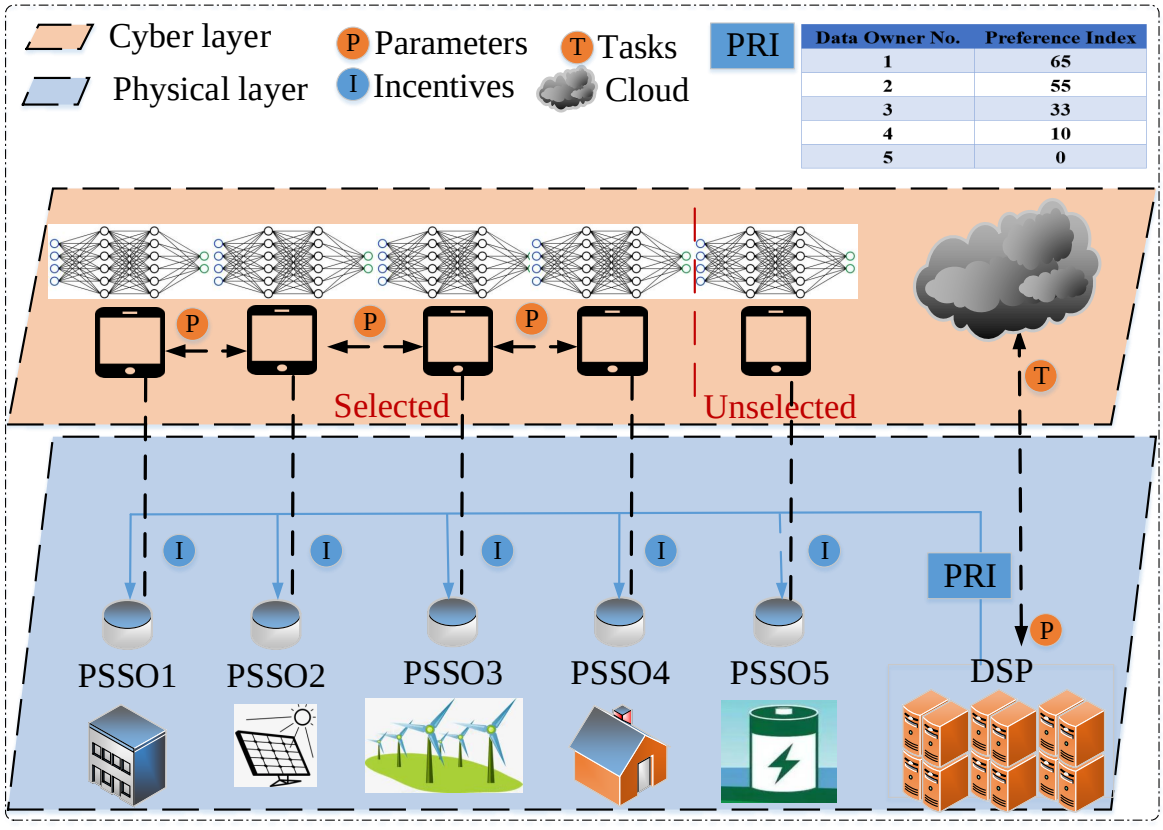
- A novel federated learning framework is proposed for FDI attack detection.
- Unknown system parameters and small decentralized data sets are considered.
- An incentive mechanism is designed to deal with the strategic data owners.
- The impact of incentive mechanism on detection accuracy is characterized.
- Optimal detection accuracy is achieved under a given incentive budget.

Graphical Abstract

Incentive Edge-Based Federated Learning for False Data Injection Attack Detection on Power Grid State Estimation: a Novel Mechanism Design Approach

Wen-Ting Lin,Guo Chen,Yuhan Huang



Incentive Edge-Based Federated Learning for False Data Injection Attack Detection on Power Grid State Estimation: a Novel Mechanism Design Approach*

Wen-Ting Lin[a], Guo Chen[a,*] and Yuhan Huang[b]

[a]School of Automation, Central South University, Changsha, 410083, China
[b]School of Civil and Environmental Engineering, University of Technology Sydney, NSW 2007, Australia

ARTICLE INFO

Keywords:
Cyber attacks
False data injection
Federated learning
Incentive mechanism design
Smart grid

ABSTRACT

With the growing concern in security and privacy of smart grid, false data injection attack detection on power grid state estimation now faces new challenges including unknown system parameters and small decentralized data sets with strategic data owners. To deal with these technical bottlenecks, this paper proposes a novel edge-based federated learning framework for false data injection attack detection on power grid state estimation, which has great potential in real-world applications with unknown system parameters. Furthermore, to seek a high detection accuracy with small decentralized data set and strategic data owners, an incentive mechanism is designed to encourage the desired data owners contributing to false data injection attack detection. To explore the impact of the incentive mechanism on the detection accuracy, a bi-level model depicting the data owners' participation in false data injection attack detection is formulated, based on which the impact is quantified. Moreover, a novel preference criterion is proposed for optimal mechanism design. It can achieve the optimal detection accuracy under a certain incentive budget. The incentive mechanism is designed and tested for 100 Monte Carlo scenarios. Simulations of false data injection attack detection on power grid state estimation show that the proposed framework outperforms the existing works without mechanism design.

1. Introduction

With the prevalence of smart meters and the information network, traditional power system is experiencing an integration with information and communication technologies. The integration makes the traditional power grid evolve into a cyber-physical system [1], which generates, transmits and distributes electricity in a modernized manner [2]. Although the transition improves the reliability, flexibility and efficienc-y of the power system, its reliance on the information network exposes it to cyber attacks [3, 4, 5].

As a confirmed cyber attack targeting the power system, the 2007 Aurora cyber attack led to the explosion of large numbers of generators [6]. Since then, cyber attacks have become a growing concern in power grid operation, especially for the power system state estimation [7, 8]. The stability control will be disrupted if the state estimation operates under a cyber attack, which disables the total energy management strategy. Among all the cyber attacks, false data injection (FDI) attacks show great threats on power system state estimation with its various types and dramatic impacts. FDI attackers pour large amounts of interference data into the measurement set with an expectation to obtain illegal income or to commit sabotage acts, misleading the whole state estimation process [9, 10]. This leads to a great concern on the reliability and security of the power grid [11].

Due to its dramatic damage, recently FDI attack detection has attracted a wide range of research interests from both energy and information fields. Various methods were explored for detecting FDI attacks, which can be categorized into model-based and data-driven methods. For the first category, the weighted least squares method was used for FDI attack detection for resilient control of a DC micro grid under the assumption that the power system operates in a steady state [12]. As we know, apart from the stability impact, FDI attacks can also interrupt the information exchange tunnel. In [13, 14], the impact of FDI attack on the information exchange topology was quantified, where weighted least squares method was employed for the attack detection. In [15], a recursive state estimation method was proposed by combining the historical data with the current measurement, which achieved the FDI attack detection of power systems. All of these methods are based on the weighted least squares approach. Restricted by the fitting accuracy of the weighted least squares methods, the detection accuracy of these approaches are limited. To overcome this problem, [16] proposed a novel fusion detection approach by incorporating the cyber security incidents into the state estimation model, which showed improvement on detection accuracy. These methods were built under the assumption that the power system operates in a steady state. However, due to the uncertainties in real-time load and power generation [17, 18, 19], the power system usually operates in a dynamic environment, which cannot be solved directly by the aforementioned detection methods. Thus dynamic estimation based methods quickly became the most popular solution, with Kalman filter being the main approach. In [20], the Kalman filter was

*This work is supported by the National Natural Science Foundation of China under Grant 62073344.
*Corresponding author
linwentinghust2017@gmail.com (W. Lin); guochen@ieee.org (G. Chen); Yuhan.Huang@uts.edu.au (Y. Huang)
ORCID(s):

adopted for estimation of various state processes, which can achieve FDI attack detection in a dynamic environment.

All the aforementioned detection methods are model-based, which means that their effectiveness relies directly on the accurate system parameters. Recently, the emergence of stealthy attack has driven the existing FDI attack detection mechanism evolving into a proactive FDI attack detection manner, which is achieved by employing distributed flexible AC transmission system (D-FACTS) devices [21, 22]. In these proactive FDI attack detection mechanisms, the D-FACTS devices are used for topology perturbation. It prevents the attackers from acquiring the measurement matrix, thus makes the stealthy attacks unavailable. Although the use of D-FACTS devices is effective in detecting the stealthy attacks, it also prevents the detection system from obtaining the information of the measurement matrix. This means the aforementioned model-based detection methods will lose their effectiveness under this circumstance.

This problem can be solved by the data-driven methods, which are model-free and are classified as the second category. In [23], support vector machine (SVM) was employed for FDI attack detection in smart grid, which showed an acceptable accuracy in locating the electricity theft. Motivated by the efficiency of biological neural network, in [20, 24, 25], various neural networks were designed for FDI attack detection, including the feedforward, recurrent, deep and convolutional neural networks. The data-driven methods do not require the system parameters, while they need a large amount of local data [26]. However, the measurement data sets are usually distributed, each possessed by an independent power system state owner (PSSO). Direct data transmission among PSSOs is time-consuming and expensive, which also leads to data privacy issue. Thus, the strategic PSSOs will not agree to transmit their local data over the network, which means a large local data set is unavailable in real-world applications. How to coordinate these PSSOs to detect FDI attacks while preserving the data privacy remains a challenging problem.

As discussed above, we can see that FDI attack detection on state estimation now faces new challenges including unknown system parameters and small decentralized data sets with strategic data owners. In this paper, a novel edge-based federated learning framework is proposed for FDI attack detection on power grid state estimation. A direct illustration of the proposed framework is given in Fig.1. In the proposed framework, monetary incentives are given to the desired PSSOs, based on which the coordination of PSSOs is formed to execute the detection task using the edge-based federated learning method. The novelty and contribution of this paper are summarized as follows:

1) The proposed framework can achieve FDI attack detection on power grid state estimation with unknown system parameters and small decentralized data sets, which preserves the PSSOs' private data from exposure. Moreover only the intermediate model parameters are required to be exchanged among the nodes, which further prevents the system parameters from being divulged.

2) An incentive mechanism is designed to encourage the desired PSSOs contributing to FDI attack detection on power grid state estimation, which achieves a high detection accuracy with strategic PSSOs.

3) A bi-level model depicting the PSSOs' participation in FDI attack detection is proposed. Compared with the existing works in [27] where only monetary cost was considered in the incentive mechanism design, both the detection accuracy and the monetary cost are considered in this study, which characterizes the impact of the incentive mechanism on the detection accuracy.

4) The impact of the incentive mechanism on the detection accuracy is explored and quantified. A novel preference criterion is proposed to achieve the optimal detection accuracy under a given incentive budget.

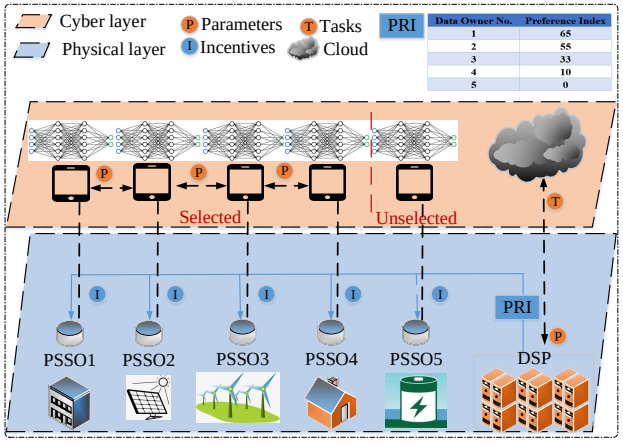


Figure 1: The proposed edge-based federated learning framework.

2. PRELIMINARIES

In this section, the fundamental model of the power system estimation problem is given, which follows the traditional residual test detection method.

2.1. Power System State Estimation

State estimation in smart grid aims to estimate the system state variables (voltage phase angles) based on measurements obtained from various sensors that are located in different places. Based on the characteristics of the measurement matrix, the state estimation model can be divided into two categories, which corresponds to the linear models in DC system and the nonlinear models in AC system, respectively. As is revealed in [28], the nonlinear AC state estimation model can be linearized by replacing the nonlinear relationship with the Jacobian matrices at the current state. Thus the DC power flow model is used to design the federated learning framework for FDI attack detection in this study. Without loss of generality, the proposed mechanism is also suitable for FDI attack detection in AC state estimation by using the conversion method in [28].

Specifically, the following DC power flow model is analyzed [26]:

$$y = Hx + \epsilon, \tag{1}$$

where $y \in R^n$ represents the measurement vector (voltage phase angle); $x \in R^m$ is the system state vector; $H \in R^{n\times m}$ represents the system-defined measurement matrix which maps the system state values to measurement values. $\epsilon \in R^n$ is the random measurement error of Gaussian distribution, with zero mean and the following covariance matrix:

$$V = diag(\delta_1^{-2}, \delta_2^{-2}, ..., \delta_n^{-2}), \tag{2}$$

where δ_i represents the standard deviation of the ith measurement.

2.2. FDI Attack Detection on Power System State Detection

By employing the least squares method, the estimation of system states can be obtained by solving the following optimization problem:

$$\hat{x} = \underset{x}{argmin}(y - Hx)^T V^{-1}(y - Hx) \tag{3}$$

The solution can be deduced by using equation (4):

$$\hat{x} = (H^T V^{-1} H)^{-1} H^T V^{-1} y \triangleq \Phi y \tag{4}$$

where $\Phi = (H^T V^{-1} H)^{-1} H^T V^{-1}$. Based on the state estimation $\hat{x}$, the estimation of the measurement can be obtained as $\hat{y} = Hx = H\Phi y$. Thus we can further calculate the measurement residual as follows:

$$r = y - \hat{y} = (I - H\Phi)x. \tag{5}$$

Following the calculation of the residual, to accomplish the FDI attack detection task, the detection test based on largest normalized residual (LNR) test method is employed for FDI attack detection. This can be realized as follows:

$$D(y_t) = \begin{cases} 1, if \ \|\bar{r}\|_\infty \geq \tau, \\ 0, otherwise, \end{cases} \tag{6}$$

where $\bar{r} = \sqrt{V^{-1}}r$ is normalized based on covariance V.

Remark 1. *The residual test in equation (6) is called the bad data detection (BDD), which is widely used in FDI detection on power state estimation. However, in the existing works, it is assumed that the information of the measurement matrix H is known to all, which is the premise of using BDD. However, due to use of D-FACTS devices, it is hard for the detection service provider (DSP) to know the full information of the measurement matrix, which means the existing methods relying on the knowledge of the measurement matrix will not be available for the DSP. Thus in this paper, a novel edge-based federated learning framework is proposed for model prediction of the measurement matrix H.*

3. Network Model of Federated Learning for FDI Attack Detection

As we can see in section 2, the parameters in matrix model H are necessary for estimation-based FDI attack detection. From the viewpoint of adversaries, the information of the parameters in matrix model H is needed for launching a stealthy attack. Thus, it is necessary for us to learn the information of the matrix H while keeping it from exposure to the adversaries.

FDI attack detection problems are commonly solved in a centralized framework, which has been pervasively utilized in smart grid. Although it shows great convenience in centralized control on one single device, it requires all the information to be collected on a central device. Note that the measurement data are distributed across the network, it requires data transmission to a central node when using a centralized approach. This leads to a large amount of data transmission, and the potential of data leakage to the adversaries. Moreover, the centralized data collection process is costly due to the strategic data owners. In this case, it is necessary to employ the federated learning framework. In this section, we design a federated learning framework for distributed training of the measurement models. In the proposed framework, a wireless network is employed, in which the desired power system state owners (PSSOs) cooperatively perform parameter learning based on local data sets. The network can execute federated learning algorithm to estimate the parameters of the measurement matrix, which further enables FDI attack detection in power system state estimation. Note that the local training is decentralized and distributed in different devices, it avoids data transmission among multiple devices. A DSP is designed to publish the FDI attack detection task and coordinate the participation of PSSOs. The detailed description of the PSSOs and the DSP will be given in the following sections.

3.1. Power System States Owners

The key procedure is to construct the system measurement matrix H with multiple geographically distributed local PSSOs. The accuracy of the model prediction depends on the PSSOs participation and offering sufficient high quality data sets. To promote PSSOs' participation, it is necessary to explore their cost during the model prediction process.

Here we introduce Q_i to characterize the data quality of the samples provided by PSSO i.

$$Q_i = \begin{cases} 0, & \text{PSSO is cheating}, \\ (0, 1], & \text{otherwise}. \end{cases} \tag{7}$$

Specifically, the cost of PSSO i, denoted as $W_i(\vartheta_i, s_i, Q_i)$, can be characterized by equation (8) using the data size s_i, the data quality Q_i and the marginal data cost ϑ_i:

$$W_i(\vartheta_i, s_i, Q_i) = \vartheta_i s_i Q_i. \tag{8}$$

3.2. Detection Service Provider

In the proposed edge-based federated learning framework, a DSP is designed for task publishing and leading the PSSOs'

participation. Distinguished from the centralized model, the model updates are executed locally. Thus it is not required to deliver the local data to the DSP, which preserves the data's privacy. Furthermore, compared with the existing centralized federated learning framework, in the proposed edge-based federated learning framework, each PSSO updates based on local information and the information it receives from the neighbors. Thus, it is not necessary for the DSP to collect the model parameters or execute an aggregation operation with the proposed framework, which further reduces data transmission and preserves the information privacy. The essential function of DSP is to coordinate the PSSOs' participation with proper incentives, which will be explained in detail in the section 4.

4. Incentive Federated Learning for False Data Injection on Power Grid State Estimation

In this section, we focus on the incentive federated learning (IFL) for FDI attack detection on power grid state estimation. As we can see in equation (8), the revenues of PSSOs are negative without incentive payments from the DSP. This means additional time and efforts are required for PSSOs to participate in FDI attack detection. Note that the PSSOs are geographically distributed and are owned by different entities, they are probably strategic and will not participate in FDI attack detection with negative revenues. Nevertheless, as discussed in section 3, to obtain the model parameters which are necessary for FDI attack detection, the edge-based federated learning framework estimates the global model parameters through coordination learning of several PSSOs. The global parameter learning will fail without enough PSSOs' participation, so will the FDI attack detection. Thus, the feasibility of IFL for FDI attack detection needs further discussion. To ensure the feasibility of the proposed framework, the most efficient method is monetary reward from the DSP to the PSSOs. In this paper, this will be refined into contractual transaction mechanism, and the detailed design will be given in section 4.1. Moreover, to further explore the economy of the IFL framework, a bi-level model which depicts the PSSOs' participation in FDI attack detection is proposed. On one hand, the incentive decisions for PSSOs minimize the incentive cost while keeping a certain data quality, which impacts the FDI attack detection decision based on federated learning. On the other hand, the FDI attack detection decision based on the PSSOs' federated learning is achieved based on the incentive decisions for PSSOs, and conversely influences the incentive decisions. Thus, the whole IFL framework is formalized as a bi-level structure, in which the optimal incentive mechanism is designed in the upper layer and the economical and efficient FDI attack detection relying on edge-based federated learning framework is achieved in the lower layer. The detailed model description will be given in section 4.2 and section 4.3, respectively, which follows by the details of the incentive mechanism design in section 4.4.

4.1. Transaction Mechanism Design

To guarantee that there are enough PSSOs to participate in edge-based federated learning for FDI attack detection, here we model the participation as a service transaction process. During the whole learning process, the server trades the high quality model learning service with monetary rewards. Note that the PSSOs are different in data and time costs, several different transaction items are provided by the DSP to specify these differences. Specifically, the transaction items contain the maximum learning time, the data size and the data quality. To guarantee the effectiveness of the model learning process, monetary rewards are also specified as a transaction item. Let I be the total number of the transaction types, t_m denotes the maximum computational time, $s = \{s_i | i \in \{1, 2, ..., I\}$ denotes the data size set for a total number of I transaction types, $Q = \{Q_i | i \in \{1, 2, ..., I\}$ denotes the data quality set, and $r = \{r_i | i \in \{1, 2, ..., I\}$ be the monetary reward set. Thus, the transaction rules can be embodied as set $\varsigma = (t_m, s, Q, r)$, which provides a total number of I transaction types for the PSSOs to choose. The detailed procedures in transaction mechanism are listed as follows:

1) The DSP refines trading rules based on its preference: the DSP sets the maximum computational time t_m first, then it builds I transaction types based on the complexity of FDI attack detection, i.e., there exist I choices in each transaction items except for the maximum computational time.

2) Each PSSO chooses a transaction type: each PSSO chooses a transaction type strategically, making sure it benefits from participating in the FDI attack detection.

3) The PSSOs execute the FDI attack detection based on the transaction rules: if a PSSO chooses transaction type i and obeys the rules, i.e., it contributes a data set with scale no smaller than s_i and quality no worse than Q_i, and accomplishes the model learning task in t_m, then it receives reward r_i from the DSP accordingly. Otherwise, it will get a zero reward.

4.2. Upper-Layer Model

Let $C(t_m, s, Q, r, w)$ be the total cost of DSP. For the convenience of further analysis, here we assume that the number of rows and columns of the measurement matrix H are both D. Let $w = [w^1, w^2, ..., w^D]$, and denote the ith column of the measurement matrix as w^i. Then the measurement matrix prediction problem can be converted to estimation of w^i, $i = 1, 2, ..., D$. From an economical viewpoint, when executing the federated learning framework to achieve FDI attack detection, the total cost needs to be minimized while keeping a certain data quality. In other words, the total cost of the DSP should be minimized under the condition that a certain number of PSSOs are willing to participate in the federated learning process, which admits the following upper layer model.

$$\begin{aligned} &\min_{t_m, s, Q, r, w} C(t_m, s, Q, r, w) \\ &s.t. \quad w \in argmin_w f(w, x, y, r). \end{aligned} \tag{9}$$

where $C(t_m, s, Q, r, w)$ is the total cost of DSP. During the service transaction process, the DSP pays the PSSOs for FDI attack detection service. Thus the utility function of the DSP consists of two parts, the total rewards given to the PSSOs and the accuracy loss of the federated learning model. Here we consider the total rewards given to the PSSOs first. Note that the reward is designed for each iteration, the total rewards given to PSSO i should be the production of number of iterations, denoted as E, and the reward r_i for each iteration. From this viewpoint, the total cost $C(t_m, s, Q, r, w)$ can be formulated as follows:

$$C(t_m, s, Q, r, w) = \beta_1(f(w) - f(w^*)) + \beta_2 E \sum_{i=1}^{M} \mathbb{1}_{t_i \leqslant t_m} N_i r_i. \tag{10}$$

where

$$\mathbb{1} = \begin{cases} 1, & \text{if } t_i \leqslant t_m, \\ 0, & \text{otherwise}, \end{cases} \tag{11}$$

β_1 and β_2 are weight coefficients of the accuracy loss and the rewards, respectively.

The total cost of the DSP consists of two parts, the accuracy loss $(f(w) - f(w^*))$ and the rewards it pays to the PSSOs, $E\sum_{i=1}^{M} 1_{t_i \leqslant t_m} N_i r_i$. On one hand, it can achieve a balance between the rewarding cost and the accuracy loss by tuning the weight coefficient β_1 and β_2. On the other hand, given a certain incentive budget, the impact of the incentive mechanism on the detection accuracy can be explored and quantified based on equation (10). This leads to the problem of the optimal incentive mechanism design, which is characterized in equation (9). Note that it is a bi-level optimization problem, the detailed mechanism design will be given in section 4.4, following the analysis of the lower-layer model.

Specifically, note that the PSSOs are strategic, it is necessary to ensure the desired PSSOs receive non-negative revenues. In this way, the desired PSSOs will accept the transaction items and obey the transaction rules, i.e., to ensure the feasibility of IFL for FDI attacks, it is necessary that

$$W_r(t_i, s_i, Q_i, r_i) = r_i - \vartheta_i s_i Q_i \geqslant 0. \tag{12}$$

As we can see from equation (12), from the perspective of DSP, it is optimal to choose $r_i = \vartheta_i s_i Q_i$. Then we can obtain that to guarantee the feasibility of PSSO i's participation, the minimum choose of the reward is $r_i = \vartheta_i s_i Q_i$. Nevertheless, the PSSOs are different in the computation time t_m, the data quality Q_i and the data size s_i it can provide, which has great influence on the model learning process. The model learning process will work more efficiently and economically with a good choice of the PSSOs. This will be discussed in section 4.4.

4.3. Lower-Layer Model

In our model, each PSSO i collects a matrix $x_i = [x_{i1}, x_{i2}, ..., x_{iM_i}]$ of voltage angle data and a matrix $y_i = [y_{i1}, y_{i2}, ..., y_{iM_i}]$ of power data, with M_i being the number of measurements collected by each PSSO i. For local PSSO i, it learns the local state estimates $\hat{x_i}$ based on the measurement inputs x_i and y_i. Let $x = [x_1, x_2, ..., x_U]$, $y = [y_1, y_2, ..., y_U]$ with U being the number of participating PSSOs. To detect the FDI attack in smart grid, calculation of the estimates should be accomplished first. For static estimation, to obtain the estimates of system states, the following problem should be solved:

$$\min_{w_1, w_2, ..., w_U} f(w, x, y, r) \tag{13a}$$

$$s.t. \quad w_1(i,j) = w_2(i,j) = ... = w_U(i,j) = H_g(i,j), \quad \forall i = 1, 2, ..., D, j = 1, 2, ..., D, \tag{13b}$$

where H_g is the global measurement model, $f(w, x, y, r)$ is the loss function which is relative to the first-stage decision variable r. Specifically, let

$$f(w, x, y, r) = \frac{1}{M} \sum_{i \in \Gamma(r)} (y_i - w_i x_i)^T V^{-1} (y_i - w_i x_i) \tag{14}$$

where $M = \sum_{i=1}^{U} M_i$ is the total number of measurement data from all local devices, and

$$\Gamma(r) = \{i \in \{1, 2, ..., U\} | r \geqslant \vartheta_i s_i Q_i\}. \tag{15}$$

Note that the loss function $f(w, x, y, r)$ increases with the prediction error, by minimizing $f(w, x, y, r)$, we can obtain the optimal measurement model. Constraint (13b) is designed to guarantee that all the measurement data sets are coordinated for a global consensus measurement model, which captures the characteristic of federated learning algorithm that all the local users acquire the same global model. To explain the bi-level model intuitively, in Fig.2, the bi-level framework is given for the proposed IFL for FDI attack detection.

4.4. Incentive Mechanism Design

To realize IFL for FDI attack detection, the following procedures need to be undertaken at each training epoch:

1) DSP announces the task and provide preferential contracts: When the DSP receives a FDI attack detection task, it announces the task on cloud. Then based on PSSOs' type information, the DSP provides several preferential contracts to incentive PSSOs' participation in the FDI attack detection task.

2) Each PSSO analyzes the feasibility and choose rationally: At the beginning of the model learning process, each PSSO analyze the revenue and the cost in participating in the FDI attack detection. Note that the PSSOs are controlled directly by machines or people, here it is assumed that they are strategic, i.e., they will participate in the FDI attack detection only if the benefit of participation outweighs the cost.

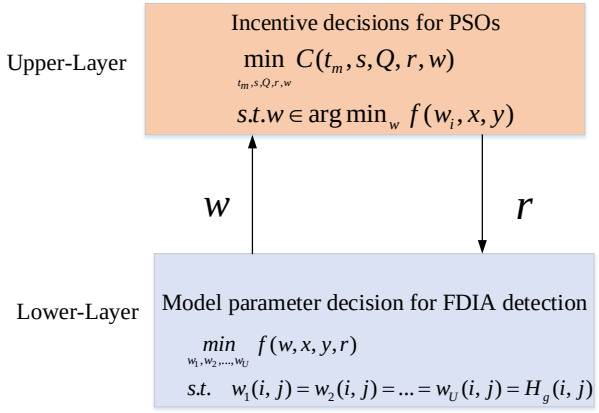


Figure 2: The bi-level framework for the proposed IFL for FDI attack detection.

3) Each PSSO executes the edge-based federated learning: Let w_i^j be the estimate of PSSO i for w^j, and z_i^j be the auxiliary variables. The strategy $w_i^j(0)$ is initialized without additional requirement, while the auxiliary variables z_i^j are all set to 0. Let a_{im} be the connectivity index of PSSO i and PSSO m, $a_{im} = 1$ if they are connected and communicate with each other, otherwise $a_{im} = 0$. Without loss of generality, here it is assumed that all the participating PSSOs constitute a connected graph. Then for $i \in \Gamma(r)$, $j = 1, 2, ..., D$, the local model parameters are updated iteratively as follows:

$$\begin{aligned} w_i^j(k+1) =& w_i^j(k) - \alpha(\nabla f_i(w_i^j) + z_i^j(k)) \\ & - \sum_{i\in\Gamma(r)} a_{im}(w_i^j(k) - w_m^j(k)) \end{aligned} \tag{16}$$

$$z_i^j(k+1) = z_i^j(k) + \sum_{i\in\Gamma(r)} a_{im}(w_i^j(k) - w_m^j(k)) \tag{17}$$

4) Learning ends: The model learning process ends if the learning parameters reach a predefined accuracy.

From the perspective of mathematical modeling, the proposed bi-level model in Fig.2 is a nested optimization problem, which means the upper-layer incentive decision cannot be obtained before the federated learning process. However, as we can see in section 4.1, in real applications, the incentive mechanism should be clarified at first. To solve this problem, the upper-layer incentive decision optimization problem is converted, and a preference index is introduced as a reference for a timely incentive mechanism design.

As we know, the preference for certain PSSOs can be realized by monetary reward, thus the choice on PSSOs is converted into the problem of optimal reward design. The social welfare of the DSP can be maximized through incentivizing the optimal PSSOs to the model learning process. From this viewpoint, firstly, it is necessary to quantify the DSP's preference for each PSSO. Here we start by considering its cost characterized in (10). During the service transaction process, the DSP pays the PSSOs for FDI attack detection service, thus the utility function of the DSP consists of two parts, the total reward given to the PSSOs and the accuracy loss of the federated learning model. Here we consider the total reward given to the PSSOs first. Note that the reward is designed for each iteration, the total reward given to PSSOs of type i should be the production of number of iterations, denoted as E, and the reward r_i for each iteration. Recalling that the upper limit of time for each iteration is t_m, we can obtain that for a certain time period T, the number of iterations is $E = \frac{T}{t_m}$. Thus the total reward given to the PSSOs can be characterized as $\frac{T}{t_m}\sum_{i=1}^{M} 1_{t_i\leqslant t_m} N_i r_i$, with N_i being the number of PSSOs of type i.

We consider the accuracy loss of the federated learning model next. The accuracy loss of algorithm (16)-(17) after E iterations, i.e., $f(w^E) - f(w^*)$, is upper bounded by $O(1/\sqrt{\sum_{i=1}^{M} 1_{t_i\leqslant t_m} N_i s_i E} + 1/E)$. To summarize, the total cost for the DSP can be characterized as

$$\begin{aligned} C(t_m,s,Q,r) =& \beta_1 min\{\frac{1}{\sqrt{\sum_{i=1}^{M} 1_{t_i\leqslant t_m} N_i s_i Q_i E}} + 1/E, \\ & F\} + \beta_2 E \sum_{i=1}^{M} 1_{t_i\leqslant t_m} N_i r_i \\ =& \beta_1 min\{\frac{1}{\sqrt{\sum_{i=1}^{M} 1_{t_i\leqslant t_m} N_i s_i Q_i \frac{T}{t_m}}} + \frac{t_m}{T}, \\ & F\} + \beta_2 \frac{T}{t_m} \sum_{i=1}^{M} 1_{t_i\leqslant t_m} N_i r_i. \end{aligned} \tag{18}$$

Through the conversion in (18), the total cost for the DSP, denoted as $C(t_m, s, Q, r)$, is irrelevant to the lower-layer model parameter w now. This means the upper-layer incentive mechanism characterized by (18) can be designed before the lower-layer federated learning process, which coincides with the real application scenarios. As we can see from (18), for a certain upper time limit t_m, the DSP's total cost increases with the individual reward r_i. Note that optimal value of r_i is proportional to the product $\vartheta_i s_i Q_i$, it costs more for the DSP to choose a PSSO with a large value of the product $\vartheta_i s_i Q_i$, which means a lower value of the preference index for this PSSO.

In the following, we consider the case where the PSSOs are with the same value of the product $\vartheta_i s_i Q_i$ and different upper time limits t_m. Given a certain value of the product $\vartheta_i s_i Q_i$, the DSP's cost function can be derived as follows:

$$\begin{aligned} C(t_m,s,Q,r) =& \beta_1 min\{\frac{1}{\sqrt{\sum_{i=1}^{M} 1_{t_i\leqslant t_m} N_i s_i Q_i \frac{T}{t_m}}} + \frac{t_m}{T}, \\ & F\} + \beta_2 \frac{T}{t_m} \sum_{i=1}^{M} 1_{t_i\leqslant t_m} N_i \vartheta s_i. \end{aligned} \tag{19}$$

Recalling that the data size s is positive, the cost function $C(t_m, s, Q, r)$ is convex, thus we can obtain that

$$s^* = \frac{1}{N\frac{T}{t_m}[\frac{2\beta_2\vartheta}{\beta_1}]^{\frac{2}{3}} Q_i^{\frac{1}{3}}}. \tag{20}$$

Given the optimal data size s^*, we can obtain the cost function of the DSP as follows:

$$C(t_m, s, Q, r) = \frac{\beta_1 t_m}{T} + (2^{\frac{1}{3}} + 2^{-\frac{2}{3}})\beta_1^{\frac{2}{3}}\beta_2^{\frac{1}{3}}\vartheta_i^{\frac{1}{3}}Q_i^{-\frac{1}{3}}. \quad (21)$$

Note that in (21), the cost function increases with t_m. Given the same value of the product $\vartheta_i s_i Q_i$, the DPS prefers PSSO with smaller upper time limit t_m.

From the perspective of the DSP, it is easy to construct a preference order given the same value of the cost $\vartheta_i s_i Q_i$ or the same quality of service level. However, in practice, it is common that there exist differences in both the marginal cost ϑ_i, the quality of data Q_i and the upper time limits t_m. To strike a balance between these conflicting objectives, some balancing index needs to be constructed. Here we consider the most complicated case, where the marginal cost satisfying $\vartheta_1/Q_1 < \vartheta_2/Q_2 < ... < \vartheta_M/Q_M$ and the upper time limit satisfying $t_1 > t_2 < ... > t_M$. Recalling the analysis in the case with the same value of the product $\vartheta_i s_i Q_i$, for the PSSOs of type-i, the optimal data size $s^* = \frac{1}{N_i \frac{T}{t_i}[\frac{2\beta_2\vartheta_i}{\beta_1}]^{\frac{2}{3}}Q_i^{\frac{1}{3}}}$, and the corresponding reward is $r^* = \frac{\vartheta_i}{N_i \frac{T}{t_i}[\frac{2\beta_2\vartheta_i}{\beta_1}]^{\frac{2}{3}}Q_i^{\frac{1}{3}}}$. Note that the DSP is strategic, it will choose the optimal PSSOs and set the rewards for other PSSOs as 0. Thus, by substituting the optimal data size s^* and the optimal reward r^* into the cost function, we can obtain the minimum cost for the DSP as follows:

$$C_{min} = \frac{\beta_1 t_i}{T} + (2^{\frac{1}{3}} + 2^{-\frac{2}{3}})\beta_1^{\frac{2}{3}}\beta_2^{\frac{1}{3}}\vartheta_i^{\frac{1}{3}}Q_i^{-\frac{1}{3}}, \quad (22)$$

which conflicts between the cost and the quality of service level. By choosing PSSOs with smaller C_{min}, the economy of the DSP and the quality of service on the FDI attack detection can be balanced, which consists of the preference index PRI_i.

Based on the formulation in (22), the following preference index PRI_i is introduced for PSSO i,

$$PRI_i \triangleq \frac{\beta_1 t_i}{T} + (2^{\frac{1}{3}} + 2^{-\frac{2}{3}})\beta_1^{\frac{2}{3}}\beta_2^{\frac{1}{3}}\vartheta_i^{\frac{1}{3}}Q_i^{-\frac{1}{3}}, \quad (23)$$

where t_i is the computational time of PSSO i, β_1 is quantified accuracy loss factor and β_2 is quantified payment factor. The preference index PRI_i characterizes the economy of PSSOs by quantifying their potential cost for DSP. Given PSSO i and j, $PRI_i \leqslant PRI_j$ means the marginal cost of choosing PSSO i is smaller than PSSO j, thus the DSP will have a high preference for PSSO i. For FDI attack detection based on federated learning framework, the difficulty lies in how to employ the PSSOs with different data quality and computational ability efficiently. The PSSOs with high data quality and good computational ability should be taken in priority. However, in the incentive mechanism design, considering the economy of the DSP, it is key to balance between the incentive cost and the computational accuracy. Thus here, the criterion in (23) is introduced, which aims to strike a balance between these two conflicting objectives. Based on this criterion, the PSSOs can be ranked according to their comprehensive performance in cost and serve. In this way, by selecting the PSSOs in order, the FDI attack detection task can be accomplished both efficiently and economically.

Recalling the procedures of transaction mechanism design, it remains to refine the transaction rules based on the criterion in (23), i.e., the transaction items which contain the maximum learning time t_m, the data size s and the reward r. This can be solved by exploring the establishment of criterion (23). Specifically, the preference index PRI_i is built based on the following considerations. First, note that the preference index PRI_i is built from the interest of the DSP, the utility function of the DSP should be built.

From the aforementioned analysis, we can obtain that the optimal mechanism design as follows: By using criterion (23), find the DSP's most preferred type, denoted as type i; build the most popular transaction type, in which the transaction rules are set as $t_m^* = t_i$, $s^* = \frac{1}{N\frac{T}{t_m}[\frac{2\beta_2\vartheta}{\beta_1}]^{\frac{2}{3}}Q_i^{\frac{1}{3}}}$, $r^* = \frac{\vartheta_i}{N_i \frac{T}{t_i}[\frac{2\beta_2\vartheta_i}{\beta_1}]^{\frac{2}{3}}Q_i^{\frac{1}{3}}}$, $Q = Q_i$. For other transaction types, set $r = 0$.

5. Simulation

In this section, the effectiveness of bi-level model depicting the PSSOs' participation in FDI attack detection is verified based on IEEE 30-bus system [29], where both the multiple-bus and single-bus FDI attacks are considered. By employing the proposed preference criterion, the impact of the incentive mechanism on the detection process is explored in terms of the model prediction accuracy and the FDI attack detection accuracy. The 30th node is chosen as the reference node. It should be noted that the voltage angle of the reference node is set to be fixed. Thus the state estimation of node 30 is not considered here, which makes the measurement matrix H to be 29×29. To verify the robustness of the proposed mechanism, multiple-bus FDI attacks and single-bus FDI attacks are considered for 100 Monte Carlo (MC) scenarios, and attack magnitudes are randomly distributed in the interval $[1, 10]$.

Define the threshold for the largest normalized residual (LNR) as τ. Without loss of generality, the measurement data from advanced metering infrastructure is only available for local PSSOs with the consideration of data privacy.

As for the system parameters, we choose $T = 30$, $\beta_1 = 17885$, $\beta_2 = 1$. The measurement data are distributed in 50 PSSOs, which can be divided into five types (each type with 10 PSSOs, and each PSSO possesses 10 groups of valid data), with the transaction parameters being $(\vartheta_A^{\frac{1}{3}}Q_A^{-\frac{1}{3}}, t_A) = (1, 3)$, $(\vartheta_B^{\frac{1}{3}}Q_B^{-\frac{1}{3}}, t_B) = (1.7, 2.5)$, $(\vartheta_C^{\frac{1}{3}}Q_C^{-\frac{1}{3}}, t_C) = (1.8, 2.4)$, $(\vartheta_D^{\frac{1}{3}}Q_D^{-\frac{1}{3}}, t_D) = (1.9, 2.7)$, $(\vartheta_E^{\frac{1}{3}}Q_E^{-\frac{1}{3}}, t_E) = (2, 2)$. $Q_B = Q_C = Q_C = Q_E = 0.5$, $Q_A = 1$, $\vartheta_A = 1$, $\vartheta_B = 0.597$, $\vartheta_C = 0.608$, $\vartheta_D = 0.619$, $\vartheta_E = 0.630$. For the convenience of the preference comparison, based on the proposed crite-

rion (23), the heatmap of DSP's preference is given in Fig.3, where the five types are marked with $*$. The red line divides the whole area into two parts with $PRI = 3167$, where the part close to the origin refers to $PRI < 3167$ and the remaining refers to $PRI > 3167$. It is clear in Fig.3 that the PSSOs can be ranked as $A > B > C > E > D$ according to the DSPs preference. While when using the price-based incentive mechanism in [27], the preference order is $B > C > D > E > A$. In the simulations, the effectiveness

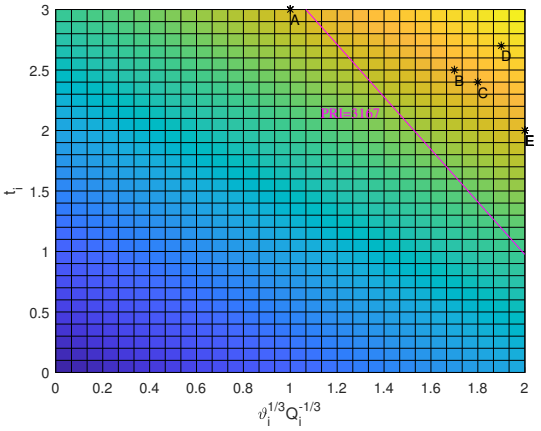


Figure 3: The heatmap of DPS's preference.

of the proposed mechanism is verified by setting the total incentive as 100, where 100 Monte Carlo attack scenarios are considered. For the convenience of comparisons, the local data based mechanism in [26] and the price-based incentive mechanism in [27] are also carried out with the same total incentive cost. For the proposed edge-based framework, by using proposed criterion (23), PSSOs of type A are chosen. Furthermore, based on the theoretical results in section 4.4, the optimal data size is $s^* = \frac{1}{N_A \frac{T}{t_A}[\frac{2\beta_2\vartheta_A}{\beta_1}]^{\frac{2}{3}} Q_A^{\frac{1}{3}}} = 10$, and the optimal reward is $r^* = \frac{\vartheta_i}{N_i \frac{T}{t_i}[\frac{2\beta_2\vartheta_i}{\beta_1}]^{\frac{2}{3}} Q_i^{\frac{1}{3}}} = 10$. Thus, given the incentive cost of 100, the DSP can afford to employ 10 PSSOs of type A, which are willing to participate in the federated learning process with data size $s^* = 10$. While for the price-based incentive mechanism in [27], limited by the incentive cost, the number of participating PSSOs are only 2, which leads to insufficient data source for model prediction. For the convenience of comparison, the model prediction accuracy is defined first.

5.1. Model Prediction Accuracy

For the FDI attack detection without knowledge of measurement matrix H, the accuracy of model prediction is a key step. To compare the performance of the proposed mechanism in model prediction with other methods, the mean absolute error ε is introduced, which acts as the prediction accuracy metric:

$$\varepsilon = \frac{\|H^p - H\|^2}{m^2}, \tag{24}$$

where H^p is the prediction of measurement matrix, H is the real one, m is the dimension of H.

To demonstrate the accuracy of model prediction, the heatmap of measurement matrix (Fig.5(a)) based on the proposed mechanism is given and compared with the real one (Fig.4), from which we can see the proposed mechanism has a good performance. The prediction results with the local data based mechanism in [26] and that using price-based incentive mechanism in [27] are described in Fig.5(b) and Fig.5(c),respectively, showing unacceptable prediction errors. To characterize the model prediction error in detail, the mean absolute errors ε of these three mechanisms with different measurement noise levels are given in Table I. It can be seen from Table I that the proposed framework with optimal mechanism design can achieve high precision prediction of the model, while that with the local data based mechanism in [26] and that using price-based incentive mechanism in [27] cannot.

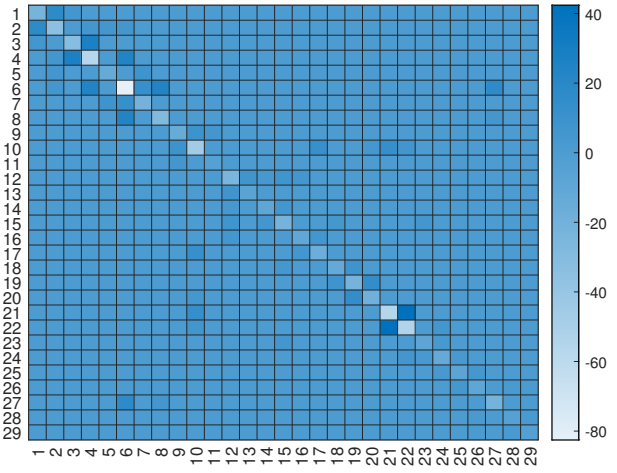


Figure 4: The heatmap of the actual Jacobian matrix.

5.2. Advantage of the incentive mechanism

In this section, the effectiveness of the proposed incentive edge-based federated learning framework is explored on detection of multiple-bus and single-bus FDI attacks. As shown in Fig.5, the proposed edge-based framework with optimal mechanism design can achieve an exact model prediction of the measurement matrix H, while the prediction results with the local data based mechanism in [26] and that using price-based incentive mechanism in [27] are far from the real value. The model prediction results directly impact the accuracy of the FDI attack detection result. From Fig.6, we can see that although the specific LNR values with the proposed mechanism vary with different non-attack scenarios, they remain in the interval $[0.02, 0.25]$. While for the attack scenarios, the LNR values show much bigger values in the interval $[2.5, 35]$. Thus FDI attacks can be detected effectively with the proposed mechanism by choosing $\tau = 2$. However, in Fig.7, the LNR values with or without multiple-bus attacks are both in the interval $[20, 75]$, which are too close to distinguish. The FDI attacks cannot be accurately

Table I: Model prediction accuracy comparison.

Mechanism	Federated learning with optimal contract			Local prediction			Federated learning with random constract		
Noise	0	5%	10%	0	5%	10%	0	5%	10%
ε	0.788	0.9251	1.0092	107.9003	108	108.0685	33.9764	35.0697	21.1091

detected no matter how the LNR threshold value τ is chosen. Moreover, similar test results are shown in Fig.8, where the price-based incentive mechanism in [27] is employed. This further demonstrates that the proposed incentive edge-based federated learning framework can detect FDI attacks efficiently, while the local data based mechanism in [26] and that using price-based incentive mechanism in [27] cannot.

As we know, the multiple-bus FDI attacks act on several buses, which leads to bigger LNR values and thus is relatively easier to detect. To verify the robustness of the proposed edge-based framework, in the following, single-bus FDI attack is launched over an IEEE 30-bus system. The parameters are chosen to be the same as those in section 5.2. As shown in Fig.9-11, the model prediction results also directly impact the accuracy of the single-bus FDI attack detection.

From Fig.9, we can see that the LNR values with the proposed mechanism under no attacks remain small in the interval $[0, 0.205]$, while the values with single-bus FDI attacks show much bigger values. Thus, the single-bus FDI attack can be detected effectively based on the proposed mechanism by choosing $\tau = 0.5$. However, as shown Fig.10, due to the incorrect model prediction results, the LNR values with the local data based mechanism in [26] under no attacks and single-bus FDI attacks are too close to distinguish in the interval $[15, 65]$. Moreover, the LNR values with the price-based incentive mechanism in [27] show similar test results in Fig.11, which means both of them fail to detect the FDI attacks.

5.3. Advantage of the federated framework

In this section, to further discuss the performance of the proposed federated learning mechanism, the local data based mechanism in [26] without limiting the budget has also been carried out for comparison. It executes the FDI attack detection in a single device, which is centralized. With adequate monetary rewards, here it is assumed that the PSSOs are willing to deliver their local state data to a central node. Thus the local data based mechanism in [26] without limiting the budget empowers a centralized FDI attack detection with sufficient data. However, the data transmission process also discloses the key state data to the adversaries, through which they can obtain the information of the measurement matrix indirectly. This provides the necessary information of stealthy attacks, which can be avoided in the proposed federated formulation. Thus here, we consider the case where the local data based mechanism in [26] without limiting the budget is used to detect the stealthy attacks based on 100 Monte Carlo scenarios. As we can see in Fig.12, the LNR results with and without stealthy attacks show close values in the interval $[0, 0.3]$, which means the local data based mechanism in [26] without limiting the budget fails in FDI detection. While for the proposed federated mechanism, no state data is required to be delivered, which prevents the adversaries from obtaining the information of the measurement matrix. Thus, the proposed federated mechanism prevents the stealthy attacks originally, which outperforms the centralized mechanism.

6. Conclusion

This paper proposed a novel edge-based federated learning framework for FDI attack detection on power grid state estimation, which shows great potential in real-world applications with unknown system parameters. The major findings are summarized as follows:

1) To seek a high detection accuracy with limited measurement data sets, an incentive mechanism is designed to encourage the desired data owners to contribute to FDI attack detection. By careful design of the transaction items in the incentive mechanism, the participation of the desired PSSOs can be achieved.

2) A novel preference criterion has been proposed to achieve the optimal detection accuracy under a given incentive budget.

3) A bi-level model depicting the PSSOs' participation in FDI attack detection has been proposed, in which both the detection accuracy and the monetary cost are considered. This characterizes the impact of the incentive mechanism on the detection accuracy.

4) The incentive mechanism has been tested for 100 Monte Carlo scenarios on different FDI attacks, including detection of multiple-bus and single-bus FDI attacks. The simulation results demonstrate that the proposed framework outperforms the existing works (e.g. local data base mechanism, price-based mechanism) without mechanism design.

References

[1] Yu X, Xue Y. Smart grids: A cyber–physical systems perspective. Proceedings of the IEEE 2016;104(5):1058–70.

[2] Li C, Liu C, Yu X, Deng K, Huang T, Liu L. Integrating demand response and renewable energy in wholesale market. In: IJCAI. 2018, p. 382–8.

[3] Mishra DK, Ray PK, Li L, Zhang J, Hossain M, Mohanty A. Resilient control based frequency regulation scheme of isolated microgrids considering cyber attack and parameter uncertainties. Applied Energy 2022;306:118054.

[4] Fu Y, O'Neill Z, Yang Z, Adetola V, Wen J, Ren L, et al. Modeling and evaluation of cyber-attacks on grid-interactive efficient buildings. Applied Energy 2021;303:117639.

[5] Chen C, Cui M, Fang X, Ren B, Chen Y. Load altering attack-tolerant defense strategy for load frequency control system. Applied Energy 2020;280:116015.

[6] Swearingen M, Brunasso S, Weiss J, Huber D. What you need to know (and don't) about the aurora vulnerability. Power 2013;157(9):52–.

[7] Choeum D, Choi DH. Trilevel smart meter hardening strategy for mitigating cyber attacks against volt/var optimization in smart power distribution systems. Applied Energy 2021;304:117710.

[8] Ibrahim MS, Dong W, Yang Q. Machine learning driven smart electric power systems: Current trends and new perspectives. Applied Energy 2020;272:115237.

[9] Musleh AS, Chen G, Dong ZY. A survey on the detection algorithms for false data injection attacks in smart grids. IEEE Transactions on Smart Grid 2019;11(3):2218–34.

[10] Liang G, Weller SR, Zhao J, Luo F, Dong ZY. The 2015 ukraine blackout: Implications for false data injection attacks. IEEE Transactions on Power Systems 2016;32(4):3317–8.

[11] Lin WT, Wang YW, Li C, Yu X. Predefined-time optimization for distributed resource allocation. Journal of the Franklin Institute 2020;357(16):11323–48.

[12] Duan J, Zeng W, Chow MY. Resilient distributed dc optimal power flow against data integrity attack. IEEE Transactions on Smart Grid 2018;9(4):3543–52.

[13] Chung HM, Li WT, Yuen C, Chung WH, Wen CK. Local cyber-physical attack with leveraging detection in smart grid. In: 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm). 2017, p. 461–6. doi:10.1109/SmartGridComm.2017.8340712.

[14] Jiang Q, Chen H, Xie L, Wang K. Real-time detection of false data injection attack using residual prewhitening in smart grid network. In: 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm). 2017, p. 83–8. doi:10.1109/SmartGridComm.2017.8340659.

[15] Sreenath JG, Meghwani A, Chakrabarti S, Rajawat K, Srivastava SC. A recursive state estimation approach to mitigate false data injection attacks in power systems. In: 2017 IEEE Power Energy Society General Meeting. 2017, p. 1–5. doi:10.1109/PESGM.2017.8274070.

[16] Liu T, Sun Y, Liu Y, Gui Y, Zhao Y, Wang D, et al. Abnormal traffic-indexed state estimation: A cyber–physical fusion approach for smart grid attack detection. Future Generation Computer Systems 2015;49:94–103.

[17] Zhao J, Gómez-Expósito A, Netto M, Mili L, Abur A, Terzija V, et al. Power system dynamic state estimation: Motivations, definitions, methodologies, and future work. IEEE Transactions on Power Systems 2019;34(4):3188–98.

[18] Zhao J, Zhang G, Dong ZY, La Scala M. Robust forecasting aided power system state estimation considering state correlations. IEEE Transactions on Smart Grid 2016;9(4):2658–66.

[19] Zhao J, Zhang G, Dong ZY, Wong KP. Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation. IEEE Transactions on Smart Grid 2015;7(1):6–8.

[20] Kurt MN, Yılmaz Y, Wang X. Real-time detection of hybrid and stealthy cyber-attacks in smart grid. IEEE Transactions on Information Forensics and Security 2019;14(2):498–513.

[21] Tian J, Tan R, Guan X, Liu T. Enhanced hidden moving target defense in smart grids. IEEE Transactions on Smart Grid 2019;10(2):2208–23.

[22] Liu C, Wu J, Long C, Kundur D. Reactance perturbation for detecting and identifying fdi attacks in power system state estimation. IEEE Journal of Selected Topics in Signal Processing 2018;12(4):763–76.

[23] Jindal A, Dua A, Kaur K, Singh M, Kumar N, Mishra S. Decision tree and svm-based data analytics for theft detection in smart grid. IEEE Transactions on Industrial Informatics 2016;12(3):1005–16.

[24] Yin X, Zhu Y, Hu J. A subgrid-oriented privacy-preserving microservice framework based on deep neural network for false data injection attack detection in smart grids. IEEE Transactions on Industrial Informatics 2022;18(3):1957–67.

[25] Zhang G, Li J, Bamisile O, Cai D, Hu W, Huang Q. Spatio-temporal correlation-based false data injection attack detection using deep convolutional neural network. IEEE Transactions on Smart Grid 2022;13(1):750–61.

[26] Li B, Xiao G, Lu R, Deng R, Bao H. On feasibility and limitations of detecting false data injection attacks on power grid state estimation using d-facts devices. IEEE Transactions on Industrial Informatics 2020;16(2):854–64.

[27] Niu J, Tian Z, Zhu J, Yue L. Implementation of a price-driven demand response in a distributed energy system with multi-energy flexibility measures. Energy Conversion and Management 2020;208:112575.

[28] Hug G, Giampapa JA. Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks. IEEE Transactions on Smart Grid 2012;3(3):1362–70.

[29] Choudekar P, Sinha S, Siddiqui A. Congestion management of ieee 30 bus system using thyristor controlled series compensator. In: 2018 International Conference on Power Energy, Environment and Intelligent Control (PEEIC). 2018, p. 649–53. doi:10.1109/PEEIC.2018.8665413.

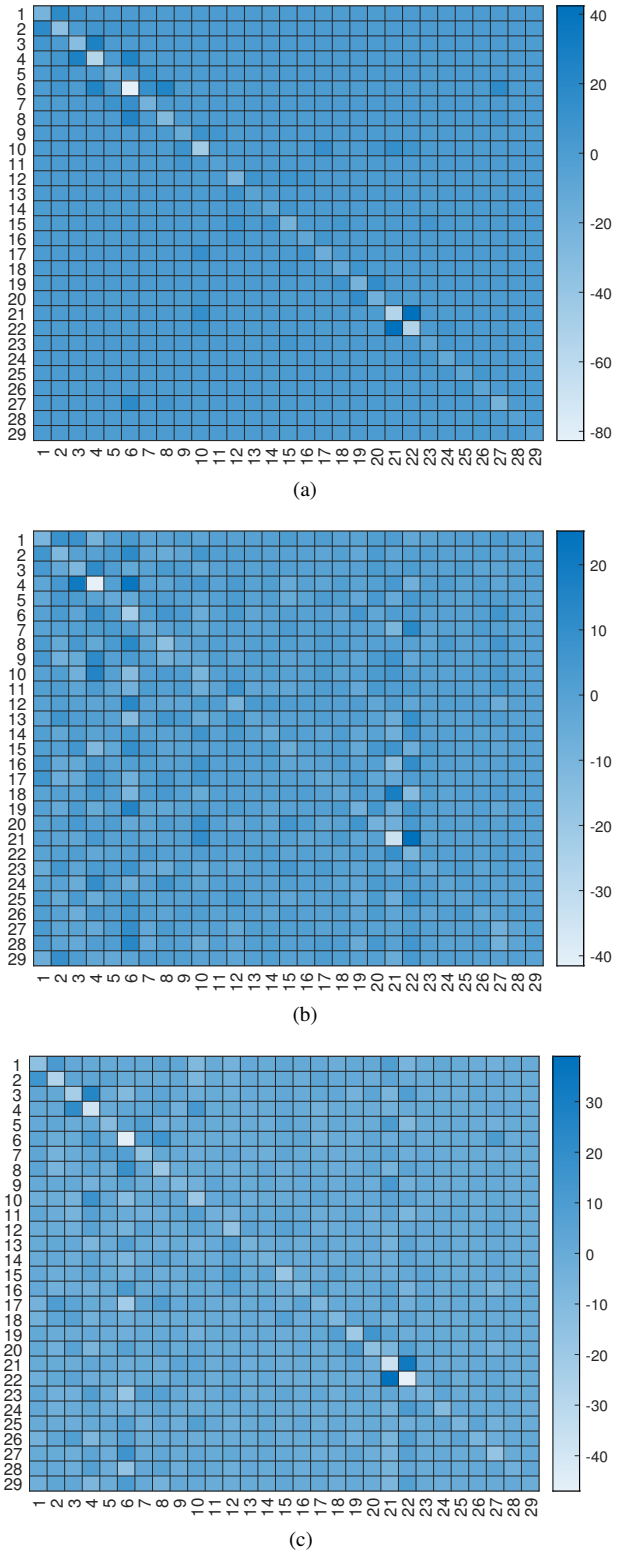


Figure 5: The heatmaps of the predicted Jacobian matrix using the proposed federated learning framework (a), using the local data based mechanism in [26] (b), using price-based incentive mechanism in [27] (c).]

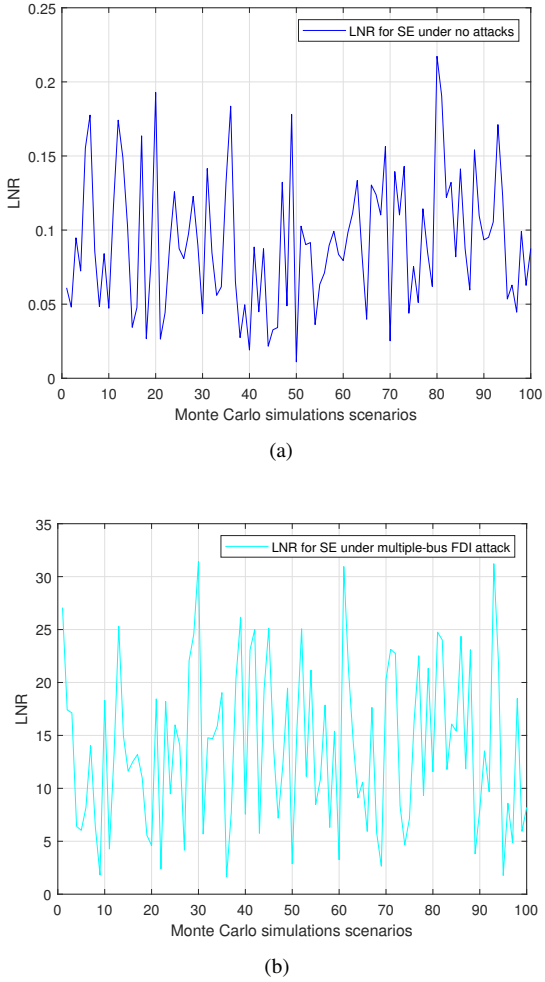
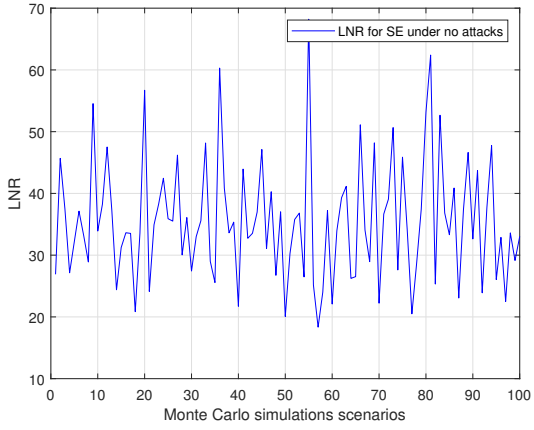
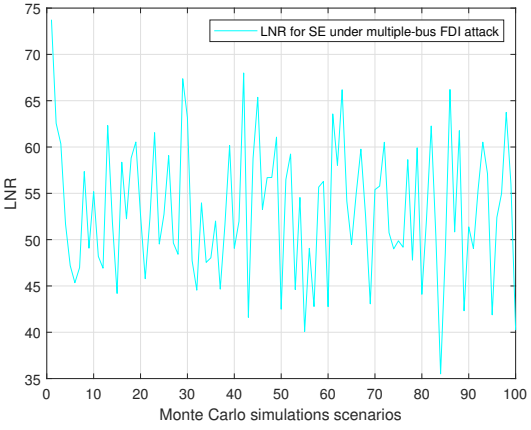


Figure 6: The LNR results for 100 Monte Carlo simulations with the proposed mechanism under no attacks (a), under multiple-bus FDI attacks (b).

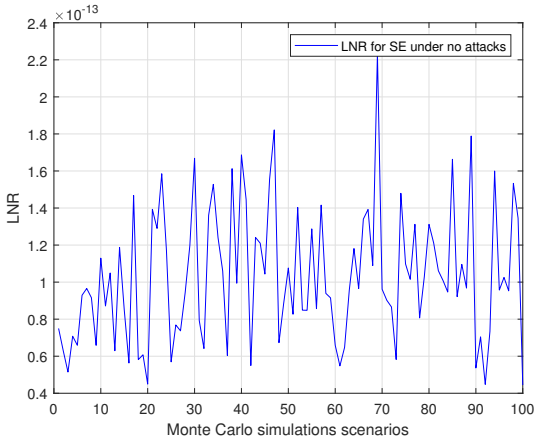


(a)

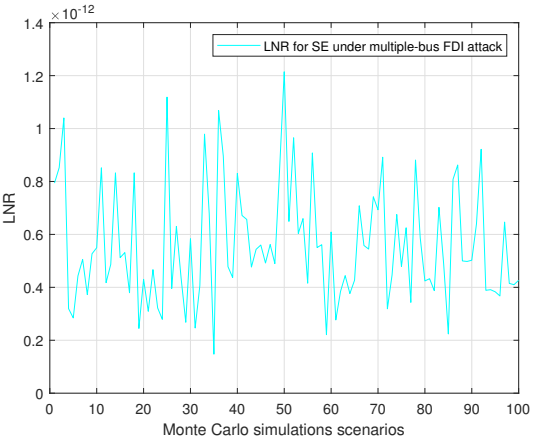


(b)

Figure 7: The LNR results for 100 Monte Carlo simulations with the local data based mechanism in [26] within limited budget, under no attacks (a), under multiple-bus FDI attacks (b).

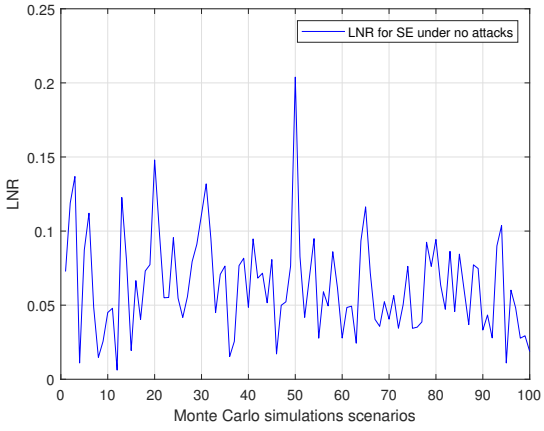


(a)

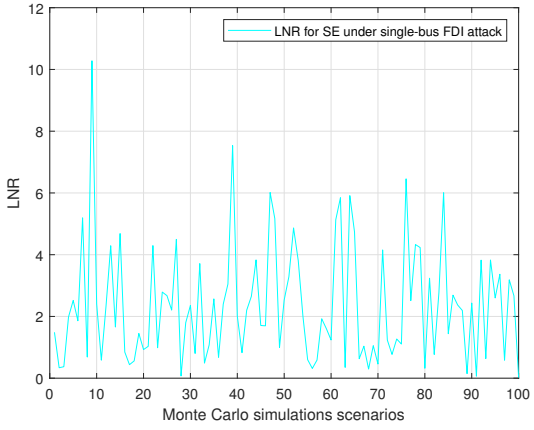


(b)

Figure 8: The LNR results for 100 Monte Carlo simulations with the price-based incentive mechanism in [27], under no attacks (a), under multiple-bus FDI attacks (b).

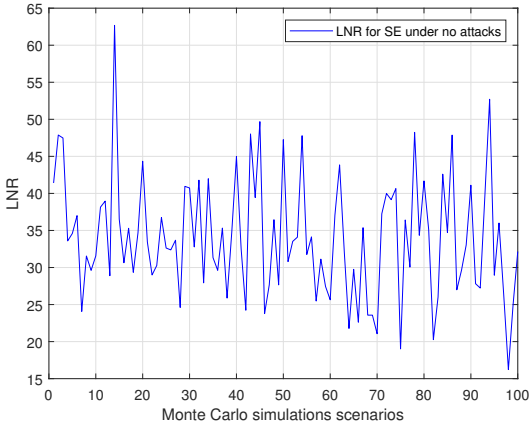


(a)

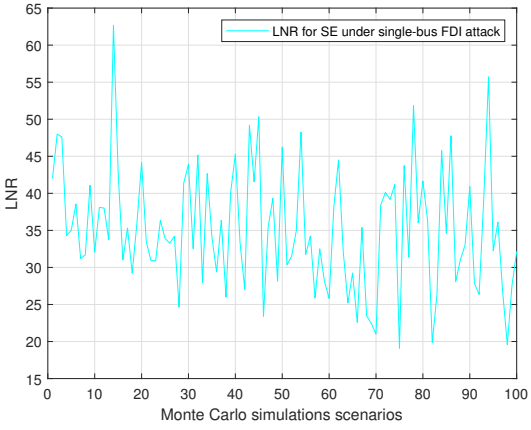


(b)

Figure 9: The LNR results for 100 Monte Carlo simulations with the proposed mechanism, under no attacks (a), under single-bus FDI attacks (b).

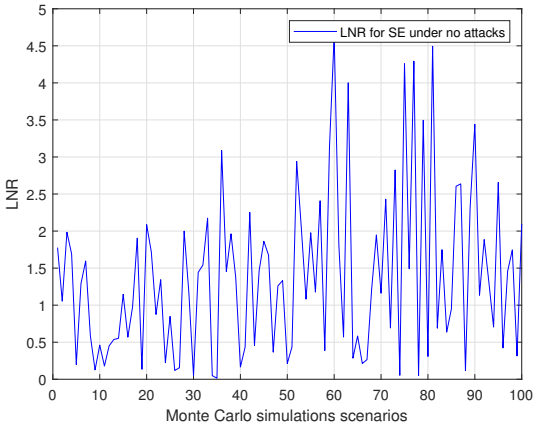


(a)

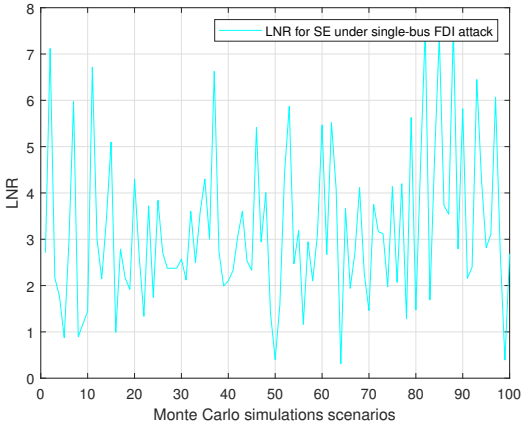


(b)

Figure 10: The LNR results for 100 Monte Carlo simulations with the local data based mechanism in [26] within limited budget, under no attacks (a), under single-bus FDI attacks (b).

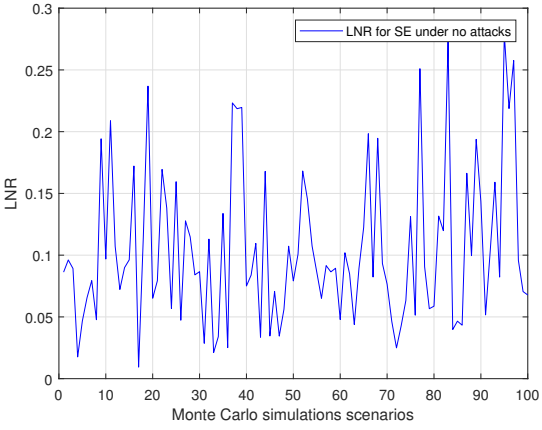


(a)

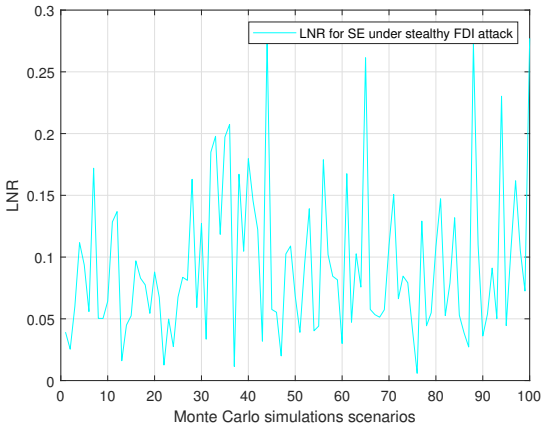


(b)

Figure 11: The LNR results for 100 Monte Carlo simulations with the price-based incentive mechanism in [27], under no attacks (a), under single-bus FDI attacks (b).



(a)



(b)

Figure 12: The LNR results for 100 Monte Carlo simulations with the local data based mechanism in [26] without limiting the budget, under no attacks (a), under stealthy FDI attacks (b).

Wen-Ting Lin: Modeling, Data acquisition, Simulation, Original draft preparation

Guo Chen: Reviewing and Editing

Yuhan Huang: Conceptualization, Methodology