Élagage Non Structuré pour l'Identification des Empreintes Radio-fréquences

Emma BOTHEREAU[1] Alice CHILLET[1] Robin GERZAGUET[1] Matthieu GAUTIER[1] Olivier BERDER[1]
[1]Université de Rennes, CNRS, IRISA

Résumé – L'identification des empreintes radio-fréquences pourrait améliorer les protocoles d'identification sans fil, mais son usage actuel, fortement dépendant de l'apprentissage profond, limite son déploiement sur les systèmes embarqués en raison des contraintes de mémoire et de calcul. Pour alléger la charge calculatoire, ce travail analyse l'impact de l'élagage non structuré, sans réentraînement, sur plusieurs bases de données publiques. Nous montrons qu'il est possible de supprimer de 35% jusqu'à 70% des poids d'un réseau tout en conservant un F1-score supérieur à 99%.

Abstract – Radio frequency fingerprint identification improves wireless identification protocols, but its use of deep learning limits its deployment on embedded systems due to memory and computation constraints. To mitigate this issue, this work analyses the impact of unstructured pruning, without retraining, on several public databases. We show that it is possible to remove from 35% up to 70% of a network's weights while maintaining an F1-score greater than 99%.

1 Introduction

L'identification des empreintes Radio-fréquences (RF) est une méthode émergente qui permet d'authentifier les appareils de transmission sans fil grâce aux distorsions uniques générées par les imperfections des composants. Cette approche pourrait permettre d'améliorer voire de remplacer les protocoles de sécurité en se basant sur des caractéristiques non usurpables.

L'essor de l'apprentissage profond a renforcé le développement de l'identification d'empreintes RF, mais son coût en calcul et en mémoire complique son déploiement sur des systèmes embarqués. Pour pallier ces limites, des approches d'identification plus légères [1] sont développées, telles que l'élagage, la quantification ou le transfer learning.

L'élagage, introduit par Yann Le Cun en 1989 [2], consiste à supprimer les éléments les moins influents d'un réseau afin de réduire sa complexité. Il peut être structuré (suppression de groupes cohérents de poids) ou non structuré (suppression de poids individuels). L'élagage est encore peu utilisé pour l'identification des empreintes RF. De plus, les méthodes utilisées (Triple-S [3], ADMM [4], Fisher [5]) nécessitent un réentraînement coûteux en données et en ressources. Nous proposons ici un élagage sans réentrainement [6], permettant de réduire la taille des réseaux neuronaux tout en préservant leurs capacités d'identification, sans surcoût computationnel. Les travaux existants n'explorent pas non plus le comportement des réseaux face aux variations temporelles et contextuelles, un enjeu clé pour l'identification RF. Cette capacité d'adaptation, appelée *résilience*, est essentielle pour reconnaître un appareil malgré les changements de conditions.

Le contributions de ce travail sont :

- Une étude comparative de l'élagage non structuré sur deux CNN appliqués à quatre bases de données, montrant qu'il est possible de supprimer 35 à 70% des paramètres, tout en conservant un score F1 de 99%.
- Une analyse de la résilience des réseaux, révélant que l'élagage non structuré n'affecte pas leur capacité à identifier les appareils sur différentes périodes.

2 Identification des Empreintes RF

2.1 Empreintes RF

La transmission sans fil d'un signal consiste en plusieurs étapes essentielles : la modulation des deux canaux I et Q en fréquence porteuse, l'amplification, le filtrage avant la transmission via une antenne. La réception du signal se fait de manière similaire : reçu par une antenne, il est ensuite amplifié, filtré, puis démodulé en phase et en quadrature (IQ), avant de récupérer les données d'origine. En raison des imperfections des composants de l'émetteur et de l'impact du canal, le signal reçu contient une légère distorsion appelée empreinte radio-fréquence ($\mathcal{F}$). Le signal complexe reçu $x_r(t)$ dépendant du signal original $x(t)$, peut s'exprimer comme :

$$x_r(t) = \mathcal{F}_{Canal} \circ \mathcal{F} \circ x(t) = \mathcal{F}_{Canal} \circ \mathcal{F}_{AP} \circ \mathcal{F}_{OL} \circ x(t) \quad (1)$$

avec $\circ$ la fonction de composition, $\mathcal{F}_{OL}$ l'empreinte de l'oscillateur local, $\mathcal{F}_{AP}$ l'empreinte de l'amplificateur de puissance, et $\mathcal{F}_{Canal}$ l'empreinte du canal ou de l'environnement.

L'empreinte du récepteur ne sera pas prise en compte, car elle est la même pour tous les signaux reçus.

2.2 Base de données

Les Bases De Données (BDD) utilisées, connues pour l'identification des empreintes RF, sont composées de signaux WiFi en accès libre . Elles présentent l'avantage de présenter deux scénarios distincts, nommés ici Scénario 1 (S1) et Scénario 2 (S2). Les ensembles de données sont décrits dans la Table 1, Tx désignant le nombre d'appareils à identifier.

BDD	POWDER [7]	WiSig [8]	SWRFF [9]	ORACLE [10]
Tx	4	6	15	16
S1	Jour 1	Jour 1	Matin	Run 1 - 2ft
S2	Jour 2	Jours 2 à 4	Soir	Run 2 - 2ft

TABLE 1 : Présentation des BDD utilisées.

Les signaux du scénario 1 sont mélangés et divisés en un ensemble d'entraînement et un ensemble de test (90%-10%). Le scénario 2 est utilisé pour évaluer la *résilience* des réseaux, soit la capacité des réseaux à reconnaître les émetteurs dans un contexte différent ou à un moment ultérieur.

2.3 Intégration de l'élagage dans le système d'identification

Le système présenté reprend les étapes typiques de l'entraînement d'un classifieur, à l'exception de l'ajout de l'étape d'élagage après l'entraînement du réseau. Ce système est représenté en Figure 1. L'étape d'élagage a été sélectionnée pour ne pas nécessiter de données additionnelles, associées à une charge calculatoire importante, et réduire les poids de façon non structurée, de façon indépendante de l'entraînement. Cette méthode crée des réseaux clairsemés, c'est-à-dire des réseaux dans lesquels certains des poids ont été neutralisés et mis à 0, ces poids n'ont alors plus d'impact dans le réseau. Le taux de poids neutralisés est appelé *sparsité*. L'utilisation d'un élagage non structuré permet d'obtenir des valeurs de sparsité plus élevées que l'élagage structuré. Les réseaux clairsemés, combinés à l'accélération matérielle et à l'optimisation de la mémoire, sont prometteurs, mais cet article n'entrera pas dans le détail de ces considérations matérielles.

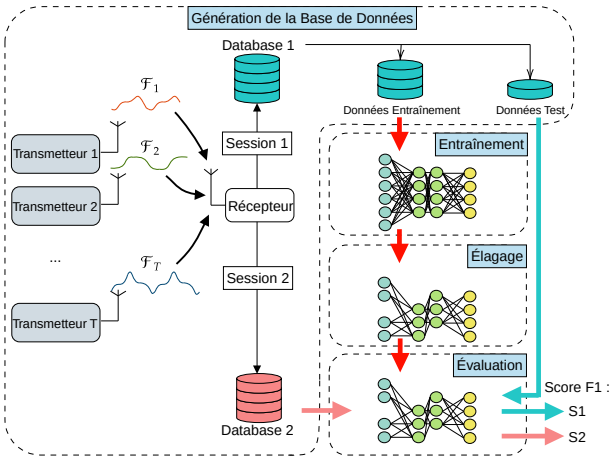

FIGURE 1 : Système proposé pour l'identification des empreintes RF.

Le but est d'obtenir la spasité la plus élevée, tout en préservant les performances en terme de F1-score, sans réutiliser de donnée lors de l'étape d'élagage.

3 Apprentissage Profond pour l'Identification d'Empreintes RF

3.1 Définition

Soit $\mathcal{N} = \{(W^k, B^k), k \in [\![1, K]\!]\}$ un réseau de neurones convolutif constitué de K couches, chacune définie par une matrice W^k représentant les poids et une matrice B^k représentant les biais de la couche considérée. Pour simplifier, les poids des matrices sont représentés comme w_j. De plus, on définit $N = \sum_{k=1}^{K}(|W^k| + |B^k|)$ le nombre total de poids dans un réseau $\mathcal{N}$, où $|W^k|$ et $|B^k|$ représentent respectivement le nombre d'éléments dans les matrices W^k et B^k.

3.2 Réseaux de Neurones Convolutifs

Pour ce papier, deux architectures ont été sélectionnées. La première est un réseau classique de l'état de l'art (CNN$_L$), tandis que la seconde est un réseau particulièrement léger (CNN$_S$) présenté avec la base de données WiSig [8]. Cela permet de montrer que deux réseaux différents peuvent suivre la méthodologie présentée. Ces réseaux prennent en entrée des signaux IQ bruts dans le domaine temporel de dimensions 256×2, soit 256 échantillons temporels sur deux canaux (I et Q). Avec ces signaux, CNN$_L$ et CNN$_S$ présentent respectivement 1 232 774 et 39 778 paramètres pour une classification de 6 émetteurs.

3.3 Méthodologie

Tous les réseaux sont entraîné 5 fois avec les mêmes 5 graines aléatoires fixées différentes (valeurs utilisées pour le générateur de nombres pseudo-aléatoires). Ces graines impactent la répartition des données dans les jeux de données d'entraînement et de test, ainsi que la valeur d'initialisation des réseaux. La performance des réseaux est mesurée par le macro score F1 (%).

Les réseaux initiaux sont entraînés en utilisant l'optimiseur Adam avec une loss (crossentropie). Le taux d'apprentissage est paramétré pour diminuer de 10% toutes les 10 époques. L'entraînement se déroule sur 200 époques, avec un arrêt anticipé si la perte ne diminue pas pendant 10 époques. À la fin de chaque période d'entraînement, nous évaluons le score F1 des réseaux sur deux ensembles de données différents : Scénario 1 (S1) et Scénario 2 (S2).

3.4 Performances des réseaux initiaux

Les scores F1 moyens, minimaux et maximaux des deux CNN pour les différentes bases de données sont présentés dans le Table 2. Les meilleurs résultats entre CNN_L et CNN_S, pour chaque scénario et ensemble de données, sont soulignés.

Scénario	Moy	Min	Max	Moy	Min	Max
	CNN$_L$			CNN$_S$		
	POWDER [7]					
S1	99.99	99.98	100.0	99.78	99.24	99.96
S2	91.14	86.09	95.67	79.41	66.59	98.89
	WiSig [8]					
S1	99.73	99.34	100.0	99.57	99.02	99.85
S2	58.55	51.47	69.32	56.98	49.23	72.75
	SWRFF [9]					
S1	99.63	99.36	99.80	99.61	99.15	99.85
S2	6.74	3.64	9.40	15.06	13.21	16.88
	ORACLE [10]					
S1	99.92	99.67	100.0	98.35	97.36	99.55
S2	29.70	26.26	32.89	26.40	25.10	27.67

TABLE 2 : Networks F1-Scores on the different datasets.

Disparité entre les scénarios : Si les performances des réseaux sont similaires sur S1, elles varient significativement sur S2. Par exemple, SWRFF obtient un mauvais score F1 sur S2 (entre 3,64 et 16,88%), en raison des changements d'emplacement, tandis que POWDER maintient de bonnes performances sur les deux scénarios grâce à des conditions plus stables, perdant moins de 10% en moyenne sur CNN_L et environ 20% sur CNN_S.

Disparité entre les réseaux : CNN_L surpasse CNN_S sur S1 grâce à sa profondeur et son plus grand nombre de paramètres, lui permettant de mieux traiter des données complexes. CNN_S, bien que plus léger, conserve une bonne précision avec des baisses mineures de score F1 (0,02 % à 1,57 % en moyenne sur S1). La BDD ORACLE s'avère la plus difficile pour CNN_S, qui manque de capacité pour s'entraîner au maximum.

Résilience et Variabilité : Sur S2, CNN_S surpasse parfois CNN_L, probablement parce que sa taille plus réduite favorise une meilleure généralisation, en évitant une sur-spécialisation du réseau. Il présente toutefois une forte dépendance sur la valeur d'initialisation des poids et à la façon dont les données sont séparées en entraînement-test, ce qui peut affecter la résilience. Certaines instances de CNN_S surpassent CNN_L, mais cette performance dépend fortement de la graine d'entraînement.

Choix de l'architecture : Le choix du réseau est crucial : les grands modèles sont plus fiables et adaptatifs, tandis que les petits offrent une meilleure résilience au prix d'une instabilité accrue.

La section suivante explore l'élagage pour optimiser la complexité des réseaux tout en maintenant leurs performances.

4 Élagage des Réseaux

4.1 Métriques

L'élagage peut être défini par la suppression ou la mise à zéro de poids sélectionnés au sein d'un réseau. Dans l'élagage non structuré, les poids sont généralement mis à zéro individuellement, ce qui revient à les considérer comme des composants inexistants du réseau. CNN_L, avec une sparsité de 97%, serait équivalent à CNN_S en termes de paramètres utiles.

Dans le contexte de l'élagage, définissons r comme le ratio de sparsité d'un réseau. Un masque $\mathcal{M} = \{(M_{W^k}, k \in [\![1, K]\!]\}$ est considéré pour le réseau $\mathcal{N}$. Les matrices M_{W^k} ont les mêmes dimensions que W^k. m_{w_j} désigne la valeur du masque pour un poids donné w_j, elles prennent la valeur 1 si le poids du réseau doit être conservé et 0 s'il doit être élagué. Le réseau élagué est définit de la façon suivante :

$$\mathcal{N}_r = \{(W^k \odot M_{W^k}), k \in [\![1, K]\!]\}, \tag{2}$$

avec $\odot$ la mutliplication point à point. La sparsité r est alors définie par :

$$r = 1 - \frac{1}{N} \times \sum_{w_j \in \mathcal{N}} m_{w_j}. \tag{3}$$

Le nombre de biais dans un réseau neuronal est négligeable par rapport au nombre de poids. Les biais sont donc ignorés lors de l'élagage.

4.2 Critère pour l'élagage non structuré

Plusieurs critères d'élagage existent pour réduire la complexité des réseaux (random, L1, SynFlow, ...) [6]. Ici, le critère LAMP [11] a été choisi car il s'agit d'un critère adaptatif, ne dépendant pas des données et relativement peu coûteux à mettre en place. Ce critère prend en compte l'importance de chaque poids relative à chaque couche et retire les poids indépendamment de la couche à laquelle celui-ci se trouve. Les poids ayant l'importance la plus faible seront éliminés en priorité. En considérant un poids $w_j \in W^k$, avec k la couche correspondante, on a l'importance associée à chaque poids :

$$S(w_j, W^k) = \frac{(w_j)^2}{\sum_{w_i \geq w_j, w_i \in W^k} w_i^2}. \tag{4}$$

4.3 Algorithme d'élagage

Les réseaux CNN_L et CNN_S initiaux (Table 2) sont élagués avec des niveaux de sparsité de 5% à 95% (incréments de 5%) et évalués pour S1 et S2 sur 5 graines. Les réseaux élagués sont ensuite testés sur diverses bases de données (Figures 2 à 5). Chaque point, représentant la moyenne de cinq graines, avec les valeurs extrêmes en transparence. Pour chaque courbe, le point le plus à droite représente une sparsité de 5%, celui à gauche de 95%. Les réseaux avec un score F1 > 99% présentant le moins de paramètres actifs sont en noir. Le taux d'élagage correspondants sont indiqués.

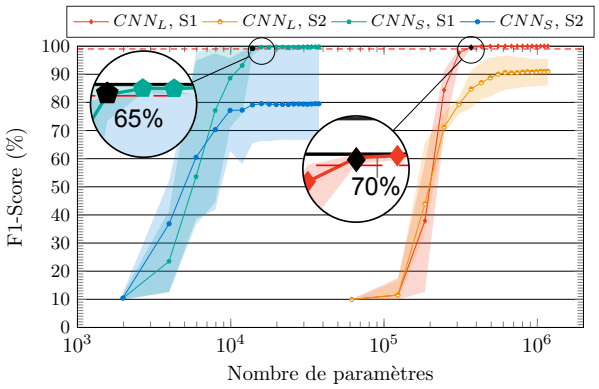

FIGURE 2 : Élagage des réseaux pour la BDD Powder.

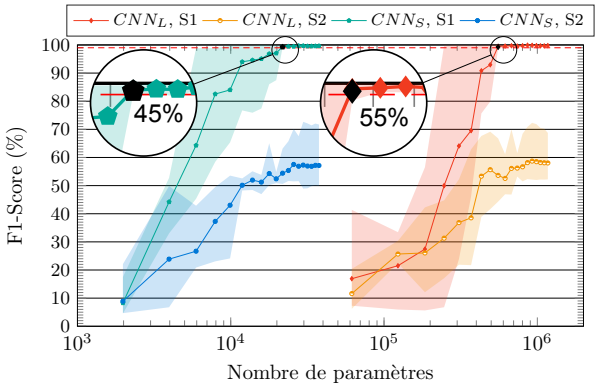

FIGURE 3 : Élagage des réseaux pour la BDD WiSig.

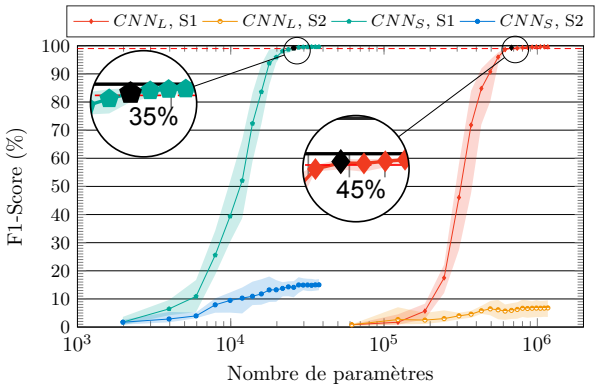

FIGURE 4 : Élagage des réseaux pour la BDD Oregon.

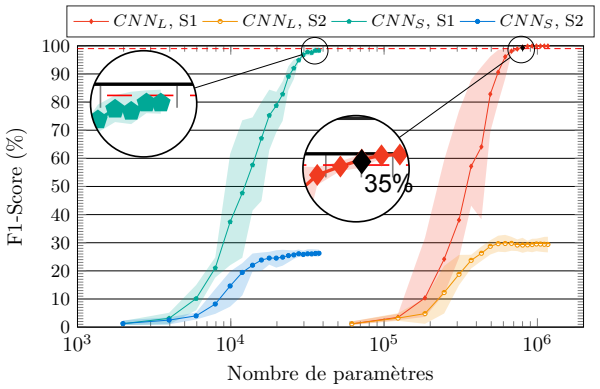

FIGURE 5 : Élagage des réseaux pour la BDD ORACLE.

Nombre de paramètres et score F1 : Pour toutes les BDD, les courbes de CNN_S restent à gauche de tous les CNN_L, car même élagué à 95%, CNN_L possède plus de paramètres que le CNN_S non élagué. Par exemple, si on souhaite conserver un score F1 supérieur à 99%, CNN_L peut être élagué jusqu'à 70% sur la BDD POWDER, mais cela représente toujours neuf fois plus de paramètres actifs que CNN_S original. Toutefois, CNN_L offre de meilleures performances sur toutes les bases de données et permet des taux d'élagage élevés, grâce à sa plus grande profondeur et son nombre de paramètres.

Stabilité sur les BDDs : On peut remarquer également que plus les BDD ont une tâche d'identification complexe (ex. SWRFF et ORACLE), plus l'élagage dégrade rapidement les performances, car la stabilité du réseau repose sur une plus grande proportion des poids du réseau.

Conservation des caractéristiques : L'élagage non structuré maintient le score F1 sur S1 tout en préservant les performances originales sur S1 ainsi que la résilience et la variabilité sur S2. En effet, les caractéristiques présentes en Table 2 sont retrouvées pour des réseaux élagués entre 35% et 70%, à condition que le réseau ait pu se stabiliser sur la base de données (ce qui n'est pas le cas de CNN_S sur la BDD ORACLE). Cette conservation de la variabilité est particulièrement visible pour CNN_S, sur la BDD POWDER.

La conception initiale du réseau est donc essentielle pour optimiser le score F1 et la taille du modèle. L'élagage non structuré sans réentraînement se montre efficace pour réduire le nombre de paramètres des réseaux pour l'identification des empreintes RF et s'adapter facilement à la cible matérielle voulue.

5 Conclusions

Cet article explore l'élagage non structuré pour compresser les CNN sans réentraînement, générant des réseaux clairsemés pour l'identification des empreintes RF. La comparaison de deux réseaux : un complexe, CNN_L, et un léger, CNN_S, sur quatre bases de données montre que CNN_L, avec neuf fois plus de paramètres, est plus stable, tandis que CNN_S affiche une forte variabilité selon les graines. L'élagage non structuré permet d'atteindre des taux de sparsité entre 35% à 60% en conservant 99% de score F1, mais le choix du réseau initial reste déterminant. L'élagage itératif, bien que nécessitant des données d'entraînement, pourrait optimiser à la fois la précision et la robustesse.

Remerciements

Ce travail est financé par l'Agence Nationale de la Recherche (ANR) sous le numéro ANR-22-CE25-0007-01 (RedInBlack).

Références

[1] Alice Chillet and *al.* Tangled Program Graph for Radio-Frequency Fingerprint Identification. In *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2023.

[2] Yann Le Cun and *al.* Optimal brain damage. In D. Touretzky, editor, *Advances in Neural Information Processing Systems*, volume 2. Morgan-Kaufmann, 1989.

[3] Yu Wang and *al.* An Efficient Specific Emitter Identification Method Based on Complex-Valued Neural Networks and Network Compression. *IEEE Journal on Selected Areas in Communications*, 39(8) :2305–2317, 2021.

[4] Tong Jian and *al.* Radio Frequency Fingerprinting on the Edge. *IEEE Transactions on Mobile Computing*, 21(11) :4078–4093, 2022.

[5] Yun Lin and *al.* GLR-SEI : Green and Low Resource Specific Emitter Identification Based on Complex Networks and Fisher Pruning. *IEEE Transactions on Emerging Topics in Computational Intelligence*, pages 1–12, 2023.

[6] Emma Bothereau and *al.* Investigating Sparse Neural Networks for Radio Frequency Fingerprint Identification. In *IEEE 100th Vehicular Technology Conference (VTC Fall)*, 2024.

[7] Guillem Reus-Muns and *al.* Trust in 5G Open RANs through Machine Learning : RF Fingerprinting on the POWDER PAWR Platform. In *IEEE Global Communications Conference*, 2020.

[8] Samer S. Hanna and *al.* WiSig : A Large-Scale WiFi Signal Dataset for Receiver and Channel Agnostic RF Fingerprinting. *IEEE Access*, 10 :22808–22818, 2021.

[9] Abdurrahman Elmaghbub and Bechir Hamdaoui. Distinguishable IQ Feature Representation for Domain-Adaptation Learning of WiFi Device Fingerprints. *IEEE Transactions on Machine Learning in Communications and Networking*, 2 :1404–1423, 2024.

[10] Kunal Sankhe and *al.* No Radio Left Behind : Radio Fingerprinting Through Deep Learning of Physical-Layer Hardware Impairments. *IEEE Transactions on Cognitive Communications and Networking*, 6(1) :165–178, 2020.

[11] Jaeho Lee and *al.* Layer-adaptive sparsity for the magnitude-based pruning. In *International Conference on Learning Representations (ICLR)*, 2020.