Use of Machine Learning for Radio Modulation Classification

Supervisor: He Chen *(IE)*
Student: Ruyi DAI *(AIST)*
The Chinese University of Hong Kong
1155173812@link.cuhk.edu.hk

***Abstract*—Wireless signals with specific features of transmitters can be used to verify the identity of transmitters and assist the authorization system. Recently, there has been a wide interest in using deep learning (DL) and neural networks for transmitter authorization. I studied an approach that identifies authorized transmitters. Besides, I learned the adaptation of Convolutional Neural Network (CNN) to complex-valued temporal radio signal domain and compared the efficiency of radio modulation classification using learned features against expert features-based methods on Google Colab, which can also be applied to the identification of Wi-Fi devices as I change the dataset. The advantage of these approaches is that DL operates on raw I/Q samples and distinguishes devices using only the signal modifications induced by hardware that serves as a unique signature for a particular device.**

***Keywords*: Crypto and Security, Deep Learning, Convolutional Neural Networks, modulation classification, RF Fingerprinting, Communication and Networking Theory**

I. INTRODUCTION

In the context of smart cities, autonomous vehicles, the Internet of Things (IoT), and wirelessly connected devices require the ability to reconfigure the systems and the protocol within the communications architecture, and it has become more challenging to secure them. Authentication is part of securing wireless devices to verify the identity. Despite the existence of many cryptography or security-based methods for authentication, they are not suitable for many IoT devices as the performance of these approaches depends on the receiver quality [1] and requires manual feature engineering.

Machine learning (ML) techniques have been remarkably successful in image and speech recognition; their potential for device-level fingerprinting by feature learning has been gradually demonstrated. Specifically, DL approaches are more robust and can extract better features from signals, thus leading to higher accuracy compared to feature-based approaches [2].

The approach of providing raw time series radio signals by serving the complex data as a dimension of two real-valued in-phase and quadrature (I/Q) inputs to the CNN is motivated by modulation classification [3]. I learned this approach which is based on strategies from image and voice recognition domains in ML using CNN, which offers flexibility to learning features across a wide range of tasks and demonstrates increased accuracy in classification among current approaches. It has been found to be a promising technique for feature learning on large time-series data.

II. RELATED WORK

The main idea behind RF-fingerprinting is to extract unique patterns (or features) and use them as signatures to identify devices. A variety of features at the physical (PHY) layer, medium access control (MAC) layer, and upper layers have been utilized for RF fingerprinting [4].

In my research project, our research group is interested in studying those features that are inherent to a device's hardware, which is also unchanging and not easily replicated by malicious agents.

Deep learning offers a useful framework for a supervised learning approach. It can learn functions of increasing complexity, leverages large datasets, and greatly increases the number of layers, in addition to neurons within a layer. There are also other works [2, 5] that apply deep learning at the physical layer, specifically focusing on modulation recognition using CNNs.

A. Baseline Classification Approach

Statistical Modulation Features: For digital modulation techniques, high order statistics and cyclo-stationary moments [6]are among the most widely used features to compactly sense and detect signals with strong periodic components, which is created by the structure of the carrier, symbol timing, and symbol structure for certain modulations. By incorporating knowledge of the structure, expected values of peaks in auto-correlation function (ACF) and spectral correlation function (SCF) surfaces have been used successfully to provide robust classification for signals with unknown or purely random data. For analog modulation where symbol timing does not produce these artifacts, other statistical features are useful in performing signal classification. Additionally, a number of analog features which capture other statistical behaviors which can be useful, including mean, standard deviation, instantaneous frequency, absolute normalized instantaneous frequency.

Decision Criterion: When mapping baseline features to a class label, machine learning or analytic decision processes can be applied. Decision trees on expert modulation features were firstly used in this field, but such decision processes have also been trained directly on datasets represented in their feature space. Popular methods here include support vector machines (SVMs), decision trees (DTrees) and other methods which combine a number of classifiers to improve performance.

B. Radio Channel Models

When modeling a wireless channel there are many stochastic models for propagation effects [7 a]. Primary impairments seen in any wireless channel include: carrier frequency offset, symbol rate offset, delay spread and thermal noise. Each of these effects can be modeled well and is present in some form on any wireless propagation medium.

C. Deep Learning Classification Approach

DL relies on SGD to optimize large parametric neural network models and the core approach remains mainly unchanged. Neural networks consist of a series of layers which map each layer h_0 to output h_1 using parametric dense matrix operations. This can be expressed as follows, where weights W, have the dimension $|\, h_0 \times h_1 \,|$, bias b, has the dimension $|\, h_1 \,|$, and max is applied element-wise per-output $|\, h_1 \,|$.

$$h_1 = max(0, h_0 W + b) \tag{1}$$

Convolutional layers can be formed by assigning a shape to inputs and outputs and forming W from the replication of filter tap variables at regular strides across the input.

Training typically leverages a loss function (L), in this case categorical cross-entropy, between one-hot known class labels y_i (a zero vector, with a one value at the class index i of the correct class) and predicted class values $\hat{y}_i$.

$$\mathscr{L}(y,\hat{y}) = \frac{-1}{N}\sum_{i=0}^{N}\left[y_i \log\left(\hat{y}_i\right) + (1-y_i)\log\left(1-\hat{y}_i\right)\right]$$

Back propagation of loss gradients can be used to iteratively update network weights for each epoch n within the network until validation loss is no longer decreasing.

Regularization is used to reduce over fitting to training data. I used batch normalization [8 a] for regularization of convolutional layers and Alpha Dropout [9 a] for regularization of fully connected layers.

III. METHODOLOGY

A. *Modulation Recognition*

Modulation Recognition is the task of classifying the modulation type of a received radio signal as a step towards understanding what type of communications scheme and transmitter is present.

This can be served as an N-class decision problem where the input is a complex base-band time series representation of the received signal. That is, in-phase and quadrature components of a radio signal are sampled at discrete time steps through an analog to digital converted with a carrier frequency roughly centered on the carrier of interest to obtain a $1 \times N$ complex-valued vector.

B. *CNN Architecture*

Several other feature learning methods are also evaluated, but the principal method is that of a CNN provided with a windowed input of the raw radio time series.

The proposed method consists of two stages: a training stage and an identification stage. In the former, the CNN is trained using raw IQ samples to solve a multi-class classification problem. In the identification stage, raw IQ samples of the unknown transmitter are fed to the trained neural network, and the transmitter is identified based on the observed value at the output layer.

The convolution layer is the core building block of CNN, whose primary purpose is to extract features from the input data. It consists of a set of spatial filters (also called kernels) that perform a convolution operation over input data. Each convolution layer consists of a set of filters, which in turn operate independently to produce a set of two-dimensional feature maps. The CNN architecture is composed of the convolution layer followed by an activation step that performs a predetermined nonlinear transformation on each element of the feature map. There are many possible activation functions, such as *sigmoid* and *tanh*; the most used activation\n function in this architecture is the rectified linear unit (*ReLU*), as CNNs with *ReLU* train faster compared to alternatives. Figure 1 illustrates the flow-process of the network.

The output of the pooling layer is provided as input to the fully connected layer. A fully connected or dense layer is a traditional multi-layer perceptron (MLP), where the neurons have full connections to all activation steps in the previous layer, similar to regular neural networks. Its primary purpose is to perform the classification task on high-level features extracted from the preceding convolution layers. At the output layer, a *softmax* activation function on the one-hot output layer is used. The classifier with a *softmax* activation function gives probabilities for different class labels.

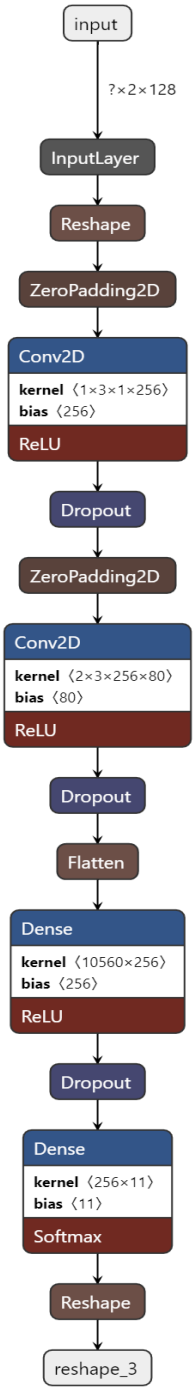

Fig. 1: Flow-progress Diagram of CNN

C. Dataset Parameters

The dataset is available in pickled python-format on the website[1], consisting of time-windowed examples and corresponding modulation class and SNR labels [10].

In this approach, they focus on a dataset consisting of 11 modulations: 8 digital and 3 analog modulations, all widely used in wireless communications systems. These consist of BPSK, QPSK, 8PSK, 16QAM, 64QAM, BFSK, CPFSK, and PAM4 for digital modulations, and WB-FM, AM-SSB, and AM-DSB for analog modulations.

[1] http://radioml.com

IV. TECHNICAL APPROACH

A. *Evaluation Networks*

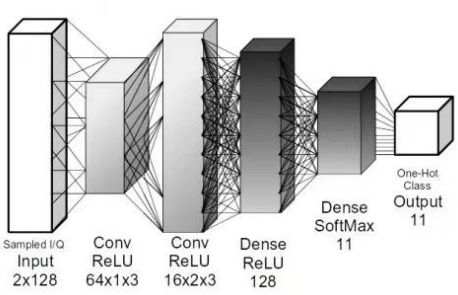

Fig. 2: CNN Architecture [6]

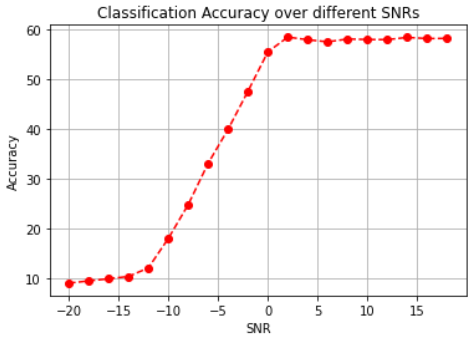

Fig. 3: Classification Accuracy of ANN over Different SNRs

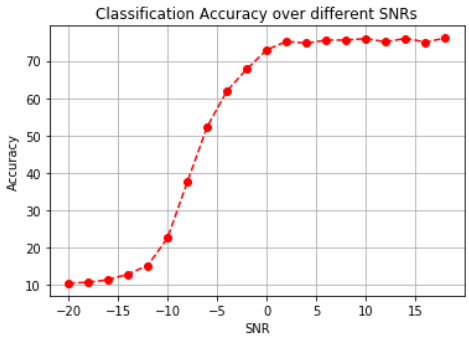

Fig. 4: Classification Accuracy of CNN over Different SNRs

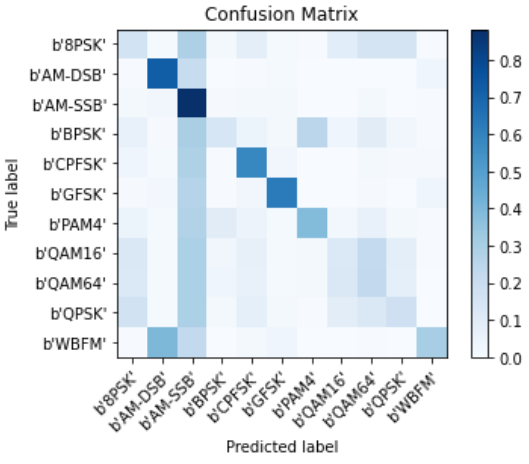

Fig. 5: 11-Modulation Confusion Matrix for ANN

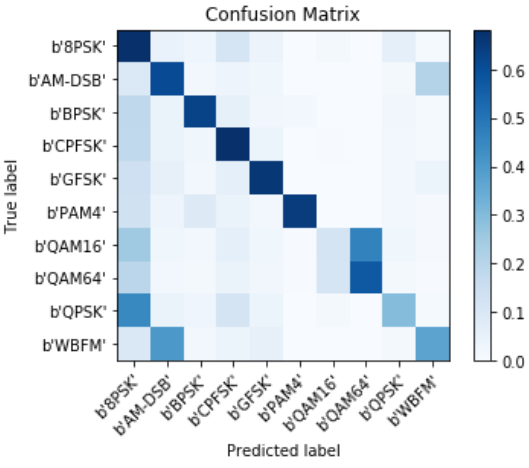

Fig. 6: 11-Modulation Confusion Matrix for CNN

Several candidate neural networks are trained. A 4-layer network utilizing 2 convolutional layers and 2 dense fully connected layers. Layers use rectified linear (*ReLU*) activation functions except for a *Softmax* activation on the one-hot output layer. An illustration of the CNN architecture is shown in figure 2.

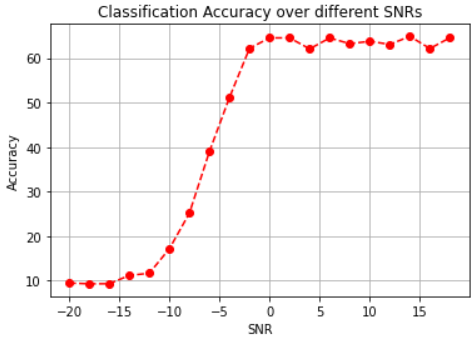

Fig. 7: Improved Classification Accuracy of CNN over Different SNRs

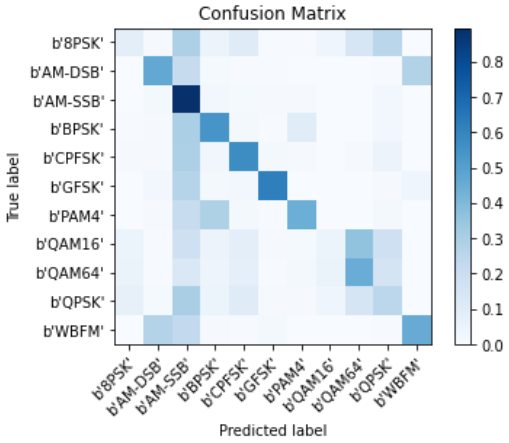

Fig. 8: Improved Confusion Matrix for CNN

B. Training Complexity

The highest complexity model is trained with the Adam solver over approximately 900,000-sample training set in batch sizes of 1024. Although validation loss does not significantly inflect, the best validation loss model is kept.

V. RESULTS

To evaluate the performance of the classifier, 12 million complex samples are divided into training examples of 128 samples in length across the 11 modulations. These samples are uniformly distributed in SNR from -20dB to +20dB.

In figure 4, degradation of the classifier under impairments is shown, 75% classification accuracy across all SNRs on the test dataset is achieved after training. In cases where SNR is higher, a clean diagonal in the confusion matrix can be seen. At low SNR, the accuracy is around 50% with +－20%. In figure 5 and figure 6 I show a confusion matrix for the classifier across all 11 classes where SNR is greater than zero. Besides, I limited the SNRs before the dataset is put into the training model. And improved results can be seen in figure 7 and figure 8. It can be seen that one of the largest sources of error are between phase shift keying (PSK) and AM modes, as well as between high order quadrature amplitude modulation (QAM) (16/64-QAM). This is largely to be expected as for short-time observations, and under noisy observations, QAM and PSK, especially for high order ones, can be extremely difficult to tell apart through any approach.

The classification time using CNN architecture with Keras compiled python is significantly faster than most of the other models including nearest-neighbor and SVM models. A ConvNet-based classification model of this scale for such a dataset presents an attractive choice for this task when classification performance is considered.

VI. DISCUSSION

In this work, I have extended prior work on using deep convolutional neural networks for radio signal classification. The approach has shown that deep networks do provide significant performance gains for time-series radio signals, contrary to prior work. This approach classifies 11 different modulation schemes. I have to mention that the approach does not identify a device, only the modulation type used by the transmitter.

My work mainly focuses on training the model with actual experimental data instead of similar problems with synthetic data in previous work. So there is no standard dataset to evaluate the performance of the classifier or network. I have also conducted a much more thorough set of performance evaluations on how this type of classifier performs over a wide range of parameters and training dataset parameters.

Finally, as a future goal during the research, my objective is to validate the performance of the classifier to identify signals and devices at different distances or under different SNRs. This may also require us to effect major changes in the architecture or dataset to increase robustness to signal amplitude and channel variations.

VII. CONCLUSION

DL methods continue to show enormous promise in improving radio signal identification sensitivity and accuracy. I learned this RF fingerprinting approach to train based on DL CNN architecture using I/Q sequence examples. The design enables learning features embedded in the signal transformations of wireless transmitters and identifies specific devices. Although the results are not a comprehensive comparison of expert feature-based modulation classifiers in the case of the CNN method, they do show that CNN on time series radio signal data are applicable. The approach also holds the possibility to easily scale to additional modulation classes and Wi-Fi devices [11], and this may be a step towards real world use. The performance trades shown in this work help shed light on some key parameters in data training, hopefully helping increase understanding and focus future efforts on the improvement of the CNN architecture and optimization of such systems.

REFERENCES

[1] S. U. Rehman, K. Sowerby, and C. Coghill, “Analysis of receiver front end on the performance of RF fingerprinting,” in *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*, pp. 2494–2499, Sept. 2012.

[2] S. Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury, “Deep Learning Convolutional Neural Networks for Radio Identification,” *IEEE Communications Magazine*, vol. 56, pp. 146–152, Sept. 2018.

[3] T. J. O’Shea, T. Roy and T. C. Clancy, "Over-the-air deep learning based radio signal classification", *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 168-179, Feb. 2018.

[4] Q. Xu et al., “Device Fingerprinting In Wireless Networks: Challenges and Opportunities,” *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 1, 2016, pp. 94–104.

[5] T. J. O’Shea and J. Hoydis, “An Introduction to Machine Learning Communications Systems,” *CoRR*, vol. abs/1702.00832, 2017; http://arxiv.org/abs/1702.00832

[6] C. M. Spooner, A. N. Mody, J. Chuang, and J. Petersen, “Modulation recognition using second- and higher-order cyclostationarity,” in *Dynamic Spectrum Access Networks (DySPAN), 2017 IEEE International Symposium on*, IEEE, 2017, pp. 1–3.

[7] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[8] S. Ioffe and C. Szegedy, “Batch normalization: Accelerating deep network training by reducing internal covariate shift,” in International Conference on Machine Learning, 2015, pp. 448–456.

[9] Klambauer, T. Unterthiner, A. Mayr, and S. Hochreiter, “Self-normalizing neural networks,” *ArXiv preprint arXiv:1706.02515*, 2017.

[10] T. J. OShea, J. Corgan, and T. C. Clancy, “Convolutional radio modulation recognition networks,” in *Proc. Int. Conf. Eng. Appl. Neural Network.*, 2016, pp. 213–226.

[11] S. Hanna, S. Karunaratne and D. Cabric, "Open Set Wireless Transmitter Authorization: Deep Learning Approaches and Dataset Considerations", *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, pp. 59-72, Mar. 2021.