國立清華大學 電機工程學系

實作專題研究成果摘要

Device Identification based on RF Fingerprint

基於射頻指紋的裝置識別

專題領域：通訊領域

組　　別：B244

指導教授：劉光浩 教授

組員姓名：鄭德穌

研究期間：111年 2 月至 111 年 11 月止，共 10 個月

摘要

射頻訊號在經過不同的硬體設備發送時，因為硬體的不完美性，導致傳送之射頻訊號會帶有些微的硬體特徵，這些特徵就像是指紋，藉由辨別指紋即可達到射頻裝置的識別。而 ORACLE(Optimized Radio clAssification through Convolutional neuraL nEtworks)是利用射頻指紋，以機器學習的方式，對射頻訊號進行識別的模型，在 2019 年被 Sankhe 等人提出，發表在 IEEE INFOCOM 會議上。

此次專題，主要研究 ORACLE 如何對動態環境下的射頻裝置進行穩健、高正確率的分類，由於作者並未提供程式碼，我們以 TensorFlow 實際建立模型，利用美國 Northeaster University 的開源資料庫，進行模型訓練，並畫出損失函數曲線(loss function curve)，判別模型學習情況。

從損失函數曲線、正確率曲線判別，ORACLE 方法在動態通道環境下具有極佳的分類成果。

報告內容

一、前言

射頻指紋是一種新興的裝置識別技術，但是這種技術大多都仰賴特定儀器和硬體設備，對於大規模測試及佈建相當難以達成。

2019 年，Sankhe 等人提出了基於卷積神經網路的最佳射頻裝置識別(Optimized Radio clAssification through Convolutional neuraL nEtworks)，在 802.11a 的協議下，靜態通道環境和動態通道環境都獲得良好的分類結果。尤其是其在動態通道環境的辨識方法，以特殊的方式達成可擴展性以並兼顧正確性，讓射頻裝置識別不再只侷限在特定環境的實驗中。

在此次專題中主要了解 ORACLE 方法中，動態通道環境下的裝置識別方式，並且使用 tenserflow 做出實際模型，利用美國 Northeaster University 的開源資料庫之資料集，對模型進行訓練，並畫出損失函數曲線判讀模型學習情況。

二、原理分析與系統設計

2.1 原理分析

2.1.1 ORACLE (Optimized Radio clAssification through Convolutional neuraL nEtworks)

這次專題主要是使用 Sankhe 等人在 2019 年提出的利用卷積神經網路的最佳射頻分類方法，以下簡稱 ORACLE。這個卷積神經網路模型是由 AlexNet 得到啟發，在簡化改造而成。整體模型為四層卷積神經網路架構，由兩層卷積層和兩層密集層所構成。為了確保模型能夠學習到正確的特徵，輸入層的大小為 2*128，其中 2 代表輸入訊號有實部和虛部，128 代表長度為 128 的 window sequence。而在第一層卷積層中，包含 50 個 filter，尺寸為 1*7。第二層卷積層中，包含 50 個 fliter，尺寸為 2*7。在兩層卷積層中階使用 ReLU 當作 activation function。第三和第四層皆為密集層，分別含有 256 及 80 個 neurons，並且在最後使用 softmax 為輸出層進行類別分類。為了避免過度擬合，在兩層密集層中都設置了 dropout，比率為 50%，並且在模型中加入 L2 正則化，設定正則化參數 $\lambda = 0.0001$。模型中的權重訓練則是採用 Adam optimizer，設定 learning rate = 0.0001。而 loss function 則是採用 categorical cross-entropy。

2.1.2 射頻指紋 (RF fingerprinting)

在訊號傳送與接收時，因為硬體設備的不完美，進而影響到輸出訊號。這種訊號跟設備間的特殊連結，再加上硬體瑕疵的不可複製性，使其具備如同指紋般的性質，因此可以藉由觀察這些射頻指紋，達到辨識裝置的目的。

在 ORCLE 當中，主要是利用 IQ Imbalance 和 DC Offset 當作裝置識別的主要依據。

(1) IQ Imbalance

受到放大器以及本地端震盪器的影響，在接收端的訊號，可能產生實部與虛部的振幅不匹配和相位不匹配的情況。

以下將接收訊號表示成

$$y(t) = \alpha x_I(t)cos\left(2\pi f_c t + \frac{\phi}{2}\right) + \beta x_Q(t)sin\left(2\pi f_c t - \frac{\phi}{2}\right) \quad (1)$$

其中$x_I(t)$、$x_Q(t)$為基頻訊號之實部及虛部，α、β為實部和虛部各自的放大倍率，ϕ代表兩者間的相位差。若是沒有 IQ Imbalance 的情況下，$\alpha = 1$、$\beta = 1$且$\phi = 0$。

而為了比較每個系統訊號不平衡的程度，這裡使用了 IMRR (Image Rejection Ratio)當作判別系統抑制不平衡性能的指標。

IMRR (Image Rejection Ratio)可以衡量系統抑制不平衡的程度，是因為 IQ 不平衡會在接收端頻譜，以$f = 0$為對稱軸產生鏡向頻率，鏡向頻率越大，帶表不平衡影響越嚴重。因此，IMRR 的計算方式為，計算接收之頻譜功率除鏡向之頻譜功率的比值，比值越小，抑制不平衡的效果越加。

利用(1)，先求出接收端經過本地震盪器的訊號

$$x_I'(t) = \frac{2}{T}\int_0^T y(t)\cos(2\pi f_c t)\,dt = \alpha x_I(\mathrm{t})\cos\left(\frac{\phi}{2}\right) + \beta x_Q(\mathrm{t})\sin\left(\frac{\phi}{2}\right)$$

$$x_Q'(t) = \frac{2}{T}\int_0^T y(t)\sin(2\pi f_c t)\,dt = \alpha x_I(\mathrm{t})\sin\left(\frac{\phi}{2}\right) + \beta x_Q(\mathrm{t})\cos\left(\frac{\phi}{2}\right) \quad (2)$$

現在將$x(\mathrm{t})$帶入$e^{j2\pi f_c t}$，因此$x_I(\mathrm{t}) = \cos(2\pi f_c t)$，$x_Q(\mathrm{t}) = \sin(2\pi f_c t)$。接著對接收訊號乘上$e^{-j2\pi f_c t}$並積分，可以得到$Y_{+\omega}$。

$$\begin{aligned} Y_{+\omega} &= \frac{2}{T}\int_0^T [x_I{}'(t) + jx_Q{}'(t)]e^{-j2\pi f_c t}dt \\ &= \frac{1}{2}\left(\left[\alpha\cos\left(\frac{\phi}{2}\right) + \beta\cos\left(\frac{\phi}{2}\right)\right]\right. \\ &\qquad \left. + j\left[\alpha\sin\left(\frac{\phi}{2}\right) - \beta\sin\left(\frac{\phi}{2}\right)\right]\right) \end{aligned} \tag{3}$$

對接收訊號乘上$e^{j2\pi f_c t}$並積分，則可以得到$Y_{-\omega}(t)$。

$$\begin{aligned} Y_{-\omega} &= \frac{2}{T}\int_0^T [x_I{}'(t) + jx_Q{}'(t)]e^{j2\pi f_c t}dt \\ &= \frac{1}{2}\left(\left[\alpha\cos\left(\frac{\phi}{2}\right) - \beta\cos\left(\frac{\phi}{2}\right)\right]\right. \\ &\qquad \left. + j\left[\alpha\sin\left(\frac{\phi}{2}\right) + \beta\sin\left(\frac{\phi}{2}\right)\right]\right) \end{aligned} \tag{4}$$

其中$Y_{+\omega}$代表受 IQ 不平衡影響的接收頻率訊號(正頻)，而$Y_{-\omega}$則代表 IQ 不平衡所產生出的鏡向訊號(負頻)。藉由計算兩者的平方並相除，可得到

$$\begin{aligned} IMRR &= \frac{|Y_{-\omega}|^2}{|Y_{+\omega}|^2} \\ &= \frac{\alpha^2 + \beta^2 - 2\alpha\beta\cos(\phi)}{\alpha^2 + \beta^2 + 2\alpha\beta\cos(\phi)} \end{aligned} \tag{5}$$

(2) DC Offset

在接收端，由於接收端震盪器洩漏(LO Leakage)，導致接收直流頻率變大，進而使訊號產生偏移。而藉由測量 main tone 在 DC frequency 的功率，找出 DC offset。

2.1.3 EMD (Earth Mover's Distance)

Earth Mover's Distance 是 Rubner 於 2000 年提出，用於衡量圖片相似度的一個做法。這個方式，也在 ORACLE 中，用來衡量兩個訊號的相似程度。

假設在$\mathbb{R}^2$有兩個集合 A、B，另這兩個集合大小相同。另有從 A 到 B 的所有可能對射(bijection)函數集合 F，則 A 和 B 的 EMD 可以表示為

$$EMD(A,B) = \min_{f\in F}\sum_{x\in A}\|x - f(x)\| \tag{6}$$

EMD 越小，代表集合 A、B 間的相似度愈高。

2.1.4 Dataset

由於本次專題是使用的 dataset 為 ORACLE 論文中所使用之實驗數據，因此在此說明數據產生的方式。

原本 ORACLE 訓練 ML 模型的方式，是直接將軟體定義無線電 USRP 產生之未解調訊號輸入模型，可是用這個方式訓練出來的模型，即使分類和訓練時相同的設備，仍會因為時間環境不同，使得分類結果變得不可預測。

因此 ORACLE 對於動態通道的裝置辨識，採用一種特殊的 feedback 迴路，這個設置會將接收端的訊號用有限的方式接回傳送端，校正通道並加入特殊的 impairment，使得模型訓練的是經過特殊處理過的解調訊號，在該論文中也證明這樣的設計可以讓裝置辨識與時間環境無關，達成動態通道下的識別。

2.1.5 Impairment set

ORACLE 在論文中，將 IMRR 和 DC offset 分成不同的程度(IMRR 從-9dB 到-44dB 分成 80 個 level；DC offset 從-82dB 到-140dB 分成 120 個 level)，接著根據實驗環境的 SNR，選擇在不超出 BER 限制下，能添加的 IMRR 和 DC offset 上限。

這些 impairment 會結合至傳送訊號上，當成識別裝置最重要的依據。在這個過程中，有兩個必須滿足的條件，第一，訊號加入 impairment 後不能超過 BER 限制；第二，加入 impairment 的訊號要能夠跟其他訊號做出一定程度以上的區別。

因此，定義一個集合 S，並根據產生的 BER 大小，將不同程度的 IQ imbalance 由大到小排列，產生 $[c_1, c_2, \cdots, c_{max}]$，其中，$c_{max}$ 不超出 BER 限制。接著從 c_1 開始，依序將不同程度的 IQ imbalance 加入 S 中。而任何將被加入的 c_i 都必須與 S 裡的所有元素計算 EMD，如果 EMD 大於設定的 threshold，即可加入 S 中。這樣的步驟是確保每個加入的 IQ imbalance 都要互相保有足夠的差異，以確保模型能夠正確分辨每個裝置。

2.1.6 Impairment allocation

在產生出可用的 impairment 集合後，需要將這些 impairment 實際配置到裝置上。而因為添加 impairment 後會導致 BER 增加，而且 SNR 也可能不同，因此必須在滿足 BER 限制下達成分配。

給定 K 個裝置 $[r_1, r_2, \cdots, r_K]$，其對應的平均 SNR 為 $[snr_1, snr_2, \cdots, snr_K]$。接著找出每個裝置 r_i 可以承受的最大 impairment，記作 c_{max}^i，並依據 c_{max}^i 重新排序

$[r_1, r_2, \cdots, r_K]$。給定兩個集合 R_1、R_2，分別容納可以被歸類的裝置及不可被歸類的裝置。

最後，從 r_1 開始依序配置$[c_1, c_2, \cdots, c_n]$，只要 $c_i \leq c_{max}^i$ 就將 c_i 配置給 r_i，並將 r_i 加入 R_1；反之將 r_i 加入 R_2。配置完一輪後，如果 R_2 不為空集合，則重複上述動作，並使用其他種類的 impairment (例如 DC offset)，直到所有的裝置都配置到 impairment。

2.2 系統設計

這次專題中，主要是使用 ORACLE 的模型，並將 Northeaster University 的開源資料集，也就是 ORACLE 一文中的實驗資料，匯入模型並觀察其結果。

首先是模型的搭建，整體的架構取用 ORACLE 中的卷積神經網路模型，並使用 tensorflow 2.8 在筆電上運行。接著是資料引入，為了觀察模型在動態通道下的辨識效能，因此使用所提供的第二個資料集，其資料採用 SigMF 格式紀錄。為了確保載入後的資料是模型正確的輸入，因此在載入後先將資料在 IQ 平面作圖，並對照 ORACLE 文中圖片，確定其是訊號解調後的複數資料。確認資料正確後，進一步觀察資料是否需要做預處理。最後則是將資料分成訓練、驗證及測試三個部分。

三、實驗結果

此次專題中，使用美國 Northeaster University 的開源資料庫之資料集，執行 ORACLE 文中的卷積神經網路模型，進行動態通道下的裝置辨識訓練，並畫出訓練過程中的損失函數曲線。

3.1 損失函數曲線

下圖為訓練次數 60 次，對 16 個裝置進行識別的 ORACLE 模型之損失函數曲線圖。訓練模型時使用 GPU 加速運算，訓練時間約在 30~40 分鐘。

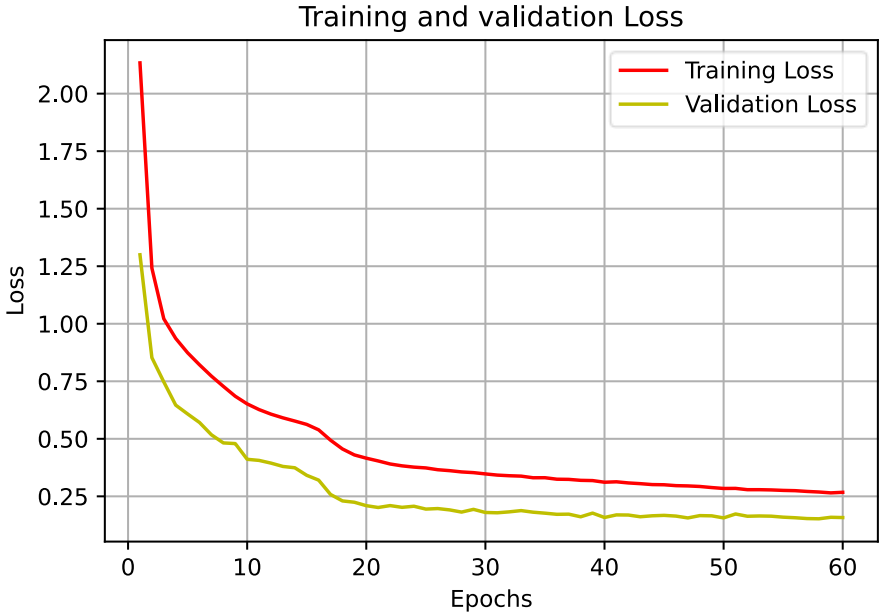

圖 3.1.1 Training and validation loss curve

損失函數的判別是為了確保模型沒有過擬合(overfitting)及欠擬合(underfitting)，藉由判讀損失函數曲線，可以對模型的訓練方向進行推估，進而調整參數使模型效能最佳化。而因為本次實驗模型中含有 L2 正則化(L2 regularization)以及 dropout，導致損失函數曲線必須特別判讀。

其中 L1、L2 正則化會讓訓練集的 loss 較驗證集高，但會隨著訓練次數增加而漸漸縮短差距。Dropout 也會讓訓練集的 loss 較高，不同的是，訓練集和 驗證集間 loss 的差距並不會隨著訓練次數增加而降低，而是會維持著差不多的距離，且訓練集的損失函數曲線會有些許波動。

從以上所述，可以看出，ORACLE 模型並未出現過擬合(overfitting)以及欠擬合(underfitting)，且損失函數曲線較偏向受 dropout 的影響，因此判定此模型得到正確的學習。並且正確率曲線與測試集對模型之效能評估，也皆出現高於 99%之準確率，說明模型有高正確性。

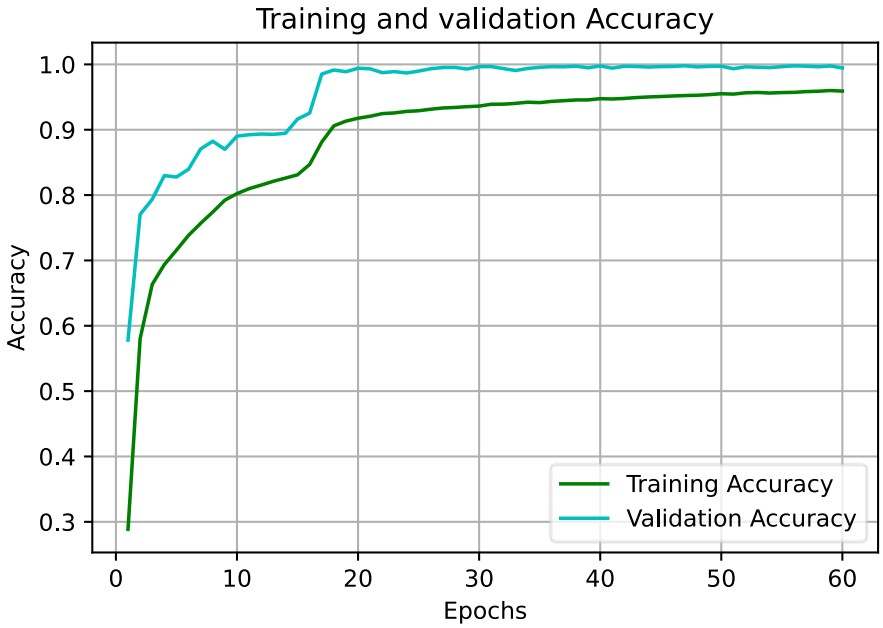

圖 3.1.2 Training and validation accuracy curve

四、結論

這次專題使用 ORACLE 模型及其提供之資料集訓練該模型，由損失函數曲線判讀模型得到正確學習，並由正確率曲線及測試集測試結果實證模型有高達 99%之正確率。

心得感想

首先感謝劉光浩教授，在這一年的專題過程中所有的指導及照顧，一步一步地帶著我完成這個專題。

起初在選擇專題題目時，因為自己就對通訊領域非常有嚮往，再加上這個題目又會碰上機器學習，電機資工兩邊的知識都會學到，讓我更加感興趣。不過在做這個題目之前，我完全沒有任何機器學習的背景，所以剛開始也花了相當多的時間自學，過程中遇到不懂的觀念，老師都會給予很詳盡的指導。在建置模型的過程中，時常碰到各式各樣的 coding 問題，常常需要花上大把的時間到處尋找解法，不過努力的解決這些問題之後，也學會了不少東西。整個專題就像是一個培養研究能力的訓練，之後研究所的求學過程會遇上越來越多的難題，很多都需要自己找尋答案，這樣的訓練讓我對這樣找尋答案的過程不再陌生，是我在大學生涯中一個寶貴的經驗。

整體來說，雖然是個跌跌撞撞的學習過程，但努力付出時間精力後再回頭看，自己這段時間也因此成長不少。