Titre

Stage M2 : étude de convergence des algorithmes d'apprentissage fédéré dans le cas non-iid

Mots clés

Machine Learning ; Apprentissage fédéré ; IA de confiance.

Présentation du service : CEA LIST / SID

Situé à Saclay, en Ile-de-France sud, le CEA LIST (http://www-list.cea.fr/) est un centre de recherche scientifique et technologique dédié au développement de logiciels, de systèmes embarqués et de capteurs pour des applications destinées à la défense, la sécurité, l'énergie, le nucléaire, l'environnement et la santé. Le CEA LIST fait partie de l'écosystème dynamique et stimulant de l'Université Paris Saclay - le plus grand pôle scientifique français comptant 60 000 étudiants. Il compte plus de 700 chercheurs se focalisant sur les systèmes numériques intelligents, centrés autour de l'intelligence artificielle, l'usine du futur, l'instrumentation innovante, les systèmes cyberphysiques et la santé numérique. Au sein de cet institut, le SID (Service d'Intelligence des Données) travaille sur les algorithmes et méthodologies de l'intelligence artificielle et du traitement du signal. Les recherches et avancées technologiques du service sont guidées par des applications variées, pour lesquelles les spécificités et contraintes sur les données ou l'environnement d'exécution nécessitent une conception fine des IA et de leur intégration comme briques unitaires de systèmes complexes.

Description du projet

En 2016, Google publie les principes fondateurs de l'apprentissage fédéré [1] avec la promesse de créer des IA sans compromettre les données des utilisateurs. Cette méthode est en train de changer le paradigme actuel de l'IA centralisée, où construire de meilleurs modèles se résume souvent à collecter toujours plus de données personnelles et les centraliser sur un serveur. L'apprentissage fédéré est une approche collaborative où tous les utilisateurs d'un service participent à l'apprentissage du modèle sans transmettre leurs données personnelles mais uniquement les paramètres du modèle mis à jour localement (voir Fig.1). Au lieu de centraliser les données, seuls les paramètres du modèle sont agrégés sur le serveur central ce qui permet d'améliorer la confidentialité des données et de limiter les coûts de communication.

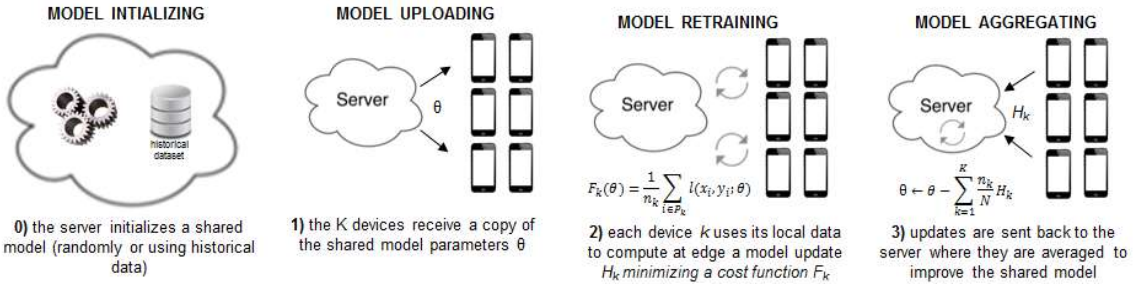

Fig-1 : illustration de l'apprentissage fédéré

L'apprentissage d'un réseau de neurones nécessite un ensemble de données iid (indépendantes et identiquement distribuées) afin de garantir que le gradient stochastique soit une estimation non biaisée du gradient entier. Contrairement à un apprentissage centralisé, il est impossible dans le cadre de l'apprentissage fédéré d'assurer que les données locales de chaque utilisateur soient toujours iid. Le cas non-iid (où la distribution des données entre utilisateurs sera différente) va entrainer une dégradation des performances du modèle fédéré par rapport à l'approche centralisée [2].

L'objectif du stage consiste à étudier les algorithmes qui permettent d'améliorer le processus d'apprentissage d'un modèle fédéré avec données non-iid (voir par exemple [3 ;4]). L'analyse portera sur la vitesse de convergence de l'optimisation ainsi que la précision du modèle. L'étude sera menée de manière empirique en évaluant les algorithmes sur la base de données EMNIST [5] et également de manière théorique en étudiant les preuves de convergence (voir par exemple [6 ;7]).

[1] Google AI blog: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

[2] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, and V. Chandra. Federated learning with non-iid data. arXiv preprint 1806.00582, 2018.

[3] T. Li, A.K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith. Federated Optimization in Heterogeneous Networks. arXiv preprint 1812.06127, 2020.

[4] S.P. Karimireddy, S. Kale, M. Mohri, S.J. Reddi, S.U. Stich, and A.T. Suresh. SCAFFOLD: Stochastic Controlled Averaging for Federated Learning. arXiv preprint 1910.06378, 2021.

[5] https://www.nist.gov/itl/products-and-services/emnist-dataset

[6] X. Li, K. Huang, W. Yang, S. Wang, and Z. Zhang. On the Convergence of FedAvg on Non-IID Data. arXiv preprint 1907.02189, 2020.

[7] A. Khaled, K. Mishchenko, and P. Richtarik. Tighter Theory for Local SGD on Identical and Heterogeneous Data. arXiv preprint 1909.04746, 2020.

Profil recherché

Le stage s'adresse à un(e) étudiant(e) du cycle ingénieur/universitaire cherchant un stage M2 et manifestant l'envie de travailler dans le milieu de la recherche.

Idéalement, le candidat suit actuellement une formation en lien avec le domaine de l'Intelligence Artificielle/Machine Learning. La connaissance des algorithmes d'optimisation en Machine Learning ainsi que la maîtrise de Python sont indispensables.

Le/la candidat(e) devra être capable d'apporter ses idées novatrices, son enthousiasme, sa rigueur et devra faire preuve d'un esprit d'équipe prononcé.

La durée du stage est de 6 mois minimum et pourra se poursuivre par une thèse de doctorat. Le stage est rémunéré.

Informations administratives et contacts

Nature du contrat de travail : stage

Type du contrat de travail : Droit privé

Délai administratif pour début de contrat : environ 3 mois

Envoyer CV et lettre de motivation à :

Aurélien Mayoue (aurelien.mayoue@cea.fr)