RF Fingerprint Extraction
無線訊號特徵抽取

組別：B229 組員姓名：林益民、鄧萬霖、溫泓惟 指導教授：劉光浩教授

摘要

物聯網需要大量的無線連網裝置，而硬體的性能隨著製程的演進，有巨大的提升，所傳輸的流量也迅速上升。Wi-Fi 被廣泛應用於無線通訊上，由 IEEE (Institute of Electrical and Electronics Engineers) 所定義的 IEEE802.11 規範，從二十年前的 802.11a 推進為 802.11ax，理論傳輸速率接近 10Gbit/s，其提升約 180 倍。若單純以軟體層面的密碼金鑰認證，恐怕無法保障連網的安全性，特別是車用聯網關乎生命安全的裝置，在安全性方面更需要重視。因此，利用硬體特徵不可複製的唯一性，找出每個硬體的特徵，以期望能做到硬體認證安全，配合軟體進一步提升安全性。

本專題搭配IEEE802.11p的規範，使用高度開發彈性的USRP (Universal Software Radio Peripheral) 軟體定義無線電為收發裝置並利用 GNU Radio 搭配自行開發的射頻指紋抽取演算法在 Linux 系統收集不同裝置的射頻指紋並予以分析。

一、前言

隨著物聯網的蓬勃方展，較以往更大數量的無線裝置將透過各種無線技術連結網際網路，為了確保無線裝置聯網安全的首要機制是身份識別。 射頻指紋 (Radio Frequency Fingerprinting) 為一種新興的裝置識別技術，透過分析無線訊號中的訊號特徵，達到分辨不同裝置的目的。

本次專題係使用軟體定義無線電 (SDR, Software Defined Radio) 的方式在通用軟體無線電外設 (USRP，Universal Software Radio Peripheral) 上模擬無線訊號的傳送與接收，藉由接收端所收取的數據，演算後可獲得傳送裝置的訊號特徵。

專題中所擷取的訊號特徵係較爲廣知的三種特徵有載波頻率偏移 (CFO , Carrier Frequency offset)，符元時序偏移 (STO, Symbol Time offset) 和 IQ 不平衡 (IQ-Imbalance)。除了使用不同裝置獲取及觀察特徵，本次專題也有觀察無線訊號在不同頻段上的特徵變化。本次專題的環境與設備架設為實驗室資源，使用的 Wi-Fi Simulation 模組為網路資源，抽取特徵值的演算方法和資料統計之程式撰寫為自己實作部分。

二、實驗設計

2.1 射頻指紋抽取方法

在正交分頻多工中，因為傳送端與接收端的振盪器存在頻率差，使得正交分頻多工載波間的正交特性消失，導致子載波間互相干擾。

2.1.1 載波頻率偏移 (Carrier Frequency offset)

對具有週期性訓練序列的正交多頻分工系統，經過通道和載波頻率偏移影響後所接收到的訊號為

$$\boldsymbol{y[n] = e^{j2\pi\epsilon n} \sum_{l=0}^{L} h[l]s[n-l] + v[n]} \quad \textbf{(1)}$$

其中$\boldsymbol{\epsilon}$為載波頻率偏移，利用 Moose 演算法可估計載波頻率偏移為

$$\boldsymbol{\epsilon = \frac{\arg\left(\sum_{l=L}^{N-1} y[l+N]y^{*}[l]\right)}{2\pi N}} \quad \textbf{(2)}$$

其中$\boldsymbol{N}$為訓練數列的長度 。

2.1.2 符元時序偏移 (Symbol Time offset)

根據循環前綴 (Cyclic Prefix, CP) 的重複性，利用滑動視窗的方式，計算出能使損失函數 (Cost function) 為最小值的δ ，其為取樣頻率偏移的特徵值。 定義三種損失函數為

$$\boldsymbol{STO1 = \arg_{\delta}\min\left\{\sum_{i=\delta}^{N_G-1+\delta} |y_l[n+i] - y_l[n+N+i]|\right\}} \quad \textbf{(3)}$$

$$\boldsymbol{STO2 = \arg_{\delta}\min\left\{\sum_{i=\delta}^{N_G-1+\delta} (|y_l[n+i]| - |y_l^{*}[n+N+i]|)^2\right\}} \quad \textbf{(4)}$$

$$\boldsymbol{STO3 = \arg_{\delta}\min\left\{\sum_{i=\delta}^{N_G-1+\delta} |y_l[n+i] - y_l^{*}[n+N+i]|\right\}} \quad \textbf{(5)}$$

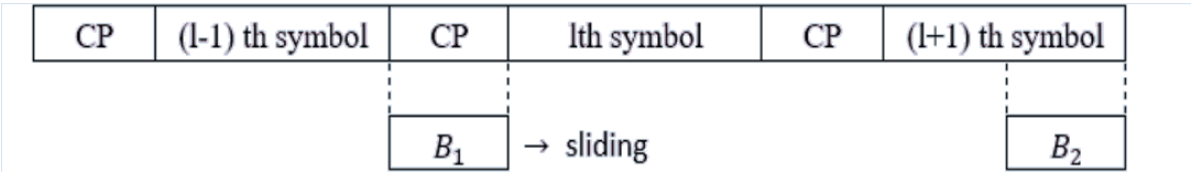

圖 1:以滑動視窗的方式計算出損失函數示意圖

其中，$\boldsymbol{N_G}$代表循環前綴 (cyclic prefix)的數量，而$\boldsymbol{\delta}$則表示滑動(sliding)的過程。

2.1.3 IQ 不平衡 (IQ Imbalance)

訊號因為其振幅與相位變化而可具有 in-phase 與 quadrature-phase 兩成分，分別為 $\boldsymbol{y_I(t) = \cos(\omega_0 t)}$和$\boldsymbol{y_Q(t) = \sin(\omega_0 t)}$，受到硬體不完美的影響，訊號會在傳遞的過程失真[6]，失真的基頻訊號可表示為

$$\boldsymbol{y_I(t) = \alpha \cos(\omega_0 t) + \beta_I} \quad \textbf{(6)}$$

$$\boldsymbol{y_Q(t) = \sin(\omega_0 t + \phi) + \beta_Q} \quad \textbf{(7)}$$

其中可以觀察的三種特徵值為

$$\textbf{直流偏移}= \frac{1}{NT}\int_{t-NT}^{t} \boldsymbol{y(u)du}$$

$$\textbf{振幅偏移}=\boldsymbol{\alpha}$$

$$\textbf{相位偏移}=\boldsymbol{\phi}$$

2.2 系統設計

本次專題使用 WIME Project 的 Wi-Fi Simulation 模組，實作 IEEE802.11 的傳輸環境，我們使用的軟體環境係操作在 Linux 系統上的 GNU Radio，而硬體部分係使用 NI 發行的 SDR 裝置 USRP-2910 ，C++版本為 GNU C++ version 5.3.1 20151219 ，並使用相同型號的四台 USRP，一台作為接收端，三台作為傳送端，測試不同裝置的接收和傳送情形。

實驗方法為固定一台接收端，三台作為傳送端，程式執行時間為三十分鐘，觀察在 2.4GHz 和 5GHz 下所得到三種訊號特徵，經由四台裝置搭配組合，共會有 6 組結果。

三、實驗結果與分析

藉由上述實驗設計在不同設備在 5GHz 頻段之情況下，蒐集所產生的特徵值以及利用統計方法所得出的統計數據，該統計數據係將蒐集到的該特徵值利用 Python 整理及繪圖。

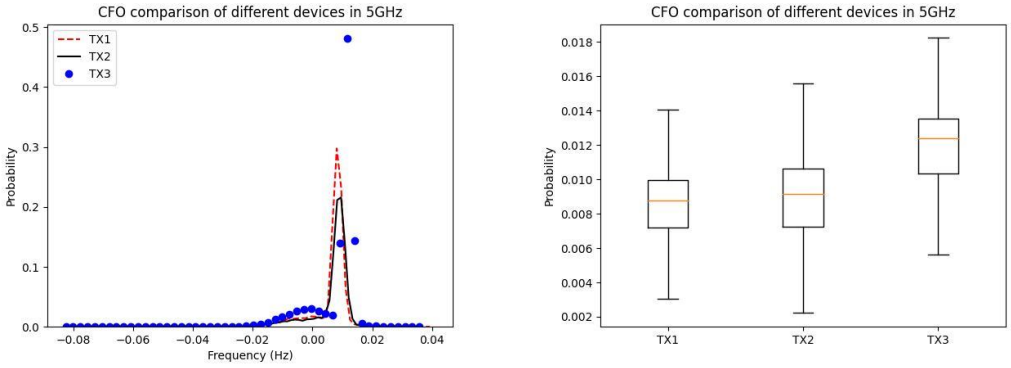

圖 2: 在 5GHz 之情況下比較 TX1、TX2 與 TX3 之 CFO 的機率與箱型圖

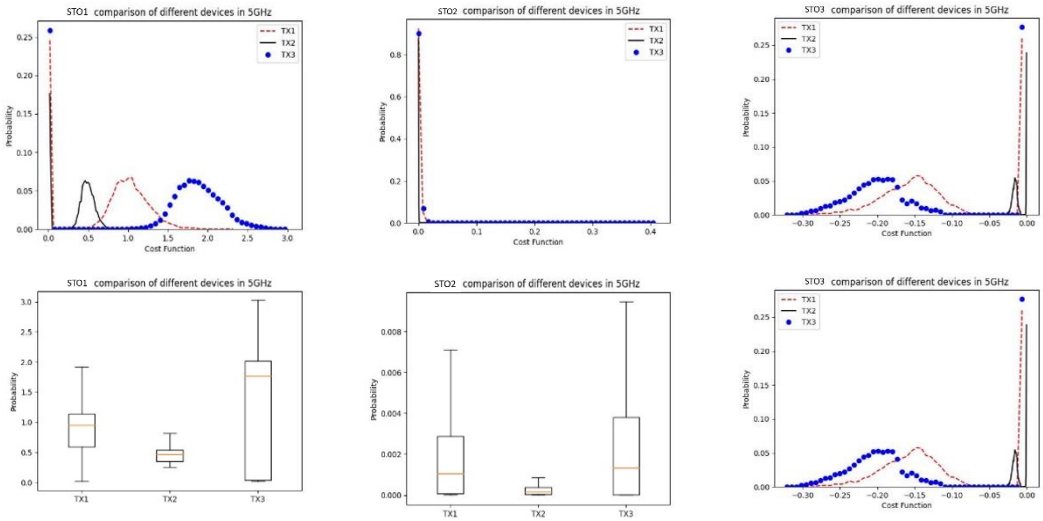

圖 3: 在 5GHz 之情況下比較 TX1、TX2 與 TX3 之各 STO 的機率與箱型圖

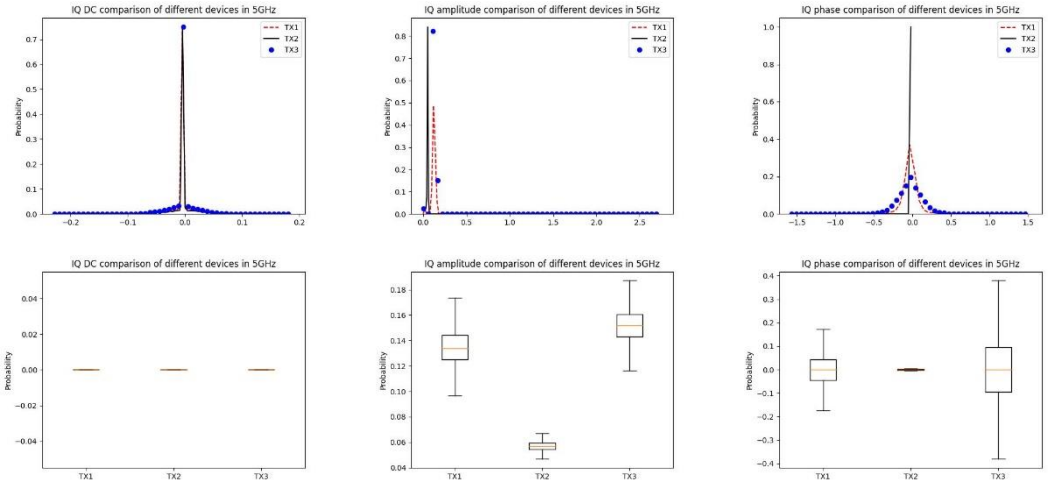

圖 4: 在 5GHz 之情況下比較 TX1、TX2 與 TX3 之各 IQ 的機率與箱型圖

觀察各特徵的分佈情形，可見除了 IQ DC 外，其他的分散之程度皆不同。IQ DC 係由於 USRP 內部的硬體電路中有補償機制，故總為零值。

總結上述結果，分佈有細微差異，若進行多次實驗而確定環境等其餘因素變化不大，則能初步相對辨別三者，再利用機率最高點之數值，以 STO1 為主並配合其餘特徵值的判斷，可見指紋辨識的可行性。

四、結論

本專題建立一套方法，可成功抽取無線裝置之無線訊號特徵值，且能藉由軟體，快速地執行資料蒐集並統整繪圖。實驗結果顯示除了不同裝置間的STO，多數特徵值僅有些許差異，可能是由於本次專題採用之統計方法較為簡易，不足以清楚地分辨裝置，故需要透

過更進一步的統計分析方法，例如，利用機器學習於特徵值分析，而加強無線訊號特徵抽取的應用性。以本專題為基礎，後續可根據需求，發展一套解決方案，快速且穩定地辨識裝置，提高物聯網的安全性。

五、參考資料

[1] IEEE std 802.11p-2010, IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments, pp. iv, 17 June 2010.
[2] IEEE std 802.11-2007, IEEE Standard for Information Technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, pp. 594-603, 8 March 2007.
[3] Simon Haykin, “Communication systems 4th,” pp. 369-371.
[4] Simon Haykin, “Communication systems 5th,” pp. 333-336.
[5] Yong Soo Cho, Jaekwon Kim, Won Young Yang and Chung G. Kang, “MIMO-OFDM Wireless Communications with Matlab,” pp. 162-163, Wiley-IEEE Press, 2010.
[6] S.W. Ellingson, “Correcting I-Q imbalance in direct conversion receivers,” 13 February 2007.

六、心得感想

在這次的實作專題中，由於我們是指導教授在本校第一屆的專題生，所以沒有做過相關題目的學長姐可以詢問內容，因此，前期花了不少時間查找資料和摸索，從而訓練了解決問題的能力。

經由專題的機會，我們學會如何在網路上找到相關的論文，並且適應閱讀大量的英文，而快速從中找出重點和需要的內容。硬體建置的方面也是讓我們上了一課，一開始安裝的 Linux 系統，USRP 收發都沒有成功，雖然重新安裝軟體或者補足驅動程式，解決了所有跳出來的錯誤訊息，仍然沒有效果。當初認為是版本不相容的問題，但不論怎麼切換版本仍沒辦法正常運作，反覆折騰好幾個月，直到有一天我們選擇從作業系統重頭建置，從此就一帆風順，USRP 收發就好了。

我們從這次專題之中學到了很多，了解對於通訊的相關過程及協定，並得到使用 C 或 Python 將其應用於通訊的經驗，學會怎麼規劃較大型的專題計畫，如何分配時間和團隊合作。非常感謝實驗室的學長姐提供的相關支援，也很感謝我們的指導教授，耐心並詳細地指導我們研究進行的方向，使得我們能完成實作專題。