GR-77

A Robust Federated Machine Learning Framework for Security Analytics in Solar Farms

Abstract

Smart grids face more cyber threats than before with the integration of photovoltaic (PV) systems. Data-driven based machine learning (ML) methods have been verified to be effective in detecting attacks in power electronics devices. However, standard ML solution requires centralized data collection then processing that is becoming infeasible in more and more applications due to efficiency issues and increasing data privacy concerns. In this research, we propose a novel decentralized ML framework for detecting false data injection (FDI) attacks on solar PV DC/DC and DC/AC converters. The proposed paradigm incorporates the emerging technology named federated learning (FL) that enables collaboratively training across devices without sharing raw data. To the best of our knowledge, this work is the first application of FL for power electronics in the literature. Extensive experimental results demonstrate that our approach can provide efficient FDI attack detection for PV systems and aligned with the trend of critical data privacy regulations.

Introduction

With the rapid integration of renewable energy resources, such as solar photovoltaic (PV), power grids are encountering more challenges in defending against cyber-attacks [1], [2]. PV farms are controlled and connected to the grid via power electronics devices equipped with sensors that may frequently exchange information with control centers for monitoring and control purposes. This inevitably creates vulnerabilities in the power grid that adversaries can exploit, especially when the sensors lack tamper-resistance hardware.

Thus, there is a demand in developing a collaborative ML paradigm for attack detection in PVs without the need of sharing raw data. To close this gap, we propose a novel framework incorporating the concept of federated learning (FL) [3]. We use measurements from voltage and current sensors at the point of common coupling (PCC) to construct the ML model for detecting FDI attacks [4] on DC/DC and DC/AC converters in solar farms. Our design leverages the computational capacity of local sensors and decentralizes the computing tasks into devices near to where the raw data are generated. Compared with centralized ML implementation, our FL-based approach reduces the communication bandwidth consumption. Moreover, only the model parameters instead of the raw data are shared during the entire process.

Research Question(s)

1. How to use machine learning techniques to detect cyber attacks so that protect solar photovoltaic grid system?
2. Will federated learning technique train a good model without accessing the raw data?
3. How efficient will this federated learning framework be (in communication perspective)?

Materials and Methods

We propose a novel decentralized ML framework for detecting false data injection (FDI) attacks on solar PV DC/DC and DC/AC converters. The proposed paradigm incorporates the emerging technology named federated learning (FL) that enables collaboratively training across devices without sharing raw data. We use measurements from voltage and current sensors at the point of common coupling (PCC) to construct the ML model for detecting FDI attacks on DC/DC and DC/AC converters in solar farms。

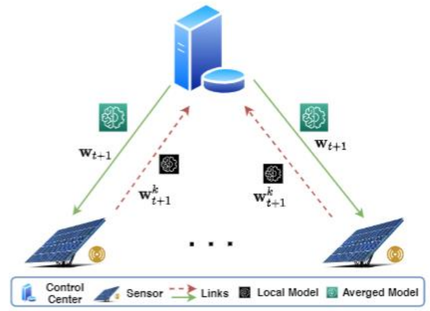

Fig. 1: The proposed FL framework for FDI attack detection

Our design leverages the computational capacity of local sensors and decentralizes the computing tasks into devices near to where the raw data are generated. In the proposed framework, as Figure 1 indicates, each sensor first learns a local model using its private data and then uploads its learned model parameters to the control center. Upon aggregating the local models from sensors, the control center fuses the local models and feeds the averaged model back to the sensors for the next round of updates. After iterating multiple rounds of local updating and global aggregation, the model training phase completes when convergence is reached. Finally, the trained model is deployed at sensors for FDI attack detection.

Results

We designed several experiments to prove the proposed method are feasible. The dataset we used are the current and voltage sensor readings of the DC/DC and DC/AC converters in solar farms, labeled with normal or attacked. To simulate the real-world situation, the experiments were conducted in both IID and Non-IID scenarios. 90% of the total data is used for training the local models, and the rest of 10% data is used for testing the global model.

Fig. 2: Training and testing losses of the LSTM model trained based on the proposed FL paradigm with four clients under (left) IID and (right) Non-IID data distributions.

Figure 2 demonstrates the loss value changes over each communication for the training and testing set under ID and Non-IID distributions, respectively. We can see that our proposed framework is convergent in all experiments. For the results of the IID scenario in Fig.2(left), the four clients show a similar convergence behavior as the ratios of abnormal/normal samples are close across the clients' local datasets, and each client learns the model comparably. Note that for the Non-IID situation in Fig.2(right), Client-0 learns slower than the other clients during the first few communications rounds.

Because Client-0's dataset has a relatively similar amount of abnormal and normal samples, it takes more time to train the local model compared to other clients to distinguish the two types of data. We observe that Client-0's loss value quickly approaches the same level of performance as the other clients when more communication rounds are carried out between the clients and the server.

Type	Accuracy	Precision	Recall	F1 Score
FL with IID	0.9750	0.9690	0.9613	0.9651
FL with Non-IID	0.9735	0.9566	0.9561	0.9606
Centralized	0.9768	0.9693	0.9646	0.9627

Table 1. Evaluation Results Comparison

Table 1. shows the evaluation results of the global model on the testing set under IID and Non-IID data distributions together with the centralized approach. We can see our approach archives the similar level performance with the centralized model.

Cost of one communication in FL	158,804 bytes (0.35%)
Cost of transferring the raw data	44,695,441bytes (100%)

Table 2. Communication Cost Comparison

We also tested the communication cost for the FL method and the centralized method. It is shown that the cost for transmitting the model weights is only 0.35% of sharing the raw data.

Conclusions

We proposed a new FL-based collaborative framework for FDI attack identification in PV systems. First, we analyzed the FDI attack in solar farms and presented a centralized ML solution for attack detection. Then, we incorporated the concept of FL and developed a decentralized approach for model training without sharing raw data. Experimental results verified that our paradigm significantly outperforms standard ML implementation in communication efficiency with preserving data privacy. Besides, our methodology is highly transferable and can be extended and customized for other privacy-centric power electronics applications.

Contact Information

Dr. Liang Zhao, lzhao10@kennesaw.edu

Jiaming Li, jli36@students.kennesaw.edu

References

[1] S. Sarangan, V. K. Singh, and M. Govindarasu, "Cyber attack-defense analysis for automatic generation control with renewable energysources," in2018 North American Power Symposium (NAPS), 2018, pp.1–6.

[2] F. Li, Q. Li, J. Zhang, J. Kou, J. Ye, W. Song, and H. A. Mantooth,"Detection and diagnosis of data integrity attacks in solar farms basedon multilayer long short-term memory network,"IEEE Transactions onPower Electronics, vol. 36, no. 3, pp. 2495–2498, 2021.

[3] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A.y Arcas, "Communication-Efficient Learning of Deep Networksfrom Decentralized Data," inProceedings of the 20th InternationalConference on Artificial Intelligence and Statistics, ser. Proceedingsof Machine Learning Research, A. Singh and J. Zhu, Eds., vol. 54.Fort Lauderdale, FL, USA: PMLR, 20–22 Apr 2017, pp. 1273–1282.[Online]. Available: http://proceedings.mlr.press/v54/mcmahan17a.html

[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacksagainst state estimation in electric power grids,"ACM Trans.Inf. Syst. Secur., vol. 14, no. 1, Jun. 2011. [Online]. Available:https://doi.org/10.1145/1952982.1952995

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Author(s) Jiaming Li
Advisors(s) Dr. Liang Zhao