エッジサーバを用いた連合学習方式の提案と評価

2018SE045 溝口真央
指導教員：宮澤元

1　はじめに

携帯電話などの利用者側にあるエッジ端末のデータを機械学習の学習モデルの作成に利用するようなアプリケーションが増加している．しかし，多数のエッジ端末からの大量のデータを用いて機械学習を行うためにクラウドにデータを集約するアプローチには大量のデータ通信が必要である．また，利用者のプライバシーに関わる学習データをクラウドに送信するには配慮が必要である．

連合学習 (Federated Learning，FL) は分散機械学習手法のひとつである．FL では，利用者が実際に使用しているスマートフォンのようなエッジ端末で取得されるデータを用いてエッジ端末自体で機械学習を行い，得た更新データをクラウド上のサーバに集約して全体で共有される学習モデルを更新する．

FL ではエッジ端末で取得されるデータは外部に送信されることはないので，学習データのプライバシー性を保ち学習モデルを作成することが出来る．一方，エッジ端末内で機械学習を行うことで，エッジ端末の電力や計算リソースを消費してしまう問題がある．

本研究の目的は，エッジサーバを用いて FL を行い FL 時のエッジ端末の処理負荷を軽減することである．エッジ端末のデータをエッジサーバに送信しエッジサーバで機械学習を行うことで，エッジ端末の負荷を軽減することができる．

研究課題は以下の二点である．

- エッジサーバを用いた FL 方式の提案
- 提案方式による機械学習の性能や学習モデルの精度に与える影響の評価

2　連合学習

本節では研究の背景として，連合学習 (FL) について述べる．従来の FL では，クラウド上のサーバからエッジ端末に学習モデルを送り，エッジ端末内で機械学習を行い，学習モデルの更新を行っている (図 1)．FL では，まずエッジ端末に共有学習モデルを配布し，エッジ端末で取得されるデータを用いてエッジ端末で機械学習を行いモデルを更新する．次に，更新した学習モデルの差分をエッジ端末からサーバに集めて，サーバ内では受け取った差分をデータ量で重み付けして共有学習モデルを更新する．最後に再度サーバからエッジ端末に対して更新した共有学習モデルを配布する．これらを繰り返すことで精度の高い学習モデルを作成している．

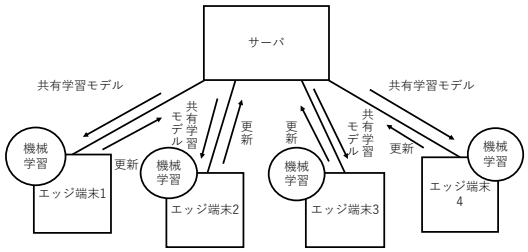

図 1　従来の FL の形式

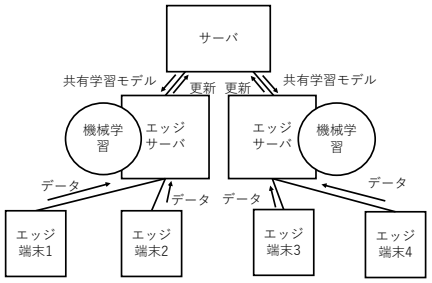

図 2　エッジサーバを用いた FL の形式

3　エッジサーバを用いた連合学習

本研究で提案するエッジサーバを用いた連合学習方式について示す (図 2)．エッジ端末の近くに設置されたエッジサーバはクラウド上のサーバから共有学習モデルを受け取り，エッジ端末で取得されるデータを受け取って機械学習を行い，学習モデルを更新する．更新された学習モデルの差分をサーバに送って共有の学習モデルを更新する．

このようにエッジ端末に対して共有学習モデルを送信せずに，エッジサーバ内で共有学習モデルの更新を行うことでエッジ端末に機械学習の負荷をかけず，データの送信のみで精度の高い共有学習モデルの作成が期待できる．

4　提案方式の実装

オープンソースで利用できる Python のライブラリやフレームワークを用いて提案方式を実装した．具体的には PyTorch[3] や TensorFlow[4] などのディープラーニングフレームワークを利用して FL を行う PySyft ライブラリ [2] を用いた．

提案方式では，各エッジ端末が近くに設置されたエッジサーバに TCP/IP で接続を行う．各エッジサーバは，クラウド上のサーバとも同様に接続を行う．接続後，エッジ端末はエッジサーバにデータを送信する．エッジサーバは送信されたデータを用いて機械学習を行い，学習モデルを

更新する．エッジサーバからサーバには学習モデルの更新データのみが送信される．

5　実験

提案方式における学習モデル生成にかかる時間や学習モデルの精度について評価するために，提案方式と従来の FL とで機械学習を行う実験を行った．従来の FL プログラムでは，エッジ端末とサーバ間のデータ協調を PySyft ライブラリで提供されている Duet[5] を用いて行った．

5.1　実験環境

エッジ端末として Raspberry Pi 4 Model B を 4 台用いた．サーバには PC(CPU:Intel Core i5-7200U 2.50GHz, Memory 8.00GB) を用いた．提案方式のエッジサーバには Raspberry Pi 4 Model B，または NVIDIA Jetson Nano を用いた．有線は各マシンを 1000Base-T ネットワークで接続し，無線では各マシンを IEEE 802.11n 無線ネットワークで接続した．

5.2　実験内容

初項 4，公差 8 の階差数列で 4 から 84 までを教師データ，教師データの値にそれぞれ -2，-1，$+1$，$+2$ したことで作成したテストケースを用いて機械学習を行い，1 回の学習にかかる時間を測定した．学習を 100 回行い，平均値を求めた．次に，作成した更新済み学習モデルに教師データの値と同じテストケースを与え，得られた予測値から，求めたい値である実測値に対しての正解率を求める．また機械学習中のエッジ端末の CPU 使用率を vmstat コマンドを用いて 1 秒間隔で確認した．実験を従来方式の FL と提案方式とでそれぞれ行い，結果を比較した．提案方式はエッジサーバに Raspberry Pi 4 を用いた場合 (RPi) と Jetson Nano を用いた場合 (JNano) の両方で実験を行った．

5.3　実験結果

実験結果を表 1 に示す．機械学習 1 回にかかった時間の平均では，提案方式の方が従来 FL よりも短い. 学習モデルの精度は従来 FL が一番高い. エッジ端末の CPU 使用率も従来 FL が一番高いことがわかった. 一方，提案方式ではエッジサーバが RPi でも JNano でも結果に大きな差はなかった.

表 1　計測結果

実験	従来 FL	提案方式	
		RPi	JNano
学習時間 (ms)	878.18	1.80	1.75
モデル正解率 (%)	97.02	90.23	92.86
エッジ端末 CPU 使用率 (%)	23.15	4.02	4.02

機械学習 1 回にかかった時間の平均では，従来 FL では一回の機械学習中に共有学習モデルや更新値を送受信しているので，その時間が計測に含まれる．一方，提案方式では機械学習を行った後に行っている共有学習モデルや更新値の送信時間を計測に含めていない．従って，両者で大きな差が出ている．

5.4　考察

実験から，提案方式を用いた場合従来の FL と比べエッジ端末の負荷を軽減できることがわかった．

また，実装上の問題で，5.3 節に示すように機械学習に要する時間として計測した値が提案方式と従来方式とで十分公平な比較ができないものとなってしまっていた．

しかし，従来の FL に比べて提案方式は機械学習自体に要する時間が少なく，提案方式の機械学習回数を増やしても従来の FL よりも機械学習に要する時間が大幅に増加することはない．だが提案方式では，エッジ端末からエッジサーバにデータを送信しているため更新データのみしか送信していない従来 FL と比べるとプライバシー性が低い．このことから，提案方式ではプライバシー性が従来の FL と比べて劣ってしまうが，エッジ端末にかかる負荷を軽減して学習モデルが作成できたといえる．

提案方式ではエッジサーバに用いる機材が違っても，結果には大きな差がなかった．Jetson Nano には比較的高性能な GPU が搭載されているが，今回の実装ではこれを有効に利用できなかったと考えられる．

6　おわりに

エッジサーバを用いた FL を提案した．機械学習中のエッジ端末の CPU 負荷を計測する実験を行った．実験結果から，提案方式では従来の FL と比較してエッジ端末にかかる負荷を減らすことができることがわかった．一方，提案方式ではエッジ端末からエッジサーバへとデータを送信する必要があり，従来 FL ほどプライバシー性は高くない．今後は実装を改善して，提案方式と従来の FL とのより正確な比較を行うとともに，エッジサーバ上の GPU を活用した場合の効果も確認する．

参考文献

[1] H.Brendan McMahan, et al., “Communication-Efficient Learning of Deep Networks from Decentralized Data, ” *in Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, AISTATS 2017, Vol. 54, 2017.*

[2] PySyft:https://openmined.github.io/PySyft/ (2021/1/16 アクセス)

[3] PyTorch:https://pytorch.org/ (2021/1/16 アクセス)

[4] Tensorflow: https://www.tensorflow.org/federated (2021/1/16 アクセス)

[5] Duet:https://blog.openmined.org/duet-dem-how-to-do-data-science-on-da ta-owned-by-a-different-organization/ (2021/1/16 アクセス)