Privacy-Preserving Aggregated Load Forecasting Based on Vertical Federated Learning

Rui Xie and Yue Chen

Department of Mechanical and Automation Engineering,
The Chinese University of Hong Kong

May 9, 2024

Outline

Introduction

Background

- The nodal load is usually an **aggregated load** composed of some agents' loads (Wang et al. 2018; Huang et al. 2020).
- However, the agents may have **privacy concerns** and do not want to share the information.
- The operator **cannot** use individual load information **centrally**.

Our Goal

- Predict the aggregated load of **inhomogeneous** individual loads
- Exploit **agents' information** on individual loads
- Preserve the agents' privacy

Introduction

Federated Learning (FL)

- FL is an alternative to centralized learning
- The training is conducted **collaboratively among multiple agents** and each agent has a dataset (McMahan et al. 2017)
- Classification (Yang et al. 2019):
  1. **Horizontal** FL (HFL): Datasets have **different samples**
     Applications: Load forecasting, voltage control, attack detection, etc.
     The effectiveness depends on the **similarity** between datasets
  2. **Vertical** FL (VFL): Datasets have **different feature spaces**
     Previous methods preserve privacy to a limited degree because of **gradient leakage** (Liu et al. 2022)
  3. Federated transfer learning: Datasets differ in samples and features

Problem Description

Aggregated Load Forecasting Scenarios

- A **household load** is the aggregation of electricity demand of multiple electrical appliances.
- A **transformer** aggregates the individual loads from different agents and connects the **upstream power system**.

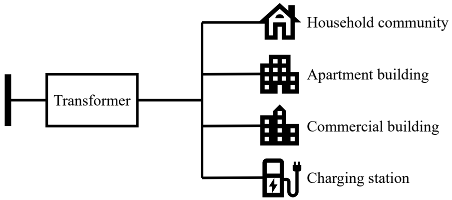


Figure: An example of aggregated load

The upstream power system operator can only observe the aggregated load. Individual load data may help the operator predict better.

Problem Description

Dataset Structure

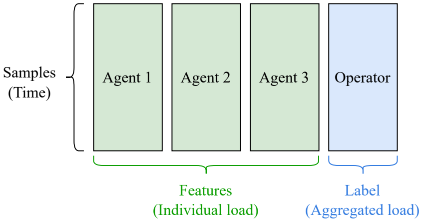
Each data sample contains both individual and aggregated loads.

Aggregated load → **label**
Individual loads → **features**

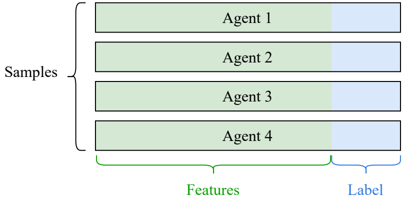
Inhomogeneous agents may have various patterns and their loads are different features.

⇓

VFL is suitable for the problem



Vertical FL (VFL): Datasets have different feature spaces



Horizontal FL (HFL): Datasets have different samples

Methodology

Homomorphic Encryption-Based Secure Multi-Party Computation

Secure Multi-Party Computation (SMPC)

- Multiple parties compute a function together
- Each party cannot learn the others' inputs

Homomorphic Encryption

- A way to implement SMPC
- Allow **direct computation on the encrypted data** due to the homomorphic property:

$$[m_1] \star [m_2] = [m_1 \star m_2], \ [\cdot] \text{ denotes ciphertext}$$

Compute $m_1 \star m_2$ without revealing m_1 and m_2

Methodology

Homomorphic Encryption-Based Secure Multi-Party Computation

Cheon-Kim-Kim-Song (CKKS) Homomorphic Encryption Scheme

- Suitable for **floating numbers** and the precision can be estimated and controlled
- Effective and efficient for addition
- An **asymmetric** encryption scheme
  - One can encrypt the data if they know the **public key**
    $\rightarrow$ Each party encrypts the input
  - One who has the **private key** can decrypt the ciphertext
    $\rightarrow$ The private key holder decrypts the computation result and obtains the final output

Methodology

Proposed Network and Privacy-Preserving Algorithm

- Each agent has a **local LSTM** block
- The LSTM outputs will be the input of a distributed **linear regression** block, whose **weight** is divided and held by the agents, while the operator owns the **bias** parameter

Forward Propagation

Compute the linear regression output using the CKKS scheme

Backpropagation

1. The operator posts the forecast error
2. Conduct ordinary backpropagation

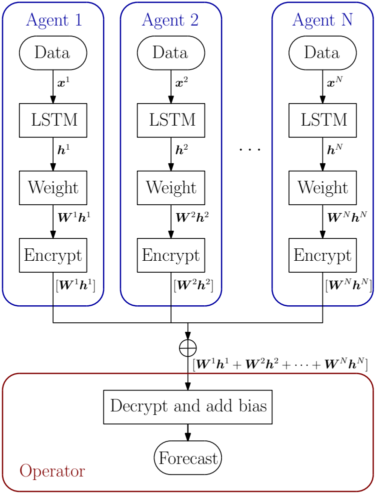


Figure: The proposed network

Methodology

Proposed Network and Privacy-Preserving Algorithm

Preserving Privacy

1. The original load data of agents, the local parameters, and their updates are **never sent out**
2. The CKKS encryption scheme guarantees the **secure computation** of the intermediate variable
3. The operator only receives the **aggregated intermediate variable** and cannot learn agents' data

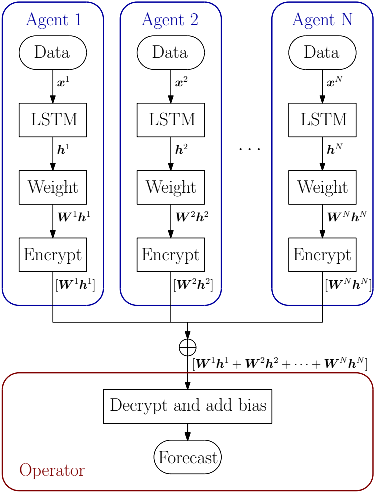
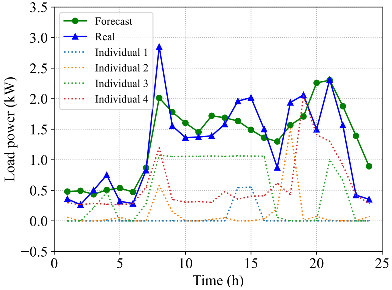


Figure: The proposed network

Case Studies

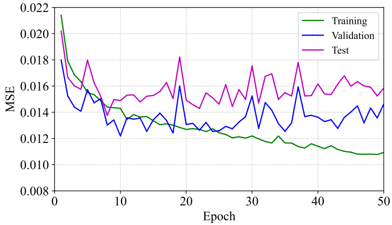
Experiment tools: TensorFlow, Microsoft SEAL, TenSEAL

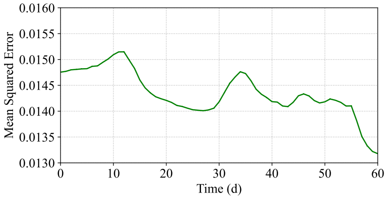
Case study 1: Household load



The proposed method is **effective** in aggregated load forecasting and compatible with online usage

Case study 2: Electricity customer dataset in Australia





Case Studies

Comparison of methods

1. VFL with SMPC (Proposed)
2. VFL without SMPC
3. Forecast centrally
4. Forecast individually & SMPC
5. HFL

Method No.	Individual information	Privacy-preserving	MSE	Training time (s)
1	✓	✓	0.0149	7098.5
2	✓	✗	0.0149	197.5
3	✗	✓	0.0157	59.4
4	✓	✓	0.0241	580.4
5	✓	✓	0.0168	1829.0

Findings:

- The CKKS encryption achieves high accuracy
- The computation time of the proposed method is much longer but still acceptable
- The MSE is decreased by 5.1% due to the agents' information
- HFL does not perform well for highly inhomogeneous loads

The proposed method outperforms other methods regarding **privacy** and **accuracy**

Conclusion

Contribution

This paper proposes a **privacy-preserving VFL** method for **aggregated load forecasting** based on LSTM and CKKS encryption. The neural network is divided into parts and each agent holds a part, where the **individual information** and **local model** are kept private.

Findings of Case Studies

- Reduce the MSE by 5.1%
- Can be used in online scenarios

Future Work

Reduce forecasting error

- Incorporate advanced machine learning techniques
- Employ other related features

References

- Huang, Nantian et al. (2020). “Incorporating load fluctuation in feature importance profile clustering for day-ahead aggregated residential load forecasting”. In: *IEEE Access* 8, pp. 25198–25209.
- Liu, Haizhou et al. (2022). “A Hybrid Federated Learning Framework With Dynamic Task Allocation for Multi-Party Distributed Load Prediction”. In: *IEEE Transactions on Smart Grid* 14.3, pp. 2460–2472.
- McMahan, Brendan et al. (2017). “Communication-efficient learning of deep networks from decentralized data”. In: *Artificial intelligence and statistics*. PMLR, pp. 1273–1282.
- Wang, Yi et al. (2018). “An ensemble forecasting method for the aggregated load with subprofiles”. In: *IEEE Transactions on Smart Grid* 9.4, pp. 3906–3908.
- Yang, Qiang et al. (2019). “Federated machine learning: Concept and applications”. In: *ACM Transactions on Intelligent Systems and Technology (TIST)* 10.2, pp. 1–19.

Thank you!