UNIVERSITÉ DE RENNES 1

Direction de la Recherche et de l'Innovation

Appel à projets - Année 2023

Contrats doctoraux «Ordinaires»

ECOLE DOCTORALE : MATISSE **POLE DE RECHERCHE : Mathématiques-Numérique**

Unité de recherche d'accueil

Unité de Recherche : IRISA

Equipe : Granit

Encadrement

Directeur de thèse : GAUTIER Matthieu **Unité de recherche** : IRISA

Employeur/Établissement d'origine : UR1

HDR : ☑ oui ☐ non **Nb de thèses en cours** : 2

Mail : matthieu.gautier@irisa.fr **Tél**. : 0296469301

Co-directeur de thèse : BERDER Olivier **Unité de recherche** : IRISA

Employeur/Établissement d'origine : UR1

HDR : ☑ oui ☐ non **Nb de thèses en cours** : 4

Mail : olivier.berder@irisa.fr **Tél.** : 0296469345

Sujet

Titre : Apprentissage frugal pour l'identification des empreintes radio-fréquence

Mots clés :

Cotutelle internationale (oui/non) : non **Si oui, préciser l'établissement et le pays de rattachement** :

Descriptif (15-30 lignes) :
Contexte socioéconomique et scientifique ; Les hypothèses et questions posées ; Les grandes étapes de la thèse et démarche ; Approches méthodologiques et techniques envisagées

Contexte : Le sujet se place dans le contexte de la sécurité des dispositifs sans fils communicants. Chaque émetteur (Dongle Bluetooth, puce Wifi, cellulaire, …) distord de manière unique le signal qu'il envoie. Cette empreinte unique nommée Radio-Frequency (RF) Fingerprint peut permettre une identification sans devoir recourir à un processus d'authentification réseau dédié (e.g adresse MAC) [1]. Très récemment, ces techniques ont suscité l'intérêt des chercheurs dans le contexte de la cybersécurité. Les signaux transmis peuvent en effet contenir des informations compromettantes dans des canaux cachés (clefs de cryptage, signal audio non protégé, …) : authentifier un émetteur de manière certaine permet ensuite de chercher et cibler ces vulnérabilités [2].

Problématiques : Depuis deux ans, les efforts en matière d'identification RF portent sur des techniques de deep learning (DL) [3]. Ces méthodes sont prometteuses mais les réseaux utilisés, issus du traitement de l'image, ne sont pas parfaitement adaptés à la détection d'empreinte RF. En particulier, ces réseaux sont souvent très complexes et disposent d'un nombre important d'opérations et de paramètres, rendant leur empreinte énergétique pendant l'apprentissage importante et une implémentation temps réel délicate pour l'inférence.
L'approche de classification s'appuie sur une bonne connaissance de l'utilisateur à identifier avec une phase d'entraînement réalisée à partir de l'empreinte de cet utilisateur. Cette phase d'entraînement et les modèles associés doivent prendre en compte les potentielles variations des paramètres du fait de la non-stationnarité de l'environnement RF. Le nombre de dispositifs à distinguer peut également être variable. L'adaptation et la reconfiguration de l'inférence doit permettre de pallier ces variations de l'environnement.

Objectifs : Le premier objectif de la thèse est de concevoir des méthodes frugales et flexibles de classification des empreintes RF : frugales pour être déployées sur des systèmes embarqués et flexibles pour s'adapter aux variabilités des données à classer. Pour valider ces méthodes sur des systèmes temps réel, un second objectif est de proposer une méthodologie et des outils permettant de pouvoir développer rapidement des applications et d'intégrer des algorithmes d'apprentissages sur des architectures embarquées.

Différents axes de travail sont donc envisagés :

- **Frugalité** : De nombreuses techniques permettent la réduction de la complexité des réseaux de neurones qui réalisent des tâches de classification. Certaines travaillent sur le format des données d'entrées [4], d'autres sur la suppression de tout ou d'une partie des éléments des couches des réseaux [5]. Enfin, des architectures de réseaux de neurones (e.g. TinyML ou Thin MobileNet [8]) ont été spécifiquement pensées et étudiées pour réduire leur complexité de manière à pouvoir envisager une implémentation temps réel sur une ressource matérielle [7,8]. Ces travaux demandent une analyse approfondie pour une application aux données d'identification RF.
- **Flexibilité** : Le système devra être capable de détecter des modifications de l'environnement de déploiement RF. Cette détection pourra s'appuyer sur des méthodes issues de l'apprentissage [9] (mesures de similarité ou d'anomalie) ou sur des algorithmes liés au contexte applicatif (e.g. estimation du canal). Il s'agira ensuite d'adapter l'algorithme de classification à ces nouvelles conditions en modifiant les pré-traitements potentiels, ou en effectuant un réentrainement. L'impact de cette reconfiguration sur les performances (précision, énergie) de l'implémentation associée sera pris en compte.
- **Exploration de l'espace de conception** : La réduction de complexité des réseaux de neurones a un impact sur la consommation d'énergie qu'il faut analyser et qui dépend de la cible d'exécution et de l'implémentation associée. Il s'agit de proposer des méthodes pour utiliser efficacement les ressources Hardware (HW) et Software (SW) des cibles (GPU, GPP, FPGA). On s'appuiera sur un modèle énergétique des cibles afin de choisir l'implémentation offrant le meilleur compromis entre précision de classification et énergie.

[1] N. Soltanieh, Y. Norouzi, Y. Yang, et N. C. Karmakar, « A Review of Radio Frequency Fingerprinting Techniques », IEEE Journal of Radio Frequency Identification., vol. 4, no 3, p. 222-233, sept. 2020, doi: 10.1109/JRFID.2020.2968369.
[2] C. Lavaud, R. Gerzaguet, M. Gautier, O. Berder, E. Nogues, et S. Molton, « Whispering Devices: A Survey on How Side-channels Lead to Compromised Information », Journal of Hardware System Security, vol. 5, no 2, p. 143-168, juin 2021, doi: 10.1007/s41635-021-00112-6.
[3] K. Sankhe et al., « No Radio Left Behind: Radio Fingerprinting Through Deep Learning of Physical-Layer Hardware Impairments », IEEE Trans. Cogn. Commun. Netw., vol. 6, no 1, p. 165-178, mars 2020, doi: 10.1109/TCCN.2019.2949308.
[4] M. Sabih, F. Hannig, et J. Teich, « Utilizing Explainable AI for Quantization and Pruning of Deep Neural Networks », 2020, doi: 10.48550/ARXIV.2008.09072.
[5] H. Tessier, V. Gripon, M. Léonardon, M. Arzel, D. Bertrand, et T. Hannagan, « Energy Consumption Analysis of Pruned Semantic Segmentation Networks on an Embedded GPU », in Advances in System-Integrated Intelligence, vol. 546, M. Valle, D. Lehmhus, C. Gianoglio, E. Ragusa, L. Seminara, S. Bosse, A. Ibrahim, et K.-D. Thoben, Éd. Cham: Springer International Publishing, 2023, p. 553-563. doi: 10.1007/978-3-031-16281-7_52.
[6] Y. Hu, S. Sun, J. Li, X. Wang, et Q. Gu, « A novel channel pruning method for deep neural network compression », 2018, doi: 10.48550/ARXIV.1805.11394.
[7] S. Tripathi, G. Dane, B. Kang, V. Bhaskaran, et T. Nguyen, « LCDet: Low-complexity fully-convolutional neural networks for object detection in embedded systems », juill. 2017.
[8] D. Sinha et M. El-Sharkawy, « Thin MobileNet: An Enhanced MobileNet Architecture », in 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York City, NY, USA, oct. 2019, p. 0280-0285. doi: 10.1109/UEMCON47517.2019.8993089.
[9] B. Desgraupes, « Clustering indices », University of Paris Ouest-Lab Modal'X, 2013.

➢ **Ce document est à renvoyer par la direction de l'unité de Recherche aux animateurs du Pole Recherche et à l'école Doctorale pour le 6 février 2023 au plus tard**