Electric Power Systems Research 229 (2024) 110150

Contents lists available at ScienceDirect

Electric Power Systems Research

journal homepage: www.elsevier.com/locate/epsr

Privacy-preserving federated learning for detecting false data injection attacks on power system ☆

Wen-Ting Lin [a,b], Guo Chen [a,*], Xiaojun Zhou [a]

[a] School of Automation, Central South University, Changsha, 410083, China
[b] School of Computer and Information Science, Chongqing Normal University, Chongqing 401331, China

ARTICLE INFO

Keywords:
Energy management
Cyber attacks
False data injection
Federated learning
State estimation

ABSTRACT

False data injection attacks (FDIA) against power system state estimation have been well studied due to its potential threat to real-time energy management. However, the existing works either focus on the case with a sufficiently large local data sets or the local data can be transmitted to a central node, or the case where the system parameters can be easily acquired through communication. This contradicts with real-world applications where the measurement data is geographically distributed and the system parameters are unknown, and also leads to data leakage issues. To solve the problem, a novel FDIA detection algorithm is proposed based on federated learning, through which a global detection model is generated. In the proposed algorithm, the state owners execute a federated learning algorithm using their own data, which avoids massive data transmission and protects the data privacy. Moreover, to prevent the model parameter from exposure to attackers, artificial noise is added into the model estimations to guarantee differential-privacy. Theoretical results show a trade-off in algorithm accuracy and its privacy preserving level. Simulations on the IEEE 30-bus system validate the effectiveness of the proposed mechanism on FDIA detection and its trade-off in accuracy and privacy preserving.

1. Introduction

Driven by the IEEE Grid Vision 2050 [1], the power grid is facing the transition from traditional power grid to an intelligent and automatic version [2–4], which can be realized by introducing large quantities of smart devices [5], and integrating them through information and communication technologies (ICT). However, with the prevalence of the ICT in smart grid, recent years have witnessed a sharp increase in the vulnerability of the power system caused by cyber attacks [6,7].

From the perspective of information network, the smart grid can be seen as a cyber–physical system (CPS) [8], which is vulnerable to cyber attacks. Specifically, optimal functioning of power systems necessitates meeting key requirements, particularly reliability and security, which are closely linked to cyber-attacks. Cyber attacks pose a significant threat to power system reliability, potentially causing widespread outages and disruptions that impede optimal functioning. Additionally, these attacks encompass unauthorized access, data manipulation, denial-of-service attacks, and malware infections, compromising the system's security and hindering its optimal function. Consequently, cyber attacks pose a serious menace to the optimal functioning of power systems.

As one of the most challenging cyber attacks, the false data injection (FDI) attack can act on all the layers of CPS and lead to significant threats against real-time energy management, thus have drawn extensive research attention recently. FDI attackers conduct the attacks by imitating the real-time measurement signals and injecting falsified data into them, with an expectation to destroy the energy management system by disrupting the stability of the power grid [9,10] or the order of the electricity market [11,12].

To mitigate these effects, a large number of FDI attack detection algorithms have been developed. In [13], a comprehensive overview of AI-based techniques for detecting and mitigating cyber-attacks in microgrids is provided. While the algorithm frameworks differ massively, they can be categorized as either data-driven algorithms [14] or

☆ This work is supported by the National Natural Science Foundation of China under Grant 62073344 and 72301048, the Natural Science Foundation of Chongqing, China (Grant No. CSTB2023NSCQ-MSX0316), the Science and Technology Research Program of Chongqing Education Commission, China (Grant No. KJQN202300510), the Chongqing Social Science Planning Project, China (Grant No. 2023NDQN28), and the Chongqing Normal University Doctoral Start-up Program, China (Grant No. 22XWB027).

* Corresponding author.
E-mail addresses: linwentinghust2017@gmail.com (W.-T. Lin), guo.chen@csu.edu.cn (G. Chen), michael.x.zhou@csu.edu.cn (X. Zhou).

https://doi.org/10.1016/j.epsr.2024.110150
Received 22 October 2023; Received in revised form 25 December 2023; Accepted 10 January 2024
Available online 22 January 2024

model-based algorithms [15]. For the first category, in [16], a machine-learning-based method is proposed by training a distributed support vector machine (SVM), which aims at detecting stealthy FDI attacks from the perspective of power system stability. Considering from the economic impacts of FDI attacks, in [17], SVM is used to develop a detection mechanism for real-time detecting and locating the electricity theft. In [18], an anomaly identification technique based on Multi-class Support Vector Machines (SVMs) is presented, demonstrating superior efficiency compared to conventional methods. To achieve a certain detection accuracy, the SVM-based methods admit an extensive computation time, which restricts its wide spread. Note that the back-propagation procedure in the artificial neural networks can improve the accuracy greatly, recent years they have been widely used in FDI detection in smart grid [19,20]. In [21], a neural network is used to develop a FDI attack detection mechanism for power system state estimation, and it admits 99% detection accuracy of replay attacks. To model the dynamics of power system, in [22], a recurrent neural network is employed, and an artificial intelligence-based method is proposed for FDI attack detection in direct current (DC) microgrids. Note that the network with more hidden layers shows greater potential in accuracy improvement, deep neural networks have been utilized in FDI attack detection [23,24]. Though the back-propagation technic shows a good performance in accuracy improvement, it leads to an extensive time consumption of the training process. To solve this problem, in [25], an enhanced approach utilizing the extreme learning machine (ELM) method is proposed for the detection of false data injection (FDI) attacks in smart grid systems. This innovative method combines the principles of the artificial bee colony algorithm with the differential evolution theory.

Although the data-driven methods are model-free, a large amount of data is required for the training process, which also leads to the requirement for large local data sets or all local data to be transmitted to a central node [26]. However, for FDI attack detection in smart grid, it is difficult to acquire a sufficiently large data set. Furthermore, the extensive data transmission incurs significant time and cost implications, while also raising concerns regarding data confidentiality in the process. This made the data-driven methods inapplicable in real-world applications where a sufficiently large data set is unavailable. Under this circumstance, various model-based FDI attack detection algorithms are proposed. Traditionally, the model-based detection methods contain two major procedures, which are state estimation based on system parameter and residual test [27,28]. While these methods operate adequately for basic FDI attacks, they fail in detection of a malicious case, i.e., the stealthy FDI attacks [29]. As we can see in Fig. 1, the state estimation is initially conducted, and subsequently, the results are utilized for the residual test. For the stealthy FDI attacks, the attackers can bypass measurement residual tests and evade being detected, which deceives the residual tests and further manipulates the security assessment results. The stealthy attack can be easily launched, since the measurement matrix is usually fixed and can be acquired easily by the adversaries. To solve this problem, the proactive false data detection (PFDD) mechanism is proposed by using the distributed flexible ac transmission system (D-FACTS). Given the D-FACTS devices are activated, the negative branch susceptance values are dynamically changing and cannot be harvested by the attacker. In this way, the attackers cannot execute effective stealthy attacks. Therefore, the FDI attacks can be revealed [30,31]. In [32], an optimal D-FACTS placement algorithm is proposed, which ensures the maximum effectiveness of the defense strategy to detect FDI attacks against the power system state estimation. In [33], the feasibility and limitations of the PFDD mechanism is explored, and the minimum efforts required for effective FDI attack detection are evaluated. In PFDD approaches, the measurement matrix can be dynamically changing with the activating of D-FACTS device. Although these proactive approaches are effective in FDI detection, they all based on the fact that the changed measurement matrix information is known only by the detection entity while it

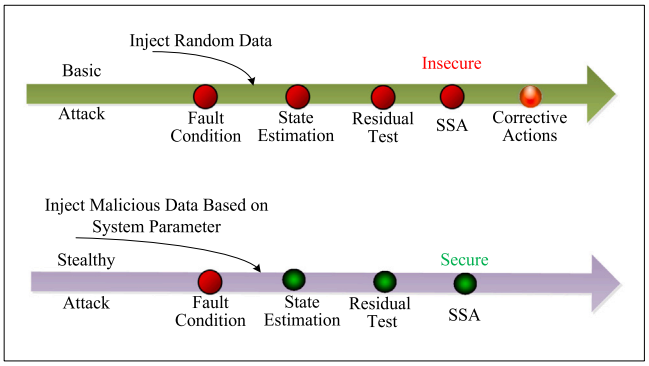


Fig. 1. The impacts of stealthy attacks on power system state estimation and security assessment.

remains totally unknown to the adversaries. However, in practice, owing to the decentralized nature of the D-FACTS device (e.g., switched filter compensator for AC systems and green plug filter compensator for DC systems), the detection entity encounters challenges in acquiring complete information about the altered measurement matrix. Consequently, this limitation results in inaccuracies in state estimation. Moreover, the acquisition of the matrix is hard based on limited data. Without effective privacy-preserving strategies, the acquisition process may lead to matrix information leakage to adversaries, which further leads failures in detecting FDI attacks.

As we can see from the above discussion, although FDI attack detection has been extensively studied, it remains the following major gaps:

- The state data sets are individually owned by respective state owners, while the existing detection methods either require a sufficiently large local data set or full information of the measurement matrix, leading to a heavy data transmission burden.
- The existing attack detection schemes are not privacy-preserving. On one hand, for the existing data-driven algorithms, the requirement for a central data collection process leads to data privacy issues. On the other hand, the existing model-based methods publish the system parameters to all entities, which risks divulging the system parameters to attackers.
- The centralized data collection and computation process is both insecure and expensive, since the state data is massive and contains private information. A distributed attack detection mechanism needs to be designed enabling effective attack detection by coordinating the local devices with respective data sets.

To solve these technical bottlenecks, in this paper, a federated learning framework is proposed for distributed learning of the model parameters, and the learning results work directly for a PFDD process. The local training is decentralized and distributed in different devices, which achieves model parameter learning with geographically distributed data sets. Moreover, to further prevent the model parameters from exposure to attackers, artificial noise is added to the model estimations before information transmission, which leads to accuracy in detecting FDI attacks. The main contributions of this paper are listed as follows:

- A novel distributed mechanism rooted in the federated learning paradigm is introduced for FDI attack detection. The proposed mechanism embraces a decentralized and distributed training process across various devices, Effectively circumventing the need for transmitting a large amount of sensitive data among multiple devices.
- The proposed mechanism ensures privacy preservation by incorporating artificial noise into the model estimations prior to information transmission. This design effectively thwarts adversaries

from illicitly acquiring the model parameters, thereby thwarting their ability to mount stealthy attacks. Consequently, this approach enhances the accuracy of FDI attack detection.

- The trade-off between the accuracy loss and privacy-preserving level is explored over the IEEE 30-bus system. The experimental analysis substantiates the theoretical convergence and privacy analysis findings.

The remaining sections of the paper are structured as follow. Section 2 describes the system model and problem formulation in power systems. Building on this, Section 3 presents a federated learning-based detection framework. Then in Section 4, a privacy-preserving detection algorithm corresponding to the framework in Section 3 is proposed. Finally, Section 5 validates the framework and algorithm through a case study.

2. System model and problem formulation

This section presents the fundamental principles of power system state estimation, followed by an exposition of the underlying attack mechanism and an elucidation of the detection approach.

2.1. Power system state estimation

Given the widespread adoption of smart meters, which furnish real-time dynamic measurement data for power system monitoring purposes, state estimation has been widely used in the power system control since some key states cannot be measured directly. In classical state estimation of power system [24], the power flow model between the measurements and the estimated states can be characterized as follows:

$$z = h(x) + \varepsilon. \tag{1}$$

In this context, the measurement vector is denoted as $o \in R^n$, while the system state vector is represented as $x \in R^m$. The system-defined nonlinear relationship between the measurements and the estimated states is captured by $h(x)$. Additionally, the random measurement error $\varepsilon \in R^n$ follows a Gaussian distribution with a mean of zero and a covariance matrix as specified below:

$$V = diag(\tau_1^2, \tau_2^2, \dots, \tau_n^2), \tag{2}$$

Here τ_i represents the standard deviation of the ith measurement.

The state estimation aims to acquire the accurate value of the estimated states based on the value of the measurement variable. Note that DC state estimation model is linear and widely used in power system state estimation, here we consider the DC power flow model instead. As disclosed in [34], for the sake of analysis convenience, the AC state estimation model can be linearized by utilizing the Jacobian matrices computed at the present state. This linearization technique enables a more tractable representation of the system dynamics. By replacing $h(x)$ with a linear formulation, we can obtain the DC power flow model as follows [33]:

$$z = Hx + \varepsilon. \tag{3}$$

Here, the system-defined measurement matrix $H \in R^{n\times m}$ is introduced, serving as the mapping between the system state values and the corresponding measurement values.

Given the availability of the system measurement matrix H and sufficient measurement data, the power flow-based state estimation, as described in Eq. (3), can be achieved by solving the subsequent optimization problem:

$$\hat{x} = \underset{x}{argmin}(z - Hx)^T V^{-1}(z - Hx). \tag{4}$$

Note that there exists a closed solution for (4), the state estimation can be achieved through the following equation:

$$\hat{x} = (H^T V^{-1} H)^{-1} H^T V^{-1} z \triangleq \Phi z \tag{5}$$

where $\Phi = (H^T V^{-1} H)^{-1} H^T V^{-1}$.

2.2. Adversary model and residual test

When the FDI attack happens, the measurement vector is injected with a malicious vector a. For basic FDI attacks, the detection process consists of two steps, the state estimation and the residual test. Building upon the state estimation $\hat{x}$ discussed in the preceding section, we can derive the estimated measurement value as $\hat{o} = Hx = H\Phi o$. Subsequently, the measurement residual can be calculated using the following procedure:

$$r = z - \hat{z} = (I - H\Phi)x. \tag{6}$$

The second step can be conducted based on largest normalized residual test method with the exact value of the measurement residual. Specifically, it can be realized as follows:

$$D_{LNR}(z) = \begin{cases} 1, if \ \|\bar{r}\|_\infty \geq \varrho, \\ 0, otherwise, \end{cases} \tag{7}$$

Here, the normalized residual $\bar{r} = \sqrt{V^{-1}}r$ is computed with respect to the covariance V, while ϱ represents the threshold for residual values.

Although the aforementioned method is adequate for the basic FDI attacks, this design assumes that the system measurement matrix is universally known to all parties involved. In the scenario where adversaries have access to the system measurement matrix, there is an increased likelihood of them orchestrating stealthy attacks. For this kind of attack, the adversaries fabricate an attack vector $a = Hb$ based on the measurement matrix H, with $b \in R^m$ specifically designed. Define the attacked measurements as z_a, it is straight forward that $z_a = z + a$. Under this circumstance, recalling that $\Phi H = I$, we can obtain the estimated system states as follows:

$$\hat{x}_a = \Phi z_a = \Phi(z + a) = \Phi(z + Hb) = \hat{x} + b. \tag{8}$$

Following the aforementioned two steps for FDI attack detection, we can obtain the normalized residual as

$$\begin{aligned} \|\bar{r}_a\| &= \left\| \sqrt{V}^{-1}(z_a - H\hat{x}_a) \right\| \\ &= \left\| \sqrt{V}^{-1}[(z - H\hat{x}) + (a - Hb)] \right\| \\ &= \left\| \sqrt{V}^{-1}[(z - H\hat{x})] \right\| \leq \varrho, \end{aligned} \tag{9}$$

from which we can see that the stealthy attacks designed based on system measurement matrix can bypass the residual test. However, as we can see in the above analysis and in [29,35], to obtain a desired attack vector a, the adversaries must have full information of measurement matrix H. In this paper, we introduce a proactive FDI detection mechanism that employs D-FACTS devices to induce perturbations in reactance. Moreover, this approach effectively safeguards against the adversaries' acquisition of the measurement matrix H, thereby preventing their access to such information. Nevertheless, the introduction of D-FACTS devices also makes the measurement matrix unknown to the estimators. To obtain an accurate system measurement matrix information without revealing it to the adversaries, a federated learning framework with differential privacy is proposed, which allows for secure FDI detection for stealthy attacks.

3. FDI attack detection employing federated learning

As demonstrated in Section 2, there are two crucial aspects to consider. Firstly, acquiring the parameters within the matrix model H is essential for implementing FDI detection based on estimation. Secondly, another important consideration is privacy issues during the acquiring process. Once these parameters are disclosed, the adversaries can easily launch stealthy attacks, which directly reduces the accuracy of the state estimation. To conduct an accurate state estimation, an imperative requirement arises for a private-preserving learning process

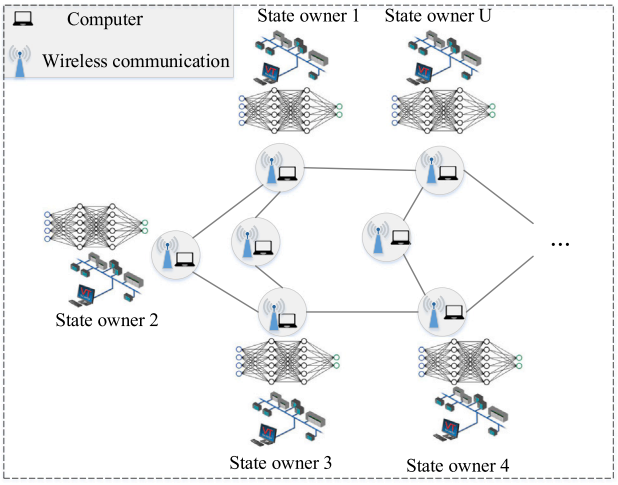


Fig. 2. The architecture of the proposed federated learning framework for false data injection attacks in smart grid.

that safeguards the information contained in the matrix H from exposure to adversaries, while still enabling the acquisition of necessary knowledge.

It should be noted that the measurement data is distributed in different smart meters. If a centralized algorithm is employed, a central data collection process is required, leading to large data transmission. This is expensive, moreover, the noise-free data transmission risks leaking the data to the adversaries. Given this scenario, the utilization of the federated learning framework becomes imperative. In this section, we propose a federated learning framework tailored for distributed training of the measurement models. In this context, we specifically consider a wireless network where a collaborative parameter learning approach is adopted by the state owners denoted as U, leveraging their individual local datasets. The architecture of the proposed federated learning framework is illustrated in Fig. 2. The network can leverage the federated learning algorithm to estimate the characteristics of the measurement matrix, enabling the detection of false data injection (FDI). The decentralized and distributed nature of local training across various devices within the network mitigates the need for extensive data transmission among multiple devices. To further prevent the model parameter from exposure to attackers, the federated learning algorithm is designed to be differential-private, which is achieved by adding artificial noise to the model estimations before information transmission, this will be illustrated in Section 4.

3.1. Machine learning model

To acquire the accurate measurement parameter information based on the distributed data sets, the state owners need to execute a cooperated learning process. Each state owner i gathers an estimated state data matrix $x_i = [x_{i1}, x_{i2}, ..., x_{iM_i}]$ as the input data, where M_i denotes the number of measurements collected by the respective state owner i. The corresponding measurement data (output data) for x_i is denoted as $z = [z_{i1}, z_{i2}, \dots, z_{iM_i}]$, which is also collected and stored by state owner i. For an effective false data injection detection without the measurement matrix information, the challenge lies in predicting the measurement matrix with these local data sets (x_i, z_i). For the convenience of mathematical modeling, by stacking all the columns of the measurement matrix H, it is converted into a vector form, denoted as w_g. Let w_i be the local prediction of the measurement vector w_g, then the total model learning problem can be formulated as follows:

$$\min_{w_1, w_2, \dots, w_U} f(w_i, x_{ij}, z_{ij}) \tag{10}$$

$$s.t. \quad w_1 = w_2 = \cdots = w_U = w_g, \tag{11}$$

where $M = \sum_{i=1}^{U} M_i$ represents the aggregate count of measurement data across all local devices, encompassing the total number of measurements available, and w_g is the global measurement parameter, $f(w_i, x_{ij}, z_{ij}) = \frac{1}{M} \sum_{i=1}^{U} \sum_{j=1}^{M_i} (z_{ij} - w_i x_{ij})^T V^{-1} (z_{ij} - w_i x_{ij})$ is the loss function. It is important to note that the loss function $f(w_i, x_{ij}, z_{ij})$ increases as the prediction error grows. By minimizing this loss function, we can attain the optimal measurement model. Constraint (11) is specifically designed to ensure the coordination of all measurement datasets, leading to a globally agreed-upon measurement model. This constraint encapsulates the fundamental characteristic of the federated learning mechanism, where all local state owners converge towards the same global model.

In fact, we have considered the impact of measurement errors in the paper. However, similar to the references, we assumed the measurement error to have a zero mean and a variance of $V \in R^n$. Therefore, such errors do not affect the predictive results of the model. This assumption is justified because typically, grossly corrupted measurements are only a small fraction of the total number of measurements. These measurements exhibit substantial deviations from their anticipated or accurate values, thus making them susceptible to exclusion. Therefore, they are already excluded from the datasets at an early stage, leading to a small size of the dispersed dataset, necessitating the introduction of the federated learning framework in this paper. To solve problem (10)–(11), a distributed optimization algorithm is employed over the network, which enables the global model acquirement with a privacy-preserving manner. The optimization algorithm consists of two parts, one for local model learning, and the other for privacy-preserving global model seeking. A comprehensive explanation of this topic will be provided in the subsequent section, offering detailed insights into the aforementioned aspects.

4. Privacy preserving federated learning for proactive FDI detection

In this section, a privacy-preserving model learning algorithm is proposed for proactive FDI detection based on solving problem (10)–(11), and the detailed architecture is illustrated in Fig. 3. To seek the optimal model parameter, each local state owner updates the local model w_i based on gradient descent. Then based on a differential privacy mechanism, each local models w_i is added with a random noise and the noisy model parameters w_i^s, $i = 1, 2, \dots, U$ are exchanged over the wireless network. By employing a distributed privacy-preserving algorithm, each state owners can obtain the optimal global model. The detail algorithm design is given as follows.

Algorithm 1: Federated learning for FDI detection.

1: **For** each state owner **do**
2: Initialize the strategy $w_i(0)$, choose auxiliary variable $z_i(0) = 0$;
3: **Noise generation**: each state owner generates a random variable $r_i(k)$ conforming to the standard normal distribution with mean 0 and variance γ.
4: **Model encryption:** each state owner encrypts the local model by adding random noise $s_i(k)$ to w_i:

$$s_i(k) = \begin{cases} r_i(0), & if \quad k = 0, \\ \delta^k r_i(k) - \delta^{k-1} r_i(k-1), & otherwise, \end{cases} \tag{12}$$

where $|q - 1| < \delta < 1$ with $0 < q < 1$. Encrypt the model as

$$w_i^s(k) = w_i(k) + s_i(k). \tag{13}$$

5: **Federated model update**:

$$w_i(k+1) = w_i(k) - \alpha(\nabla f_i(w_i) + z_i(k))$$

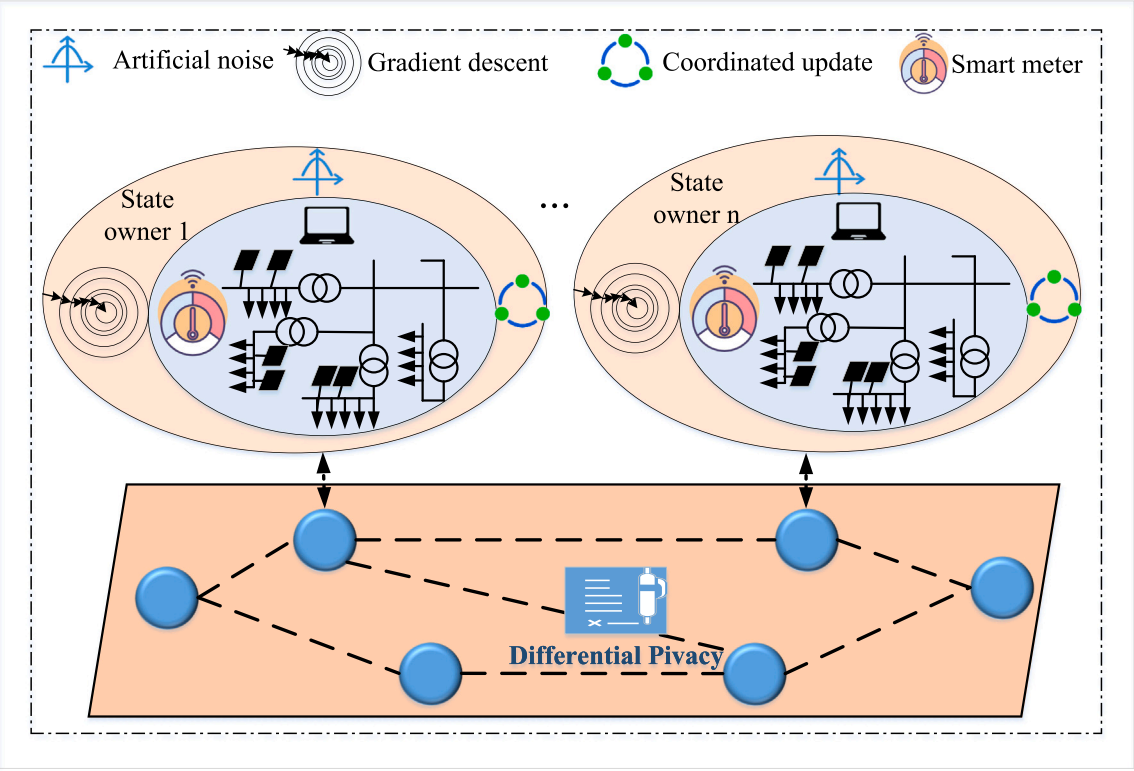


Fig. 3. The architecture of the proposed privacy-preserving model learning algorithm.

$$-\sum_{j=1}^{U} a_{ij}(w_i^s(k) - w_j^s(k)) \tag{14}$$

$$z_i(k+1) = z_i(k) + \sum_{j=1}^{U} a_{ij}(w_i^s(k) - w_j^s(k)) \tag{15}$$

6: Update $k = k + 1$;
7: Until $\|w(k+1) - w(k)\| \le \varsigma$.
8: Return w_i.
9: **End procedure**

As we can see from algorithm 1, it is fully-distributed and no central units is needed during the federated learning process. Furthermore, the transmission of solely encrypted model data over the network effectively mitigates the risk of adversaries pilfering critical model information. To provide a more direct elucidation of the procedures, we present the flowchart outlining the proposed algorithm in Fig. 4.

4.1. Convergence analysis

Theorem 1. *Let κ be the Lipschitz constant of $f(w)$, then for arbitrary $w(0)$, and $\alpha < 1/\kappa$, $w(k)$ converges to the exact model parameter w^* in the mean square sense with following mean square convergence rate ρ:*

$$\rho = max\{\delta^2, |\lambda_2|^2, |\lambda_n|^2, \alpha^2\kappa^2\}. \tag{16}$$

Firstly, we present the following lemma, which plays a crucial role in proving Theorem 1.

Lemma 1. *Let $B \triangleq A - \mathbf{1}\mathbf{1}^T/N$, $\forall k \in N^+$, the following equalities holds:*

$$A^k(A - I) = B^k(A - I), \tag{17}$$

$$A^k - \mathbf{1}\mathbf{1}^T/N = B^k(I - \mathbf{1}\mathbf{1}^T/N). \tag{18}$$

Proof. Note that the right hand of (16) is strictly small than 1, it only remains to prove (16) holds for all k.

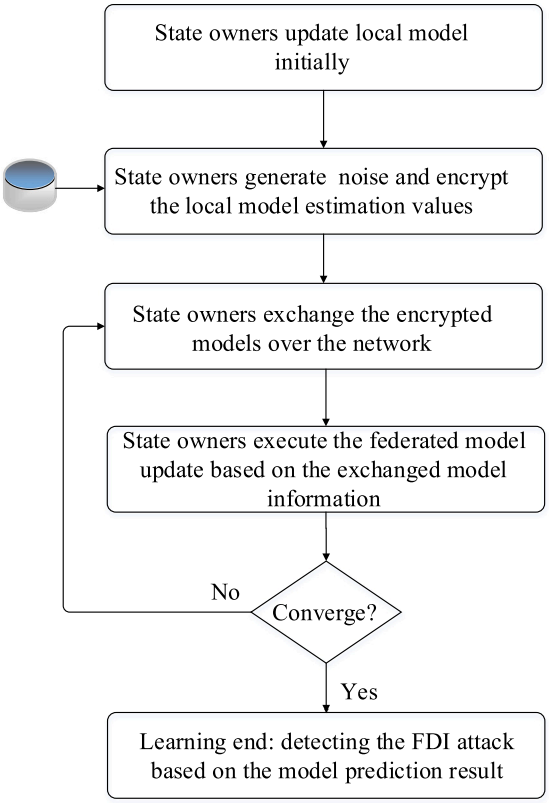


Fig. 4. Flowchart depicting the proposed algorithm.

By revisiting the definitions of the adjacency matrix A and Laplacian matrix L, Eqs. (14)–(15) can be expressed in a more concise manner as

follows:

$$\begin{aligned} w(k) =& A^k w(0) + \sum_{t=0}^{k-1} A^{k-t} s(t) - \sum_{t=0}^{k-1} \alpha \nabla f(w(t)) \\ &+ \sum_{t=0}^{k-1} \alpha L z(t-1) \\ =& A^k w(0) + A\delta^{k-1} r(k-1) + \sum_{t=0}^{k-2} \delta^t A^{k-t-1} \\ & (A-I) r(t) - \sum_{t=0}^{k-1} \alpha(\nabla f(w(t)) + L z(t)) \end{aligned} \tag{19}$$

Define $u(k) = w(k) - \mathbf{1} \otimes w^*$, recalling Lemma 1, we can obtain that

$$\begin{aligned} u(k) =& B^k u(0) + A\delta^{k-1} r(k-1) + \sum_{t=0}^{k-2} \delta^t B^{k-t-1} (A-I) r(t) \\ & - \sum_{t=0}^{k-1} \alpha(\nabla f(w(t)) - \nabla f(w^*) + L(z(t) - z^*)) \end{aligned}$$

Since the sequences $\{r(k)\}$ are independent and identically distributed with 0 mean value, we can obtain the mean square error as follows:

$$\begin{aligned} & \mathbb{E} u(k)^T u(k) \\ =& u(0)^T B^{2k} u(0) + tr(A^2)\delta^{2k-2} \\ & + \sum_{t=0}^{k-2} \delta^{2t} tr[B^{2k-2t-2}(A-I)^2] \\ & + \sum_{t=0}^{k-1} \alpha^2 (\nabla f(w(k)) - \nabla f(w^*) + L(z(t) - z^*))^T \\ & \cdot (\nabla f(w(k)) - \nabla f(w^*) + L(z(t) - z^*)). \end{aligned} \tag{20}$$

Note all the terms on the right hand of (20) are non-negative, it admits that

$$\mathbb{E} u(k)^T u(k) \geqslant u(0)^T B^{2k} u(0), \tag{21}$$

$$\mathbb{E} u(k)^T u(k) \geqslant tr(A^2)\delta^{2k-2}, \tag{22}$$

$$\mathbb{E} u(k)^T u(k) \geqslant \sum_{t=0}^{k-2} \delta^{2t} tr[B^{2k-2t-2}(A-I)^2], \tag{23}$$

and

$$\begin{aligned} & \mathbb{E} u(k)^T u(k) \\ \geqslant & \sum_{t=0}^{k-1} \alpha^2 (\nabla f(w(k)) - \nabla f(w^*) + L(z(t) - z^*))^T \\ & (\nabla f(w(k)) - \nabla f(w^*) + L(z(t) - z^*)). \end{aligned} \tag{24, 25}$$

Thus, we can further obtain that

$$\rho \geqslant max\{\delta^2, |\lambda_2|^2, |\lambda_n|^2, \alpha^2\kappa^2\}. \tag{26}$$

On the other hand, recalling that $\lambda_1 \leqslant \lambda_2 \leqslant \cdots \leqslant \lambda_n$, it is straight forward that

$$u(0)^T B^{2k} u(0) \leqslant max\{\delta^{2k}, |\lambda_2|^{2k}, |\lambda_n|^{2k}, \alpha^{2k}\kappa^{2k}\}, \tag{27}$$

$$tr(A^2)\delta^{2k-2} \leqslant max\{\delta^{2k}, |\lambda_2|^{2k}, |\lambda_n|^{2k}, \alpha^{2k}\kappa^{2k}\}, \tag{28}$$

$$\begin{aligned} & \sum_{t=0}^{k-2} \delta^{2t} tr[B^{2k-2t-2}(A-I)^2] \\ \leqslant & (n-1)(k-1) max\{\delta^{2k}, |\lambda_2|^{2k}, |\lambda_n|^{2k}, \alpha^{2k}\kappa^{2k}\}, \end{aligned} \tag{29}$$

Recalling (20), we can obtain that

$$\rho \leqslant max\{\delta^2, |\lambda_2|^2, |\lambda_n|^2, \alpha^2\kappa^2\}. \tag{30}$$

Combining with (26), we can obtain (16) directly, which ends the proof. ■

4.2. Privacy preserving for the proposed federated learning framework

Definition 1 (*Differential Privacy*)**.** Given $\varepsilon > 0, \tau > 0$, the two vectors $w'(k)$ and $w''(k)$ are τ-adjacent if and only if there exist $i_k \in \nu$ such that $\forall i \in \nu$, the following inequality holds:

$$|w'_i(k) - w''_i(k)| \leqslant \begin{cases} \tau, & if \quad i = i_k, \\ 0, & otherwise, \end{cases} \tag{31}$$

Moreover, given an arbitrary set J, if the following inequality holds for any pair of $w'(k)$ and $w''(k)$,

$$P[s \in \Omega \mid \chi^{out}_{w'(k)} \in J] \leqslant exp(\varepsilon) P[s \in \Omega \mid \chi^{out}_{w''(k)} \in J] \tag{32}$$

where $\chi^{out}_{w'(k)}$ is the transmitted message for $w'(k)$, Ω and J denote the total sample space and status output space with Algorithm 1, respectively. Then Algorithm 1 is said to be ε differential-private.

We continue to show the differential privacy of Algorithm 1. Define the following sets $S'(K)$ and $S''(K)$:

$$S'_k(K) = \{s_k(K) \in \Omega_k^K \mid \chi^{out}_{s'(k)} \in J_k^K\} \tag{33}$$

$$S''_k(K) = \{s_k(K) \in \Omega_k^K \mid \chi^{out}_{s''(k)} \in J_k^K\} \tag{34}$$

where Ω_k^K denotes the sample space from time k to K during the update of Algorithm 1, and J_k^K is the subset of J from time k to K. Denote the density function of $s_i(t)$ as $D(s_i(t))$. Recalling the continuity of probability density function, we can obtain that $P[s \in \Omega \mid \chi^{out}_{s'_k(K)} \in J] = \lim_{K\to\infty} \int_{S'_k(K)} D(s'_k(K)) s'_k(K)$, where $D(s'_k(K)) = \prod_{i=1}^{U} \prod_{t=k}^{K} s_i(t)$ is the joint probability density function.

Let $w''_{i_k}(k) = w'_{i_k}(k) + \tau$, $w''_i(k) = w'_i(k)$ for all $i \neq i_0$. For $s'_k(K) \in S'_k(K)$, define

$$s''_k(K) = \begin{cases} s'_k(K) - (1-q)^{K/2}\delta, & if \quad i = i_k, \\ s'_k(K), & otherwise, \end{cases} \tag{35}$$

It is straight forward that $\chi^{out}_{s''_k(K)} = \chi^{out}_{s'_k(K)}$, which admits $s''_k(K) \in S''_k(K)$. Hence, there exists a unique $(s'_k(K), \Delta s'_k(K))$ such that $s''_k(K) = s'_k(K) + \Delta s'_k(K)$. Note that $\Delta s'_k(K)$ is independent of $s''_k(K)$, we can further obtain that

$$\begin{aligned} & P[s \in \Omega \mid \chi^{out}_{s'_k(K)} \in J] \\ =& lim_{K\to\infty} \int_{S'_k(K)} D(s'_k(K) + \Delta s'_k(K)) d s'_k(K). \end{aligned} \tag{36}$$

Recalling the definition of joint probability density function and normal distribution of $s_i(k)$, we can further obtain that $\frac{D(s'_k(K))}{D(s'_k(K)+\Delta s'_k(K))} \leqslant exp(\sum_{t=k}^{K} \frac{(1-q)^K\delta}{4\gamma^2\delta^{k-1}})$, which leads to $\frac{D(s'_k(K))}{D(s'_k(K)+\Delta s'_k(K))} \leqslant exp(\frac{(1-q)^2\delta}{4\gamma^2(\delta+q-1)})$. By integrating over $S'_k(K)$ on both sides and make $K\to\infty$, we can further obtain that

$$\begin{aligned} & P[s \in \Omega \mid \chi^{out}_{s'_k(K)} \in J] \\ \leqslant & exp(\frac{(1-q)^2\delta}{4\gamma^2(\delta+q-1)}) P[s \in \Omega \mid \chi^{out}_{s''_k(K)} \in J] \end{aligned} \tag{37}$$

This means the $exp(\frac{(1-q)^2\delta}{4\gamma^2(\delta+q-1)})$-differential privacy for state owner i_0. Note that i_0 can be chosen arbitrarily, thus Algorithm 1 can achieve $exp(\frac{(1-q)^2\delta}{4\gamma^2(\delta+q-1)})$-differential privacy for model prediction in FDI detection.

5. Simulation

In this section, the efficacy of the proposed mechanism is demonstrated through experiments conducted on the IEEE-30 bus system, utilizing publicly available standard information [36,37]. All the experiments is conducted on Lenovo notebook with an Intel Core i5

Table 1
Values of the parameters involved in the simulation.

δ	q	γ	α
0.75	0.5	1	0.05

processor and Windows 10 system. The software implemented in the experiments is MATLAB R2020b. First, the model estimation results of the proposed federated learning mechanism will be compared with the local prediction methods in [38]. To explore the dual performance of the algorithm which includes the convergence and privacy protection, the trade-off between the accuracy loss will be explored. Furthermore, the practicality of employing the proposed mechanism for FDI attack detection will be extensively investigated, encompassing scenarios involving both multiple-bus and single-bus FDI attacks. Subsequently, the outcomes of corresponding experimental evaluations will be presented within this section.

5.1. Model estimation: federated learning VS local learning

In this section, the model estimation accuracy of the proposed federated learning framework is tested and compared with the local prediction method in [38]. The values of the parameters involved in the simulation are displayed in Table 1. First, the comparison of the model estimation results with the proposed federated learning and that of the local prediction framework in [38] is given in Fig. 5. Here in Fig. 5, True represents the true values of the model parameter, FL i represents the model estimation values obtained by agent i with the proposed federated learning framework, while LP denotes the model estimation values with the local prediction framework in [38]. From Fig. 5, we can see that an unbiased estimate of the model parameters can be obtained with the proposed method, while a wrong one is achieved with the local prediction method in [38], which demonstrates the effectiveness of the proposed mechanism. Figs. 6 and 7 present a comparison of the root mean square error between the federated learning framework proposed in this study and the local prediction method introduced in [38]. This comparison provides further evidence that the proposed mechanism yields highly accurate model prediction results in contrast to the local prediction method in [38]. Let H_1 be the first column of the measurement matrix H, and H_1^p be its estimation vector. To quantitatively assess the accuracy of the model estimation results, we utilize the mean absolute error (MAE), mean squared error (MSE), and root mean square error (RMSE) metrics to evaluate the discrepancy between H_1 and H_1^p, and the comparison results are given in Table 2, which further demonstrates that the proposed mechanism achieves accurate model estimation while the model prediction method cannot. As for the training time, thanks to the federated learning framework, the training time and efficiency for the proposed algorithm in our study is efficient. For 100 scenarios involved in the manuscript, we were able to obtain accurate model training results within a short duration. To precisely determine the algorithm's training time, we incorporated a timer during the simulation. The timer indicated that the algorithm required only 6.9307 s to achieve the correct FDI detection results. In our study, by using the proposed algorithm within the federated learning framework, we were able to obtain accurate FDI detection results within seconds for 100 scenarios. The high efficiency of the federated learning algorithm, which achieves fast model predictions within a few seconds, makes it well-suited for situations requiring model updates and retraining.

Next, leveraging the theoretical findings outlined in Section 4, the trade-off between the reduction in accuracy and the level of privacy preservation is explored. To explore this trade-off in an exact way, the following metrics concerning the privacy level and the accuracy loss are introduced first. Let $\delta = \frac{3}{4}$, $q = \frac{1}{2}$, define $\epsilon = \frac{(1-q)^2\delta}{4\gamma^2(\delta+q-1)}$, which reflects the privacy level of Algorithm 1. Additionally, to facilitate the

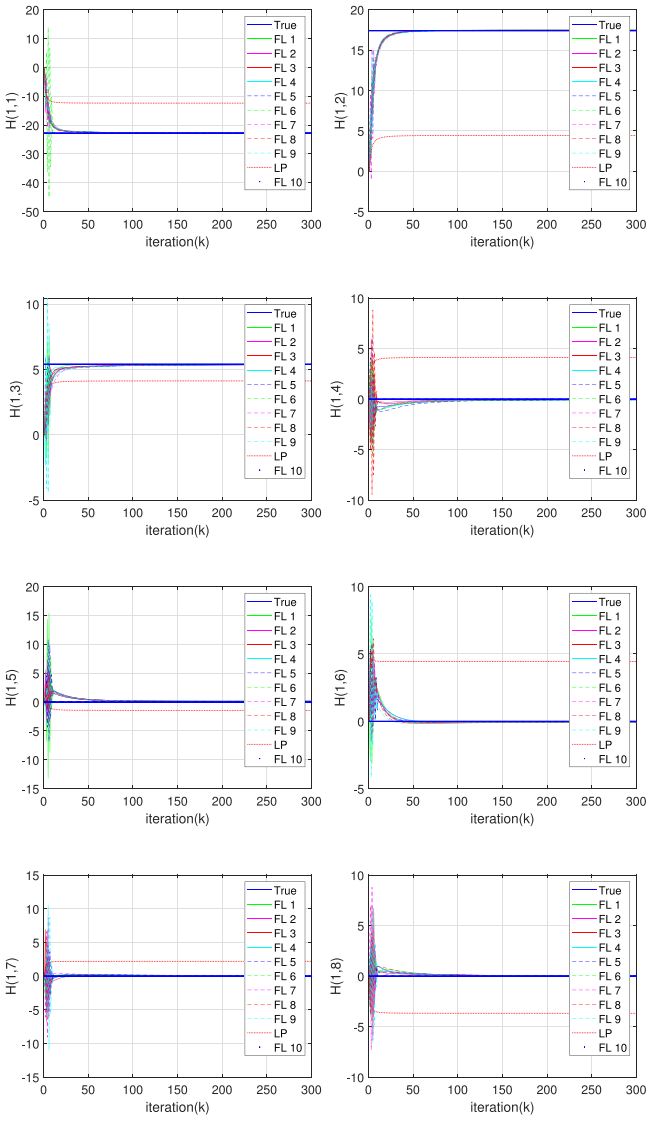


Fig. 5. The evolutionary trajectories of the model estimation values with the proposed mechanism and the local prediction methods in [38].

characterization of model prediction accuracy, we introduce the root mean square error (ρ) as a metric for quantifying accuracy loss. The ρ is defined as follows:

$$\rho = \sqrt{\frac{\|H^p - H\|^2}{m^2}}, \tag{38}$$

Here, H^p represents the predicted measurement matrix, H denotes the actual measurement matrix, and m signifies the dimension of H. Based on the aforementioned settings, the trade-off between the accuracy loss and privacy preserving level is depicted in Fig. 8, from which we can see these two are negatively related as we expected. These findings provide additional evidence that the precise estimation of the measurement matrix can be accomplished using local datasets within the presented federated learning framework. Moreover, from Fig. 8 we can see that by choosing a proper value for γ, the accuracy loss can be well balanced with privacy preserving level. This means the accurate model estimation can be achieved without disclosing the key model information to the adversaries, which is of great significance to the FDI attack detection. This will be further illustrated in the next section.

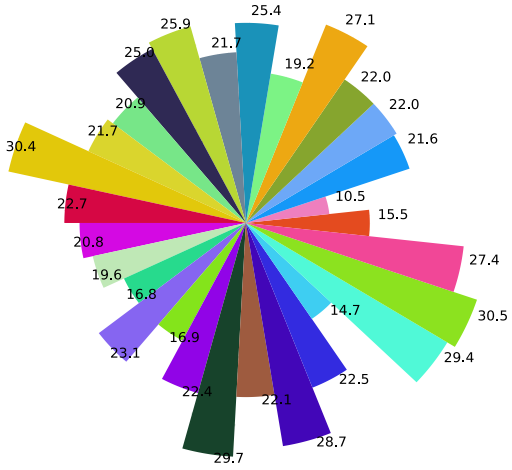


Fig. 6. Root mean square error of local prediction framework in [38].

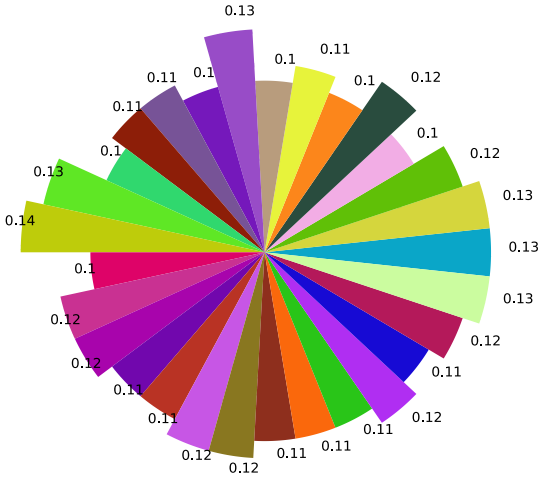


Fig. 7. Root mean square error of the proposed federated learning framework.

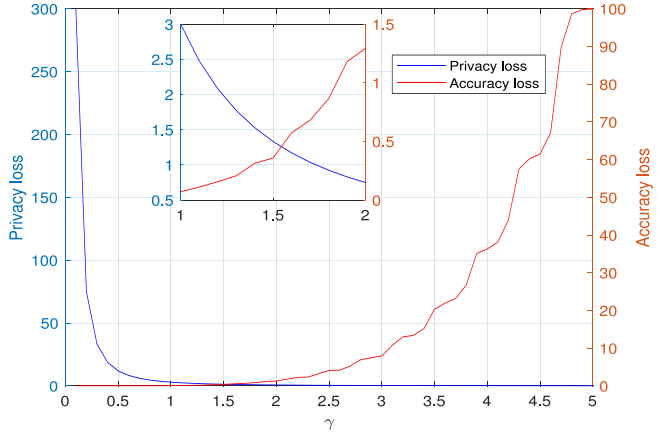


Fig. 8. The trade-off between the accuracy loss and privacy preserving level.

5.2. False data injection detection: federated learning VS local learning

In this section, we validate the efficacy and accuracy of the proposed federated learning framework by examining the model prediction results obtained in the previous section. To facilitate a comprehensive comparison, we also present the FDI attack detection results utilizing the local prediction method introduced in [38]. The experiments are conducted with two FDI attacks, i.e., the multiple-bus FDI attacks and the single-bus FDI attack. The details are given as follows:

(1) Multiple-bus FDI attacks This kind of attack focuses on multiple buses, for instance, the attacks vectors presents as $b = (0, \theta_{a1}, 0, 0, 0, \theta_{a2}, \ldots, \theta_{a3}, \ldots)^T$ with θ_{a1} being heterogeneous attacking voltage angle. To verify the robustness of the proposed mechanism, largest normalized residuals (LNR) tests are conducted for 100 Monte Carlo scenarios. The test results for the LNR, examining the proposed mechanism's

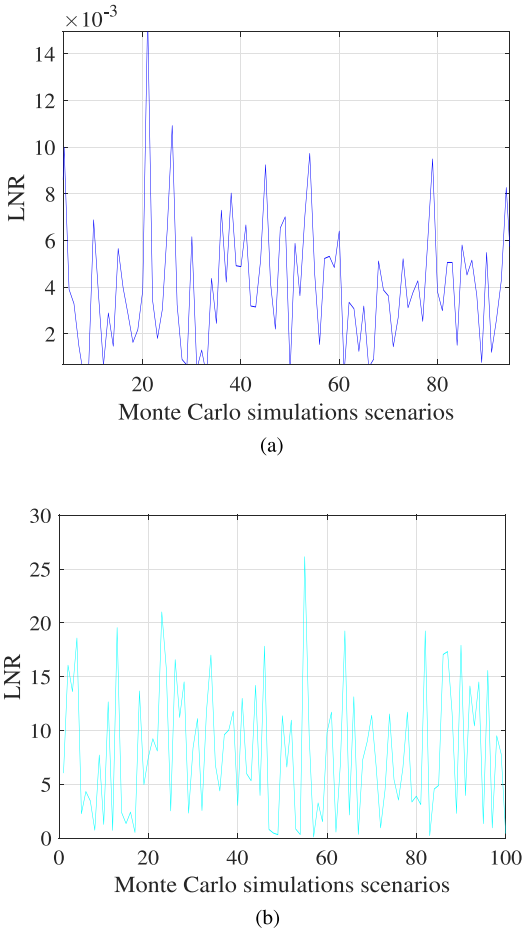


Fig. 9. LNR outcomes from 100 Monte Carlo experiments: proposed framework under no attacks (a) and under multiple-bus FDI attack (b).

Table 2
Comparison of H_1 estimation accuracy: Proposed federated learning vs. Local prediction framework in [38].

Index	MAE	MSE	RMSE
Federated learning	0.1532	0.0173	0.1314
Local prediction	29.1393	2680	51.7811
	26.8044	2590	50.9370
	28.9687	3910	62.5075
	30.0601	4760	69.0270
	27.0020	3670	60.5426
	30.9852	5200	72.0979
	26.4169	4380	66.2103
	24.2739	3560	59.6466
	30.2119	3090	55.5476
	26.5895	2560	50.5478

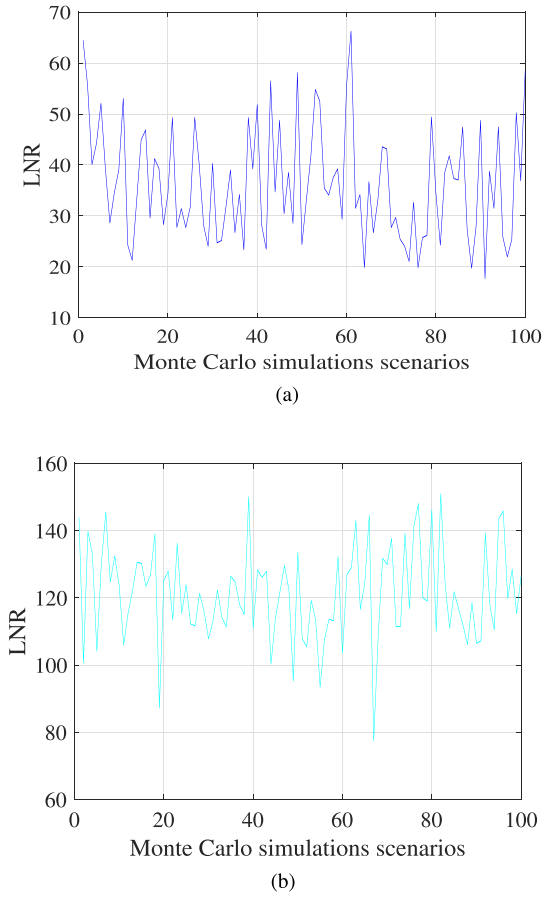


Fig. 10. LNR outcomes from 100 Monte Carlo simulations: Local prediction framework in [38] under no attacks (a), under multiple-bus FDI attack (b).

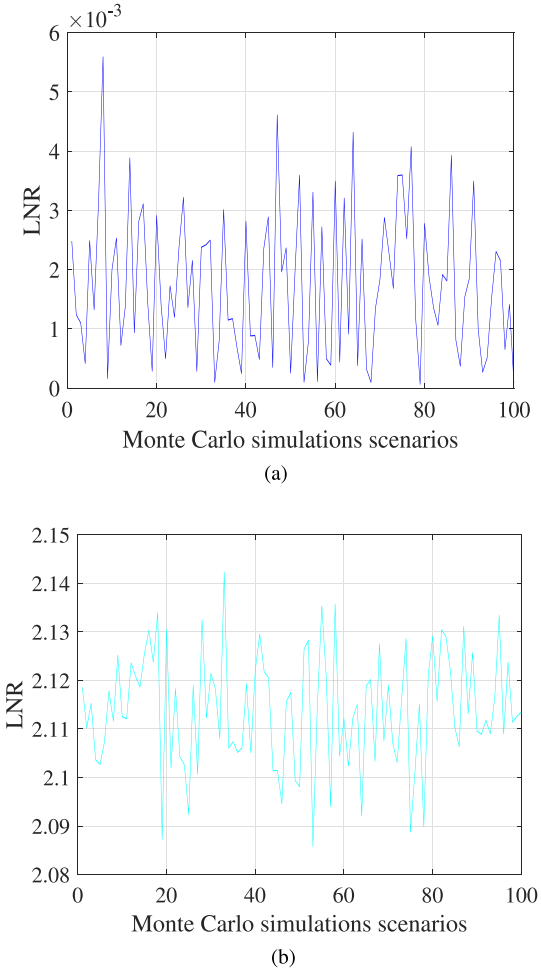


Fig. 11. LNR outcomes from 100 Monte Carlo simulations: Proposed framework under no attacks (a), under single-bus FDI attack (b).

performance under both multiple-bus FDI attack scenarios and no attack scenarios, are illustrated in Fig. 9, from which we can see that by choosing a residual threshold value on $[0.014, 1]$, successful FDI attacks detection can be achieved with the proposed federated learning framework. The LNR values obtained from the experiments, as depicted in Fig. 10, reveal that the local prediction method proposed by [38] fails to effectively detect multiple-bus false data injection attacks. This failure is evident from the negligible difference observed between the LNR values under multiple-bus attack scenarios and those under no attack scenarios.

(2) Single-bus FDI attack: it refers to the activation of an FDI attack on a particular bus, denoted as $b_i = \theta a$, where i represents an arbitrarily selected node, and $bj = 0$ for all $j \neq i$ and $j \in N$. Here we choose $i = 1$. Similar to the last section, largest normalized residuals (LNR) tests are conducted for 100 Monte Carlo scenarios. The LNR test results with the mechanism of this paper under single-bus FDI attacks and under no attacks are given in Fig. 11, respectively, from which we can see that by choosing a threshold value on $[0.006, 2.08]$, successful FDI attacks detection can be achieved with the proposed federated learning framework. While from Fig. 12, it shows that the LNR values under single-bus attack shows little difference with the ones under no attack using the local prediction method in [38], which means they failed to detect the single-bus false data injection attacks.

(3) Sensitivity analysis: to explore the detection sensitivity over the attack amplitude, the LNR tests results of the proposed mechanism and the local methods are compared with different attack amplitude. In Figs. 13 and 14, the relationships between the LNR values and the attack amplitude under multiple-bus FDI attacks and single-bus attacks are depicted, respectively, from which we can see that both the LNR values present an increasing trend with larger attack amplitude. Furthermore, we can see from Figs. 13(a) and 14(a) that comparing with the case under no FDI attacks, the LNR values under FDI attacks show big differences with the proposed mechanism, which further verifies the effectiveness of the proposed mechanism. However, as is shown in Figs. 13(b) and 14(b), although the LNR values of the local prediction method in [38] increase with the attack amplitude, the values with or without attacks are indistinguishable, which leads to failures in FDI attack detection.

6. Conclusion

This study presents a novel algorithm for detecting false data injection attacks by employing a privacy-preserving approach and leveraging federated learning. The key findings are summarized as follows:

(1) The decentralized and distributed training process avoids data transmission among multiple devices.

(2) Artificial noise has been added to the model estimations before information transmission, which achieves privacy preserving.

(3) The trade-off between the accuracy loss and privacy preserving level is characterized.

(4) Simulations on the IEEE 30-bus system validate the theoretical convergence and privacy analysis results.

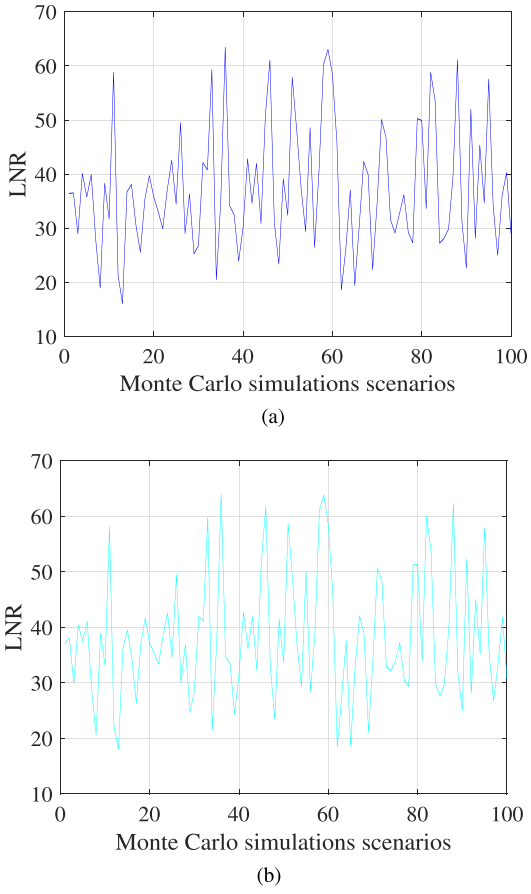
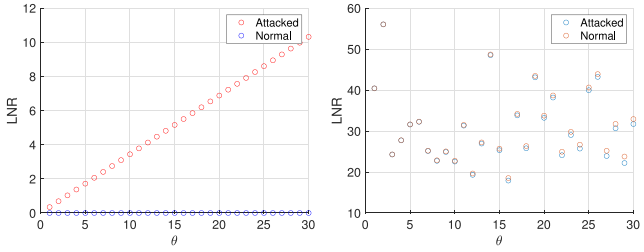
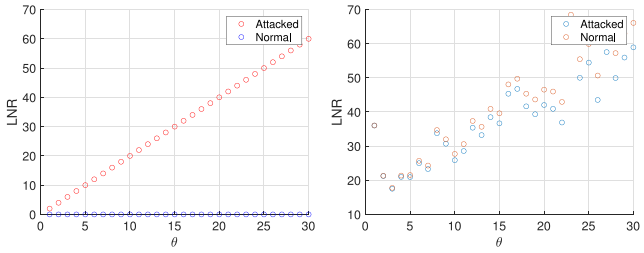


Fig. 12. LNR outcomes from 100 Monte Carlo simulations: Local prediction framework in [38] under no attacks (a), under single-bus FDI attack (b).



(a) The proposed mechanism (b) The local prediction method in [38]

Fig. 13. Relationship between the LNR values and the attack amplitude on the single-bus FDI attack.



(a) The proposed mechanism (b) The local prediction method in [38]

Fig. 14. Relationship between the LNR values and the attack amplitude on the multiple-bus FDI attack.

CRediT authorship contribution statement

Wen-Ting Lin: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Validation, Visualization, Writing – original draft, Writing – review & editing. **Guo Chen:** Methodology, Project administration, Resources, Software. **Xiaojun Zhou:** Software, Supervision, Validation, Visualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

[1] G. Simard, IEEE Grid Vision 2050, IEEE, 2013.
[2] X. Li, Y. Wang, Z. Lu, Graph-based detection for false data injection attacks in power grid, Energy 263 (2023) 125865.
[3] W.-T. Lin, G. Chen, X. Zhou, Distributed carbon-aware energy trading of virtual power plant under denial of service attacks: A passivity-based neurodynamic approach, Energy 257 (2022) 124751.
[4] H. Wang, A. Meng, Y. Liu, X. Fu, G. Cao, Unscented Kalman Filter based interval state estimation of cyber physical energy system for detection of dynamic attack, Energy 188 (2019) 116036.
[5] Y.L. Qiu, Y.D. Wang, B. Xing, Grid impact of non-residential distributed solar energy and reduced air emissions: Empirical evidence from individual-consumer-level smart meter data, Appl. Energy 290 (2021) 116804.
[6] H. Yang, R. Liang, Y. Yuan, B. Chen, S. Xiang, J. Liu, H. Zhao, E. Ackom, Distributionally robust optimal dispatch in the power system with high penetration of wind power based on net load fluctuation data, Appl. Energy 313 (2022) 118813.
[7] A.A. Khan, O.A. Beg, Cyber vulnerabilities of modern power systems, in: H. Haes Alhelou, N. Hatziargyriou, Z.Y. Dong (Eds.), Power Systems Cybersecurity: Methods, Concepts, and Best Practices, Springer International Publishing, Cham, ISBN: 978-3-031-20360-2, 2023, pp. 47–66, http://dx.doi.org/10.1007/978-3-031-20360-2_2.
[8] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, Y. Xiang, Deep learning based attack detection for cyber-physical system cybersecurity: A survey, IEEE/CAA J. Autom. Sin. (2021).
[9] D. Curto, S. Favuzza, V. Franzitta, A. Guercio, M.A.N. Navia, E. Telaretti, G. Zizzo, Grid stability improvement using synthetic inertia by battery energy storage systems in small islands, Energy (2022) 124456.
[10] H. Yang, J. Qiu, K. Meng, J.H. Zhao, Z.Y. Dong, M. Lai, Insurance strategy for mitigating power system operational risk introduced by wind power forecasting uncertainty, Renew. Energy 89 (2016) 606–615.
[11] Y. Zhao, Z. Zhou, K. Zhang, Y. Huo, D. Sun, H. Zhao, J. Sun, S. Guo, Research on spillover effect between carbon market and electricity market: Evidence from Northern Europe, Energy (2022) 126107.
[12] X. Zhang, X. Guo, X. Zhang, Bidding modes for renewable energy considering electricity-carbon integrated market mechanism based on multi-agent hybrid game, Energy 263 (2023) 125616.
[13] O.A. Beg, A.A. Khan, W.U. Rehman, A. Hassan, A review of AI-based cyber-attack detection and mitigation in microgrids, Energies 16 (22) (2023) http://dx.doi.org/10.3390/en16227644, URL: https://www.mdpi.com/1996-1073/16/22/7644.
[14] R. Nawaz, R. Akhtar, M.A. Shahid, I.M. Qureshi, M.H. Mahmood, Machine learning based false data injection in smart grid, Int. J. Electr. Power Energy Syst. 130 (2021) 106819.
[15] Y. Chen, S. Huang, F. Liu, Z. Wang, X. Sun, Evaluation of reinforcement learning-based false data injection attack to automatic voltage control, IEEE Trans. Smart Grid 10 (2) (2019) 2158–2169, http://dx.doi.org/10.1109/TSG.2018.2790704.
[16] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, Z. Han, Detecting stealthy false data injection using machine learning in smart grid, IEEE Syst. J. 11 (3) (2014) 1644–1652.
[17] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, S. Mishra, Decision tree and SVM-based data analytics for theft detection in smart grid, IEEE Trans. Ind. Inform. 12 (3) (2016) 1005–1016.
[18] A.A. Khan, O.A. Beg, M. Alamaniotis, S. Ahmed, Intelligent anomaly identification in cyber-physical inverter-based systems, Electr. Power Syst. Res. 193 (2021) 107024.

[19] M.R. Habibi, H.R. Baghaee, T. Dragičević, F. Blaabjerg, False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks, IEEE Trans. Circuits Syst. II 68 (2) (2020) 717–721.
[20] Z. Liu, J. Tang, Z. Zhao, S. Zhang, Adaptive neural network control for nonlinear cyber-physical systems subject to false data injection attacks with prescribed performance, Phil. Trans. R. Soc. A 379 (2207) (2021) 20200372.
[21] E.M. Ferragut, J. Laska, M.M. Olama, O. Ozmen, Real-time cyber-physical false data attack detection in smart grids using neural networks, in: 2017 International Conference on Computational Science and Computational Intelligence, CSCI, 2017, pp. 1–6, http://dx.doi.org/10.1109/CSCI.2017.1.
[22] M.R. Habibi, H.R. Baghaee, T. Dragičevi, F. Blaabjerg, et al., Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks, IEEE J. Emerg. Sel. Top. Power Electron. (2020).
[23] M. Dehghani, A. Kavousi-Fard, M. Dabbaghjamanesh, O. Avatefipour, Deep learning based method for false data injection attack detection in AC smart islands, IET Gener. Transm. Distrib. 14 (24) (2020) 5756–5765.
[24] Y. Zhang, J. Wang, B. Chen, Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach, IEEE Trans. Smart Grid 12 (1) (2020) 623–634.
[25] L. Yang, Y. Li, Z. Li, Improved-ELM method for detecting false data attack in smart grid, Int. J. Electr. Power Energy Syst. 91 (2017) 183–191.
[26] X. Wang, B. Li, Y. Yan, N. Gao, G. Chen, Predicting of thermal resistances of closed vertical meandering pulsating heat pipe using artificial neural network model, Appl. Therm. Eng. 149 (2019) 1134–1141.
[27] J. Zhao, A. Gómez-Expósito, M. Netto, L. Mili, A. Abur, V. Terzija, I. Kamwa, B. Pal, A.K. Singh, J. Qi, et al., Power system dynamic state estimation: Motivations, definitions, methodologies, and future work, IEEE Trans. Power Syst. 34 (4) (2019) 3188–3198.
[28] A. Monticelli, Electric power system state estimation, Proc. IEEE 88 (2) (2000) 262–282.
[29] Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Trans. Inf. Syst. Secur. 14 (1) (2011) 1–33.
[30] J. Tian, R. Tan, X. Guan, T. Liu, Enhanced hidden moving target defense in smart grids, IEEE Trans. Smart Grid 10 (2) (2018) 2208–2223.
[31] D. Divan, H. Johal, Distributed FACTS-A new concept for realizing grid power flow control, in: 2005 IEEE 36th Power Electronics Specialists Conference, IEEE, 2005, pp. 8–14.
[32] B. Liu, H. Wu, Optimal D-FACTS placement in moving target defense against false data injection attacks, IEEE Trans. Smart Grid 11 (5) (2020) 4345–4357.
[33] B. Li, G. Xiao, R. Lu, R. Deng, H. Bao, On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices, IEEE Trans. Ind. Inform. 16 (2) (2019) 854–864.
[34] G. Hug, J.A. Giampapa, Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks, IEEE Trans. Smart Grid 3 (3) (2012) 1362–1370.
[35] R. Deng, H. Liang, False data injection attacks with limited susceptance information and new countermeasures in smart grid, IEEE Trans. Ind. Inform. 15 (3) (2018) 1619–1628.
[36] H.J. Touma, Study of the economic dispatch problem on IEEE 30-bus system using whale optimization algorithm, Int. J. Eng. Technol. Sci. 3 (1) (2016) 11–18.
[37] P. Choudekar, S. Sinha, A. Siddiqui, Congestion management of IEEE 30 bus system using thyristor controlled series compensator, in: 2018 International Conference on Power Energy, Environment and Intelligent Control, PEEIC, IEEE, 2018, pp. 649–653.
[38] Y. Tang, G. Qu, N. Li, Semi-global exponential stability of augmented primal–dual gradient dynamics for constrained convex optimization, Systems Control Lett. 144 (2020) 104754.