Work in Progress: Deep Learning vs. Traditional Learning for Radio Frequency Fingerprinting

Andréas J. Otto*, Seani Rananga*, Moshe Masonta†
*Department of Computer Science, University of Pretoria, South Africa
[1]u19218525@tuks.co.za
[2]seani.rananga@up.ac.za
†Council for Scientific and Industrial Research, Pretoria, South Africa
[3]MMasonta@csir.co.za

***Abstract*—Radio Frequency (RF) Fingerprinting is the theory of identifying a wireless device based on its unique transmitting characteristics which can improve authentication and security in wireless networks. This research project will briefly discuss RF Fingerprinting, Machine Learning, and implement and compare both deep learning and traditional learning techniques for RF Fingerprinting.**

***Index Terms*—Radio Frequency Fingerprinting, Deep Learning, Convolutional Neural Networks, Support Vector Machines, Supervised Learning.**

I. Introduction

RF fingerprinting refers to the premise of being able to identify a wireless device based on its unique electromagnetic emissions. These distinct transmissions produced by a wireless device are caused by physical attributes such as manufacturing imperfections [1]. RF fingerprinting consists of three steps, feature identification, feature extraction, and finally device identification. The identified features are inherent to the device's chipset and are independent of its physical location. The slight inconsistencies in the manufacturing of microcircuit components such as power amplifiers, filters, and clocks can result in substantial variations in phase offset and clock skew [1], [2] and thus signal variations as unique as our own fingerprints [3]. The main drive of RF fingerprinting is to add an additional Physical layer of security to wireless communication by means of improved device identification and authentication [4]. Incorporating a physical layer of security can mitigate wireless communication threats such as spoofing. [1].

Machine learning has proven to be an effective tool for extracting and interpreting features from complex datasets and can generally be divided into two categories, supervised and unsupervised learning. In supervised learning, algorithms are trained on labelled data to learn the relationship between input and output. This is used for tasks like classification, regression, and prediction. In unsupervised learning, algorithms find patterns in unlabelled data without prior knowledge of the output. This is used for tasks like clustering, anomaly detection, and dimensionality reduction. Both types have been effective in various applications, with supervised learning being effective when the output is known and unsupervised learning being effective when discovering hidden patterns in unstructured data. Furthermore advances in machine learning algorithms have resulted in deep learning which mimics the function of the brain and incorporates models like multilayered neural networks. [5], [6].

In this research project, we will investigate the use of supervised deep learning algorithms and supervised traditional learning algorithms for RF fingerprinting. Traditional learning algorithms refer to machine learning techniques that are based on statistical models, these include models such as K-Means clustering and Linear Regression. We will discuss the models to be utilized, Convolutional Neural Networks (CNN), and Support Vector Machines (SVM), and their applications to RF fingerprinting. These discussions will be found in the complete paper.

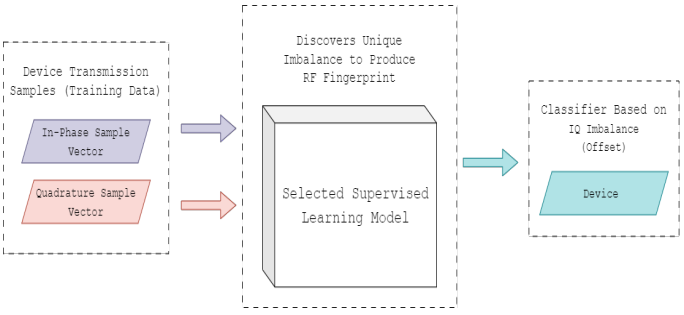

Figure: 1. Basic approach to RF Fingerprinting

II. Problem Domain of Radio Frequency Fingerprinting

It has become increasingly important to ensure secure and authorized wireless communication, and the accurate identification of wireless devices plays a critical role in this process. RF fingerprinting is a technique that has been proposed as a security and authorization measure to identify wireless devices

based on their unique electromagnetic emissions. As previously mentioned this technique exploits the physical attributes of devices such as manufacturing imperfections that result in unique signal transmission patterns. RF fingerprinting has the potential to address and improve wireless communication-authorization and -security within multiple sectors.

A. Research Objectives

The purpose of this research project is to compare the performance of traditional machine learning methods against deep learning techniques in the context of RF fingerprinting for wireless device identification. The primary objective of this project will be to implement and compare two machine learning models, one based on traditional learning and the other on deep learning. These models should be able to accurately classify transmitting devices based on their unique transmitting signatures. Only after both models have been implemented and tested can it be determined which of the techniques are best suited for the task.

The sub-objectives of the project include: (1) Evaluate and analyse the effectiveness of CNNs and SVMs. Gain insights into both their respective capabilities as well as their limitations for the task of RF fingerprinting. (2) Find and suggest further research to improve the task of RF fingerprinting. (3) Suggest additional use cases for RF fingerprinting and its real-world feasibility. Potential use cases such as improved spectrum access, and wireless device identification and localization.

B. Methodology

This section outlines the approach that will be used to achieve the objectives of this study:

1) Dataset Selection: We will utilize the ORACLE dataset, which contains a diverse collection of RF fingerprint samples from various wireless devices.
2) Pre-processing: The ORACLE dataset provides pre-processed, demodulated signals optimized for RF fingerprinting, addressing feature extraction and data pre-processing. [7]
3) Model Development: We will develop two machine learning models, namely CNN and SVM, using the PyTorch and Scikit-learn libraries, respectively.
4) Model Training and Evaluation: The ORCALE dataset will be split into training and testing datasets. Models will be trained and developed on the training set and then evaluated on the testing set. Comparative analysis and statistical methods will be used to compare the models and determine the significance of the different results.
5) Result Interpretation: The findings of the comparative analysis will be interpreted to identify the most effective technique for RF fingerprinting.
6) Proposed Development: Based on the results and insights gained, we will propose further development and potential real-world use cases for RF fingerprinting by means of machine learning.

III. Limitations and Outcome

Aspects such as other deep learning and traditional learning models, spectrogram datasets [8] and real-world testing will be out of scope. The useful developments and conclusions in this project will help investigate the limitations and uses of RF fingerprinting and the machine learning models tasked for RF fingerprinting. By creating and implementing models that can correctly identify a wireless device based on a constructed RF fingerprint it will provide insight into the potential real-world applications and implementation feasibility for RF fingerprinting.

Acknowledgement

References

[1] N. Soltanieh, Y. Norouzi, Y. Yang, and N. C. Karmakar, "A review of radio frequency fingerprinting techniques," *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 3, pp. 222–233, 2020.

[2] A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, "A comprehensive survey on radio frequency (rf) fingerprinting: Traditional approaches, deep learning, and open challenges," *Computer Networks*, vol. 219, p. 109455, 2022.

[3] O. Ureten and N. Serinken, "Wireless security through rf fingerprinting," *Canadian Journal of Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27–33, 2007.

[4] S. U. Rehman, K. W. Sowerby, S. Alam, and I. Ardekani, "Radio frequency fingerprinting and its challenges," in *2014 IEEE Conference on Communications and Network Security*, 2014, pp. 496–497.

[5] S. Ben-David and S. Shalev-Shwartz, *Understanding machine learning: From theory to algorithms*. Cambridge: Cambridge University Press, 2022.

[6] O. F.Y, T. AkinsolaJ.E., O. Awodele, O. HinmikaiyeJ., O. Olakanmi, and J. Akinjobi, "Supervised machine learning algorithms: Classification and comparison," *International Journal of Computer Trends and Technology*, vol. 48, pp. 128–138, 2017.

[7] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "Oracle: Optimized radio classification through convolutional neural networks," 2018.

[8] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, "Radio frequency fingerprint identification for lora using spectrogram and cnn," 2020.

Andréas Otto is currently working in the defence and aerospace industry with a focus on radio frequency spectrum monitoring and management. He is simultaneously completing his Honours degree in Computer Science at the University of Pretoria. He has a strong interest in the radio spectrum, neural networks, and general machine learning.

Seani Rananga is passionate about teaching, learning, researching, and sharing knowledge with students. She has gained experience working in both research establishments and tertiary institutions. Currently, she holds the position of a Computer Science lecturer at the University of Pretoria. She is involved with radio frequency spectrum management, machine learning, and natural language processing.

Moshe Masonta is a principal researcher and a research group leader for the Spectrum Access and Management Innovation research group at the CSIR, Pretoria, South Africa.