

Une possibilité pour contrer la mauvaise répartition est de grouper les classes trop minoritaires ensembles (déjà implémenté chez nous).

Les meilleurs résultats seront obtenus en combinant Undersampling et Oversampling. On peut crop les données trop représentées et appliqué Smote sur les moins représentées.

Certains champs sont précalculé et ne sont pas forcément généralisable dans le cadre de l'analyse réseau.

Pour contrer cela on peut appliquer :

- Clipping (Min/Max)
- Discrétisation
- Masking

Il faut faire une liste des invariants et des features ayant une relation logique avec d'autres. On peut les mettre en FALSE lors de l'entraînement et/ou désactiver leur gradient. Puis les récupérer à la fin. Il faudra alors faire une fonction permettant de vérifier si les features sont toujours relié ou seulement recalculé celle qui sont dépendantes de relation logique.

Les solveur quadratique type CVX-OPT peuvent être utile mais pas indispensable.

Au sujet des techniques de génération adverse:

- Il existe une probabilité non négligeable qu'une attaque marchant pour un modèle soit transferrable un autre.
- Surrogate : entraînement puis attaque adverse sur le gradient, entraîner sur les mêmes données que le random forest
- Substitute : un peu plus avancé, entraîner le MLP sur les directions du random forest (meilleur proba de réussite). On imite vraiment le random forest

Prochains RDV : Mardi 10h, Jeudi 10h