Review on CNN Algorithm based Radio Classification and RF Printing for Classifying Physical Layer Based Radio Signals

Unnikrishnen Nampoothiry[1] Prof. V. M. Lomte[2]
[1]Student [2]Head of Department
[1,2]Department of Computer Engineering
[1,2]R.M.D.Sinhgad School of Engineering, Warje, Pune, Maharashtra, India

Abstract— Every entity in this universe need to have a unique identification characteristic for it to associate with other components, in retrospect to this concept only the concept of Radio classification was carried out. The main prospect of this concept was the development of a unique way to give identification for radio signal using radio fingerprinting and identifying their uniqueness using CNN based and ML based algorithms. The key innovation here is to intentionally introduce controlled imperfections on the transmitter side through software directives, while minimizing the change in bit error rate. Unlike previous work that imposes constant environmental conditions, ORACLE adopts the 'train once deploy anywhere' paradigm with near perfect device classification accuracy (Kunal Sankhe, 2019).

Keywords: CNN, ML, Physical Layer, IQ Imbalance, K-nn, SVM, Oracle, RF, Radiofingerprinting, Shared Spectrum, MAC-ID, RSS, DC Offset, RELU, Deep Learning, USRP, MATLAB WLAN, Static Channel, Dynamic Channel, Confusion Matrix, EMD Matrix

Motivation: The main aspect that piqued the author for researching in this topic was the discrepancies produced in the physical level signals because of the lack of unique identification and characterization. This bounded with the current expansion of CNN based algorithms and efficient ML algorithms made it seem possible to provide a unique identification this signals. The first step in distinguishing radios in a shared spectrum environment by using machine learning to detect characteristic reference signatures embedded in their transmitted electromagnetic waves, a process known as RF fingerprinting. Combined with CNN based filtering this made the efficient implementation of the system plausible and implemented for further actions.

I. INTRODUCTION

To initiate an approach for detecting a unique radio from a large pool of bit-similar devices (same hardware, protocol, physical address, MAC ID) using only IQ samples at the physical layer.

Sensing the wireless spectrum and identifying active radios within the bands of interest directly impacts spectrum usage. The first step in distinguishing radios in a shared spectrum environment by using machine learning to detect characteristic reference signatures embedded in their transmitted electromagnetic waves, a process known as RF fingerprinting.

Our goal is to achieve this with information that can be leveraged at the radio hardware front-end.

We separately consider situations where the channel is unchanging between training and validation (idealized) and when the channel is dynamic (practical).

The key innovation in our approach, termed ORACLE, is that it learns the unique modifications present within the in-phase (I) and quadraturephase (Q) samples that are introduced in the signal as it passes through the transmitter chain. (Kunal Sankhe, 2019)

ML techniques have been remarkably successful in image and speech recognition; however, their utility for device-level fingerprinting by feature learning has yet to be conclusively demonstrated. True autonomous behaviour of SDRs, not only in terms of detecting spectrum usage, but also in terms of self-tuning a multitude of parameters and reacting to environmental stimulus, is now a distinct possibility. We collect over 20 * 10^6 RF I/Q samples over multiple transmission rounds for each transmitter-receiver pair composed of off-the-shelf USRP SDRs. The SDRs transmit standards-compliant IEEE 802.11ac physical layer waveforms to create a database of received signals. These I/Q samples carry embedded signatures characteristic of different active transmitter hardware, but are also subject to alterations introduced by the wireless channel. The approach of providing raw time series radio signal by treating the complex data as a dimension of two real valued I/Q inputs to the CNN is motivated by modulation classification. It has been found to be a promising technique for feature learning on large time series data. We develop a CNN architecture composed of multiple convolutional and max-pooling layers optimized for the task of radio fingerprinting. We partition the collected samples into separate instances and perform offline training on a computational cloud cluster, assigning weights to the inter-neuron connections. A holdout dataset composed of totally unseen samples is used for estimation of detection accuracy. (Shamnaz Riyaz, 2018)

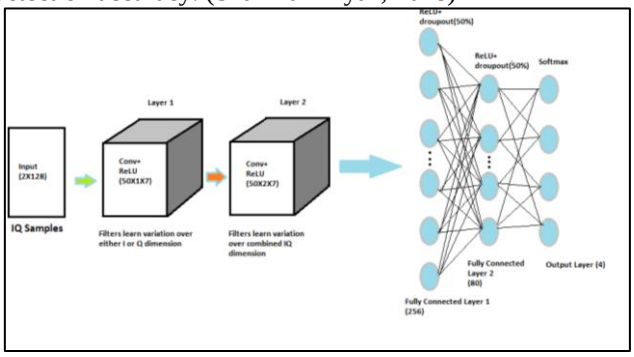

Fig. 1: Our proposed CNN architecture with two convolution and two fully connected layers.

II. LITERATURE SURVEY

Sr No.	Published Year	Published By	Research Topic	Access Parameter	Research Gap

1.	2006	J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Van Randwyk, D. Sicker	Passive data link layer 802.11 wireless device driver fingerprinting	Fingerprinting of devices connected on a wireless LAN	Various hindrance are present which can stop the fingerprinting procedure including automatic generation of noise, driver code modification, MAC address masquerading, and driver vulnerability patching.
2.	2008	I. O. Kennedy, P. Scanlon, F. J. Mullany, M. M. Buddhikot, K. E. Nolan, T. W. Rondeau	Radio Transmitter Fingerprinting: A Steady State Frequency Domain Approach	Radio Transmitter identification.	Limited efficiency in high SNR environments and other non-ideal environments
3.	2008	V. Brik, S. Banerjee, M. Gruteser, S. Oh	Wireless device identification with radiometric signatures	Radiometric Signature using PARADIS server.	Limited access to interfering networks or signals.
4.	2010	K. Gao, C. Corbett, R. Beyah	A passive approach to wireless device fingerprinting	Black-box Technique for device fingerprinting.	The experiments were conducted using a wireless testbed with emulated traffic as opposed to a live network with real traffic.
5.	2012	A. Krizhevsky, I. Sutskever, G. E. Hinton	Imagenet classification with deep convolutional neural networks	Training a large , deep CNN.	Usage of large and deep convolutional networks for extended applications.
6.	2015	S. V. Radhakrishnan, A. S. Uluagac, R. Beyah	GTID: A technique for physical device and device type fingerprinting	Device Fingerprinting using GTID	GTID to provide remote detection of resource utilization on a node.
7.	2016	Q. Xu, R. Zheng, W. Saad, Z. Han	Device fingerprinting in wireless networks: Challenges and opportunities	Device Fingerprinting	Fingerprinting Non-WiFi devices, Signal conditioning.
8.	2017	A. Selim, F. Paisana, J. A. Arokkiam, Y. Zhang, L. Doyle, L. A.DaSilva	Spectrum monitoring for radar bands using deep convolutional neural networks	Spectrum monitoring framework for radar signals.	Dataset should include other RATs, such as LAA-LTE, Multefire, and NB-IoT as SUs, and more radar waveforms.
9.	2017	T. J. O'Shea J. Hoydis	An Introduction to Deep Learning for the Physical Layer	Neural Network	Certain ML models and NN algorithms have different behaviour under similar circumstances.
10.	2018	S. Riyaz, K. Sankhe, S. Ioannidis, K. Chowdhury	Deep learning convolutional neural networks for radio identification	Radio network classification using CNN.	Varied CNN architectures may lead to significantly different results. Finding an optimal architecture that enhances device classification is an open research issue.

Table 1: Literature Survey for the given software system.

III. LIVE SURVEY

A. Radio Frequency Fingerprinting Extraction Based on Multidimensional Permutation Entropy.[14]

Just like we each have unique fingerprints, radio transmitters also have different radio frequency fingerprints, namely, RF fingerprints. This research was carried out by Shouyun Deng, Zhitao Huang, Xiang Wang, and Guangquan Huang.

Radio transmitter equipment has a complicated structure, and it is composed of many electronic devices. Baseband signal is processed in digital signal processor block and then goes into analog circuit parts. There are many nonlinear elements and unit circuits in analog circuit parts. Examples of nonlinear elements include power amplifier, nonlinear resistors, diodes, transistors, and field-effect tubes. The unit circuits may contain operational amplifiers, multipliers, absolute value circuits, and so on. The existence of these

nonlinear devices makes communication signals have nonlinear components.
Carried out on:
Received 08th Feb 2017
Revised 28th Jun 2017
Accepted 30th Jul 2017
Published 28th Aug 2017

B. Real-Time Recursive Fingerprint radio map creation algorithm combining Wi-Fi and Geomagnetism.[15]

Unlike Time of Flight (TOF)-based ultra-wide band (UWB) and chirp spread spectrum (CSS), which measure signal arrival times, fingerprint is an indoor-positioning technology based on measuring the received signal strength (RSS). Indoor spaces where it can be used are gradually expanding, owing to the increase in the use of wireless local area networks (WLANs) and the Internet of Things (IoT). Fingerprint can be divided into two types of technologies. One is node-based localization, which is based on indoor wireless communication technologies such as Wi-Fi. Published by Ju-Hyeon Seong and Dong-Hoan Seo
Carried out on:
Published online 2018 Oct 10

IV. ALGORITHMIC SURVEY

A. ORACLE based CNN algorithms[16]

A convolutional neural network consists of an input and an output layer, as well as multiple hidden layers. The hidden layers of a CNN typically consist of a series of convolutional layers that convolve with a multiplication or other dot product. The activation function is commonly a RELU layer, and is subsequently followed by additional convolutions such as pooling layers, fully connected layers and normalization layers, referred to as hidden layers because their inputs and outputs are masked by the activation function and final convolution.

Though the layers are colloquially referred to as convolutions, this is only by convention. Mathematically, it is technically a sliding dot product or cross-correlation. This has significance for the indices in the matrix, in that it affects how weight is determined at a specific index point.

Recall that logistic regression produces a decimal between 0 and 1.0. For example, a logistic regression output of 0.8 from an email classifier suggests an 80% chance of an email being spam and a 20% chance of it being not spam. Clearly, the sum of the probabilities of an email being either spam or not spam is 1.0.

Softmax extends this idea into a multi-class world. That is, Softmax assigns decimal probabilities to each class in a multi-class problem. Those decimal probabilities must add up to 1.0. This additional constraint helps training converge more quickly than it otherwise would.
Consider the following variants of Softmax:

Full Softmax is the Softmax we've been discussing; that is, Softmax calculates a probability for every possible class.

Candidate sampling means that Softmax calculates a probability for all the positive labels but only for a random sample of negative labels. For example, if we are interested in determining whether an input image is a beagle or a bloodhound, we don't have to provide probabilities for every non-doggy example.

Full Softmax is fairly cheap when the number of classes is small but becomes prohibitively expensive when the number of classes climbs. Candidate sampling can improve efficiency in problems having a large number of classes.

B. ML Algorithms

1) k-NN

KNN can be used for both classification and regression predictive problems. However, it is more widely used in classification problems in the industry. To evaluate any technique we generally look at 3 important aspects:

1) Ease to interpret output
2) Calculation time
3) Predictive Power

2) SVM

The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data point in the correct category in the future. This best decision boundary is called a hyperplane.

Sr No.	Dataset	Access Parameter	Algorithms	Complexity
1.	--	Fingerprinting of devices connected on a wireless LAN[1]	--	--
2.	--	Radio Transmitter identification.[2]	--	--
3.	Radio frequencies and broadcasting channels.	Radiometric Signature using PARADIS server.[3]	PARADIS-kNN PARADIS-SVM k-fold Cross Validation	$O(n^3)$ $O(n^3)$ O(n)
4.	-- --	Black-box Technique for device fingerprinting.[4]	maxCXCORR(dx, di) sim(Tx, Ti) Find_Best_Binsize(T) Build_Master_Signature()	O(n) O(n) $O(n^4)$ $O(n^4)$
5.	Imagenet- contains over 15 million HD images	Training a large , deep CNN.[5]	Data augmentation Dropout	O(n) Where n is the iterative step taken
6.	--	Device Fingerprinting using GTID[6]	ANN's: feedforward networks	$O(n^n)$ Where n can be the

			Device ID and Type identification	neural divisions. O(n) Where n is the ID passed
7.	--	Device Fingerprinting[7]	White-list based algorithms	O(xM(log x)) Based on Lutzl rule.
8.	Radar system model dataset.	Spectrum monitoring framework for radar signals.[8]	Data Pre-processing and data cleaning. CNN	Complexity depends on the layers of CNN.
9.	Any dataset is applicable	Neural Network [9]	CNN	Complexity depends on the layers of CNN.
10.	Radio frequencies and broadcasting channels.	Radio network classification using CNN.[10]	CNN	Complexity depends on the layers of CNN.

Table 2: Algorithmic Survey for the given software system.

V. CONCLUSION

From the above conducted survey and reviews it can be concluded that the Oracle based CNN algorithm can be effectively used as the filtering algorithm for assigning unique identifying features to the radio signals at the physical layer by the technique termed as RF printing or Radio Fingerprinting. This can be performed by using Machine Learning on the contents of the signal and performing signal conditioning along with filtering it out through a Convolutional neural network using ReLU as the activation function and softmax as the filtering algorithm.

REFERENCES

[1] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," IEEE Communications Surveys Tutorials, vol. 18, no. 1, pp. 94–104, Firstquarter 2016.
[2] T. J. O'Shea and J. Corgan, "Convolutional radio modulation recognition networks," 2016. [Online].
[3] A. Selim, F. Paisana, J. A. Arokkiam, Y. Zhang, L. Doyle, and L. A. DaSilva, "Spectrum monitoring for radar bands using deep convolutional neural networks," in IEEE GLOBECOM 2017.
[4] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Van Randwyk, and D. Sicker, "Passive data link layer 802.11 wireless device driver fingerprinting," in ACM USENIX Security Symposium - Volume 15, 2006.
[5] K. Gao, C. Corbett, and R. Beyah, "A passive approach to wireless device fingerprinting," in IEEE DSN 2010, June 2010, pp. 383–392.
[6] I. O. Kennedy, P. Scanlon, F. J. Mullany, M. M. Buddhikot, K. E. Nolan, and T. W. Rondeau, "Radio transmitter fingerprinting: A steady state frequency domain approach," in IEEE VTC, Sept 2008, pp. 1–5.
[7] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in ACM MOBICOM 2008.
[8] S. V. Radhakrishnan, A. S. Uluagac, and R. Beyah, "Gtid: A technique for physical device and device type fingerprinting," IEEE Transactions on Dependable and Secure Computing, Sept 2015.
[9] F. Chen, Q. Yan, C. Shahriar, C. Lu, W. Lou, and T. C. Clancy, "On passive wireless device fingerprinting using infinite hidden markov random field," submitted for publication.
[10] N. T. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric bayesian method," in IEEE INFOCOM, April 2011, pp. 1404–1412.
[11] T. J. O'Shea and J. Hoydis, "An introduction to machine learning communications systems," 2017. [Online].
[12] S. Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury, "Deep learning convolutional neural networks for radio identification," IEEE Communications Magazine, vol. 56, no. 9, pp. 146–152, 2018.
[13] Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in NIPS 2012.
[14] Radio Frequency Fingerprinting Extraction Based on Multidimensional Permutation Entropy https://www.hindawi.com/journals/ijap/2017/1538728/
[15] Real-Time Recursive Fingerprint radio map creation algorithm combining Wi-Fi and Geomagnetism https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6210187/
[16] https://towardsdatascience.com/a-comprehensive-guide-to-convolutional-neural-networks-the-eli5-way-3bd2b1164a53
[17] https://en.wikipedia.org/wiki/Convolutional_neural_network

