Joint Protection of Energy Security and Information Privacy for Energy Harvesting: An Incentive Federated Learning Approach

Qianqian Pan, Jun Wu, *Member, IEEE,* Ali Kashif Bashir, *Senior Member, IEEE,*
Jianhua Li, Wu Yang, and Yasser D. Al-Otaibi

***Abstract*—Energy harvesting (EH) is a promising and critical technology to mitigate the dilemma between the limited battery capacity and the increasing energy consumption in the Internet of everything. However, the current EH system suffers from energy-information cross threats, facing the overlapping vulnerability of energy deprivation and private information leakage. Although some existing works touch on the security of energy and information in EH, they treat these two issues independently, without collaborative and intelligent protection cross the energy side and information side. To address the above challenge, this paper proposes a joint protection framework of energy security and information privacy for EH with an incentive federated learning approach. First, we design a federated learning-based malicious energy user detection method according to energy status and behaviors to provide energy security protection. Secondly, a differential privacy-empowered information preservation scheme is devised, where sensitive information is protected by the customized demand-based noise. Thirdly, a non-cooperative game-enabled incentive mechanism is established to encourage EH nodes to participate in the joint energy-information protection system. The proposed incentive mechanism derives the optimal energy-information security strategy for EH nodes and achieves a tradeoff between the protection of energy security and information privacy. Evaluation results have verified the effectiveness of our proposed joint protection mechanism.**

***Index Terms*—Energy harvesting, joint protection, federated learning, differential privacy, incentive mechanism.**

I. Introduction

WITH the ever-increasing huge amount of data and heterogeneous high-energy services, the dilemma between the increasing energy consumption and the limited battery capacity of wireless devices is intensifying [1]. Energy harvesting (EH) is a promising and critical technology to mitigate the bottleneck of energy limitation [2], [3]. EH allows wireless devices to harvest energy from surroundings, store energy in their own batteries, and transmit it to other low-power devices [4]. However, the EH system confronts energy-information cross threats, where the overlapping vulnerability of energy deprivation and private information leakage compromises EH security and sustainability. This security vulnerability does huge harm to EH system, and even causes malicious accidents, e.g. production accidents resulting from the energy exhaustion of industrial equipment, and paralyzed energy infrastructure due to the leakage of sensitive information.

Energy security and information privacy are both important issues of EH and there are overlaps between them. On the one hand, the energy security mechanism needs user data to train models for malicious node detection. Thus, it is inevitable to access and leak private information, e.g. energy status and consumption habits of users. On the other hand, the sensitive information leakage widens the attack surface of energy attacks, may helping the adversary evade detections and even destroy the system. Some works have been done to mitigate energy and information security in EH. For energy security, some admirable methods have been proposed, such as a machine learning-based preservation in [5] and the low-complexity taxation mechanism in [6]. For information privacy, source location-preserving mechanisms and energy consumption protection are studied [7], [8]. However, these prior works treat energy security and information privacy issues independently, ignoring the overlapping between them. Our work aims to establish collaborative intelligent protection across the energy side and information side, which is critically important and urgently needed.

When designing smart approaches for energy-information security, there still remain two challenges. *1) Insufficient training data:* the amount of data collected by a single EH node is not enough to train an intelligent model for energy security, which may lead to non-convergence or over-fitting. An effective method to solve this issue is distributed machine learning, which incorporates information from multiple distributed datasets. However, it is impractical for the classical distributed machine learning in EH system because of the following challenge, i.e. *2) Information privacy issues:* Distributed learning methods may result in the exposure of EHs' data to attackers, e.g. private information obtained by attackers via analyzing the uploaded parameters [9], [10]. There remains a blank in the design of joint protection of energy security and

This work was supported by the National Natural Science Foundation of China Under Grant U2003206, Grant 61972255, and Grant U20B2048. *(Corresponding author: Jun Wu.)*

Q. Pan, J. Wu, J. Li are with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China, and also with Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, Shanghai 200240, China (E-mail: panqianqian@sjtu.edu.cn; junwuhn@sjtu.edu.cn; lijh888@sjtu.edu.cn).

A. K. Bashir is with the Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M15 6BH, U.K., with the School of Electrical Engineering and Computer Science, National University of Science and Technology at Islamabad (NUST), Islamabad 24090, Pakistan, and also with the School of Engineering, University of Guelph, Guelph N1G2W1, Canada (E-mail: akashifb@uoguelph.ca).

Y. D. Al-Otaibi is with Department of Information Systems, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Jeddah 21589, Saudi Arabia (E-mail: yalotaibi@kau.edu.sa).

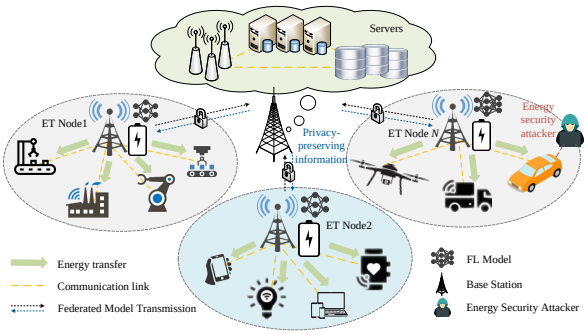


Fig. 1. Scenario for joint protection of energy security and information privacy.

information privacy for EH. All these existing problems and challenges of energy-information security motivate our work.

Federated learning (FL) is the mainstream of distributed learning technologies, which incorporates data of multiple nodes while avoiding direct data exposure to adversaries [11]. FL has arisen widespread attention in academia and industry, and has a wide range of applications [12], [13]. Differential privacy (DP) has strong capabilities of protecting privacy without any background knowledge of the attackers [14]. DP is widely utilized in various areas, e.g. location privacy protection on the Internet of Vehicles (IoV) and medical privacy protection in the E-health system [15], [16]. Since the excellent features of FL and DP, we design a joint protection mechanism of energy security and information privacy by leveraging FL and DP for EH in this paper. The scenario for the joint energy-information protection is shown in Fig. 1, where EUs request energy from the nearby ETs, and ETs transfer energy to EUs while performing the privacy-preserving FL-enabled approach to detect energy security attackers. The contributions of this paper are summarized as follows:

- We propose a joint energy-information protection framework for the EH, which enables secure and privacy-preserving energy harvesting and transfer. In this framework, a federated energy security protection scheme is established to detect and process malicious energy users.
- To avoid privacy leakage of both ETs and EUs, a DP-enabled information preservation scheme is proposed, where a customized demand-based privacy preservation approach is designed to perturb sensitive information of EH nodes according to their privacy budget.
- We propose a non-cooperative game-based incentive mechanism to encourage ETs to participate in our proposed joint protection system. We derive the optimal energy-information strategies for ETs and balance energy security protection and information privacy preservation.

The remainder of this paper is organized as follows. Section II discusses the related work. Section III proposes the energy-information threat model and protection framework. In Section IV, the joint protection mechanism of energy security and information privacy is established. The non-cooperative game-based incentive mechanism is proposed in Section V. Section VI discusses the security analysis and empirical study. The conclusion of this paper is presented in Section VII.

II. Related Work

A. Energy Harvesting for Sustainable Communication

Energy harvesting technology has obtained widespread attention recently and been applied in embedded wireless devices for sustainable communication [17]–[20]. Specifically, Saleem et al. in [17] study the EH-aided device-to-device communication in cellular networks, where an EH and gain-enabled resource allocation algorithm is proposed to optimize sum rate. In [18], Ercan et al. investigate radio frequency energy harvesting and transfer architecture for the efficient communication of the Internet of Things (IoT). The authors in [19] propose a peer-to-peer energy-knowledge trading framework, where EH technique is utilized to provide stable power edge intelligence for high efficiency. The authors in [20] design an EH-based edge computing and offloading framework, enabling the performance of energy-limited devices.

Although these works investigate the EH for sustainable communication, they mainly focus on energy capture, transmission, and allocation. The study on the security and privacy of energy harvesting and cooperation is few. Some researching works investigate the energy attack and information security [7], [21]. Specifically, Tedeschi et al. [7] investigate the vulnerabilities of EH networks including attack models, data security schemes, and physical-layer countermeasures. The authors in [21] focus on the security and privacy challenges in the energy harvesting and trading market, where blockchain is used to establish a secure energy trading system. Our work differs from the previous studies in that we consider both energy security and information privacy of EH jointly to design a more secure EH system rather than investigate them separately.

B. Federated Learning and Privacy Protection

As a promising technology of distributed machine learning, FL aggregates local data and computing resources while avoiding direct private information exposure [22], which has been applied in energy and power areas. In [23], a distributed energy management mechanism is established for smart homes, which is empowered by federated reinforcement learning methods. The authors in [24] propose an FL-enabled energy demand prediction method for vehicle networks. Only a few works exploit the FL on energy security, e.g. the FL-based electricity consumer characteristics identification approach in [25] which can be utilized to detect abnormal energy users. However, this research applies principal component analysis (PCA) to protect information privacy, which may result in an inevitable decline in accuracy and efficiency. Besides, the focus of [25] is energy characteristics analysis. The FL on energy security and privacy preservation has not been thoroughly explored.

Differential privacy is the advanced technology to prevent leakage of private information with solid mathematical foundations. DP has been utilized in multiple fields to preserving privacy, e.g. private information protection in industrial IoT [26] and genomic data privacy preservation [27]. Some works focus on the application of DP in machine learning. In [28], the authors apply DP to the distributed machine learning and quantify the model value. The authors in [29] investigate the DP-enabled federated learning mechanism, which designs the

algorithm and analyzes the performance. Although FL and DP technologies have been well studied, the combination of them for energy-information joint preservation still remains blank. In our work, we will establish a protection model for energy and information security simultaneously.

III. Energy-Information Threat Model and Joint Protection Framework

A. Threat Model

Potential threats in EH system of this paper come from attacks against energy security and information privacy. For energy security attacks, the adversaries are the malicious-but-covert EUs who try to deprive the energy of ETs by sending numerous malicious but legitimate energy demands to ETs. The energy security attackers can be malicious but legitimate EUs or hackers breaking the EH system. These attackers claim low-energy status and request excessive energy from the nearby ET even though they have sufficient power. The energy attackers counterfeit the energy demands by increasing the amounts of requesting energy randomly before sending them to the ET nodes. The energy security attack exhausts the ETs' energy, resulting in the denial of service in EH. The reliability and functionality of the EH system are severely damaged.

The information privacy leakage threat occurs in the construction of the intelligent energy security protection model. To detect malicious EUs and maintain energy security, energy data of EHs are collected and utilized to train the energy security protection model. The information adversaries are located at the server, who are honest but curious, e.g. the disgruntled administrators or hackers with illegitimate access. The honest-but-curious server performs the EH system protocols honestly but tries to deduce the private information of EHs during the distributed training process. This information privacy threat results in potential data loss of ETs, and has bad influences on the reputation of the joint energy-information protection system. Thereby, the participation and enthusiasm of EHs are greatly reduced, affecting the energy security negatively. Note that, we consider the ETs are trusted nodes as they are generators and collectors of data, and owners of energy.

B. Framework of the Proposed Joint Protection Mechanism

The framework of the proposed joint energy and information preservation mechanism is shown in Fig. 2, which consists of three planes listed as follows:

1) Energy User Plane: This plane includes numerous wireless devices with limited energy, e.g. smartphones, unmanned aerial vehicles (UAV), and industrial devices. To deal with the increasing data traffic and provide heterogeneous services, EUs request, harvest, and store the energy from ETs. However, some malicious EUs may pretend their energy is low and constantly request energy supplies to exhaust power of ETs.

2) FL and DP Empowered Energy Transmitter Plane: The energy transmitter plane consists of ETs with capacities of energy supply and joint energy-information security protection. The energy supply includes energy harvesting, energy storage, and energy transfer. ETs can harvest energy from the surrounding environment (e.g. solar, wind, or power from the grid), store the captured energy to their batteries, and transmit the energy to EUs on demand. Joint protection of energy security and information privacy is implemented based on the FL-based malicious energy user detection scheme and the DP-enabled privacy-preserving scheme.

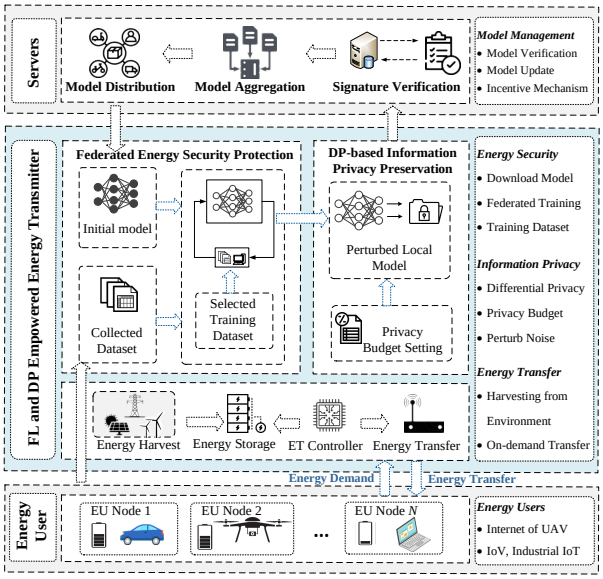


Fig. 2. Framework of the proposed joint preservation mechanism for both energy security and information privacy.

3) Server Plane: The management of the FL model is implemented in this plane. With powerful computing and storage capacity, the server plane has the potential to conduct the following functions: verifying the legality and integrity of the uploaded FL models from ETs, performing a secure model aggregation over these local models without leaking privacy information, and distributing the updated model to the ETs.

The proposed framework implements energy transmission under the joint protection of energy security and information privacy. The EU node that expects energy supply should first transmit energy demand to its nearby ET node. The ET verifies the legality of the EU. If the EU is regarded as valid, the corresponding components of ET parse and analyze the energy request, and then transfer energy to the EU over the control of its microcontroller. For energy security, an FL-enabled energy security scheme is proposed, where a designed malicious EU nodes detection method is performed periodically based on EUs' behaviors and energy status. If an EU is detected as malicious, its energy behavior will be forbidden, e.g. energy requesting and harvesting behaviors. Moreover, the privacy of information in our proposed scheme is guaranteed by DP technology when training, aggregating, and distributing the federated energy security detection model.

IV. Joint Protection of Energy Security and Information Privacy

A joint protection mechanism for energy and information security is proposed in this section. We design the FL-enabled energy security protection scheme and a DP-based information privacy preservation scheme for EH system. To ease reading, the list of the major notations is summarized in Table I.

TABLE I
MAJOR NOTATIONS AND DESCRIPTIONS

Notations	Descriptions
$\mathcal{D}_k$	The dataset owned by the k-th ET node
$\mathcal{P}^{(t)}$	The set of ETs participating in the t-th round training
$\boldsymbol{w}^{(t)}$	Weights of FL models of the t-th round training
$\mathcal{T}_k^{(t)}$, $\mathcal{T}_k^{'(t)}$	Two adjacent training datasets of the ET k at round t
$\boldsymbol{g}_k^{(t)}$, $\tilde{\boldsymbol{g}}_k^{(t)}$	Local gradient and perturbed gradient of ET k at round t
$l(\cdot)$	The loss function of the local training
C	The threshold to bound local gradients
$\epsilon_k^{(t)}$	Privacy budget of the k-th ET at the round t
$\Delta f_k^{\mathcal{T}_k^{(t)}}, \Delta f_{\mathrm{D}}^{\mathcal{T}_k^{(t)}}$	Sensitivity of ET k in model uploading and distribution
$\mathcal{M}_k$	The privacy mechanism for the k-th ET
$\mathcal{S}_{\mathcal{M}_k}$	The possible output set of the privacy mechanism $\mathcal{M}_k$
$\mathcal{L}(\mathbf{0}, \lambda_k \boldsymbol{I}_d)$	The complex Laplace distribution
$V_k^{(t)}$	Evaluated value of the trained model of ET k at round t
$U_k^{(t)}$	Energy utility of the ET k at round t
Q_t	Budget for the t-th round FL model training
$\mathcal{S}_{k\in\mathcal{P}^t}^{(t)}$	Strategy space of the k-th ET at round t
$\boldsymbol{s}^{*(t)}$	The optimal strategy for all ETs at round t

A. Federated Energy Security Protection Scheme

To protect the energy security of the EH system and mitigate the isolated data issue, we propose the FL-enabled energy security protection scheme. The details of the proposed scheme are presented as follows:

1) Registering in the proposed system: ET and EU nodes willing to participate in the federated energy security protection scheme should first register in the system to obtain legal identities, including public keys, private keys, certificates, and some initial stakes, i.e. (P_i, K_i, C_i, S_i).

2) Model training of the federated malicious energy user detection : ETs who intend to do training tasks download the initial model from the server. Then, energy security protection model training is performed by ETs based on all or part of their local dataset. To avoid sensitive information leakage, ETs perturb the trained local FL models with controllable DP-based noise. After that, ETs sign the privacy-preserving trained FL model with their private key and upload them to the server. The server collects these uploads, verify the validity of their signatures, and aggregates the valid FL models.

3) Energy security detection and protection: The server distributes the updated energy security model to each participant and rewards them based on the quality of their uploaded models. ET nodes decide whether EUs in their range are malicious based on EUs' history energy behaviors and current energy status. If one EU is judged as malicious, a certain amount of its stakes will be deduced. Once the EU's stakes are lower than a preset threshold, its behavior will be restricted, e.g. its energy requests will not be responded to by the ETs.

The federated malicious energy user detection is the critical part of our proposed energy security protection scheme. We suppose the total number of ET nodes in the proposed federated scheme is N and there are T training rounds in total. For the round $t \in \{1, 2, \cdots, T\}$, $K_t (K_t \leq N)$ ET nodes participate in the training, which is represented as $\mathcal{P}^{(t)} = \{p_1^{(t)}, p_2^{(t)}, \cdots, p_{K_t}^{(t)}\}$. The dataset of the k-th ET in $\mathcal{P}^{(t)}$ is denoted as $\mathcal{D}_k, k = 1, 2, \cdots, K_t$. Each sample s_i of the dataset includes energy features of ETs and EUs. To have a comprehensive understanding of EH nodes, the designed energy features consist of instant and relative features. The instant energy features reflect the instant status of energy harvesting, store, and transfer, including *total energy harvesting of the ET* $e_{\mathrm{TH}}^{(i)}$, *total energy transferring of the ET* $e_{\mathrm{TT}}^{(i)}$, *current energy status of the ET* $e_{\mathrm{S}}^{(i)}$, *energy transferred to the EU* $\boldsymbol{e}_{\mathrm{TU}}^{(i)}$, and *current status of the EU* $\boldsymbol{e}_{\mathrm{SU}}^{(i)}$. The relative features designed in our scheme are the ratios calculated based on the observed instant features, namely *energy transfer to harvesting ratio* $\boldsymbol{e}_{\mathrm{TU}}^{(i)}/e_{\mathrm{TH}}^{(i)}$, *energy transfer ratio* $\boldsymbol{e}_{\mathrm{TU}}^{(i)}/e_{\mathrm{TT}}^{(i)}$, *energy storage ratio* $\boldsymbol{e}_{\mathrm{SU}}^{(i)}/e_{\mathrm{S}}^{(i)}$, and *energy delivery ratio* $e_{\mathrm{TT}}^{(i)}/e_{\mathrm{TH}}^{(i)}$. These relative features are more robust against the dynamic environment of the EH system. The designed instant and relative energy features reflect the status and behaviors of EH nodes in multiple dimensions, which can be utilized to detect malicious EUs who perform abnormal energy requests.

At the beginning of each round t, ETs download the initial weights $\boldsymbol{w}^{(t)} \in \mathbb{R}^d$ from the server and initialize their network with these weights. For the k-th ET in $\mathcal{P}^{(t)}$ at round t, training data $\mathcal{T}_k^{(t)}$ is selected from its collected dataset $\mathcal{D}_k$, i.e. $\mathcal{T}_k^{(t)} \subseteq \mathcal{D}_k$. The ET trains the detection model based on $\mathcal{T}_k^{(t)}$ and $\boldsymbol{w}^{(t)}$, and obtains the local gradient as follows:

$$\boldsymbol{g}_k^{(t)} = \frac{1}{|\mathcal{T}_k^{(t)}|} \sum_{i=1}^{|\mathcal{T}_k^{(t)}|} \boldsymbol{g}_{k,i}^{(t)} = \frac{1}{|\mathcal{T}_k^{(t)}|} \sum_{i=1}^{|\mathcal{T}_k^{(t)}|} \nabla_{\boldsymbol{w}} l(\boldsymbol{w}^{(t)}, s_i), \quad (1)$$

where $l(\cdot)$ is the loss function, and $|\mathcal{T}_k^{(t)}|$ is the size of the selected dataset $\mathcal{T}_k^{(t)}$. During the local model training, clipping technology is used to bound gradients $\boldsymbol{g}_{k,i}^{(t)}$ with threshold value C, that is, $\|\boldsymbol{g}_{k,i}^{(t)}\| \leq C$.

After training the malicious energy user detection model locally, ETs can perturb their models via DP technology, which will be discussed in detail in subsection IV-B. The perturbed detection models are uploaded to the server. The server verifies the signature of the gradients packet and aggregates the valid gradients to update model weights. The aggregated model parameter of the t-th round is expressed as follows:

$$\boldsymbol{w}^{(t+1)} = \boldsymbol{w}^{(t)} - \alpha_t \sum\nolimits_{k=1}^{K_t} p_k \boldsymbol{g}_k^{(t)}, \quad (2)$$

where α_t is the learning rate of round t. p_k is the weight coefficient of the k-th ET for model training, and $p_k = 0$ if the gradients of k-th ET are not verified. After the model aggregation, the server distributes the updated model to each legally participating ET to detect malicious energy consumption, thereby protecting energy security.

B. DP-based Information Privacy Preservation

Although the proposed federated energy security protection scheme mitigates the isolated data problem, adversaries can extract sensitive information of the participated ETs via analyzing the uploaded model parameters [9], [10]. The datasets of ETs include their own energy status and energy data from

other ETs and EUs, which are privacy-sensitive and profit-sensitive. With the excellent characters of privacy preservation, DP is utilized to perturb the model parameters before uploading to the server, thereby realizing information preservation.

For the k-th ET in $\mathcal{P}^{(t)}$ and its privacy budget $\epsilon_k^{(t)}$ at round t, the privacy mechanism $\mathcal{M}_k$ satisfies $\epsilon_k^{(t)}$-DP for any two adjacent datasets $\mathcal{T}_k^{(t)}$ and $\mathcal{T}_k^{'(t)} \subseteq \mathcal{D}_k$, any $\mathcal{S}_{\mathcal{M}_k} \subseteq \mathcal{S}_k$ (the possible output set of $\mathcal{M}_k$), if

$$\Pr[\mathcal{M}_k^{\mathcal{T}_k^{(t)}}(\boldsymbol{g}_k^{(t)}) \in \mathcal{S}_{\mathcal{M}_k}] \leq e^{\epsilon_k^{(t)}} \cdot \Pr[\mathcal{M}_k^{\mathcal{T}_k^{'(t)}}(\boldsymbol{g}_k^{(t)}) \in \mathcal{S}_{\mathcal{M}_k}]. \quad (3)$$

The DP protection mechanism with smaller budget privacy introduces more noise and provides stronger protection, whereas model availability is reduced. Since the local gradients of FL model are numerical data, the most common popular method to obtain $\epsilon_k^{(t)}$-DP is adding Laplace noise which has been utilized in multiple applications [30]. The perturbed local gradient of the k-th ET at round t is expressed as follows:

$$\tilde{\boldsymbol{g}}_k^{(t)} = \mathcal{M}_k^{\mathcal{T}_k^{(t)}}(\boldsymbol{g}_k^{(t)}) = f(\boldsymbol{g}_k^{(t)}) + \boldsymbol{n} = \boldsymbol{g}_k^{(t)} + \boldsymbol{n}, \quad (4)$$

where $\boldsymbol{n} \sim \mathcal{L}(\boldsymbol{0}, \lambda_k \boldsymbol{I}_d)$ is the Laplace noise component. $\boldsymbol{I}_d$ is the $d \times d$ identity matrix. $\lambda_k = \frac{\Delta f_k}{\epsilon_k}$ and Δf_k is the sensitive function of f which is expressed as

$$\begin{aligned} \Delta f_k^{\mathcal{T}_k^{(t)}} = \max_{\mathcal{T}_k^{(t)}, \mathcal{T}_k^{'(t)}} \| & \frac{1}{|\mathcal{T}_k^{(t)}|} \sum\nolimits_{i=1}^{|\mathcal{T}_k^{(t)}|} \nabla_{\boldsymbol{w}} l(\boldsymbol{w}^{(t)}, s_i) \\ & - \frac{1}{|\mathcal{T}_k^{'(t)}|} \sum\nolimits_{i=1}^{|\mathcal{T}_k^{'(t)}|} \nabla_{\boldsymbol{w}} l(\boldsymbol{w}^{(t)}, s_i) \| = \frac{2C}{|\mathcal{T}_k^{(t)}|}, \end{aligned} \quad (5)$$

where the two adjacent datasets $\mathcal{T}_k^{(t)}$ and $\mathcal{T}_k^{'(t)} \subseteq \mathcal{D}_k$ have the same size but only one sample is different. The sensitivity $\Delta f_k^{\mathcal{T}_k^{(t)}}$ in model uploading is only related to the clipping threshold C and the training dataset $|\mathcal{T}_k^{(t)}|$. As the size of the training dataset increases, the sensitivity decreases inversely.

After adding the DP noise, the k-th ET uploads the perturbed gradients $\tilde{\boldsymbol{g}}_k^{(t)}$ to the server with its signature. We suppose the datasets $\{\mathcal{D}_1, \mathcal{D}_2, \cdots, \mathcal{D}_{K_t}\}$ of K_t ETs in $\mathcal{P}^{(t)}$ are disjoint and $\mathcal{D}^{(t)} = \mathcal{D}_1 \cup \mathcal{D}_2 \cup \cdots \cup \mathcal{D}_{K_t}$. Based on the parallel composition of DP [31], if the privacy mechanism $\mathcal{M}_k$ satisfies $\epsilon_k^{(t)}$-DP for $k = 1, 2, \cdots, K_t$, the global privacy mechanism of all updated models satisfies $\max(\epsilon_k^{(t)})$-DP and $\Delta f^{\mathcal{D}^{(t)}} = \max(\Delta f_k^{\mathcal{T}_k^{(t)}})$.

With the $\epsilon_k^{(t)}$-DP mechanism, the aggregation of the updated models in (2) can be represented as $\boldsymbol{w}^{(t+1)} = \boldsymbol{w}^{(t)} - \alpha_t \sum_{k=1}^{K_t} p_k \tilde{\boldsymbol{g}}_k^{(t)}$ by replacing $\boldsymbol{g}_k^{(t)}$ with $\tilde{\boldsymbol{g}}_k^{(t)}$. We discuss the privacy preservation for the k-th ET in the distribution of the updated model to all participants. Let $f_{\mathrm{D}}^{\mathcal{T}_k^{(t)}} = \boldsymbol{w}^{(t)} - \alpha_t \sum_{k=1}^{K_t} p_k \tilde{\boldsymbol{g}}_k^{(t)}$, and its sensitivity can be expressed as

$$\begin{aligned} \Delta f_{\mathrm{D}}^{\mathcal{T}_k^{(t)}} &= \max_{\mathcal{T}_k^{(t)}, \mathcal{T}_k^{'(t)}} \| f_{\mathrm{D}}^{\mathcal{T}_k^{(t)}} - f_{\mathrm{D}}^{\mathcal{T}_k^{'(t)}} \| \\ &= \max_{\mathcal{T}_k^{(t)}, \mathcal{T}_k^{'(t)}} \| \alpha_t p_k (\tilde{\boldsymbol{g}}_k^{(t)}[s_k^{'(t)}] - \tilde{\boldsymbol{g}}_k^{(t)}[s_k^{(t)}]) \| \\ &= \alpha_t p_k \Delta f_k^{\mathcal{T}_k^{(t)}} = \frac{2\alpha_t p_k C}{|\mathcal{T}_k^{(t)}|}. \end{aligned} \quad (6)$$

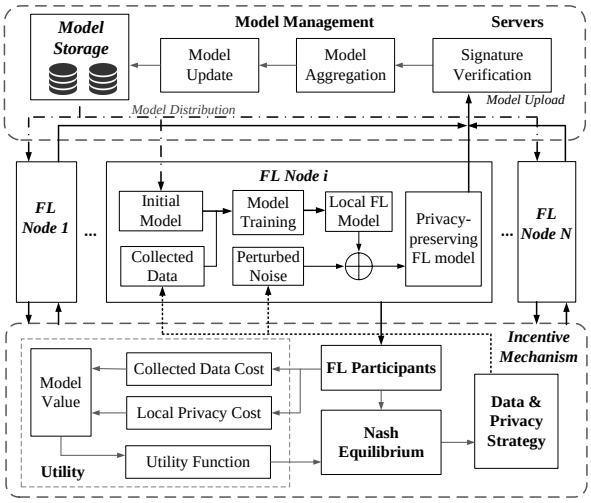


Fig. 3. Joint protection of energy security and information privacy with incentive mechanism.

where $s_k^{(t)}$ and $s_k^{'(t)}$ are the different samples of $\mathcal{T}_k^{(t)}$ and $\mathcal{T}_k^{'(t)}$. The sensitivity $\Delta f_{\mathrm{D}}^{\mathcal{T}_k^{(t)}}$ during the model distribution is proportional to $\Delta f_k^{\mathcal{T}_k^{(t)}}$ by factor $\alpha_t p_k$, which is consistent with the aggregation operation of the updated models. Note that, adding DP noise in the gradients of the training model is equivalent to adopting regularization, which can avoid the overfitting of models. Thus, the DP-empowered information privacy preservation in model training is feasible.

V. Proposed Incentive Mechanism

The non-cooperative game-enabled incentive mechanism is proposed in this section. The designed incentive mechanism plays a critical role in the joint protection of energy security and information privacy in the following aspects. First, ET nodes are selfish and unwilling to share their learning resource (e.g. data, computing, and communication resource) without proper profits. The proposed incentive mechanism encourages the participation of ETs in the federated model training via rewards. Secondly, in the proposed joint protection scheme, some ETs may choose to upload low-quality trained models under the consideration of data privacy or computing resource. The proposed incentive mechanism derives the optimal training strategy for all ETs, which simulates high-quality learning behaviors of ETs. As shown in Fig. 3, the proposed incentive mechanism calculates the optimal data and privacy strategy based on the model value and energy utility. Under the guidance of the optimal strategy, ETs allocate corresponding data resources for model training and add proper-level noise before uploading the models. The server aggregates and distributes the updated models for the joint energy-information security.

A. Model Evaluation and Energy Utility

The value of the uploaded privacy-preserving energy security detection models is evaluated by the server. We define the model value function with consideration of the following two aspects. On the one hand, the value of the model is related to the dataset size adopted for model training. More

samples in the training dataset lead to the higher quality of the trained model (e.g. accuracy). On the other hand, the value of the model is negatively correlated with the magnitude of the DP noise added by ETs. As the added noise increases, the reliability of the model decrease. Base on the above analysis and the marginal utility diminishing principle in economics, we define the evaluation function of the trained model as

$$V_k^{(t)} = 1 - e^{-\lambda \cdot |\mathcal{T}_k^{(t)}|^{\gamma_1} \cdot (\epsilon_k^{(t)})^{\gamma_2}}, \tag{7}$$

where $\lambda, \gamma_1, \gamma_2 > 0$ are coefficients of model evaluation. The evaluation function in (7) reflects that model value increases strictly with the rising dataset size $|\mathcal{T}_k^{(t)}|$ and privacy budget $\epsilon_k^{(t)}$. Besides, the defined evaluation function normalizes the model value into $[0, 1]$. If and only if the dataset size $|\mathcal{T}_k^{(t)}|$ or the privacy budget $\epsilon_k^{(t)}$ vanishes, model value tends to zero.

Then, we define the energy utility of each ET participating in the federated model training and there are two things taking into consideration: 1) *The reward from the server*. ETs who upload verified models can obtain rewards from the server according to the evaluated model values. For the privacy-preserving malicious energy user detection model, the total budget is Q and the budget for each round is $(Q_1, Q_2, \cdots, Q_T)$. The reward of the k-th ET in round t is expressed as $Q_t V_k^{(t)} / \sum_{i=1}^{K_t} V_i^{(t)}$. *2) The cost of ETs*. ETs' cost consists of two parts, i.e. data cost and privacy cost. The data cost is used by ETs to collect energy status and purchase data from other EH nodes, which is related to the dataset size. The privacy cost is paid for the information privacy leakage risks. Therefore, we design the energy utility of ETs as follows:

$$\begin{aligned} U_k^{(t)} &= Q_t \cdot \frac{V_k^{(t)}}{\sum_{i=1}^{K_t} V_i^{(t)}} - \beta_1 \cdot |\mathcal{T}_k^{(t)}| - \beta_2 \cdot \epsilon_k^{(t)} \\ &= \frac{Q_t \cdot (1 - e^{-\lambda \cdot |\mathcal{T}_k^{(t)}|^{\gamma_1} \cdot (\epsilon_k^{(t)})^{\gamma_2}})}{\sum_{i=1}^{K_t} 1 - e^{-\lambda \cdot |\mathcal{T}_i^{(t)}|^{\gamma_1} \cdot (\epsilon_i^{(t)})^{\gamma_2}}} - \beta_1 |\mathcal{T}_k^{(t)}| - \beta_2 \epsilon_k^{(t)}, \end{aligned} \tag{8}$$

where β_1 and β_2 are coefficients of the data and privacy cost, respectively.

B. Optimal Strategy in Non-Cooperative Game

All ETs participating in the model training are supposed to be independent and complete for the reward budget Q_t non-cooperatively. The goal of the ETs participating in the training of the detection model is to maximize their own energy utility. For $k \in \{1, 2, \cdots, K_t\}$, the optimization problem is formulated as follows:

$$\max_{|\mathcal{T}_k^{(t)}|, \epsilon_k^{(t)}} U_k^{(t)}(|\mathcal{T}_k^{(t)}|, \epsilon_k^{(t)}), \tag{9}$$

$$s.t. \quad |\mathcal{T}_k|_{\min} \le |\mathcal{T}_k^{(t)}| \le |\mathcal{T}_k|_{\max}, \tag{9a}$$

$$\epsilon_k^{\min} \le \epsilon_k^{(t)} \le \epsilon_k^{\max}, \tag{9b}$$

$$U_k^{\min} \le U_k^{(t)}. \tag{9c}$$

In (9), the object of the optimization problem is to maximize the energy utility of the ET subject to the training dataset size $|\mathcal{T}_k^{(t)}|$ and the privacy budget $\epsilon_k^{(t)}$. Constraint (9a) describes the range of training dataset size. Constraint (9b) is the limitation of the privacy budget. Constraint (9c) guarantees the minimum energy utility of ETs.

The optimization problem in (9) is not only related to the strategy of the k-th ET, but also has a relationship to the decisions of other participants. Thus, it is can be modeled as a non-cooperative game $\mathbb{G}^{(t)} =< \mathcal{P}^{(t)}, S_{k \in \mathcal{P}^{(t)}}^{(t)}, U_{k \in \mathcal{P}^{(t)}}^{(t)} >$, where $\mathcal{S}_{k \in \mathcal{P}^{(t)}}^{(t)}$ is the strategy space of ETs and

$$\begin{aligned} S_{k \in \mathcal{P}^{(t)}}^{(t)} = \{ & s_k^{(t)} = (|\mathcal{T}_k^{(t)}|, \epsilon_k^{(t)}) \mid \\ & |\mathcal{T}_k|_{\min} \le |\mathcal{T}_k^{(t)}| \le |\mathcal{T}_k|_{\max}, \epsilon_k^{\min} \le \epsilon_k^{(t)} \le \epsilon_k^{\max}, \forall k \in \mathcal{P}^{(t)} \}. \end{aligned} \tag{10}$$

Our goal is to find the optimal strategy for all ETs $\boldsymbol{s}^{*(t)} = (s_1^{*(t)}, s_2^{*(t)}, \cdots, s_{K_t}^{*(t)})$, which is defined as Nash equilibrium (NE). In NE, the strategy of each ET k is the best response to other ETs' choice, i.e. $U_k^{(t)}(s_k^{*(t)}, S_{-k}^{*(t)}) \ge U_k^{(t)}(s_k^{(t)}, S_{-k}^{*(t)})$, where $S_{-k}^{*(t)}$ is the best strategies of other ETs except k.

To solve the optimization problem in (9) for each ET, we should prove the unique existence of NE in the formulated problem first. The expression of (9) is continuous, and its gradient $\nabla U_k^{(t)}$ and Hessian matrix $H(U_k^{(t)})$ are expressed as:

$$\begin{aligned} \nabla U_k^{(t)} &= \frac{\partial U_k^{(t)}}{\partial s_k^{(t)}} = \left(\frac{\partial U_k^{(t)}}{\partial |\mathcal{T}_k^{(t)}|}, \frac{\partial U_k^{(t)}}{\partial \epsilon_k^{(t)}}\right) \\ &= \left(\frac{Q_t \cdot \mathcal{V}_{-k}^{(t)}}{(\mathcal{V}_{\mathcal{P}}^{(t)})^2} \cdot \frac{\partial V_k^{(t)}}{\partial |\mathcal{T}_k^{(t)}|} - \beta_1, \frac{Q_t \cdot \mathcal{V}_{-k}^{(t)}}{(\mathcal{V}_{\mathcal{P}}^{(t)})^2} \cdot \frac{\partial V_k^{(t)}}{\partial \epsilon_k^{(t)}} - \beta_2\right), \end{aligned} \tag{11}$$

where $\frac{\partial V_k^{(t)}}{\partial |\mathcal{T}_k^{(t)}|} = \lambda \gamma_1 |\mathcal{T}_k^{(t)}|^{(\gamma_1 - 1)} (\epsilon_k^{(t)})^{\gamma_2} e^{-\lambda |\mathcal{T}_k^{(t)}|^{\gamma_1} (\epsilon_k^{(t)})^{\gamma_2}}$ and $\frac{\partial V_k^{(t)}}{\partial \epsilon_k^{(t)}} = \lambda \gamma_2 |\mathcal{T}_k^{(t)}|^{\gamma_1} (\epsilon_k^{(t)})^{(\gamma_2 - 1)} e^{-\lambda |\mathcal{T}_k^{(t)}|^{\gamma_1} (\epsilon_k^{(t)})^{\gamma_2}}$, $\mathcal{V}_{\mathcal{P}}^{(t)} = \sum_{i \in \mathcal{P}^{(t)}} V_i^{(t)}$ is the sum of the model values of all ETs, and $\mathcal{V}_{-k}^{(t)} = \sum_{i \in \mathcal{P}^{(t)}, i \ne -k} V_i^{(t)}$ indicates the sum of model values except for the k-th ET.

$$H(U_k^{(t)}) = \begin{pmatrix} a[\frac{\partial^2 V_k^{(t)}}{\partial^2 |\mathcal{T}_k^{(t)}|} \mathcal{V}_{\mathcal{P}}^{(t)} - 2(\frac{\partial V_k^{(t)}}{\partial |\mathcal{T}_k^{(t)}|})^2] & a[\frac{\partial^2 V_k^{(t)}}{\partial |\mathcal{T}_k^{(t)}| \partial \epsilon_k^{(t)}} \mathcal{V}_{\mathcal{P}}^{(t)} - 2 \frac{\partial V_k^{(t)}}{\partial |\mathcal{T}_k^{(t)}|} \frac{\partial V_k^{(t)}}{\partial \epsilon_k^{(t)}}] \\ a[\frac{\partial^2 V_k^{(t)}}{\partial \epsilon_k^{(t)} \partial |\mathcal{T}_k^{(t)}|} \mathcal{V}_{\mathcal{P}}^{(t)} - 2 \frac{\partial V_k^{(t)}}{\partial \epsilon_k^{(t)}} \frac{\partial V_k^{(t)}}{\partial |\mathcal{T}_k^{(t)}|}] & a[\frac{\partial^2 V_k^{(t)}}{\partial^2 \epsilon_k^{(t)}} \mathcal{V}_{\mathcal{P}}^{(t)} - 2(\frac{\partial V_k^{(t)}}{\partial \epsilon_k^{(t)}})^2] \end{pmatrix}, \tag{12}$$

where $\frac{\partial^2 V_k^{(t)}}{\partial^2 |\mathcal{T}_k^{(t)}|} = \frac{\partial V_k^{(t)}}{\partial |\mathcal{T}_k^{(t)}|} (\frac{\gamma_1 - 1}{|\mathcal{T}_k^{(t)}|} - \lambda \gamma_1 |\mathcal{T}_k^{(t)}|^{(\gamma_1 - 1)} (\epsilon_k^{(t)})^{\gamma_2})$, $\frac{\partial^2 V_k^{(t)}}{\partial |\mathcal{T}_k^{(t)}| \partial \epsilon_k^{(t)}} = \frac{\partial^2 V_k^{(t)}}{\partial \epsilon_k^{(t)} \partial |\mathcal{T}_k^{(t)}|} = \frac{\partial V_k^{(t)}}{\partial |\mathcal{T}_k^{(t)}|} (\frac{\gamma_2}{\epsilon_k^{(t)}} - \lambda \gamma_2 |\mathcal{T}_k^{(t)}|^{\gamma_1} (\epsilon_k^{(t)})^{(\gamma_2 - 1)})$, $\frac{\partial^2 V_k^{(t)}}{\partial^2 \epsilon_k^{(t)}} = \frac{\partial V_k^{(t)}}{\partial \epsilon_k^{(t)}} (\frac{\gamma_2 - 1}{\epsilon_k^{(t)}} - \lambda \gamma_2 |\mathcal{T}_k^{(t)}|^{\gamma_1} (\epsilon_k^{(t)})^{(\gamma_2 - 1)})$, and $a = \frac{Q_t \mathcal{V}_{-k}^{(t)}}{(\mathcal{V}_{\mathcal{P}}^{(t)})^3}$. The Hessian matrix in (12) is a real symmetric matrix. Moreover, its first-order leading principle minor $|H_1(U_k^{(t)})| < 0$ and the second-order leading principle minor $|H_2(U_k^{(t)})| > 0$. Thus, $H(U_k^{(t)})$ is a negative definite matrix. Therefore, $U_k^{(t)}$ is a strictly concave function with respect to the strategy $s_k^{(t)}$. The formulated problem in (9) is the convex optimization problem. The strategy of ETs $S_{k \in \mathcal{P}^t}^{(t)}$ is limited by the bound of $|\mathcal{T}_k^{(t)}|$ and $\epsilon_k^{(t)}$, which is a nonempty and convex subset of $\mathbb{R}^n \times \mathbb{R}^n$. Thus, there is a unique NE in this formulated problem.

Since the determinant $|H(U_k^{(t)})| > 0$, the Hessian matrix is invertible. Therefore, Newton-Raphson iterative method can be utilized to find the unique NE $\boldsymbol{s}^{*(t)}$ of our proposed game. The detail of the Newton-Raphson iterative method is shown in Algorithm 1. This non-cooperative game-based incentive

Algorithm 1 Optimal strategies for energy security and information privacy based on Newton-Raphson iterative method

Input: Q_t, λ, $\mathcal{P}^{(t)}$, $\mathcal{D}_k$, $|\mathcal{T}_k|_{\min}$, $|\mathcal{T}_k|_{\max}$, $\epsilon_k^{\min}$, $\epsilon_k^{\max}$, $U_k^{\min}$, $\forall k$
Output: $\boldsymbol{s}^{*(t)}, \boldsymbol{U}^{*(t)} = (U_1^{(t)}, U_2^{(t)}, \cdots, U_{K_t}^{(t)})$
Initialization: Convergence threshold ζ, iterater $i = 0$

Initialize strategies: $\boldsymbol{s}_1^{(t)} = (s_{1,1}^{(t)}, s_{1,2}^{(t)}, \cdots, s_{1,K_t}^{(t)})$
repeat
  $i \leftarrow i + 1$
  for Each ET node $k \in \mathcal{P}^{(t)}$ **do**
    $|\mathcal{T}_{i,k}^{(t)}| \leftarrow \max(\min(|\mathcal{T}_{i,k}^{(t)}|, |\mathcal{T}_k|_{\max}), |\mathcal{T}_k|_{\min})$
    $\epsilon_{i,k}^{(t)} \leftarrow \max(\min(\epsilon_{i,k}^{(t)}, \epsilon_k^{\max}), \epsilon_k^{\min})$
    $s_{i,k}^{(t)} \leftarrow (|\mathcal{T}_{i,k}^{(t)}|, \epsilon_{i,k}^{(t)})$
  end for
  Calculate the energy utility of ETs $\boldsymbol{U}_i^{(t)}$ based on (8)
  Calculate the gradients of each ET based on (11):
    $\nabla \boldsymbol{U}_i^{(t)} \leftarrow (\nabla U_1^{(t)}, \nabla U_2^{(t)}, \cdots, \nabla U_{K_t}^{(t)})$
  Calculate the Hessian matrix of each ET based on (12):
    $\boldsymbol{H}_i^{(t)} \leftarrow (H_1^{(t)}, H_2^{(t)}, \cdots, H_{K_t}^{(t)})$
  Update the strategy of K_t ETs:
    $\boldsymbol{s}_{i+1}^{(t)} \leftarrow \boldsymbol{s}_i^{(t)} - [\boldsymbol{H}_i^{(t)}]^{-1} \nabla \boldsymbol{U}_i^{(t)}$
until $|\boldsymbol{s}_{i+1}^{(t)} - \boldsymbol{s}_i^{(t)}| \leq \zeta$ and $\boldsymbol{U}_i^{(t)} > [U_1^{\min}, U_2^{\min}, \cdots, U_k^{\min}]$
$\boldsymbol{s}^{*(t)} \leftarrow \boldsymbol{s}_i^{(t)}$, $\boldsymbol{U}^{*(t)} \leftarrow \boldsymbol{U}_i^{(t)}$

mechanism gives the optimal strategies of all ETs and guides them to select a suitable size of training dataset and privacy budget. This incentive mechanism attracts ETs participating in the construction of the joint energy-information protection and strikes a balance between protecting energy security and information privacy.

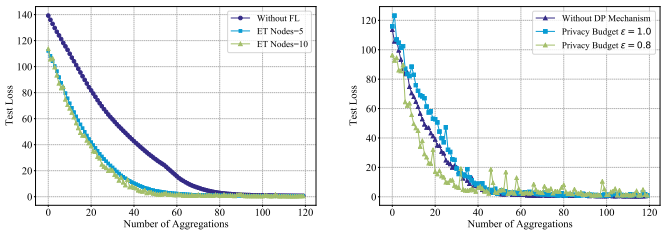
VI. Security Analysis and Empirical Study

A. Security Analysis

The security with respect to joint energy-information protection is discussed and analyzed. The proposed mechanism consists of three parties: ETs, EUs, and the server. Specifically, the ETs are considered trusted in this paper, whereas EUs are malicious-but-covert and the server is honest-but-curious.

For energy security, if an EU is compromised, its legitimate identity will be stolen, including the certificate and private key. The malicious EU uses the stolen legitimate identity to send forged energy demands to the nearby ET. Since the legal identity of the EU, these malicious demands cannot be detected by signature verification. In our proposed mechanism, this problem is addressed by the federated energy security protection scheme to detect and remove malicious EUs.

For information privacy, if the server is compromised, the uploaded information of ETs will be eavesdropped on by the attacker to infer their privacy. This threat can be easily addressed by adding some DP-based noise to preserve privacy. Besides, some ETs may have little contribution to the federated model but benefit more from others. For security fairness, the proposed incentive mechanism allocates the reward budget to ETs based on the value of their uploaded models. The ETs contributing more training data and adding less noise are given more rewards, which ensure fairness between ETs.



(a) (b)

Fig. 4. Convergence of the proposed mechanism: (a) Test loss of the energy security protection schemes, (b) test loss of the protection schemes with DP.

B. Experiment Setup

Our experiments are deployed on the hardware with 3.40GHz Intel Core i7-6700 CPU, 16G RAM, and 2T disk. The operating system is Linux Ubuntu 20.04 LTS and the simulations are conducted on Python 3.8. The parameters of the our experiments are set similarly to the previous studies [20], [29], [32], which are presented as follows:

1) Energy harvesting parameters: There are 10 ETs and 100 EUs distributed uniformly in a cell with the radius of $R = 100$m. We suppose these nodes are static and each EU requests and harvests energy from its nearest ET. The initial energy of ETs and EUs obey uniform distributions $\mathcal{U} \sim (50, 100)$mJ and $\mathcal{U} \sim (25, 50)$mJ, respectively. The amount of data that EUs need to process per time slot is distributed uniformly $\mathcal{U} \sim (250, 350)$kb and consume 0.01mJ to process 1kb data. At each slot, the amount of energy that ETs harvest from the environment distributes uniformly in $[50, 100]$mJ. Besides, the energy transfer efficiency between ETs and EUs is set as 0.7.

2) Federated energy-information security parameters: The dataset size of each ETs is 1500. The dataset for the performance test has 10000 samples. The federated model we applied for energy security is a multilayer feedforward neural network with dimensions $(9-30-20-2)$, which uses ReLU function for hidden layers and Softmax for the output layer.

C. Simulation Results

1) Convergence of the Proposed Mechanism: The convergence of our proposed federated energy security mechanism over the different number of ETs $K_t = \{5, 10\}$ is presented in Fig. 4, which is compared with the baseline without FL. From subfigure (a), we can see that along with the number of aggregations (i.e. training rounds), the test loss of the proposed schemes decreases and converges to a low value. Our proposed schemes converge faster than the baseline. Specifically, the proposed schemes with 5 and 10 ETs achieve low test loss when the number of aggregations increases to 60, whereas the baseline does not converge until the number of aggregations reaches 80. Subfigure (b) shows the test loss of the energy security protection schemes with DP, which demonstrates that the proposed schemes with DP-enabled noise still converge well although there are some fluctuations.

2) Performance of the Joint Protection Mechanism: The performance of the federated energy-information joint protection mechanism is evaluated from the following three aspects:

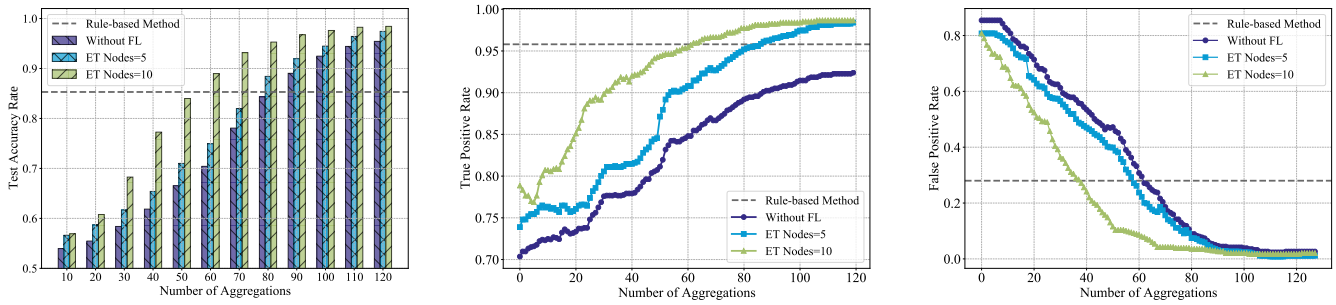


Fig. 5. Experimental results of the federated energy security detection scheme: (a) Test accuracy rate over number of aggregations, (b) true positive rate over number of aggregations, (c) false positive rate over number of aggregations.

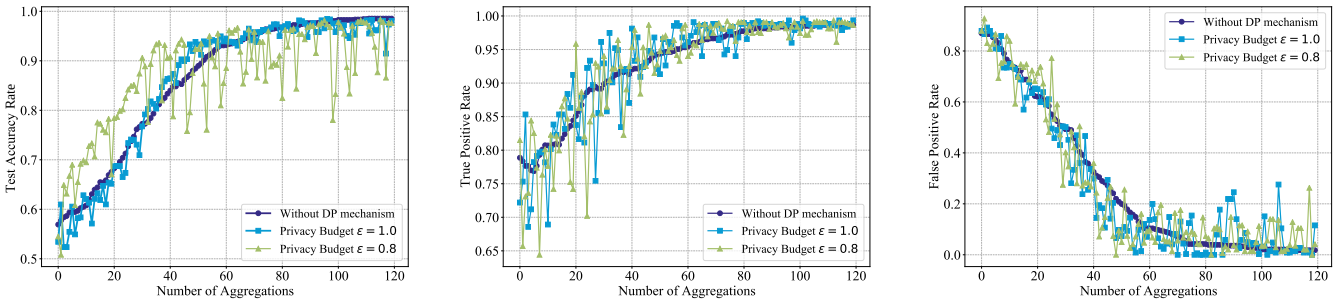


Fig. 6. Experimental results of the energy security detection with DP-enabled information privacy scheme: (a) Test accuracy rate over number of aggregations, (b) true positive rate over number of aggregations, (c) false positive rate over number of aggregations.

- *Test accuracy rate (TAR):* Ratio of the number of EUs accurately detected to the number of all EUs.
- *True positive rate (TPR):* Ratio between the amount of detected true malicious EUs and all actual malicious EUs.
- *False positive rate (FPR):* Ratio between the amount of detected false malicious EUs and all actual normal EUs.

We investigate the performance of the proposed federated energy security scheme by comparing it with the conventional rule-based method and the smart method without FL. As shown in Fig. 5 (a), with the rising number of aggregations, the TAR of our proposed scheme and the smart method without FL increases and converges to a high value. Compared with baselines, our proposed schemes achieve better performance and more ETs lead to higher accuracy over a particular number of aggregations. The performance of the TPR in Fig. 5 (b) displays the same trends as Fig. 5 (a). Our proposed schemes outperform the baselines in terms of TPR. As shown in subfigure (c), the FPR of our schemes declines to near zero as the number of aggregations increases, and schemes with more ETs converge faster. Compared with the conventional rule-based method, our proposed scheme can identify malicious users intelligently in the complex and dynamic EH system. Compared to the baseline without FL, our sheme utilizes FL to overcome the isolated data issue, thereby enhancing the detection model accuracy and energy security performance.

The performance of the proposed mechanism with information privacy preservation is shown in Fig. 6, comparing our scheme under various privacy budgets $\epsilon = \{0.8, 1.0\}$ with

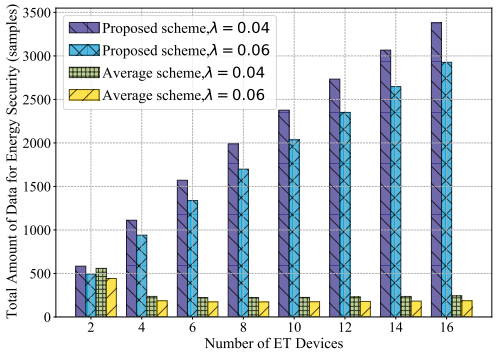


Fig. 7. Simulation results of the total amount of data used for model training.

the baseline scheme without DP. The TAR, TPR, and FPR are presented in subfigures (a), (b), and (c) respectively. The performance of the schemes with privacy preservation is a little worse than that without DP. A smaller privacy budget leads to more obvious fluctuation in terms of TAR, TPR, and FPR. The results show that our proposed DP-enabled scheme protects information privacy via adding noise to the gradients, which is equivalent to the regularization operation in model training without causing serious performance degradation.

We evaluate the performance of our proposed incentive mechanism in Fig. 7 and 8, which are compared to the average mechanism. The average mechanism performs the uniform budget for all participated ET, i.e. $\frac{Q_t}{K_t} = p \cdot V_k^{(t)}$, where p is the unit budget for the trained model. For the particular

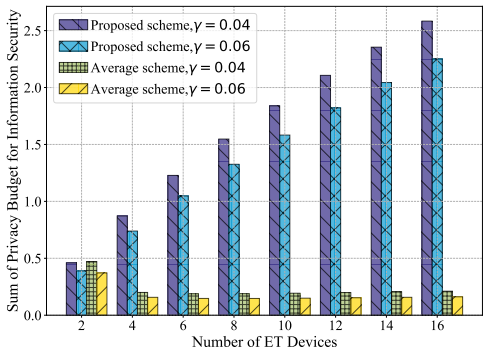


Fig. 8. Simulation results of sum of privacy budget for information privacy.

budget Q_t, we investigate the amount of the dataset size and privacy budget of all ETs for the federated energy security model training. We fix one of the above two variables to the optimal strategy value and evaluate the performance of another one. As shown in Fig. 7, our proposed mechanism encourages ETs to apply more data to the model training. On average, the total amount of data in our proposed scheme is 7.90 and 8.83 times higher than that of the baseline when $\lambda = 0.04$ and λ=0.06, respectively. Although the total amount of data in the average scheme is large when the number of ET is small, it declines as the number of ETs increases. Figure 8 presents the sum of privacy budget of our proposed incentive mechanism and the baseline without incentive. From these simulation results, we can see that the sum of privacy budget for information security in the proposed scheme is 7.00 and 7.90 times higher than that of the baseline when λ=0.04 and λ=0.06, respectively. Without the incentive mechanism, the sum of the privacy budget for information security decreases along with the number of ET devices. This means the ETs add more noise to the federated model, thereby leading to low model accuracy and poor performance for energy security. The experiments in Fig. 7 and Fig. 8 verify the effectiveness of our proposed non-cooperative incentive mechanism, which not only stimulates ETs to participant in the joint protection of energy and information, but also encourages them to contribute more data and add proper-level noise.

VII. Conclusion

In this paper, we proposed a joint protection mechanism of energy security and information privacy for EH, which integrates the FL and DP technologies to enhance system energy security while guaranteeing information privacy of EH nodes. In this proposed mechanism, we first discuss the framework of the joint energy-information protection including basic components and workflow. Next, we design the FL-based malicious energy user detection approach for energy security and devise a DP-enabled information privacy preservation scheme. Furthermore, a non-cooperative game-based incentive mechanism is proposed, which optimizes the utility of each ET, encourages their participation, and balance the joint energy-information security. Finally, experimental results verify the effectiveness of our proposed joint protection of energy security and information privacy for the EH. In the future, it is interesting to consider the mobility of EH nodes, e.g. the vehicle and UAV in the EH system. This demands the new energy security and information privacy protection mechanism accounting for the dynamic and adaptive.

References

[1] N. Hossein Motlagh, M. Mohammadrezaei, J. Hunt, and B. Zakeri, "Internet of Things (IoT) and the Energy Sector," *Energies*, vol. 13, no. 2, p. 494, 2020.

[2] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. Leung, and Y. L. Guan, "Wireless Energy Harvesting for the Internet of Things," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 102–108, 2015.

[3] J. Hu, J. Luo, Y. Zheng, and K. Li, "Graphene-Grid Deployment in Energy Harvesting Cooperative Wireless Sensor Networks for Green IoT," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1820–1829, 2019.

[4] T. J. Kazmierski and S. Beeby, *Energy Harvesting Systems*. Springer, 2014.

[5] D. Yao, M. Wen, X. Liang, Z. Fu, K. Zhang, and B. Yang, "Energy Theft Detection with Energy Privacy Preservation in the Smart Grid," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7659–7669, 2019.

[6] M. Zhang, J. Huang, and R. Zhang, "Wireless Power Transfer with Information Asymmetry: A Public Goods Perspective," *IEEE Transactions on Mobile Computing*, vol. 20, no. 1, pp. 276–291, 2019.

[7] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Security in Energy Harvesting Networks: A Survey of Current Solutions and Research Challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2658–2693, 2020.

[8] C. Huang, M. Ma, Y. Liu, and A. Liu, "Preserving Source Location Privacy for Energy Harvesting WSNs," *Sensors*, vol. 17, no. 4, p. 724, 2017.

[9] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, "Exploiting Unintended Feature Leakage in Collaborative Learning," in *2019 IEEE Symposium on Security and Privacy (S&P)*. IEEE, 2019, pp. 691–706.

[10] B. Hitaj, G. Ateniese, and F. Perez-Cruz, "Deep Models Under the GAN: Iinformation Leakage from Collaborative Deep Learning," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 603–618.

[11] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, 2020.

[12] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 1–19, 2019.

[13] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated Learning for Wireless Communications: Motivation, Opportunities, and Challenges," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 46–51, 2020.

[14] C. Dwork, "Differential Privacy: A Survey of Results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.

[15] P. Zhao, G. Zhang, S. Wan, G. Liu, and T. Umer, "A Survey of Local Differential Privacy for Securing Internet of Vehicles," *The Journal of Supercomputing*, pp. 1–22, 2019.

[16] C. Lin, Z. Song, H. Song, Y. Zhou, Y. Wang, and G. Wu, "Differential Privacy Preserving in Big Data Analytics for Connected Health," *Journal of medical systems*, vol. 40, no. 4, p. 97, 2016.

[17] U. Saleem, S. Jangsher, H. K. Qureshi, and S. A. Hassan, "Joint Subcarrier and Power Allocation in the Energy-Harvesting-Aided D2D Communication," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2608–2617, 2018.

[18] A. Ö. Ercan, M. O. Sunay, and I. F. Akyildiz, "RF Energy Harvesting and Transfer for Spectrum Sharing Cellular IoT Communications in 5G Systems," *IEEE Transactions on Mobile Computing*, vol. 17, no. 7, pp. 1680–1694, 2017.

[19] X. Lin, J. Wu, A. K. Bashir, J. Li, W. Yang, and J. Piran, "Blockchain-Based Incentive Energy-Knowledge Trading in IoT: Joint Power Transfer and AI Design," *IEEE Internet of Things Journal*, 2020.

[20] M. Min, L. Xiao, Y. Chen, P. Cheng, D. Wu, and W. Zhuang, "Learning-Based Computation Offloading for IoT Devices with Energy Harvesting," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1930–1941, 2019.

[21] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, 2018.

[22] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečnỳ, S. Mazzocchi, H. B. McMahan *et al.*, "Towards Federated Learning at Scale: System Design," *arXiv preprint arXiv:1902.01046*, 2019.

[23] S. Lee and D. H. Choi, "Federated Reinforcement Learning for Energy Management of Multiple Smart Homes with Distributed Energy Resources," *IEEE Transactions on Industrial Informatics*, 2020.

[24] Y. M. Saputra, D. T. Hoang, D. N. Nguyen, E. Dutkiewicz, M. D. Mueck, and S. Srikanteswara, "Energy Demand Prediction with Federated Learning for Electric Vehicle Networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[25] Y. Wang, I. L. Bennani, X. Liu, M. Sun, and Y. Zhou, "Electricity Consumer Characteristics Identification: A Federated Learning Approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3637–3647, 2021.

[26] C. Yin, J. Xi, R. Sun, and J. Wang, "Location Privacy Protection Based on Differential Privacy Strategy for Big Data in Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3628–3636, 2018.

[27] J. L. Raisaro, G. Choi, S. Pradervand, R. Colsenet, N. Jacquemont, N. Rosat, V. Mooser, and J. P. Hubaux, "Protecting Privacy and Security of Genomic Data in i2b2 with Homomorphic Encryption and Differential Privacy," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 15, no. 5, pp. 1413–1426, 2018.

[28] N. Wu, F. Farokhi, D. Smith, and M. A. Kaafar, "The Value of Collaboration in Convex Machine Learning with Differential Privacy," in *2020 IEEE Symposium on Security and Privacy (S&P)*, 2020, pp. 304–317.

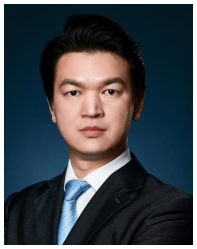
[29] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. S. Quek, and H. V. Poor, "Federated Learning with Differential Privacy: Algorithms and Performance Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3454–3469, 2020.

[30] M. Kim, O. Günlü, and R. F. Schaefer, "Federated Learning with Local Differential Privacy: Trade-Offs Between Privacy, Utility, and Communication," in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2021, pp. 2650–2654.

[31] C. Dwork, A. Roth *et al.*, "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2014.

[32] Q. Chen, H. Gao, Z. Cai, L. Cheng, and J. Li, "Energy-Collision Aware Data Aggregation Scheduling for Energy Harvesting Sensor Networks," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, 2018, pp. 117–125.

Qianqian Pan received her B.S. and M.S. degrees from the School of Information Science and Engineering, Southeast University, Nanjing, China, in 2015 and 2018, respectively. Now, she is pursuing the Ph.D. degree in the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. Her research interests include security and privacy of the next-generation network, machine learning, Internet of Things, and so on.



Jun Wu received the Ph.D. degree in information and telecommunication studies from Waseda University, Japan, in 2011. He is currently a professor of School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, China. He is also the vice director of National Engineering Laboratory for Information Content Analysis Technology, Shanghai Jiao Tong University, China. He is the chair of IEEE P21451-1-5 Standard Working Group. He has hosted and participated in lots of research projects including NFSC and JSPS. His research interests include the intelligence and security techniques of software-defined networks (SDN), information-centric networks (ICN) smart grids, Internet of Things (IoT), 5G/6G, etc., where he has published more than 170 refereed papers. He has been the Track Chair of VTC 2019/2020 and the TPC Member of more than ten international conferences including ICC, GLOBECOM, WINCON, etc. He is the Associate Editor of IEEE Networking Letters, IEEE Access, etc.

Ali Kashif Bashir is Reader at the Department of Computing and Mathematics, Manchester Metropolitan University, United Kingdom. He is also with Visual Research Intelligent Center, University of Electronics Science and Technology of China (UESTC) as an Honorary Professor and Chief Adviser; with University of Science and Technology, Islamabad (NUST) as an Adjunct Professor, and with University of Guelph, Canada as Special Graduate Faculty. He is a senior member of IEEE, member of IEEE Industrial Electronic Society, member of ACM, and Distinguished Speaker of ACM. He received his Ph.D. in computer science and engineering from Korea University, South Korea. He has authored over 200 research articles. His research interests include internet of things, wireless networks, distributed systems, network/cyber security, network function virtualization, machine learning, etc. He is serving as the Editor-in-chief of IEEE FUTURE DIRECTIONS NEWSLETTER, area editor of KSII TIIS, and associate editor of IEEE IoT Magazine, IEEE Access, etc.

Jianhua Li is a professor/Ph.D. supervisor and the dean of Institute of Cyber Science and Technology, Shanghai Jiao Tong University, Shanghai, China. He is also the director of National Engineering Laboratory for Information Content Analysis Technology and the director of Engineering Research Center for Network Information Security Management and Service of Chinese Ministry of Education. He got his BS, MS and Ph.D. degrees from Shanghai Jiao Tong University, in 1986, 1991 and 1998, respectively. He was the chief expert in the information security committee experts of National High Technology Research and Development Program of China (863 Program) of China. He was the leader of more than 30 state/province projects of China, and published more than 300 papers. He published 6 books and has about 20 patents. He got the Second Prize of National Technology Progress Award of China in 2005. His research interests include network security, data science, etc.

Wu Yang received the Ph.D. degree in computer system architecture from the Computer Science and Technology School, Harbin Institute of Technology. He is currently a Professor and a Doctoral Supervisor with Harbin Engineering University. His main research interests include wireless sensor networks, peer-to-peer networks, and information security. He is a member of ACM and a Senior Member of CCF.

Yasser D. Al-Otaibi received the Ph.D. degree in information systems from Griffith University, Brisbane, QLD, Australia, in 2018. He is currently an Assistant Professor with the Department of Information Systems, College of Computing and Information Technology in Rabigh, King Abdulaziz University, Rabigh, Saudi Arabia. His current research interests include the areas of adoption and acceptance of IT-based innovations by individuals and issues related to information systems continuance.