Federated Learning Forecasting for Strengthening Grid Reliability and Enabling Markets for Resilience

Lucas PEREIRA[1] Vineet NAIR[2] Bruno DIAS[3] Hugo MORAIS[4]
Anuradha ANNASWAMY[2]

[1]ITI/LARSyS, IST, Portugal — [2]MIT, USA — [3]UFJF, Brazil — [4]INESC-ID, IST, Portugal

Abstract

We propose a comprehensive approach to increase the reliability and resilience of future power grids rich in distributed energy resources. Our distributed scheme combines federated learning-based attack detection with a local electricity market-based attack mitigation method. We validate the scheme by applying it to a real-world distribution grid rich in solar PV. Simulation results demonstrate that the approach is feasible and can successfully mitigate the grid impacts of cyber-physical attacks.

1. INTRODUCTION AND BACKGROUND

The variability and intermittency associated with wind and solar introduce more challenges to balance supply and demand and ensure reliable grid operation. In addition, increasing penetration of batteries, electric vehicles, and flexibilities introduces more complexity and uncertainty in net-load forecast [1]. Furthermore, a grid rich in Distributed Energy Resources (DERs) is more vulnerable to cyber-physical attacks. Various types of attacks on DER-rich power grids have been described in the literature [2], [3].

Uncertainties can impact several tasks needed in power systems, such as security assessment, operational planning, wholesale electricity markets, hosting capacity, and resiliency strategies. This can result in violations of technical operating constraints, non-compliance with market rules, imposing unnecessary limits on hosting capacity, or failure to identify attacks [4]. In this sense, accurate forecasting with uncertainty quantification is crucial to successfully detecting and mitigating these issues.

The Accurate federated Learning with uncertainty quantification for DER forecasting Applied to sMart Grids planning and Operation (ALAMO [5]) project focuses on developing technologies to manage power grids with high penetration of DERs while ensuring stakeholder privacy. It aims to create accurate forecasting algorithms based on Federated Learning (FL) and address challenges in quantifying epistemic and aleatoric uncertainties. The project will explore recent FL variations of client selection and model aggregation to enhance forecasting accuracy, which is currently inferior to traditional centralized models. Additionally, it aims to develop and benchmark uncertainty quantification methods, like Quantile-Regression and deep-model ensembles, to achieve sharp and well-calibrated uncertainty estimates.

With this paper, we aim to leverage the ALAMO project framework to show that by combining accurate probabilistic forecasts and uncertainty estimates with a market mechanism, we can enhance grid reliability during nominal operation and provide resilience to various cyber-physical attacks.

This paper details the proposed framework to include FL in the forecasting tasks and market mechanisms. A use case with a five-feeder real-world Low Voltage (LV) distribution network will be presented to demonstrate the feasibility of the proposed solution. The paper is organized as follows. We briefly overview FL in Section 1.1. We then describe the methodology in Section 2, including the FL-based attack detection and market-based attack mitigation. Section 3 presents the use case, datasets, FL forecasting implementation, and some simulation results. Finally, we summarize conclusions in Section 3 along with some ideas for future work.

1.1. Federated Learning

FL is a decentralized approach that enables collaborative training of machine learning models across distributed environments where data is stored locally on different organizational devices or systems. This method enhances privacy by ensuring that sensitive data remains on local devices, addressing privacy concerns inherent in centralized models. Additionally, FL improves model training efficiency and scalability by reducing storage costs and communication burden, as it transmits data wirelessly without needing a physical connection [6], [7]. FL is particularly beneficial in the energy systems domain, as it allows information from various network points to be used during training, resulting in more accurate predictions.

For example, for household demand forecasting, [8] and [9] both utilize FL with Long-Short Term Memory Network (LSTM) networks and the FedAvg aggregation method. These approaches have demonstrated efficient network resource use, reduced training time, and enhanced privacy preservation. Additionally, [10] explores FL with Convolutional Neural Network (CNN) and LSTM models, comparing various aggregation strategies, with FedAdagrad showing resilience against false data attacks. In the realm of PV production forecasting, [11] presents an FL model using a multi-layer perceptron, achieving high accuracy while ensuring data privacy. [12] integrates CNN and Gated Recurrent Unit (GRU) networks with FL and the Orchard Algorithm, resulting in superior prediction performance. [13] introduces a federated deep learning model for PV power generation, demonstrating robustness against cyber attacks and generalizability across regions.

2. METHODS

2.1. Using FL Forecasts to Identify Cyber Attacks

Cyber-physical attacks on power grids can broadly be classified into deception, disclosure, and disruption attacks that compromise integrity, confidentiality, and resource availability, respectively [14]. Here, we focus specifically on denial of service (DoS) disruption attacks that directly disconnect resources from the network.

In this work, the FL paradigm is used to obtain day-ahead forecasts of household demand and PV production in each individual prosumer in the grid. The forecasts are then used to identify attacks using a threshold-based method that leverages the individual forecast errors and the difference between the power import at the feeder (assuming that aggregated measurements are available) and the aggregation of the forecasts of the connected prosumers. On the one hand, by studying the forecast errors of demand and PV production in each prosumer, it is possible to identify any drastic deviations that occur only in particular nodes. On the other hand, it is possible to identify any unexpected deviations by comparing the power import at the feeder with the aggregated predictions on each feeder. This allows us to detect anomalies and flag whether an attack has occurred.

A few prior works have applied FL for anomaly detection [15] and the detection of other cyber attacks like false data injection [16]. However, to our knowledge, ours is the first work to combine the distributed FL approach with a distributed market structure for attack detection and mitigation and apply this to a truly DER-rich grid.

2.2. Local Electricity Markets

We leverage a hierarchical local electricity market (LEM) structure developed in our prior work [17]. The LEM is described in Fig. 1 and Fig. 2. In previous papers, we have applied this to provide grid services like voltage control [18] and enhance grid resilience to cyber-physical attacks [19]. Here, we combine this market with FL to detect and mitigate attacks on different assets in the grid. We focus only on the primary market in this work. Each node in the feeder represents a PM agent (PMA) and has a house with rooftop solar PV and loads connected to it. The PM for the entire feeder is overseen by a PM operator(PMO). After receiving flexibility bids from each PMAs, the PM is cleared by solving an alternating current optimal power flow (ACOPF) problem. Since the distribution network is 3-phase unbalanced and radial, we apply a current injection (CI)-based power flow model that captures all the grid physics [20]. The ACOPF minimizes line losses, generation costs, and disutility due to load flexibility. The problem is solved using a distributed optimization algorithm known as proximal atomic coordination [21].

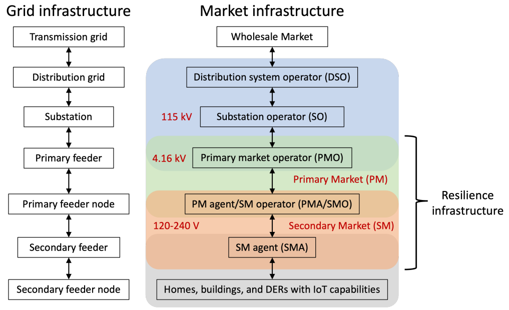

Figure 1: Overview of hierarchical LEM, with the PM and SM layers utilized for resilience.

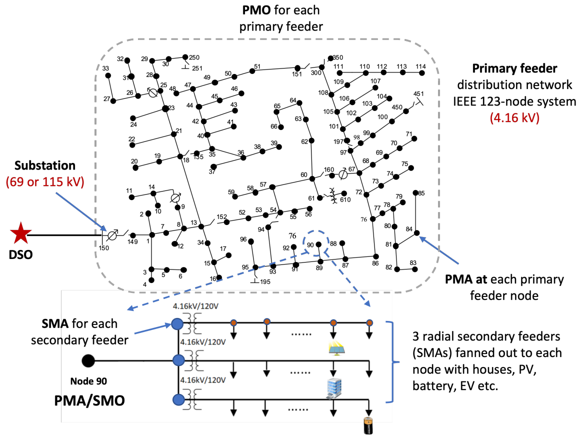
PMO for each primary feeder
Primary feeder distribution network IEEE 123-node system (4.16 kV)
Substation (69 or 115 kV)
DSO
PMA at each primary feeder node
SMA for each secondary feeder
Node 90
PMA/SMO
4.16kV/120V
4.16kV/120V
4.16kV/120V
3 radial secondary feeders (SMAs) fanned out to each node with houses, PV, battery, EV etc.

Figure 2: LEM co-located with distribution grid. This shows a primary and secondary feeder distribution network based on the modified IEEE-123 node test case.

2.3. Mitigation Approach Using Load Flexibility

After detecting an attack, the PMO raises a flag and commences mitigation efforts. It does so by comparing the actual meter reading with the attack ($\overline{\mathbf{P}}_{PCC}$) vs the forecasted value without the attack ($\mathbf{P}_{PCC}$) for the 3-phase net power injection at the substation or PCC (connected to the main grid via a tie line). It uses this information to update the cost coefficients for each of the terms in the objective function. The update rule is specified in Eq. (3). Note that we use hour-ahead forecasts for the power injections at a 1-minute resolution for the market operation.

$$\Delta = \mathbf{P}_{PCC} - \overline{\mathbf{P}}_{PCC} \tag{1}$$

$$Z_i\left(\delta_i\right) = 1 + \frac{RS_i \Delta^{\top} \delta_i}{\mu \sum_i RS_i} \Longrightarrow \gamma_{i\delta} = \frac{1}{Z_i\left(\delta_i\right)} \tag{2}$$

$$\overline{\alpha}_i = \gamma_{i\alpha}\alpha_i, \quad \overline{\beta}_i = \gamma_{i\beta}\beta_i, \quad \overline{\xi} = \left(\frac{\sum_i \gamma_{i\alpha} + \gamma_{i\beta}}{2n}\right)^{-1} \xi \tag{3}$$

α_i, β_i are 3×1 vectors representing cost and disutility coefficient for each phase at SMO node i, and ξ is a 3-phase hyperparameter that penalizes line losses in the objective function. A distributed generation attack that increases net load would result in $|\overline{\mathbf{P}}_{PCC}| > |\mathbf{P}_{PCC}|$ and $\gamma_{i\alpha}, \gamma_{i\beta} < 1$ and $\overline{\xi} < \xi$. By artificially lowering local generation costs and load disutility parameters, along with penalizing line losses more heavily, this update results in a dispatch that favors more local DER generation and load flexibility instead of relying on transmission imports. A key difference here is that the PRM also takes into account the RS of each SMO during the redispatch so that it relies more heavily on resilient SMOs for attack mitigation. Note that the PMO also accounts for the resilience scores (RS) of the PMAs while updating the coefficients, so as to rely more heavily on more resilient and reliable PMAs to provide flexibility during attack mitigation [22]. The PMO updates the new coefficients α_i', β_i' and ξ', and sends these to all the PMAs. The PM is then re-dispatched by solving the ACOPF again to assign new set points to the PMAs.

3. SIMULATION CASE STUDY

3.1. Low Voltage Distribution Grid

The simulation was conducted considering a real-world Low Voltage (LV) distribution network in Madeira Island. The secondary substation that feeds this network has a transformer with an apparent power of 250 kVA, connected in delta-wye, which transforms voltage from the transmission grid (6600 V) to the distribution grid (400 V) [23]. This radial LV network has 88 nodes connected through 87 lines. The system was originally modeled using DIgSILENT PowerFactory [24], from which the admittance matrix was later calculated.

3.2. Consumption and PV Production Data

Since the actual measurements are unavailable for each node, we relied on consumption and production data from 12 prosumers from Madeira Island. This data was collected during the Horizon 2020 SMILE project and is available at 1 sample per minute (1/60 Hz) [25]. Moreover, each of the 88 nodes in the LV grid is assumed to correspond to a single-phase prosumer. The consumption and PV production profiles were randomly assigned to one phase in each node. We synthetically generated PMA flexibility bids at each node by randomly assigning downward flexibilities between 20-40% to each.

3.3. Federated Forecasting

For the federated forecasting, we relied on the FLOWER framework[1] and the FPSeq2Quant probabilistic forecasting algorithm [23]. The models were trained with one year of data for each of the 12 prosumers using a time-series split cross-validation with an expanding training window. The model averaging was performed using the standard Federated Averaging [26]. More precisely, four federated forecasting models were trained: 1) day-ahead demand, 2) day-ahead PV production, 3) hour-ahead demand, and 4) hour-ahead PV production. The day-ahead forecasts were developed considering 15-minute aggregated values, whereas the hour-ahead forecasts consider samples every 1 minute.

3.4. Experiments and Results

We simulated the LEM over a 24-hour period. We considered that the attack occurs in the middle of the day (12:30 pm) during the period of peak PV output to maximize attack impact. In our case study, we considered that all the rooftop PV generation units have been attacked and shut down. These can be taken offline by hacking the smart inverters that connect these assets to the grid. For simplicity, we only show results for an instant period of time during the attack period.

Fig. 3 shows the PV generation over all 88 nodes before the attack. After the attack, this reduces to zero. This is a total loss of 100% of generation. This increases the power import at the feeder from the main grid. As seen in Fig. 4, the feeder exports power to the grid on phase A before the attack. However, after the attack, all 3 phases draw power from the grid, and the total net-load increases from 5.4 kW to 47.2 kW. The PMO then applies the update-based mitigation by leveraging load flexibility. The distribution of load curtailment across all the PMA nodes is shown in Fig. 5. Thus, we reduced the power import to about 29 kW, closer to the level without the attack. However, due to the relatively large scale of the attack and limiting power flow network constraints, we cannot fully resolve it even after utilizing most of the load flexibility available. Thus, the power import is still higher than before but about 40% lower than the case without mitigation. This ensures we minimize the distribution grid attack's impact on the larger transmission grid. This can help prevent more widespread impacts like frequency instability and cascading failures.

[1] `https://flower.ai/`

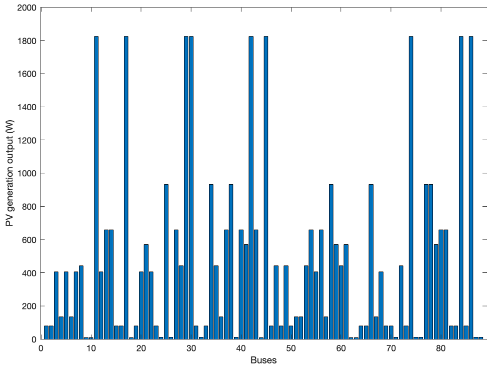

Figure 3: PV generation before the attack.

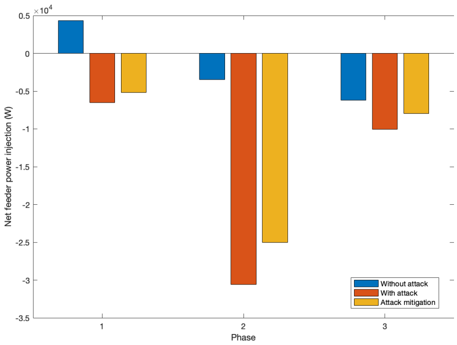

Figure 4: Net total feeder power injection (3-phase).

4. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed a method integrating federated learning with local energy markets to detect and mitigate cyber-physical attacks to DER-rich LV networks.

Still, several challenges must be addressed to advance this work, especially concerning training such FL models. In this sense, efficient communication is crucial because federated networks with many local devices can be slower than local computing. Additionally, the statistical heterogeneity of data from different devices increases delays in data processing, complicating modeling, analysis, and assessment [27], [28]. We aim to tackle these issues and improve our FL models and workflows in future work.

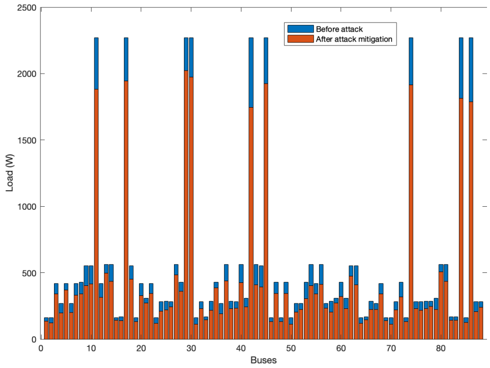

Figure 5: Distribution of load curtailment across nodes.

We will also explore more sophisticated attack detection approaches beyond our simple threshold-based method. Finally, we will make our market operation more realistic by also incorporating forecast uncertainty (for both PV and load) into the problem through approaches like robust optimization, stochastic programming and/or chance constraints.

ACKNOWLEDGEMENT

FCT supports this work through projects 10.54499/2022.15771.MIT; 10.54499/LA/P/0083/2020, 10.54499/UIDP/50009/2020, 10.54499/UIDB/50009/2020, and grant 10.54499/CEECIND/01179/2017/CP1461/CT0020 (LP).

CIRED Workshop on Resilience of Electric Distribution Systems, Chicago, November 7-8, 2024, Paper n° 118

References

[1] P. Denholm, M. O'Connell, G. Brinkman, and J. Jorgenson, "Overgeneration from Solar Energy in California. A Field Guide to the Duck Chart," National Renewable Energy Lab. (NREL), Golden, CO (United States), Tech. Rep. NREL/TP-6A20-65023, Nov. 2015. DOI: `10.2172/1226167`.

[2] S. Soltan, P. Mittal, and H. V. Poor, "{Blackiot}:{iot} botnet of high wattage devices can disrupt the power grid," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 15–32.

[3] T. Shekari, A. A. Cardenas, and R. Beyah, "{Madiot} 2.0: Modern {high-wattage}{iot} botnet attacks and defenses," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 3539–3556.

[4] E. Hassanzadeh, M. E. Hajiabadi, M. Samadi, and H. Lotfi, "Improving the resilience of the distribution system using the automation of network switches," *The Journal of Engineering*, vol. 2023, no. 2, e12238, 2023.

[5] L. Pereira, V. Nair, A. Annaswamy, B. Dias, and H. Morais, "Accurate Federated Learning with Uncertainty Quantification for Distributed Energy Resource Forecasting Applied to Smart Grids Planning and Operation: The ALAMO Vision," in *CIRED 2024 Vienna Workshop*, Vienna, Austria: IET, 2024.

[6] A. Z. Tan, H. Yu, L. Cui, and Q. Yang, "Towards personalized federated learning," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 12, pp. 9587–9603, 2023.

[7] P. Qi, D. Chiaro, A. Guzzo, M. Ianni, G. Fortino, and F. Piccialli, "Model aggregation techniques in federated learning: A comprehensive survey," *Future Generation Computer Systems*, vol. 150, pp. 272–293, 2024.

[8] A. Taïk and S. Cherkaoui, "Electrical load forecasting using edge computing and federated learning," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[9] M. Savi and F. Olivadese, "Short-term energy consumption forecasting at the edge: A federated learning approach," *IEEE Access*, vol. 9, pp. 95 949–95 969, 2021.

[10] G. Zhang, S. Zhu, and X. Bai, "Federated Learning-Based Multi-Energy Load Forecasting Method Using CNN-Attention-LSTM Model," *Sustainability*, vol. 14, no. 19, pp. 1–14, 2022.

[11] P. Hosseini, S. Taheri, J. Akhavan, and A. Razban, "Privacy-preserving federated learning: Application to behind-the-meter solar photovoltaic generation forecasting," *Energy Conversion and Management*, vol. 283, p. 116 900, 2023, ISSN: 0196-8904.

[12] S. Muhammad Salman Bukhari, S. Kumayl Raza Moosavi, M. Hamza Zafar, *et al.*, "Federated transfer learning with orchard-optimized conv-sgru: A novel approach to secure and accurate photovoltaic power forecasting," *Renewable Energy Focus*, vol. 48, p. 100 520, 2024, ISSN: 1755-0084.

[13] A. Moradzadeh, H. Moayyed, B. Mohammadi-Ivatloo, Z. Vale, C. Ramos, and R. Ghorbani, "A novel cyber-resilient solar power forecasting model based on secure federated deep learning and data visualization," *Renewable Energy*, vol. 211, pp. 697–705, 2023, ISSN: 0960-1481.

[14] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of cps security," *Annual reviews in control*, vol. 47, pp. 394–411, 2019.

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

[16] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, "Detection of false data injection attacks in smart grid: A secure federated deep learning approach," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4862–4872, 2022.

[17] V. J. Nair, V. Venkataramanan, R. Haider, and A. M. Annaswamy, "A hierarchical local electricity market for a der-rich grid edge," *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1353–1366, 2022.

[18] V. J. Nair and A. Annaswamy, "Local retail electricity markets for distribution grid services," in *2023 IEEE Conference on Control Technology and Applications (CCTA)*, IEEE, 2023, pp. 32–39.

[19] V. J. Nair, P. Srivastava, and A. Annaswamy, "Enhancing power grid resilience to cyber-physical attacks using distributed retail electricity markets," in *2024 ACM/IEEE 15th International Conference on Cyber-Physical Systems (ICCPS)*, IEEE, 2024, pp. 55–66.

[20] G. Ferro, M. Robba, D. D'Achiardi, R. Haider, and A. M. Annaswamy, "A distributed approach to the optimal power flow problem for unbalanced and mesh networks," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 13 287–13 292, 2020.

[21] J. J. Romvary, G. Ferro, R. Haider, and A. M. Annaswamy, "A proximal atomic coordination algorithm for distributed optimization," *IEEE Transactions on Automatic Control*, vol. 67, no. 2, pp. 646–661, 2021.

[22] V. J. Nair, V. Venkataramanan, P. Srivastava, *et al.*, "Resilience of the electric grid through trustable iot-coordinated assets," *arXiv preprint arXiv:2406.14861*, 2024.

[23] A. Faustine and L. Pereira, "FPSeq2Q: Fully Parameterized Sequence to Quantile Regression for Net-Load Forecasting With Uncertainty Estimates," *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2440–2451, May 2022, ISSN: 1949-3061. DOI: 10.1109/TSG.2022.3148699. (visited on 12/02/2023).

[24] P. Ponnaganti, B. Bak-Jensen, and J. R. Pillai, "Battery Energy Storage System based Voltage and Frequency Control of An Island Distribution Network: CIGRE 2020 e-session," in *CIGRE 2020*, Paris, 2020.

[25] L. Pereira, J. Cavaleiro, and L. Barros, "Economic Assessment of Solar-Powered Residential Battery Energy Storage Systems: The Case of Madeira Island, Portugal," *Applied Sciences*, vol. 10, no. 20, p. 7366, Jan. 2020. DOI: 10.3390/app10207366. (visited on 10/30/2020).

[26] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*, 2017, pp. 1273–1282.

[27] H. Zhu, J. Xu, S. Liu, and Y. Jin, "Federated learning on non-iid data: A survey," *Neurocomputing*, vol. 465, pp. 371–390, 2021.

[28] Q. Li, Y. Diao, Q. Chen, and B. He, "Federated learning on non-iid data silos: An experimental study," in *2022 IEEE 38th International Conference on Data Engineering (ICDE)*, 2022, pp. 965–978.