Decentralized Federated Learning Architecture for Networked Microgrids

Ilyes Naidji[1][a], Chams Eddine Choucha[2][b] and Mohamed Ramdani[3][c]

[1] *RLP laboratory, Mohamed Khider University of Biskra, Algeria*

[2] *LSSD laboratory, University of Science and Technology of Oran Mohamed-Boudiaf, Algeria*

[3] *Linfi laboratory, Mohamed Khider University of Biskra, Algeria*

Keywords: Federated Learning, Networked Microgrids, Decentralized Architecture, Energy Management.

Abstract: The expansion of large-scale distributed renewable energy drives the emergence of networked microgrids systems, necessitating the development of an efficient energy management approach to minimize costs and maintain energy self-sufficiency. The use of smart systems that are based on deep learning algorithms has become prevalent while addressing the energy management problem due to its real-time scheduling capabilities. However, training deep-learning algorithms requires substantial energy operation data from these microgrids, which raises concerns regarding privacy and data security when collecting data from various microgrids. To address this challenging problem, this article proposes a decentralized federated learning architecture for networked microgrids. The architecture incorporates a distributed federated learning (FL) mechanism to guarantee data privacy and security and prevent the system from signle point of failure. A decentralized networked microgrids model is constructed, where each participating microgrid has an energy management system responsible for managing its energy. The goal of the EMS is to minimize economic costs and maintain energy self-sufficiency. Initially, MGs independently undergo self-training using local energy operation data to train their individual models. Subsequently, these local models are regularly exchanged, and their parameters are aggregated to create a global model. This approach allows sharing of experiences among the microgrids without transmitting energy operation data, thereby safeguarding privacy and ensuring data security and preventing from single point of failure.

1 INTRODUCTION

Efficient energy management plays a crucial role in mitigating environmental impacts and addressing the growing demand for energy, even in the face of increasing energy consumption (Rehman et al., 2021). To achieve a balance between demand and supply, establish robust power infrastructure, optimize generation schedules, and minimize the repercussions of renewable energy production, a smart energy management should be addressed (Chouikhi et al., 2019), (Naidji et al., 2019). Utility providers can now measure and record energy usage for buildings or individual residences within an hour or less, thanks to advanced metering infrastructure and the widespread adoption of smart meters (Naidji et al., 2018). This technology has gained significant traction in the UK, where over 15 million smart meters are currently employed in homes and businesses. As a result for the large adoption for smart meters, different research work were published discussing the utilization of machine learning in smart grids (Massaoudi et al., 2021). The work in (Feng et al., 2020) detect real-time building occupancy from Advanced Metering Infrastructure (AMI) data based on a deep learning architecture. The developed deep learning model consists of a convolutional neural network (CNN) and a long short-term memory (LSTM) network. The simulation results show that the developed model outperforms the existing state-of-the-art ML classifiers and other deep learning architectures with around 90% occupancy detection accuracy.

A deep learning load prediction model is proposed in (Zhu et al., 2020). A daily time step-by-step load prediction method is employed where a deep cycle neural network (DCNN) model is established for the

[a] https://orcid.org/0000-0001-8747-0766

[b] https://orcid.org/0000-0003-0194-4890

[c] https://orcid.org/0000-0002-8723-5827

Naidji, I., Choucha, C. and Ramdani, M.
Decentralized Federated Learning Architecture for Networked Microgrids.
DOI: 10.5220/0012215200003543
In *Proceedings of the 20th International Conference on Informatics in Control, Automation and Robotics (ICINCO 2023) - Volume 1*, pages 291-294
ISBN: 978-989-758-670-5; ISSN: 2184-2809

total daily load and hourly load of users. The simulation results show the superiority of the proposed model.

The work in (Li et al., 2022) presents a novel approach for detecting FDIA (False Data Injection Attacks) by leveraging the concepts of federated learning, secure federated deep learning, and the Transformer model. The proposed method combines the multi-head self-attention mechanism of the Transformer, which is deployed as a detector in edge nodes, to explore the intricate relationships among individual electrical quantities. By adopting a federated learning framework, our approach allows collaborative training of a detection model using data from all nodes while ensuring data privacy by keeping the data locally during the training process. To enhance the security of federated learning, we have designed a secure federated learning scheme that incorporates the Paillier cryptosystem into the federated learning process.

The work proposed in (Jithish et al., 2023) introduces a smart grid anomaly detection scheme that utilizes Federated Learning (FL). The scheme involves training machine learning (ML) models locally within smart meters, without the need to share data with a central server. Initially, a global model is obtained from the server and deployed on the smart meters for on-device training. Following local training, the updated model parameters are transmitted to the server, contributing to the enhancement of the global model.

The work in (Wen et al., 2022) proposes a novel privacy-preserving federated learning framework for energy theft detection, namely, FedDetect. In this framework, the authors consider a federated learning system that consists of a data center (DC), a control center (CC), and multiple detection stations. In this system, each detection station (DTS) can only observe data from local consumers, which can use a local differential privacy (LDP) scheme to process their data to preserve privacy. To facilitate the training of the model, the authors design a secure protocol so that detection stations can send encrypted training parameters to the CC and the DC, which then use homomorphic encryption to calculate the aggregated parameters and return updated model parameters to detection stations. In this study, the authors prove the security of the proposed protocol with solid security analysis. To detect energy theft, a deep learning model based on the state-of-the-art temporal convolutional network (TCN) is designed.

However, none of the above studies consider the potential single point failure of the server which can block the entire process. To address this challenge, we propose a decentralized federated learning architecture for networked microgrids which consists of a decentralized model exchange and a decentralized aggregation model.

2 SYSTEM MODEL

2.1 Problem Formulation

Energy management in networked microgrids system requires a real-time control and monitoring of renewable energy sources which is intermittent and need to be predicted. For this reason, load forecasting and energy price forecasting should be addressed in order to reduce energy cost and improve energy availability.

2.2 Distributed Federated Learning

The optimization problem of federated learning for K devices can be formulated with objective function as follows:

$$min\, l(w) = \sum_{K=1}^{K} \frac{n_k}{n} L_k(w) \tag{1}$$

Where

$$L_k(W) = \frac{1}{n_k} \sum_{i \in p_k} l_i(w) \tag{2}$$

$l(w)$ is the loss function of the global model, $LK(x)$ is the loss of the kth device, and $l_i(w)$ is the loss for sample $i \in p_k$

Decentralized federated learning builds upon the principles of federated learning but takes the concept a step further by removing the need for a central server or coordinator. Instead, it distributes the model training process across multiple devices or entities in a peer-to-peer manner. This approach further enhances privacy and eliminates the single point of failure introduced by a central server.

Here's an overview of how decentralized federated learning works:

2.2.1 Network Formation

A network of microgrids is established in a decentralized manner. These microgrids can communicate with each other directly or through a peer-to-peer network infrastructure. Here in our case, we consider the mechanism of coalition formation between networked microgrids developped in (Naidji. et al., 2019), (Naidji et al., 2020). This mechanism allow the network to autonomously self organize in coalitions to achieve better performance in terms of energy exchange.

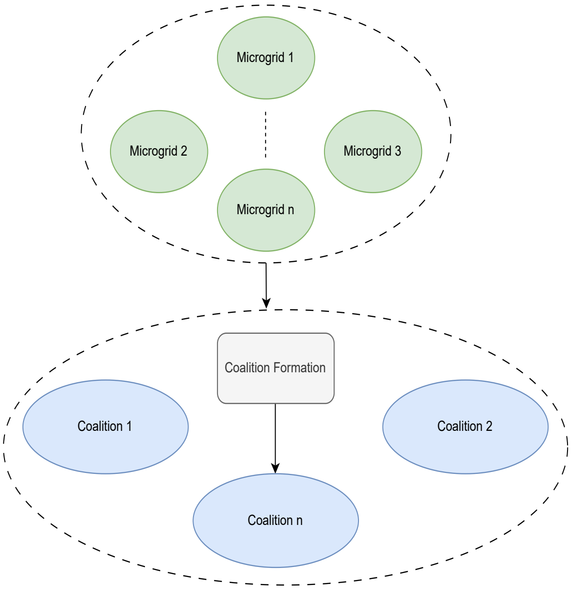

Figure 1: Network Formation.

Figure 1 shows the process of network formation which is based on an merge and split coalition formation algorithm (MSCF) proposed in (Naidji. et al., 2019). The microgrids autonomously self-organize in coalitions in order to achieve an optimal energy management. Note that, here in our case, decentralized federated learning is conducted for every coalition. The reason behind that is that microgrids belonging to the same coalition shares multiple features, and thus, sharing their learning models will bring more benefits for each one.

2.3 Model Initialization

Initially, each microgrid initializes its local model parameters, either randomly or based on a pre-trained model.

2.4 Local Model Training

Each microgrid independently trains its local model using its local data. This process is similar to traditional federated learning, where each device performs local computations on its data to update the model.

2.5 Model Exchange

After local training, microgrids exchange model updates with their neighboring microgrids. The exchange can be performed directly between microgrids or through a decentralized network infrastructure.

2.6 Model Aggregation

Each microgrid receives model updates from its neighbors and aggregates them with its own local model to create an updated model. The aggregation process can involve averaging the models. Here we use the decentralized federated averaging algorithm proposed in (Sun et al., 2021).

To begin, we provide a brief overview of the this algorithm. This algorithm follows the following steps:

1) Each microgrid, denoted as microgrid i, possesses an approximate copy of the parameters, $x(i)$.

2) Communication takes place among the microgrids. During this phase, microgrid i updates its local parameters, $x(i)$, by taking a weighted average of its neighboring microgrids' parameters. The updated value is denoted as $\overline{x}(i) = \sum_{l\in N(i)} w_{i,l}.x(l)$.

3) The training process starts. Microgrid i updates its parameters using the expression $x(i) = \overline{x}(i) - \alpha g(i)$, where α is a positive learning rate.

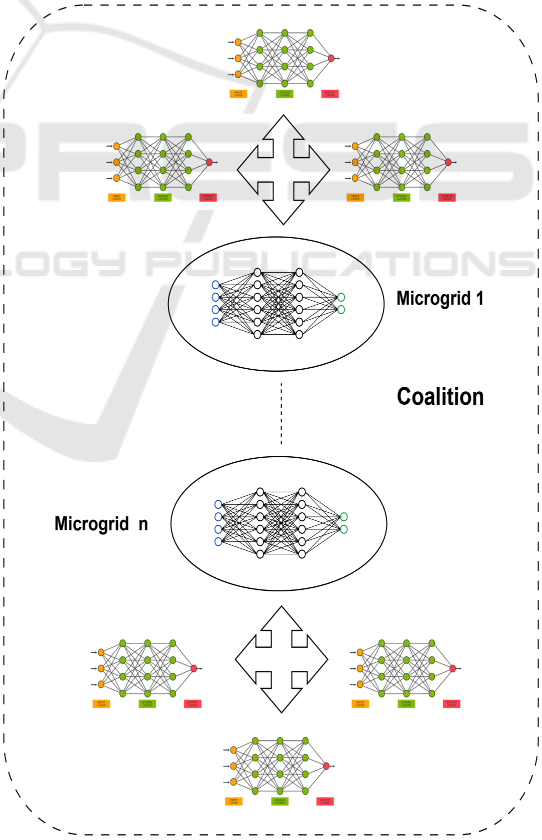

Figure 2: Model aggregation.

Figure 2 shows the process of model aggregation in each microgrid that belongs to a given coalition. The microgrid receives multiple model parameters that will be aggregated to form its final model.

2.7 Iterative Process

Steps 3-6 are repeated for multiple rounds or iterations. In each round, microgrids train their models locally, exchange model updates with neighbors, aggregate the updates, and broadcast their updated models.

2.8 Convergence

Over iterations, the models on each microgrid become more refined as they learn from the combined knowledge of neighboring microgrids. The decentralized federated learning process continues until the desired performance or convergence is achieved. Decentralized federated learning allows for collaborative model training across multiple microgrids in a peer-to-peer manner, without relying on a central server. It enables microgrids to exchange information directly with their neighbors, reducing latency and potential privacy risks associated with transmitting data to a central authority.

It's important to note that decentralized federated learning can take various forms depending on the specific network architecture, communication protocols, and consensus algorithms used. These aspects can vary based on the requirements and constraints of the decentralized system being implemented.

3 CONCLUSION

In this paper, we have proposed a decentralized federated learning architecture for networked microgrids system to improve energy management. The proposed architecture guarantees the data privacy and security of microgrids by exchanging only their models. Furthermore, the proposed decentralized architecture prevents from signle point of failure by eliminating the central server and exchanging models in a peer-to-peer manner.

REFERENCES

Chouikhi, S., Merghem-Boulahia, L., Esseghir, M., and Snoussi, H. (2019). A game-theoretic multi-level energy demand management for smart buildings. *IEEE Transactions on Smart Grid*, 10(6):6768–6781.

Feng, C., Mehmani, A., and Zhang, J. (2020). Deep learning-based real-time building occupancy detection using ami data. *IEEE Transactions on Smart Grid*, 11(5):4490–4501.

Jithish, J., Alangot, B., Mahalingam, N., and Yeo, K. S. (2023). Distributed anomaly detection in smart grids: A federated learning-based approach. *IEEE Access*, 11:7157–7179.

Li, Y., Wei, X., Li, Y., Dong, Z., and Shahidehpour, M. (2022). Detection of false data injection attacks in smart grid: A secure federated deep learning approach. *IEEE Transactions on Smart Grid*, 13(6):4862–4872.

Massaoudi, M., Abu-Rub, H., Refaat, S. S., Chihi, I., and Oueslati, F. S. (2021). Deep learning in smart grid technology: A review of recent advancements and future prospects. *IEEE Access*, 9:54558–54578.

Naidji, I., Ben Smida, M., Khalgui, M., Bachir, A., Li, Z., and Wu, N. (2019). Efficient allocation strategy of energy storage systems in power grids considering contingencies. *IEEE Access*, 7:186378–186392.

Naidji., I., Mosbahi., O., Khalgui., M., and Bachir., A. (2019). Cooperative energy management software for networked microgrids. In *Proceedings of the 14th International Conference on Software Technologies - ICSOFT*, pages 428–438. INSTICC, SciTePress.

Naidji, I., Mosbahi, O., Khalgui, M., and Bachir, A. (2020). Two-stage game theoretic approach for energy management in networked microgrids. In van Sinderen, M. and Maciaszek, L. A., editors, *Software Technologies*, pages 205–228, Cham. Springer International Publishing.

Naidji, I., Smida, M. B., Khalgui, M., and Bachir, A. (2018). Non cooperative game theoretic approach for residential energy management in smart grid. In *The 32nd Annual European Simulation and Modelling Conference*, pages 164–170, Ghent, Belgium.

Rehman, A. U., Hafeez, G., Albogamy, F. R., Wadud, Z., Ali, F., Khan, I., Rukh, G., and Khan, S. (2021). An efficient energy management in smart grid considering demand response program and renewable energy sources. *IEEE Access*, 9:148821–148844.

Sun, T., Li, D., and Wang, B. (2021). Decentralized federated averaging.

Wen, M., Xie, R., Lu, K., Wang, L., and Zhang, K. (2022). Feddetect: A novel privacy-preserving federated learning framework for energy theft detection in smart grid. *IEEE Internet of Things Journal*, 9(8):6069–6080.

Zhu, W., Zeng, Y., Kang, Z., and Fu, J. (2020). Deep learning based short term load prediction in smart grids. In *2020 IEEE 3rd International Conference on Electronic Information and Communication Technology (ICEICT)*, pages 674–678.