LISTIC

Annecy-le-Vieux, le 20 juillet 2023

Thèse CIFRE : détection d'anomalies par apprentissage fédéré pair à pair.

Contacts:

Alexandre Benoit: alexandre.benoit @ univ-smb.fr

Mickael Bettinelli: mickael.bettinelli @ univ-smb.fr>

Planning macro:

Préétude : septembre-décembre 2023, pourra intégrer la personne candidate à la thèse

Thèse : début 2024

Contexte

Le projet se situe dans un contexte industriel à grande échelle pour lequel une entreprise produit des appareils de haute précision pour des tiers à l'échelle mondiale. On s'intéresse en particulier à des matériels destinés aux fondeurs de puces électroniques. Dans ce secteur industriel international de pointe et fortement concurrentiel, la maintenance des matériels est cruciale et doit être réalisée avec un niveau maximal de sécurité et confidentialité. En effet, les arrêts de ligne de production pour cause de panne non anticipée impliquent des coûts très importants de plusieurs 100 K€. À ce jour aucune solution ne permet de planifier efficacement le retrait d'un équipement avant sa défaillance.

Les appareils cibles sont complexes et instrumentés en de nombreuses zones critiques. Les causes potentielles de pannes sont multiples et potentiellement imbriquées. Une approche classique est de définir un détecteur d'anomalie indépendant pour chaque zone d'intérêt et d'agréger les prédictions de ces détecteurs. Néanmoins, l'identification des données pertinentes pour une détection optimale et leurs interactions reste un problème ouvert.

Une piste d'exploration est d'associer la connaissance des experts du domaine à des modèles paramétriques $f(\theta)$ optimisés par apprentissage à partir des données X, X étant une agrégation de données hétérogènes $[x0, x1, ..., xn]$ issues des différents capteurs disposés sur les matériels.

Problématiques scientifiques

Se posent alors des questions scientifiques sur différents champs de recherche complémentaires :

- Comment optimiser des modèles pertinents pour des ensembles de matériels présentant de nombreuses déclinaisons, usages et contextes ? On peut parler d'optimisation de communautés de modèles/matériels qui ne sont pas forcément identifiées en amont.

- Comment associer différents modèles prédicteurs au sein d'un même matériel pour affiner la prédiction des pannes ? L'expertise du domaine faisant remonter des dépendances dynamiques, la fusion des différentes prédictions est un second grand défi.

Du point de vue de l'optimisation de modèles

Plusieurs approches classiques sont possibles :

- Optimiser un modèle avec les données de chaque matériel indépendamment. Cette approche est sous optimale dans le sens où elle se limite à une calibration locale et intègre difficilement l'expérience acquise avec les autres matériels. On peut parler de sur-apprentissage des paramètres locaux θi sur les données locales. Elle est de plus difficile à mettre en œuvre en milieu industriel, car cela nécessite des interventions systématiques sur chaque matériel.
- Optimiser un unique modèle global $f(\theta g)$ à partir de grands jeux de données intégrant une grande variété d'appareils. Cette approche très efficace et maintenant classique s'appuie sur une collecte de grandes masses de données qui doivent être centralisées et rapprochées de centres de calculs permettant alors d'optimiser le modèle. Ce paradigme d'apprentissage n'est pas envisageable, car entre en conflit avec les contraintes de confidentialités imposées par le contexte industriel. Également, il intègre plus difficilement les spécificités locales et le modèle global résultant sera alors soit compact, mais mal adapté, soit capable d'une grande capacité d'apprentissage, mais en conséquence trop lourd et difficile à mettre en œuvre localement.
- Optimiser de façon décentralisée, par apprentissage fédéré, pour augmenter les capacités de généralisation des modèles et maintenir confidentialité et pertinence locale. L'apprentissage fédéré introduit récemment [1] permet de partager les paramètres des modèles θi optimisés localement par chaque individu pour générer un modèle global pertinent. Cette approche permet de ne jamais partager les données (confidentialité), mais seulement les paramètres θi (volumétrie plus faible, réduction des coûts de communication) localement en partageant des données. Cette approche est plus intéressante. Néanmoins, elle doit être vue sous un angle différent pour être pertinente dans un cas d'usage réel et en particulier dans le contexte applicatif proposé :
- Permettre des échanges d'information directs entre les matériels, sans passer par un serveur central pour gagner en confidentialité et réduire la dépendance à un système central.
- Identifier une variété de modèles globaux plutôt qu'un seul afin de préserver la pertinence : chaque population de matériel devrait avoir son modèle global adapté.

La démarche scientifique sur ces questions sera de définir et évaluer des modèles pertinents permettant des comparaisons et de proposer des contributions en particulier sur l'apprentissage distribué pair à pair et décentralisé avec détection de communautés.

Du point de vue de la fusion dynamique des prédictions

La nature distribuée des matériels et des données réparties chez plusieurs tiers requiert une méthode d'apprentissage décentralisée ou distribuée afin de maintenir la confidentialité des données. Les systèmes multi-agents offrent un terrain fertile pour répondre à des problèmes de cette nature en permettant de voir chaque appareil comme un agent autonome. Contrairement à un programme

LISTIC – POLYTECH Annecy-Chambéry
Adresse géographique : 5 chemin de Bellevue - Annecy le Vieux
Adresse postale : BP 80439 - 74944 Annecy le Vieux Cedex (France)
Tél. : +33 (0) 4 50 09 65 80 – Fax : +33 (0) 4 50 09 65 59
Courriel : dir-listic@univ-smb.fr - Web : www.listic.univ-smb.fr

classique, ils ont la faculté de décider de leurs actions et des données qu'ils partagent avec le reste du système ce qui fait du paradigme agent un paradigme efficace dans le contexte de cette recherche.
L'une des caractéristiques innovantes de cette proposition est la détection de dysfonctionnements et la construction d'une taxonomie des pannes à travers la recherche de sous-groupes d'individus grâce à l'apprentissage fédéré. Il est en effet possible de former des groupes d'individus parmi ceux qui travaillent à l'optimisation d'un modèle commun [2]. Dans le cas de la détection d'anomalies, cette méthode présente l'avantage de regrouper les dysfonctionnements de chaque composant surveillé en plusieurs catégories tout en maintenant la confidentialité des données de chaque appareil. Les catégories de dysfonctionnements de chaque composant peuvent ensuite être fusionnées pour former une taxonomie d'anomalies globale (au niveau du matériel lui-même) ce qui pourrait, à terme, permettre la prédiction de pannes et une réparation préventive de ces appareils.

Planning prévisionnel

En amont de la thèse

Une préétude de 4 mois avec le partenaire industriel sera réalisée afin de consolider le contexte de la thèse. Les objectifs pourront être réalisé par la personne candidate à la thèse et lui permettre ainsi de s'approprier en amont les outils, le contexte et son matériel.

La thèse

Nous proposons une démarche progressive de l'avancement de la thèse :

Période 1 : travail sur les données et création de références

1.a. *Prise en main des données (T0-T0+6)*

1.b. *Création de modèles de base de référence de comparaison (T0+4-T0+8)*

Période 2 : étude de modèles optimisés par apprentissage décentralisé pair à pair, niveau méta

2.a. *Définition d'une approche d'apprentissage fédéré pair à pair (p2p) (T0+6-T0+16)*

2.b *Extension de l'apprentissage fédéré p2p avec détection de communautés (T0+16-T0+26)*. Plutôt que de converger vers un seul modèle global parfois non pertinent il sera intéressant de détecter d

2.c *Du modèle global de l'appareil aux modèles locaux intra-appareil* (*T0+26-T0+36)*.

Enfin, l'explicabilité de cette méthode de détection d'anomalies pourra être explorée pour comprendre les propriétés de chaque sous population et aider à la maintenance préventive du matériel du parc. Cette approche d'extraction de communautés à grain fin pourra être confrontée aux résultats obtenus à l'échelle macro du matériel (2.b) pour affiner encore la compréhension des anomalies et la pertinence des approches proposées.

LISTIC – POLYTECH Annecy-Chambéry
Adresse géographique : 5 chemin de Bellevue - Annecy le Vieux
Adresse postale : BP 80439 - 74944 Annecy le Vieux Cedex (France)
Tél. : +33 (0) 4 50 09 65 80 – Fax : +33 (0) 4 50 09 65 59
Courriel : dir-listic@univ-smb.fr - Web : www.listic.univ-smb.fr

Politique de publication

Les résultats de ces travaux pourront faire l'objet de publications dans des conférences et journaux scientifiques dans le respect des conditions de confidentialité du contrat entre l'entreprise et l'USMB. Chaque étape à partir de 1.b pourra faire l'objet d'au moins une publication.

Les thématiques et mots clefs de ces publications identifiées a priori sont :

- IA et modèles physiques
- IA fédérée (p2p)
- Clustering de communautés
- Systèmes multi-agent

Il conviendra de définir une politique permettant au/à la doctorant(e) de publier sur ses contributions sans compromettre la confidentialité des données industrielles. Ceci impose donc une phase amont à la thèse de préparation des données et du périmètre de travail (voir section environnement de travail ci-après).

Références

[1] McMahan, H. Brendan, et al. "Federated learning of deep networks using model averaging." *arXiv preprint arXiv:1602.05629* 2 (2016).

[2] Sattler, F., Müller, K.R., Samek, W.: Clustered federated learning. In: Proceedings of the NeurIPS'19 Workshop on Federated Learning for Data Privacy and Confidentiality. pp. 1–5 (2019)

LISTIC – POLYTECH Annecy-Chambéry
Adresse géographique : 5 chemin de Bellevue - Annecy le Vieux
Adresse postale : BP 80439 - 74944 Annecy le Vieux Cedex (France)
Tél. : +33 (0) 4 50 09 65 80 – Fax : +33 (0) 4 50 09 65 59
Courriel : dir-listic@univ-smb.fr - Web : www.listic.univ-smb.fr