, i.e., the compromised measurements can bypass the bad data detector. Here, κ is the error tolerance to the attack vector and indicates that there is a tolerance targeted to small measurement errors of the detector. The above result $\boldsymbol{r_a} \leq \tau$ shows that the measurement residual under compromised measurements $\boldsymbol{z_a}$ can present the same BDD results with the situation when there is no attack in the original normal measurements. Thus, the FDIA are stealthy. If $\boldsymbol{a} = \boldsymbol{Hc}$, we will have $\kappa = 0$ and this case is called a perfect FDIA, which is the same as those in [6], [8], [12], and [22] mentioned earlier. In summary, this carefully designed FDIA could inject any bias to the state variables $\hat{\boldsymbol{x}}$ because the introduced error $\boldsymbol{c}$ is arbitrary; and, therefore, it could circumvent the alarm of the bad data detector in the control center.

C. Characteristics of PMU

PMUs are the advanced measurement units, which can measure voltage and current signals of power grids operated on the time scale of millisecond and are mainly installed on branches, main transformers, or buses of power plants and substations. By using a common time source based on the GPS time, PMUs have the capability of providing accurate real-time synchronous phasor measurements for geographically dispersed nodes in power grids [30]. Typically, it is difficult for attackers to compromise these measurements that are relevant to PMUs, and, therefore, PMUs are robust against FDIA. In the dc linearized measurement model, when one PMU is deployed on a given bus, both voltage angles of the bus and power flows of branches adjacent to the bus can be measured in real time and, therefore, are secured [10]; moreover, voltage angles of buses adjacent to the bus are protected as well. In practice, since PMUs for large-scale deployment are expensive and it is impossible for redeployment of PMUs, the number of PMUs and their locations of placement should be optimized; furthermore, both observability of the whole power system and robustness against FDIA should be guaranteed.

IV. Hybrid Attack Scheme

There have been many techniques for defending against FDIA in power grids. Basically, they all rely on three key assumptions: 1) attackers have lots of knowledge about operations and characteristics of the target systems; 2) attackers possess critical control and operation information, such as network topology, power system parameters, details of SCADA network equipment, BDD mechanism; 3) and attackers can modify the measurements of some compromised meters [6], [8], [15]. While these conditions present a great challenge for attackers, the occurrence of power outage in Ukraine verified the existence of these conditions [15]. Hence, we suppose the following in the dc power flow model: 1) the Jacobian matric $\boldsymbol{H}$ is known by attackers; 2) a certain number of meters can also be modified; and 3) attackers have knowledge about the defend strategy and defenders can use PMUs to prevent attackers to change measurements in the protected subset. In other words, attackers know where PMUs were deployed, and defenders know the attack strategy (the attack vector) during the deployment process of PMUs. Since many existing applications of PMU deployment in power systems mainly focus on maximizing the measurement redundancy at the buses with a given number of PMUs or dealing with the analysis of power system observability when all PMUs are deployed, we further consider the interesting attacker-versus-defender dynamics in this article. The reason is that attackers can optimize their strategies to choose the introduced error c if they have certain knowledge about possible security measures, and the defender in control center can also take countermeasures to minimize the worst case caused by attackers [10], [30], [33].

From the perspective of attack goals, there are two kinds of attacks: targeted FDIA and random FDIA. The targeted FDIA is defined as the case in which attackers intend to inject specific errors into the estimation of certain chosen state variables' constraints on their own resources. The random FDIA is defined as the case in which attackers aim to find any attack vector as long as it can result in a wrong estimation of state variables by compromising smart meters in a power grid, and the introduced estimation error can be any value. Although the random FDIA is easy to be launched, the targeted FDIA, in which only a certain number of state variables are polluted in one specific region, is more harmful potentially to power system than the former.

Based on the analysis mentioned above, from the perspective of attackers, their target is to cause the maximum damage to power systems with the minimal overhead, and simultaneously to evade the system's detection. To make attack cost as low as possible, the targeted state variables, which correspond to column vectors with less nonzero elements, are preferred by attackers. Moreover, through the analysis of Jacobian matrix $\boldsymbol{H}$, these buses, which only possess one adjacent bus and locate at the edge of the system, are selected as objects being attacked first. This is because the measurements needed to be modified for these buses are particularly rare, and it is also the bottleneck of system's vulnerability and security. Here, we call this type of buses as edge buses. At the same time, attackers can still find the attack vector through the RRE-based algorithm if the whole system is unobservable during configuration process of PMU deployment.

From attackers' point of views, due to the constraints of their own resources, attackers can only compromise limited number of meters. Therefore, attackers need to minimize their attack cost, and it is called least-effort attack. Based on above considerations, since the main task for attackers is to meet the successful FDIA condition, i.e., $\boldsymbol{a} = \boldsymbol{Hc}$, and ultimately to circumvent the traditional detection mechanism. Thus, mathematically, we can obtain that attack vector $\boldsymbol{a}$ belongs to the column space of $\boldsymbol{H}$, i.e., $\boldsymbol{a} \in \mathbb{C}(\boldsymbol{H})$, where the symbol $\mathbb{C}$ denotes the set of all possible linear combinations of column vectors of matrix $\boldsymbol{H}$. The construction of FDIA can be formulated as to find k sparse attack vector for attackers, where k sparse attack vector refers to that there are k nonzero elements in attack vector $\boldsymbol{a}$.

Let $\boldsymbol{S}$ denote the set of indices of protected measurements, and $\bar{\boldsymbol{S}}$, the complementary set of $\boldsymbol{S}$, denote indices corresponding to unprotected measurements. Thus, the elements of attack vectors corresponding to protected measurements will be zeros, i.e., $\boldsymbol{H_S c} = 0$, where $\boldsymbol{H_S}$ denotes submatrix of $\boldsymbol{H}$ with rows that

are indexed by $\boldsymbol{S}$. Naturally, $\boldsymbol{H}_{\bar{\boldsymbol{S}}}$ denotes the remaining part of $\boldsymbol{H}$ with rows that are indexed by $\boldsymbol{S}$. From the analysis of network observability theory, if we can protect a sufficiently large number of measurements, then there is $\text{rank}(\boldsymbol{H}_{\boldsymbol{S}}) = n$. It means that if and only if $\boldsymbol{c} = \boldsymbol{0}$, $\boldsymbol{H}_{\boldsymbol{S}}\boldsymbol{c} = \boldsymbol{0}$. This condition implies that it is impossible for attackers to find an attack vector anymore. But if $\text{rank}(\boldsymbol{H}_{\boldsymbol{S}}) < n$, there must exists many nonzero solutions toward $\boldsymbol{H}_{\boldsymbol{S}}\boldsymbol{c} = \boldsymbol{0}$. Inspired by [30], a vector $\boldsymbol{c}$ only with large magnitude can produce significant impacts to the estimated state vector. Thus, the error vector $\boldsymbol{c}$ needs to be constrained by $||\boldsymbol{c}||_\infty \geq \xi$, where ξ is a predefined positive threshold, and ℓ_∞ norm means the maximum entries' magnitude of that vector. Based on the description above, the attack vector $\boldsymbol{a}$ can be formulated as the solution of an optimization problem presented as (5), where ℓ_0 norm means the total number of nonzero elements in a vector

$$\min_{c} ||\boldsymbol{H}_{\bar{\boldsymbol{S}}}\boldsymbol{c}||_0 \ \text{ s.t. } \ \boldsymbol{H}_{\boldsymbol{S}}\boldsymbol{c} = 0, ||\boldsymbol{c}||_\infty \geq \xi. \tag{5}$$

Considering actual smart grid applications, the measurement functions between measurements and system states are nonlinear as shown in Section III. The most probable actual state variable values are determined by weighted least square minimization in most state estimation programs in which full nonlinear power flow equations and a significant amount of system data are needed.

In the ac power flow model, the equations of real and reactive power flows on transmission lines from bus i to bus j are given by

$$\begin{aligned} P_{ij} = {} & V_i^2(g_{si} + g_{ij}) \\ & - V_iV_j\left[g_{ij}\cos(\theta_i - \theta_j) + b_{ij}\sin(\theta_i - \theta_j)\right] \\ Q_{ij} = {} & -V_i^2(b_{si} + b_{ij}) \\ & - V_iV_j\left[g_{ij}\sin(\theta_i - \theta_j) - b_{ij}\cos(\theta_i - \theta_j)\right]. \end{aligned}$$

These active and reactive power flow injections of bus i are given by

$$P_i = V_i \sum_{j\in N_i} V_j\left[G_{ij}\cos(\theta_i - \theta_j) + B_{ij}\sin(\theta_i - \theta_j)\right]$$

$$Q_i = V_i \sum_{j\in N_i} V_j\left[G_{ij}\sin(\theta_i - \theta_j) - B_{ij}\cos(\theta_i - \theta_j)\right]$$

where V_i and θ_i are voltage and phase angle of bus i, respectively, $G_{ij} + jB_{ij}$ is the line admittance between bus i and bus j, $g_{si} + jb_{si}$ is the admittance of the shunt branch at bus i, and N_i represents the number of branches that are connected with bus i. Therefore, the Jacobian matrix of $h(x)$ is given as follows:

$$H(x) = \frac{\partial h(x)}{\partial x} = \begin{bmatrix} \frac{\partial h_1}{\partial x_1} & \cdots & \frac{\partial h_1}{\partial x_{n-1}} & \frac{\partial h_1}{\partial x_n} \\ \vdots & \ddots & \vdots & \vdots \\ \frac{\partial h_{m-1}}{\partial x_1} & \cdots & \frac{\partial h_{m-1}}{\partial x_{n-1}} & \frac{\partial h_{m-1}}{\partial x_n} \\ \frac{\partial h_m}{\partial x_1} & \cdots & \frac{\partial h_m}{\partial x_{n-1}} & \frac{\partial h_m}{\partial x_n} \end{bmatrix}.$$

It shows the information of which measurement is dependent on the state variable from the Jacobian matrix. Therefore, the specific compromised measurement by an attacker satisfies the following condition, i.e., the specific element in the row that corresponds to the compromised measurement and the specific element in the column that corresponds to the state variable must be nonzero. It can be concluded that the purpose of determining which measurements must be compromised to achieve attacking one specific state variable is the same with the case in the dc power flow model.

As for what values that these compromised measurements need to be altered to in the ac case, the analysis is given as follows: $\boldsymbol{r}_a = \|\boldsymbol{z}_a - \boldsymbol{h}(\hat{\boldsymbol{x}}_{\text{bad}})\|_2 = \|\boldsymbol{z} + \boldsymbol{a} - \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c})\|_2 = \|\boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}})\|_2$. Therefore, the condition that FDIA circumventing conventional BDD mechanisms in the ac power flow model is $\boldsymbol{a} = \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}})$. It can be seen that an attacker in the ac model must know the estimated state variables, which appear in nonlinear function $\boldsymbol{h}$. But in the dc power flow model, the attacker does not need to know the values of the estimated state variables in the control center.

It can be summarized from the above analysis that, on the one hand, the principle and feasibility of FDIA to pass BDD is the same for both the ac model and the dc model, and the only difference is that the attack conditions required by the attacker in the ac model are more complicated than those in the dc case with respect to estimated state variables. On the other hand, we just focus on the security problem against FDIA during the dynamic PMU deployment process of attacker versus defender. Therefore, in addition to analyzing the feasibility of FDIA in the case of the ac power flow model, for the sake of simplicity of analysis, we adopt the dc power flow model of simplified expression in which the shunt susceptance and series resistances in the lines are neglected and the state variables only consist of voltage angles.

In the dc power flow model, it is usually considered that voltage phase differences are relatively small, and voltage amplitudes are usually normalized to unit. Thus, state variables are the bus phase angles only, and measurements in this model are just the active parts of bus power flow injections and branch power flow measurements. The Jacobian matrix H is the partial derivatives of active power injections and active power flows. If phase angles of bus i and bus j are θ_i and θ_j, respectively, the voltage amplitudes of buses are V_i and V_j, respectively, and the reactance of branch between them is represented as x_{ij}. Therefore, the real power flow from bus i to bus j can be formulated as

$$P_{ij} = \frac{V_iV_j}{x_{ij}}\sin(\theta_i - \theta_j) \approx \frac{\theta_i - \theta_j}{x_{ij}}. \tag{6}$$

Moreover, the real power flow injection of bus i can be expressed as follows:

$$P_i = \sum_{s=1}^{N_i} P_{is} = \sum_{s=1}^{N_i}\frac{\theta_i}{x_{is}} - \sum_{s=1}^{N_i}\frac{\theta_s}{x_{is}} \tag{7}$$

where N_i represents the number of branches that are connected with bus i. Combined (6) with (7), we can obtain all elements in Jacobian matrix $\boldsymbol{H}$. Directly, for a specific state variable θ_i, the number of equations related to it equates to the sum of the number of power flow injection measurements of bus i, the

number of branch power flow measurements connected with bus i, and the number of bus power flow injection measurements that are adjacent to bus i. It means that θ_i relies on solutions of these three types of equations. In other words, from (6) and (7), we obtain

$$\theta_i = x_{ij}P_{ij} + \theta_j \tag{8}$$

$$\theta_i = \left(P_i + \sum_{s=1}^{N_i} \frac{\theta_s}{x_{is}}\right) \Big/ \sum_{s=1}^{N_i} \frac{1}{x_{is}} \tag{9}$$

$$\theta_i = x_{li}\left(\sum_{s=1}^{m_l} \frac{\theta_l}{x_{ls}} - \sum_{s=1}^{m_l-1} \frac{\theta_s}{x_{ls}} - P_l\right) \tag{10}$$

which is deduced by the following expression:

$$P_l = \sum_{s=1}^{m_l} \frac{\theta_l - \theta_s}{x_{ls}} = \sum_{s=1}^{m_l} \frac{\theta_l}{x_{ls}} - \sum_{s=1}^{m_l-1} \frac{\theta_s}{x_{ls}} - \frac{\theta_i}{x_{li}} \tag{11}$$

where P_l represents the power flow injection of bus l, bus l is an adjacent bus of bus i, m_l represents the number of branches connected with bus l, and the branch from bus l to bus i is one of the elements in m_l.

Suppose that the set of attacked t state variables is represented as $M = \{x_1, x_2, \ldots, x_t\}$, where $t < n$, and all measurements needed to be manipulated corresponding to the t state variables are represented as set A. If the set of modified measurements targeted to one specific state variable is $A\{x_i\}$, $x_i \in M$, then there exists the following relationship $A = \cup_{x_i \in M} A\{x_i\}$. For FDIA targeted to a specific state variable θ_i, in order to circumvent traditional detection method, one efficient way is to manipulate the three mentioned equations above consistently to introduce an error vector $\boldsymbol{c}$ to this state variable. Moreover, if attack vector $\boldsymbol{a}$ is composed by γ times ($\gamma \in R^+$) of the ith column vector $\boldsymbol{h_i}$ of Jacobian matrix $\boldsymbol{H}$, i.e., $\boldsymbol{a} = \gamma \boldsymbol{h_i} = \boldsymbol{H}\boldsymbol{c}$, where $c_i = \gamma$, c_i is the ith element of $\boldsymbol{c}$, then the attack vector can bypass the detection. Similar to (8), if measurement P_{ij} is modified to $P_{ij} + \gamma/x_{ij}$, then we have

$$\theta_i' = x_{ij}\left(P_{ij} + \frac{\gamma}{x_{ij}}\right) + \theta_j = \theta_i + \gamma. \tag{12}$$

Similar to (9), if the measurement P_i is modified to $P_i + \gamma \sum_{s=1}^{N_i} \frac{1}{x_{is}}$, then we have

$$\begin{aligned}\theta_i' &= \left(P_i + \gamma \sum_{s=1}^{N_i} \frac{1}{x_{is}} + \sum_{s=1}^{N_i} \frac{\theta_s}{x_{is}}\right) \Big/ \sum_{s=1}^{N_i} \frac{1}{x_{is}} \\ &= \left(P_i + \sum_{s=1}^{N_i} \frac{\theta_s}{x_{is}}\right) \Big/ \left(\sum_{s=1}^{N_i} \frac{1}{x_{is}}\right) + \gamma = \theta_i + \gamma. \end{aligned} \tag{13}$$

Similar to (10), if the measurement P_l is modified to $P_l - \frac{\gamma}{x_{li}}$, then we have

$$\theta_i' = x_{li}\left(\sum_{s=1}^{m_l} \frac{\theta_l}{x_{ls}} - \sum_{s=1}^{m_l-1} \frac{\theta_s}{x_{ls}} - P_l + \frac{\gamma}{x_{li}}\right) = \theta_i + \gamma \tag{14}$$

where the parameter θ_i' represents state variable θ_i after attacks. From (12), (13), and (14), we can obtain that the bias introduced to these attacked state variables is γ, which causes incorrect state estimation.

Meanwhile, even though the solution of the optimization problem in (5) is an NP-hard problem [30], [33], there are still some near-optimal solutions, such as a heuristic-based mechanism. Utilizing the characteristics that the attack vector is the linear combination of column vectors of Jacobian matrix $\boldsymbol{H}$ and the sparseness of matrix $\boldsymbol{H}$, Yang *et al.* [10] presented an RRE form based algorithm utilizing elementary row transformations for the transpose matrix of $\boldsymbol{H}$ to derive the solution of the least effort attack problem. It is due to the reason that linear transformations of one matrix do not change its solution space. Since the optimal least effort attack vector $\boldsymbol{a}^*$ must exist in one of the RRE forms of $(\boldsymbol{H}_{\bar{\boldsymbol{S}}})^T$, which has been proved in [10], thus the following relationship holds:

$$\begin{aligned}\boldsymbol{P}(\boldsymbol{H}_{\bar{\boldsymbol{S}}})^T\boldsymbol{Q} = [(\boldsymbol{H}_{\bar{\boldsymbol{S}}})^T]_{\boldsymbol{a}} &\Leftrightarrow \boldsymbol{Q}^T\boldsymbol{H}_{\bar{\boldsymbol{S}}}\boldsymbol{P}^T = [(\boldsymbol{H}_{\bar{\boldsymbol{S}}})]_{\boldsymbol{a}} \\ &\Leftrightarrow \boldsymbol{Q}^T\boldsymbol{H}_{\bar{\boldsymbol{S}}}\boldsymbol{P}^T\boldsymbol{e_n} = \boldsymbol{a}\end{aligned} \tag{15}$$

where $\boldsymbol{P}$ and $\boldsymbol{Q}$ denote traceability matrices of elementary row transformation and column exchange of $(\boldsymbol{H}_{\bar{\boldsymbol{S}}})^T$, where $[(\boldsymbol{H}_{\bar{\boldsymbol{S}}})]_{\boldsymbol{a}}$ is an ultimately unchanged RRE form, and $\boldsymbol{a}$ represents the row, which has the least number of nonzero elements in it. Here, $\boldsymbol{e_n}$ is a column vector, in which the elements in the last row is 1 and others are all zeros. Notice that when one PMU is placed at a specific bus, the related power flow measurements, which are associated with this specific bus and its adjacent buses, can be removed to the protected set $\boldsymbol{S}$. Then, attackers can regenerate the attack vector when Jacobian matrix $\boldsymbol{H}$ is updated because attackers have knowledge of the defend strategy in the control center.

Taking the edge buses and the RRE-based attack into considerations, the proposed HAS is given in Algorithm 1.

V. PDPG Algorithm Against the HAS

Considering the characteristics of PMUs mentioned in Section III-C, we can use these advanced measurement units combined with synchronizing of GPS time to provide protection to a subset of measurements in smart grid. Since attackers are difficult to modify such protected measurements, PMUs are robust against FDIA. In other words, there are some trusted measurements when some PMUs are deployed on some specific buses. In an extreme case, if the number of deployed PMUs is large enough, all measurements can be secure protected and all state variables can be measured and guaranteed so that the whole power system is observable. It means that $\text{rank}(\boldsymbol{H}_{\boldsymbol{S}}) = n$, and FDIA can no longer occur. However, in practice, because the cost for the installation and maintenance of PMUs is very high, it is expensive to deploy a large number of PMUs. At the same time, due to limitations of their own structure and effects, PMUs will not be moved or reassembled to other locations after deployment under normal circumstances. Thus, based on these considerations, from the perspective of the control center, the defense problem is formulated as to find which buses to deploy PMUs so that the total number of PMUs is minimized, and the whole system is completely observable.

Algorithm 1: HAS Algorithm.

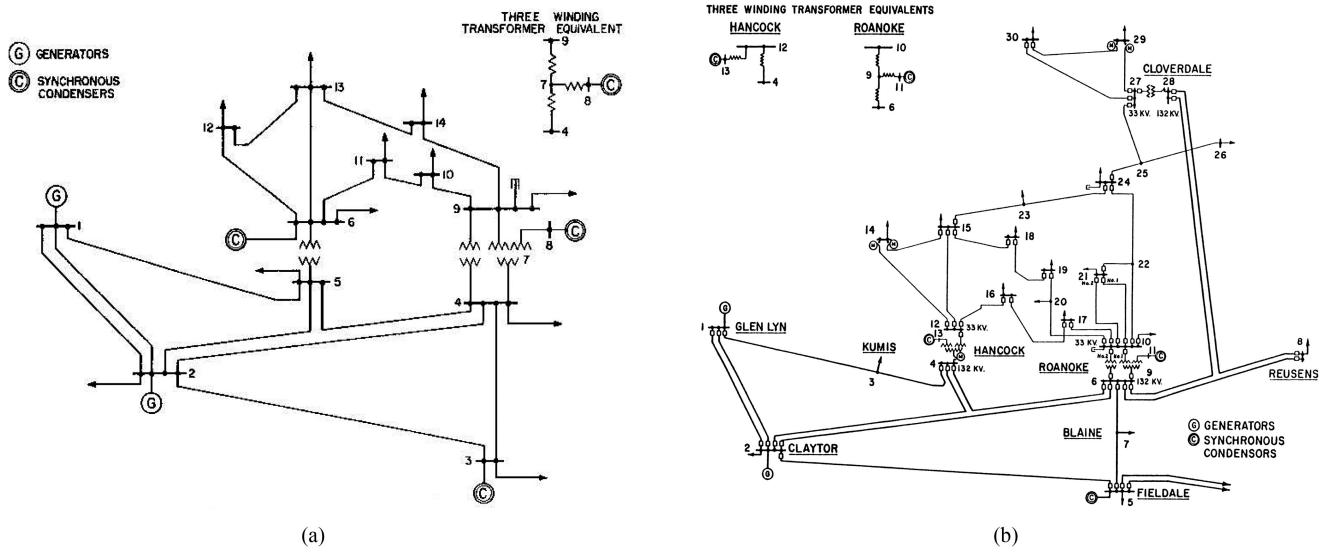
Input: Jacobian matrix $\boldsymbol{H}_{\bar{\boldsymbol{S}}}$; secure set $\boldsymbol{S}$;
Output: HAS attack vector $\boldsymbol{a}^*$;
$[m, n] = \text{size}(\boldsymbol{H}_{\bar{\boldsymbol{S}}})$;
$\boldsymbol{a_1} = \boldsymbol{a_2} = zeros(m, 1)$, which are used to initialize attack vectors;
$\boldsymbol{T} = (\boldsymbol{H}_{\bar{\boldsymbol{S}}})^T = [\boldsymbol{h_1}, \boldsymbol{h_2}, \ldots, \boldsymbol{h_n}]^T$;
$\boldsymbol{Q} = \text{eye}(m, m)$, which is an identity matrix to trace column exchange of $\boldsymbol{T}$;
$\boldsymbol{count} = zeros(1, n)$ is defined to count the number of nonzero elements in each column vector of $\boldsymbol{H}_{\bar{\boldsymbol{S}}}$;
for $i = 1$ to n **do**
  for $j = 1$ to m **do**
    if $\boldsymbol{H}_{\bar{\boldsymbol{S}}}(j, i) \neq 0$ **then**
      $\boldsymbol{count}(i) = \boldsymbol{count}(i) + 1$;
Choosing t specific state variables corresponding to smaller count(i), which are connected with the least number of buses, to find the set of $M = \{x_1, x_2, \ldots, x_t\}, t < n$;
for $i = 1$ to n **do**
  $\boldsymbol{A}(\boldsymbol{x_i}) = \gamma_i \boldsymbol{h_i}$ $(\gamma_i \in R^+)$;
  $\boldsymbol{a_1} = \boldsymbol{a_1} + \boldsymbol{A}(\boldsymbol{x_i})$;
repeat
  Elementary row transformation for matrix $\boldsymbol{T}$ to obtain RRE form;
  Find the row that has the minimum number of nonzero elements in $\boldsymbol{T}$, and all nonzero elements in this row are exchanged to last columns through column exchange;
  Traceability matrix $\boldsymbol{Q}$ is used to trace the transformation of column exchange;
  Update $\boldsymbol{T}$ and $\boldsymbol{Q}$;
until $\boldsymbol{P}$ no longer changed.
The attack vector can be obtained by $\boldsymbol{a_2} = (\boldsymbol{Q}^T)^{-1}(\boldsymbol{T}\boldsymbol{e_n})$;
return $\boldsymbol{a}^* = \boldsymbol{a_1} + \boldsymbol{a_2}$.

Algorithm 2: PDPG-Based Protection Algorithm.

Input: Jacobian matrix $\boldsymbol{H}_{\bar{\boldsymbol{S}}}$; attack vector $\boldsymbol{a}^*$;
Output: $\boldsymbol{H}_{\boldsymbol{S}}$;
$\boldsymbol{S} = \emptyset$; $[m, n] = \text{size}(\boldsymbol{H}_{\bar{\boldsymbol{S}}})$; $\boldsymbol{count1} = zeros(1, n)$;
$\boldsymbol{H}_{\bar{\boldsymbol{S}}} = [\boldsymbol{h_1}, \boldsymbol{h_2}, \ldots, \boldsymbol{h_n}]$; $\Omega = ||\boldsymbol{a}^*||_0$;
for $i = 1$ to n **do**
  for $j = 1$ to m **do**
    if $\boldsymbol{H}_{\bar{\boldsymbol{S}}}(j, i) \neq 0$ **then**
      $\boldsymbol{count1}(i) = \boldsymbol{count1}(i) + 1$;
Choosing t specific state variables corresponding to smaller $count(i)$ to find the set of $M = \{x_1, x_2, \ldots, x_t\}, t < n$;
Place PMUs at buses which adjacent to these t buses of smaller count values;
Remove rows in $\boldsymbol{H}_{\bar{\boldsymbol{S}}}$ targeted to PMU placed buses and adjacent buses to $\boldsymbol{H}_{\boldsymbol{S}}$;
Update $\boldsymbol{H}_{\bar{\boldsymbol{S}}}$ and $\boldsymbol{H}_{\boldsymbol{S}}$;
Divide $\boldsymbol{H}_{\bar{\boldsymbol{S}}}$ into $(n - t)$ submatrixes $\boldsymbol{H}_{\boldsymbol{L_i}}$, $L_i \in [1, n - t]$;
repeat
  Obtain submatrix $\boldsymbol{H}_{\boldsymbol{a}_k^*}$ from $\boldsymbol{a}^*$, where $\boldsymbol{a}_k^* = \{k | \boldsymbol{a}_k^* \neq 0\}, k \in [1, \Omega]$;
  Initial $\boldsymbol{count2} = zeros(1, n - t)$;
  $\boldsymbol{count2}(L_{\text{target}}) = \arg\max_{L_i \in [1, n-t]} \{card(\boldsymbol{H}_{\boldsymbol{a}_k^*} \cap \boldsymbol{H}_{L_i})\}$;
  Place one PMU at the bus corresponding to L_{target};
  Remove rows in $\boldsymbol{H}_{\bar{\boldsymbol{S}}}$ targeted to the PMU placed bus and adjacent buses to $\boldsymbol{H}_{\boldsymbol{S}}$;
  Update $\boldsymbol{H}_{\bar{\boldsymbol{S}}}$, $\boldsymbol{H}_{\boldsymbol{S}}$, and $\boldsymbol{a}^*$;
until $rank(\boldsymbol{H}_{\boldsymbol{S}}) = n$
return $\boldsymbol{H}_{\boldsymbol{S}}$.

Suppose that the defender in the control center is aware of possible attack schemes of an attacker and the attacker knows some specific information about the smart grid. The above interactive process describes the dynamics of attackers versus defenders [14]. As for the aforementioned defense problem, Kim and Poor [30] presented a secure PMU placement algorithm, which uses a greedy mechanism to add one PMU at a time to protect the maximum number of vulnerable state variables. Yang *et al.* [10] also present a greedy-based PMU deployment (PG) algorithm in which one PMU is placed on the best selected bus in each iteration round to protect the bus with the largest number of vulnerable measurements; the selected bus in each round is also closely related to the corresponding sparse attack vector; the placement process ends until the system is completely observable with all secure PMUs. Although the PG algorithm is near-optimal and straightforward, however, when the proposed HAS occurs, it is insufficient to defend against it. It is mainly because greedy-based mechanisms only focus on the bus with the largest number of vulnerable measurements in each round, and it naturally ignores these edge buses with fewer number of measurements. However, these edge buses are very easy to be attacked, and the attack cost targeted to them is extremely small. To solve this problem effectively, on the one hand, we need to care about the security of these state variables corresponding to these edge buses. On the other hand, the buses that are related to the largest number of vulnerable measurements in each iteration round should be seriously processed at the same time. Therefore, we propose a predeployment PDPG algorithm in Algorithm 2 to address this problem.

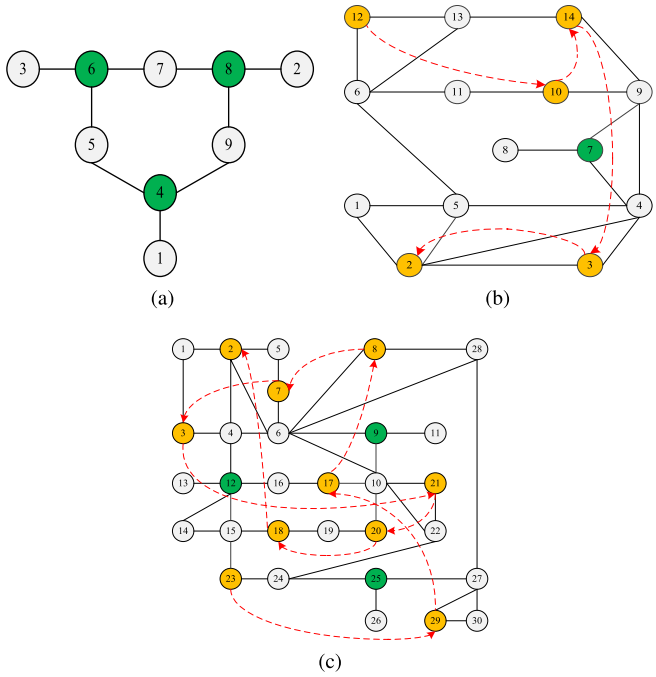
The PDPG algorithm is described as follows. Since we consider the process of PMUs configuration and suppose that the defender (i.e., the control center) is aware of attack strategies of attackers, then the defender can identify and determine vulnerable buses through the analysis of Jacobian matrix $\boldsymbol{H}$ and the topology of the power system in the control center. We count the number of nonzero elements in each column vector $\boldsymbol{h_i}$ of $\boldsymbol{H}$, then edge buses corresponding to smaller count values can be obtained. Then, we deploy PMUs on buses which are adjacent to these edge buses, because once the adjacent bus of an edge bus is placed by one PMU, state variables of the edge bus and its adjacent buses are all protected. This way



(a) (b)

Fig. 1. (a) IEEE 14-bus transmission network. (b) IEEE 30-bus transmission network [35].

we can make full use of the function of PMUs and increase the observation range of the system. After predeployment of t PMUs, the indices of row vectors of $\boldsymbol{H}$ corresponding to protected measurements are removed to $\boldsymbol{S}$, and dimensions of Jacobian matrix become smaller immediately. This can reduce the number of iterations in following steps. Then, greedy-based strategy is used to deploy one PMU to protect the largest number of vulnerable measurements in each round. The updated matrix $\boldsymbol{H}_{\bar{S}}$ is divided into $(n-t)$ submatrixes $\boldsymbol{H}_{\boldsymbol{L}_i}$, and each of them is targeted to one state variable. By utilizing the attack vector, we can obtain $\boldsymbol{H}_{a_k^*}$, which denotes the submatrix of $\boldsymbol{H}_{\bar{S}}$ related to nonzero elements in the attack vector. Finally, the bus which is corresponding to the largest number of elements of intersections between $\boldsymbol{H}_{\boldsymbol{L}_i}$ and $\boldsymbol{H}_{a_k^*}$ is selected as the object to place one PMU. Notice that if there are two or more buses that have the same number of the counter values, the bus which is adjacent with more buses is the one to deploy a PMU. Similarly, we can remove all measurements to the secure set after one PMU is placed at the given bus. With the progress of deployment process, the dimensions of matrix $\boldsymbol{H}_{\boldsymbol{S}}$ is gradually increasing. If the condition $rank(\boldsymbol{H}_{\boldsymbol{S}}) = n$ is satisfied, then the whole system is completely observable and FDIA from attackers are no longer possible to compromise the power system.



(a) (b) (c)

Fig. 2. Result of placement diagram of PMUs in (a) IEEE 9-bus system, (b) IEEE 14-bus system, and (c) IEEE 30-bus system.

VI. Experiments and Results

To illustrate the effectiveness of the proposed HAS (i.e., HAS) and the PDPG algorithm, we conduct experiments on various IEEE standard test systems including IEEE 9-bus, 14-bus, and 30-bus networks, which provide publicly available and standard information of test cases. For simplicity, parts of topologies of these systems are presented in Fig. 1(a) and (b). All experiments have been done on Lenovo desktop with 3.2 GHz Intel Core i5 processor and 4 GB RAM on Window 7 system. The configuration information of these test systems is obtained from the MATPOWER package [34], and the experimental environment used here is the MATLAB R2012b.

Next, we first present the proposed PDPG placement defense results against the HAS in various power systems. Second, we analyze and show that the PG algorithm fails to defend the HAS by comparing those with the PDPG algorithm results. Then, the performance of our proposed PDPG algorithm against the HAS is investigated and evaluated. Finally, we also evaluate the number of compromised measurements and time overhead of our proposed HAS and the RRE form attack in [10].

Fig. 2 shows the final deployment diagrams of PMUs using the PDPG algorithm in various simplified test networks topologies. Buses in green correspond to buses with predeployed PMUs. Buses in yellow represent buses on which PMUs are placed through the greedy-based strategy in the dynamic process of the PMUs deployment. Buses in gray correspond to the buses deployed without PMUs, and red arrows represent the order of each placement iteration process. Fig. 2(a) shows that the whole system of IEEE 9-bus is completely observable after the predeployment of three PMUs on bus 4, bus 6, and bus 8, and there is no need to place additional PMUs. Thus, after the procedure of PMUs predeployment, all the state variables of IEEE 9-bus system can be protected and monitored, and FDIAs are not stealthy in IEEE 9-bus system.

Fig. 2(b) shows that during the PDPG algorithm, one PMU is predeployed on bus 7 in IEEE 14-bus system. It is because bus 8 is adjacent to bus 7 in the topological structure and the bus 8 belongs to edge buses. The number of related measurements to the state variable of bus 8 is the minimal, and, hence, the attacker can easily identify this location (bus 8) through analyzing the topology of 14-bus system and the information of Jacobian matrix. To reduce the number of deployed PMUs, and according to the characteristics of PMUs, state variables of bus 4, bus 7, bus 8, and bus 9 can be simultaneously protected directly after the PMU predeployment on bus 7. Then, during the process of generating an attack vector, the dimensions of Jacobian matrix $\boldsymbol{H}$ become smaller and smaller. Rows targeted to related measurements of PMU deployed bus in $\boldsymbol{H}$ can be removed to $\boldsymbol{H_S}$, and columns targeted to protected state variables can also be removed. The greedy strategy in the proposed PDPG algorithm is, then, used to complete the PMU placement process, and the bus, which related to the largest number of vulnerable measurements, is protected in each iteration round. The whole dynamic iterative process of attackers versus defenders continues until all state variables are protected. Finally, bus 12, bus 10, bus 14, bus 3, and bus 2 are deployed with PMUs one after another with the order of red arrows presented in Fig. 2(a). Similarly, as shown in Fig. 2(c) of IEEE 30-bus system, bus 9, bus 12, and bus 25 are deployed with PMUs in advance, and, then, the follow-up iteration process is shown by the direction of red arrows. The final results about the above 14-bus system and 30-bus system are that all state variables are protected due to the reason that all state variables can be monitored by deployed PMUs, and FDIAs are impossible.

For the PG algorithm used in IEEE 9-bus system, only one PMU is deployed when bus 1, bus 2, and bus 3 are simultaneously attacked by the HAS. It is because the PG algorithm only considers the bus with the most vulnerable measurements in each iteration round, and, thus, the 9-bus system is not fully observed and is not secure. Similarly, in the first iteration round of IEEE-14 bus system, the proposed HAS can attack bus 8 and bus 12 at the same time with low attack overhead, but the PG algorithm deploys the PMU on bus 12, while ignoring the security of bus 8. Unprotected bus 8 will affect the subsequent control and decision-making in the EMS due to the introduction of attacks. The same situation occurs in the 30-bus system, which fully exposes the deficiency of the PG algorithm. All

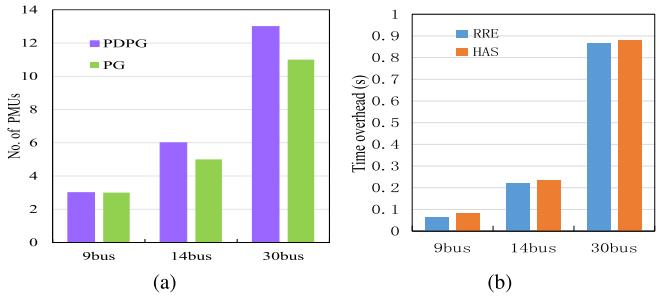


Fig. 3. (a) Number of PMUs needed of PG and PDPG algorithms in different systems. (b) Time overhead for the first round of attack of RRE based attack and HAS.

the results are based on the fact that the proposed HAS has the capability to identify weak buses and can attack multiple buses simultaneously with very little attack overhead and the PG algorithm used in the whole attacker and defender dynamic iterative process can only deploy one PMU on a specific bus. Thus, only the PMU deployed bus can be protected and secured, and the buses without deployed PMUs can still be attacked and affected during the dynamic process of attacker versus defender.

Fig. 3(a) shows the number of the needed PMUs in the PG algorithm and the proposed PDPG algorithm in various test systems. Fig. 3(a) shows that in the IEEE 9-bus system, both the two algorithms need to deploy three PMUs. In the IEEE 14-bus system, the proposed PDPG algorithm needs six PMUs, and it needs one more PMU than the PG algorithm. Moreover, in the 30-bus system, it needs two more PMUs than the PG algorithm. Although the proposed PDPG algorithm needs more PMUs, early results show that the PDPG algorithm is more secure against FDIA than the PG algorithm, and the following results show that the PDPG algorithm is more robust against FDIA than the PG algorithm.

In this article, we assume that the complete observability grants immunity to the power system against FDIAs. During the dynamic process of attacker versus defender, when edge buses are first attacked by the hybrid attack in the 14 bus system, the power system is completely observable if and only if six PMUs are deployed through our proposed PDPG algorithm rather than four PMUs. Four PMUs, which are deployed on bus 2, bus 6, bus 8, and bus 9, can guarantee the complete observability when not considering the security during PMUs deployment. However, based on the deployment result of the PDPG algorithm, it can be found that when the security during PMUs deployment is not considered, the locations of deployed PMUs are different from the result which considers the dynamic process of attacker versus defender.

The introduced additional cost of two extra PMUs of our proposed PDPG algorithm is defined by the characteristics of the new HAS and the topology of a specific power grid. It means that without the two extra PMUs, the IEEE 14 bus system cannot defend against the proposed new hybrid FDIA when considering the security during PMUs deployment. Specifically, the proposed HAS can identify these edge buses first and launch attacks with lower attack cost, while the aim of PMUs predeployment in the PDPG algorithm is to add local observability of edge buses

TABLE II
COMPROMISED MEASUREMENTS AND TIME OVERHEAD WITH INCREASE OF PMUS UNDER PG AND PDPG ALGORITHMS

	Round	Compromised measurements under PG	Time(s)	Compromised measurements under PDPG	Time(s)
IEEE 14-bus	Round1	P_7,P_8,$P_{7,8}$,$P_{8,7}$	0.250	P_6,P_{12},P_{13},$P_{6,12}$,$P_{12,13}$,$P_{12,6}$,$P_{13,12}$	0.105
	Round2	P_6,P_{12},P_{13},$P_{6,12}$,$P_{12,13}$,$P_{12,6}$,$P_{13,12}$	0.139	P_9,P_{10},P_{11},$P_{9,10}$,$P_{10,11}$,$P_{10,9}$,$P_{11,10}$	0.065
	Round3	P_9,P_{10},P_{11},$P_{9,10}$,$P_{10,11}$,$P_{10,9}$,$P_{11,10}$	0.066	P_9,P_{13},P_{14},$P_{9,14}$,$P_{13,14}$,$P_{14,9}$,$P_{14,13}$	0.046
	Round4	P_9,P_{13},P_{14},$P_{9,14}$,$P_{13,14}$,$P_{14,9}$,$P_{14,13}$	0.045	P_2,P_3,P_4,$P_{2,3}$,$P_{3,4}$,$P_{3,2}$,$P_{4,3}$	0.035
	Round5	P_2,P_3,P_4,$P_{2,3}$,$P_{3,4}$,$P_{3,2}$,$P_{4,3}$	0.034	P_1,P_2,P_4,P_5,$P_{1,2}$,$P_{2,4}$,$P_{2,5}$,$P_{2,1}$,$P_{4,2}$,$P_{5,2}$	0.024
	Round6	P_1,P_2,P_4,P_5,$P_{1,2}$,$P_{2,4}$,$P_{2,5}$,$P_{2,1}$,$P_{4,2}$,$P_{5,2}$	0.023	"–"	"–"
IEEE 30-bus	Round1	P_{29}, P_{30}, $P_{27,29}$, $P_{27,30}$, $P_{29,30}$, $P_{29,27}$, $P_{30,27}$, $P_{30,29}$	0.638	P_{15}, P_{23},P_{24}, $P_{15,23}$, $P_{23,24}$, $P_{23,15}$, $P_{24,23}$	0.269
	Round2	P_{12}, P_{13}, $P_{12,13}$, $P_{13,12}$	0.612	P_{27}, P_{29}, P_{30}, $P_{27,29}$, $P_{29,30}$, $P_{29,27}$, $P_{30,29}$	0.214
	Round3	P_{25}, P_{26}, $P_{25,26}$, $P_{26,25}$	0.383	P_{10}, P_{16}, P_{17}, $P_{16,17}$, $P_{10,17}$, $P_{17,16}$, $P_{17,10}$	0.162
	Round4	P_{15}, P_{23}, P_{24}, $P_{15,23}$, $P_{23,24}$, $P_{23,15}$, $P_{24,23}$	0.296	P_6, P_8, P_{28}, $P_{6,8}$, $P_{8,28}$, $P_{8,6}$, $P_{28,8}$	0.139
	Round5	P_6 ,P_8 ,P_{28} ,$P_{6,8}$,$P_{8,28}$,$P_{8,6}$,$P_{28,8}$	0.287	P_5 ,P_6 ,P_7 ,$P_{5,7}$,$P_{6,7}$,$P_{7,5}$,$P_{7,6}$	0.128
	Round6	P_{21}, P_{22}, P_{24}, $P_{10,21}$, $P_{10,22}$, $P_{21,22}$, $P_{22,24}$, $P_{21,10}$, $P_{22,10}$, $P_{22,21}$, $P_{24,22}$	0.245	P_1, P_3, P_4 , $P_{1,3}$, $P_{3,4}$, $P_{3,1}$, $P_{4,3}$	0.112
	Round7	P_9, P_{11}, $P_{9,11}$, $P_{11,9}$	0.160	P_{10}, P_{21}, P_{22}, $P_{10,21}$, $P_{21,22}$, $P_{21,10}$, $P_{22,21}$	0.092
	Round8	P_{18}, P_{19}, P_{20}, $P_{18,19}$, $P_{19,20}$, $P_{19,18}$, $P_{20,19}$	0.105	P_{10}, P_{19}, P_{20}, $P_{19,20}$, $P_{10,20}$, $P_{20,19}$, $P_{20,10}$	0.058
	Round9	P_{10}, P_{16}, P_{17}, $P_{16,17}$, $P_{10,17}$, $P_{17,16}$, $P_{17,10}$	0.072	P_{15}, P_{18}, P_{19}, $P_{15,18}$, $P_{18,19}$, $P_{18,15}$, $P_{19,18}$	0.044
	Round10	P_2, P_5, P_7, $P_{2,5}$, $P_{5,7}$, $P_{5,2}$, $P_{7,5}$	0.058	P_1, P_2, P_4, P_5, P_6, $P_{1,2}$, $P_{2,4}$, $P_{2,5}$, $P_{2,6}$, $P_{2,1}$, $P_{4,2}$, $P_{5,2}$, $P_{6,2}$	0.021
	Round11	P_1, P_3, P_4, $P_{1,3}$, $P_{3,4}$, $P_{3,1}$, $P_{4,3}$	0.024	"–"	"–"

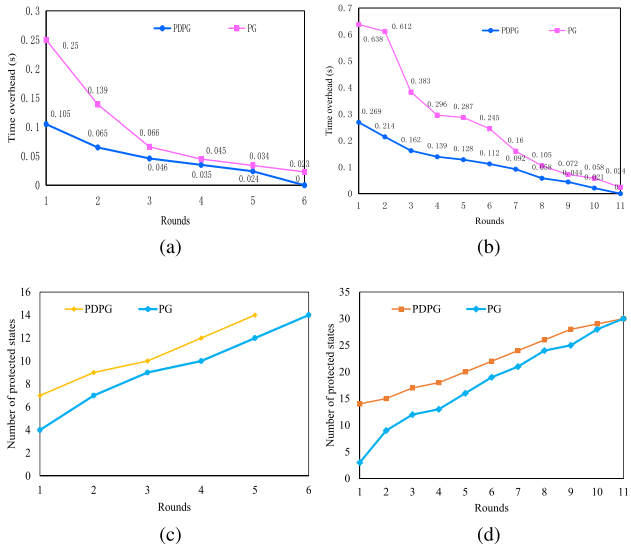


Fig. 4. Time overhead to compromise measurements and the number of protected states with the increase of PMUs. (a) 14-bus system. (b) 30-bus system. (c) 14-bus system. (d) 30-bus system. (legends: PG greedy algorithm to place PMUs, PDPG pre-deployment PMU-based greedy algorithm).

in the power system at first. Based on the topology of the 14 bus system, locally observable areas based on PMUs predeployment segment the whole grid. Other PMUs are, then, deployed based on greedy strategies until the observability of all buses is guaranteed. Similarly, in the IEEE 30 bus system, edge buses 11, 13, and 26 are first protected with PMUs, the following greedy-based deployment, then, guarantees the whole observability in which 13 PMUs are required rather than 10 PMUs.

With the increase of the number of deployed PMUs in each iteration round, the compromised measurements and time overheads of the PG algorithm and the PDPG algorithm in IEEE 14-bus network are presented in Table II. The time overhead variations of the two defense algorithms are also compared in Fig. 4(a) in each round. After the PMUs predeployment stage, the number of measurements to be compromised by attackers at the beginning increases, and it forces attackers to increase their attack cost to tamper with more meter measurements. From the point of view of attackers, Fig. 4(a) shows that the time needed to compromise meter measurements is less in each round after PMUs predeployment than the PG algorithm. It is because the dimensions of Jacobian matrix become smaller when PMUs are introduced in the initial stage, and the search space of attacks becomes smaller in order to obtain the optimal solution. With regard to protected state variables, from the defender's point of view, Fig. 4(c) shows that the number of protected state variables in the PDPG algorithm after one round is seven, which is larger than that of the PG algorithm. It means that half of all state variables in IEEE 14-bus system are protected, and, thus, the system is more robust against FDIA at the beginning. Then, with the progress of placement process by other PMUs using the greedy strategy, the number of protected states is gradually increasing. Finally, after five iteration rounds, all the state variables are protected, and there is no chance for attackers to launch FDIAs anymore.

With respect to the IEEE 30-bus system, Table II also presents the compromised measurements and time overheads in each iteration round of the PG and the PDPG algorithms, respectively. After the predeployment of the PDPG algorithm by three PMUs on bus 9, bus 12, and bus 25 in advance, the numbers of compromised measurements in each round are all seven, and this is different with the PG algorithm. Similarly, from the results of Fig. 4(b), we can see that the time overhead of the PG algorithm in the first round is 0.638 s, which is obviously larger than 0.269 s corresponding to the PDPG algorithm. Fig. 4(d) also shows that the number of protected state variables is larger for the PDPG algorithm than that for the PG algorithm. It shows the same results with the case of IEEE 14-bus system. From the above experimental results, it is clear that the PDPG algorithm is more robust against FDIAs than the PG algorithm.

Finally, we show the performance and cost of the proposed HAS algorithm when compared with the RRE attack. In the

TABLE III
NUMBER OF COMPROMISED MEASUREMENTS OF RRE AND HAS IN DIFFERENT TEST NETWORKS

Test network	RRE Attack	HAS
IEEE 9-bus	4	8
IEEE 14-bus	4	11
IEEE 30-bus	8	12

HAS, an attacker has the ability to compromise a few measurements for the purpose of attacking one or some extra specific state variables, besides the attack vector generated by the RRE attack method, which only focuses on the transformation of the Jacobian matrix. The results about the number of compromised measurements in the first round for solving the attack vector are shown in Table III. From the table, it is clear that the RRE attack needs to compromise 4, 4, and 8 measurements in IEEE 9-bus network, IEEE 14-bus network, and IEEE 30-bus network, respectively. On the other hand, the HAS needs to compromise 8, 11, and 12 measurements in IEEE 9-bus, 14-bus, and 30-bus networks, respectively. Thus, for IEEE 9-bus and 30-bus test networks, the HAS needs to compromise four more measurements than the RRE method. For the 14-bus network, it needs to compromise additional 7 m measurements compared with the RRE method. However, it is easy for the attacker to tamper with these additional measurements in practice, and the required operation that the attacker needs to do is to measure the branch impedance associated with the attacked bus in the field through analyzing the topology of the power system.

Fig. 3(b) compares time overheads of solving the first round of attack vectors for the HAS and the RRE. For the HAS, time overheads are 0.081, 0.235, and 0.880 s in the 9-bus, 14-bus, and 30-bus networks, respectively. For the RRE attack, time overheads are 0.064, 0.218, and 0.865 s, respectively. Obviously, the time needed in the HAS is slightly larger than the RRE method. But overall, the time overheads of these two methods are about the same. It can be concluded that our proposed HAS attack is little more complex than the RRE attack, and, thus, the attacker needs to pay more effort to launch the attack. But for the number of compromised measurements in practice and the time overhead of solving attack vectors from Table III and Fig. 3(b), very little effort is required for the attacker when compared with the RRE method.

VII. CONCLUSION AND FUTURE WORK

Since synthesized FDIAs could wisely circumvent conventional BDD mechanism and pose a great threat to the accurate state estimation and operation in smart grid, the protection of smart grid against such attacks is very important. From the perspective of protection-based defense by integrating PMUs in smart grid, this article concentrates on the security against FDIA during the dynamic process of attacker versus defender. In this article, considering the generalized constraints of the attacker, we first analyze the adverse effects of FDIA targeted to the state estimation of power system. We, then, show that the existing PG algorithm is failed to defend against our proposed HAS attack, which has the capability to identify weak buses and can attack multiple buses simultaneously with very little attack overhead. Moreover, the PDPG algorithm is proposed to increase the robustness of the whole power system against FDIA. In the PDPG algorithm, after the predeployment of some PMUs, a set of relatively vulnerable buses can be protected in advance, and the entire system is completely observable when the whole placement process is completed such that the attacker is no longer to attack the smart grid. Finally, experiment results have demonstrated the effectiveness of the proposed PDPG algorithms based on various IEEE standard systems. In addition, it is interesting to explore the case that how to launch attacks and the corresponding defend strategy when only part of the Jacobian matrix information is known by attackers in the future work.

REFERENCES

[1] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, Oct.–Dec. 2012.

[2] X. Jin, W. M. Haddad, and T. Hayakawa, "An adaptive control architecture for cyber-physical system security in the face of sensor and actuator attacks and exogenous stochastic disturbances," *Cyber-Phys. Syst.*, vol. 4, no. 1, pp. 39–56, 2018.

[3] J. Jow, Y. Xiao, and W. Han, "A survey of intrusion detection systems in smart grid," *Int. J. Sensor Netw.*, vol. 23, no. 3, pp. 170–186, 2017.

[4] R. Fang, J. Wang, and W. Sun, "Cross-layer control of wireless sensor network for smart distribution grid," *Int. J. Sensor Netw.*, vol. 27, no. 2, pp. 71–84, 2018.

[5] G. Tang, K. Wu, J. Lei, and W. Xiao, "SHARK: sparse human action recovery with knowledge of appliances and load curve data," *Cyber-Phys. Syst.*, vol. 1, no. 2–4, pp. 113–131, 2015.

[6] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, 2009, pp. 21–32.

[7] E. McCary and Y. Xiao, "Malicious device inspection home area network in smart grids," *Int. J. Sensor Netw.*, vol. 25, no. 1, pp. 45–62, Sep. 2017.

[8] 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," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[9] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

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

[11] M. A. Rassam, M. Maarof, and A. Zainal, "A distributed anomaly detection model for wireless sensor networks based on the one-class principal component classifier," *Int. J. Sensor Netw.*, vol. 27, no. 3, pp. 200–214, 2018.

[12] J. Jiang and Y. Qian, "Defense mechanisms against data injection attacks in smart grid networks," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 76–82, Oct. 2017.

[13] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[14] X. Liang and Y. Xiao, "Game theory for networksecurity," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 472–486, First Quarter 2013.

[15] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[16] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, Jun. 2016.

[17] S. Ma, Y. Yang, Y. Qian, H. Sharif, and M. Alahmad, "Energy harvesting for wireless sensor networks: applications and challenges in smart grid," *Int. J. Sensor Netw.*, vol. 21, no. 4, pp. 226–241, 2016.

[18] Z. Zhou, J. Bai, M. Dong, K. Ota, and S. Zhou, "Game-theoretical energy management design for smart cyber-physical power systems," *Cyber-Phys. Syst.*, vol. 1, no. 1, pp. 24–45, 2015.

[19] M. B. Do Coutto Filho, and J. C. Stacchini de Souza, "Forecasting-aided state estimation—Part I: Panorama," *IEEE Trans. Power Syst.*, vol. 24, no. 4, pp. 1667–1677, Nov. 2009.

[20] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, Jul. 2017.
[21] L. Liu, M. Esmalifalak, Q. Ding, V. A. 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.
[22] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Trans. Ind. Informat.*, vol. 11, no. 5, pp. 1–12, Oct. 2015.
[23] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.
[24] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving efficient detection against false data injection attacks in smart grid," *IEEE Access*, vol. 5, pp. 13787–13798, 2017.
[25] M. Mohammadpourfard, A Sami, and A. R. Seifi, "A statistical unsupervised method against false data injection attacks: A visualization-based approach," *Expert Syst. With Appl.*, vol. 84, pp. 242–261, 2017.
[26] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. First Workshop Secure Control Syst.*, Stockholm, Sweden 2010.
[27] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. First Workshop Secure Control Syst.*, Stockholm, Sweden, 2010.
[28] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.
[29] J. Chen and A. Abur, "Placement of PMUs to enable bad data detection in state estimation," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1608–1615, Nov. 2006.
[30] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.
[31] N. M. Manousakis and G. N. Korres, "Optimal PMU placement for numerical observability considering fixed channel capacity a semidefinite programming approach," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 3328–3329, Jul. 2016.
[32] A. Giani, R. Bent, and F. Pan, "Phasor measurement unit selection for unobservable electric power data integrity attack detection," *Int. J. Critical Infrastructure Protection*, vol. 7, no. 3, pp. 155–164, 2014.
[33] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, Sep. 2012.
[34] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.
[35] Power Systems Test Case Archive, University of Washington. [Online]. Available: https://www2.ee.washington.edu/research/pstca/. Accessed on: Jan. 10, 2017
[36] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*, 1st ed. New York, NY, USA: Marcel Dekker, Mar. 2004.
[37] Q. Yang, L. Jiang, W. Hao, B. Zhou, P. Yang, and Z. Lv, "PMU placement in electric transmission networks for reliable state estimation against false data injection attacks," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1978–1986, Dec. 2017.
[38] 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," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.
[39] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

Chao Pei is currently working toward the Ph.D. degree in control theory and control engineering with the Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China.

He is currently visiting the Department of Computer Science, University of Alabama, Tuscaloosa, AL, USA, as a Ph.D. student. His research interests include cyber-physical security of smart grid, power system state estimation, PMU deployment, and signal processing.

Yang Xiao (Fellow, IEEE) received the M.S. and Ph.D. degrees in computer science and engineering from Wright State University, Dayton, OH, USA. in 2000 and 2001, respectively.

He is currently a Professor with the Department of Computer Science, University of Alabama, Tuscaloosa, AL, USA. His current research interests include cyber-physical systems, Internet of Things, security, wireless networks, smart grid, and telemedicine. He has published more than 280 journal papers (including over 50 IEEE/ACM transactions papers) and more than 200 conference papers.

Dr. Xiao was a Voting Member of IEEE 802.11 Working Group from 2001 to 2004, involving IEEE 802.11 (WIFI) standardization work. He is an IET Fellow. He currently serves as Editor-in-Chief for *Cyber-Physical Systems* (Journal). He had(s) been an Editorial Board or Associate Editor for 20 international journals. He served(s) as a Guest Editor for over 20 times for different international journals.

Wei Liang received the Ph.D. degree in mechatronic engineering from the Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China, in 2002.

She is currently a Professor with the Shenyang Institute of Automation, Chinese Academy of Sciences. As a Primary Participant/a Project Leader, she developed the WIA-PA and WIA-FA standards for industrial wireless networks, which are specified by IEC 62601 and IEC 62948, respectively. Her research interests include industrial wireless sensor networks and wireless body area networks.

Dr. Liang received the International Electrotechnical Commission 1906 Award in 2015 as a distinguished expert of industrial wireless network technology and standard.

Xiaojia Han is currently working toward the Ph.D. degree in measurement technology and automatic equipment with the Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China.

Her research interests include sensor and actuator fault detection methods, smart grid, and signal processing.