

# 無線訊號特徵抽取

組別：B229 組員：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成的演進，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。

## 原理

專題中所擷取的訊號特徵係較為廣知的三種特徵，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)。

## 1. 載波頻率偏移 (CFO)

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

$$y[n] = e^{j2\pi\epsilon n} \sum_{l=0}^L h[l]s[n-l] + v[n]$$

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

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

其中  $N$  為訓練數列的長度。

## 2. 符元時序偏移 (STO)

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  $\delta$ ，其為符元時序偏移的特徵值。定義三種損失函數為

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

$$STO2 = \arg_{\delta} \min \left\{ \sum_{l=\delta}^{N_G-1+\delta} (|\mathbf{y}_l[\mathbf{n} + l]| - |\mathbf{y}_l^*[\mathbf{n} + N + l]|)^2 \right\}$$

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

$N_G$ 代表CP的數量，而 $\delta$ 則表示滑動(sliding)的過程。

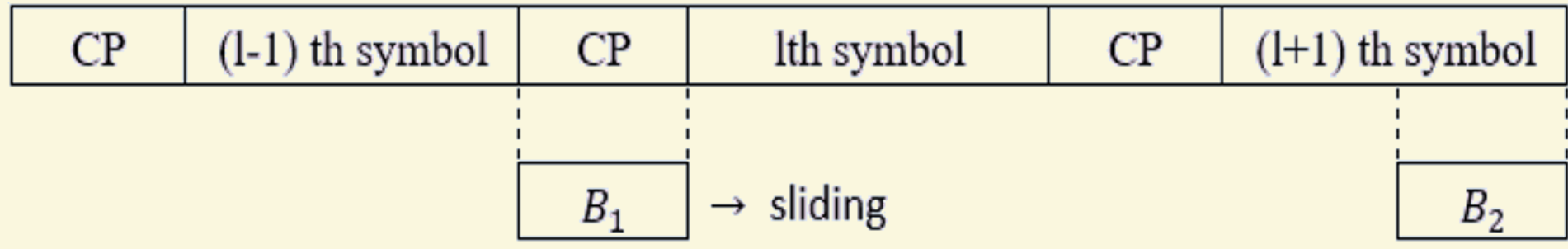


圖1: 以滑動視窗的方式計算出損失函數示意圖

### 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  $y_I(t) = \cos(\omega_0 t)$  和  $y_Q(t) = \sin(\omega_0 t)$ ，受到硬體不完美的影響，訊號會在傳遞的過程失真，失真的基頻訊號可表示為

$$y_I(t) = \alpha \cos(\omega_0 t) + \beta_I$$

$$y_q(t) = \sin(\omega_0 t + \phi) + \beta_q$$

其中我們所擷取的三種特徵值為

$$\text{IQ DC} = \frac{1}{NT} \int_{t-NT}^t y(u) du$$

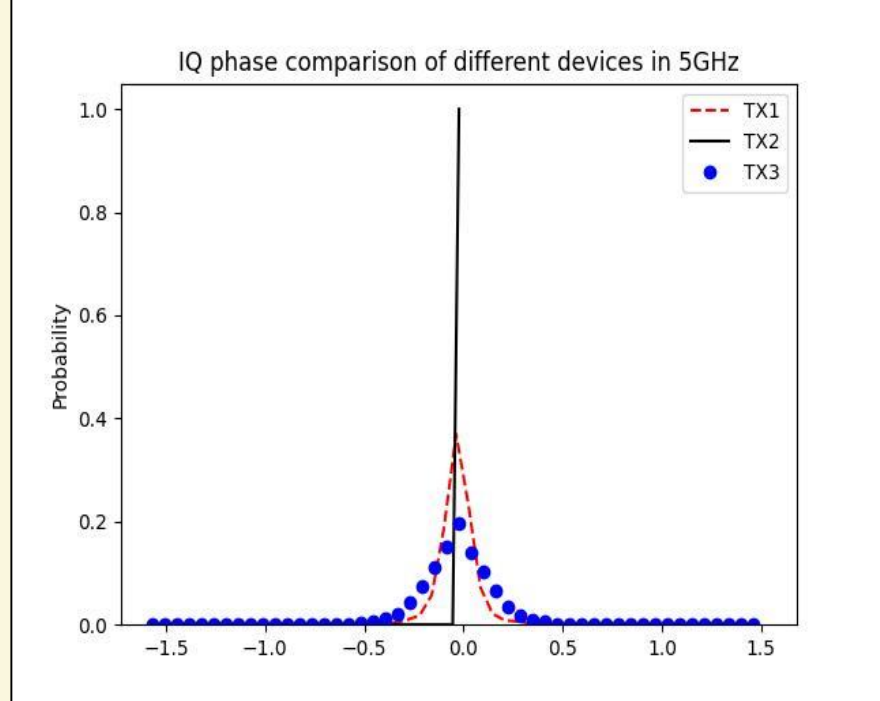
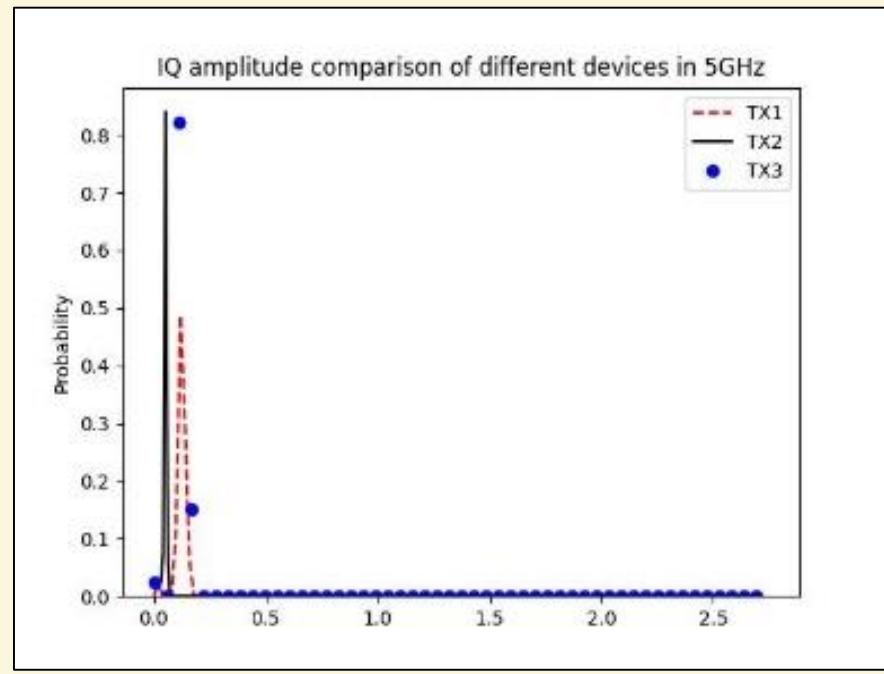
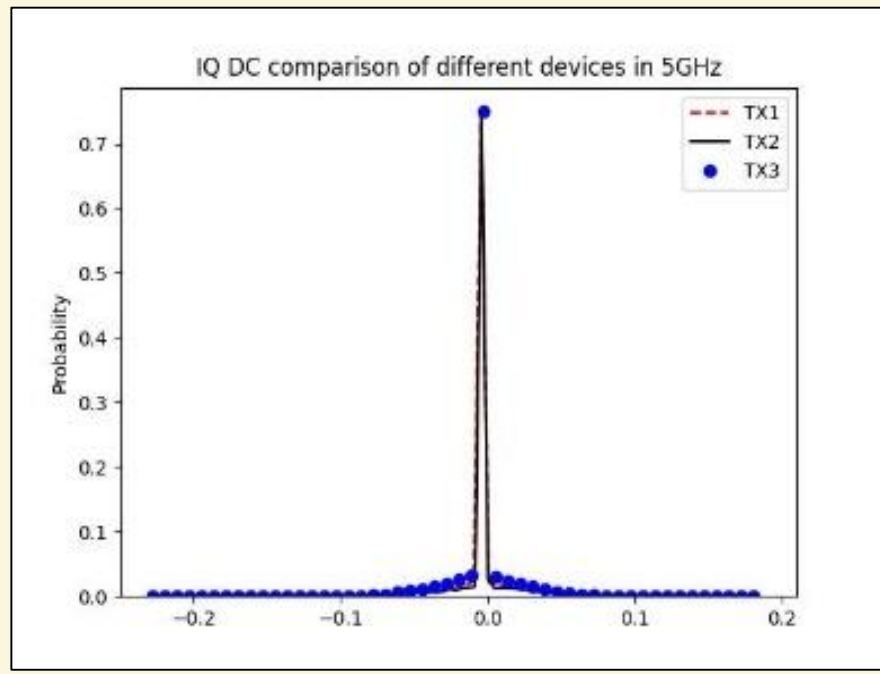
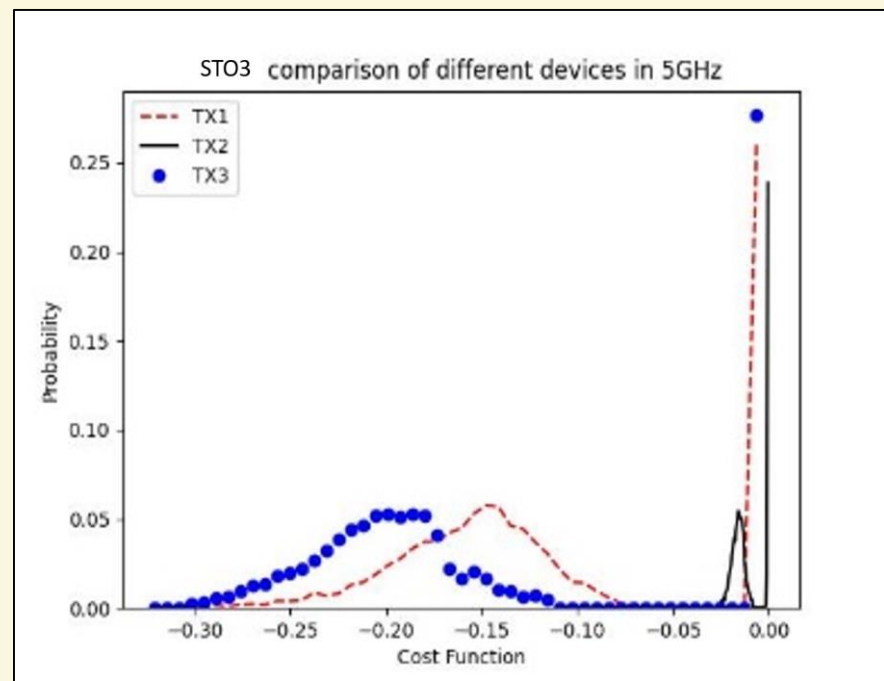
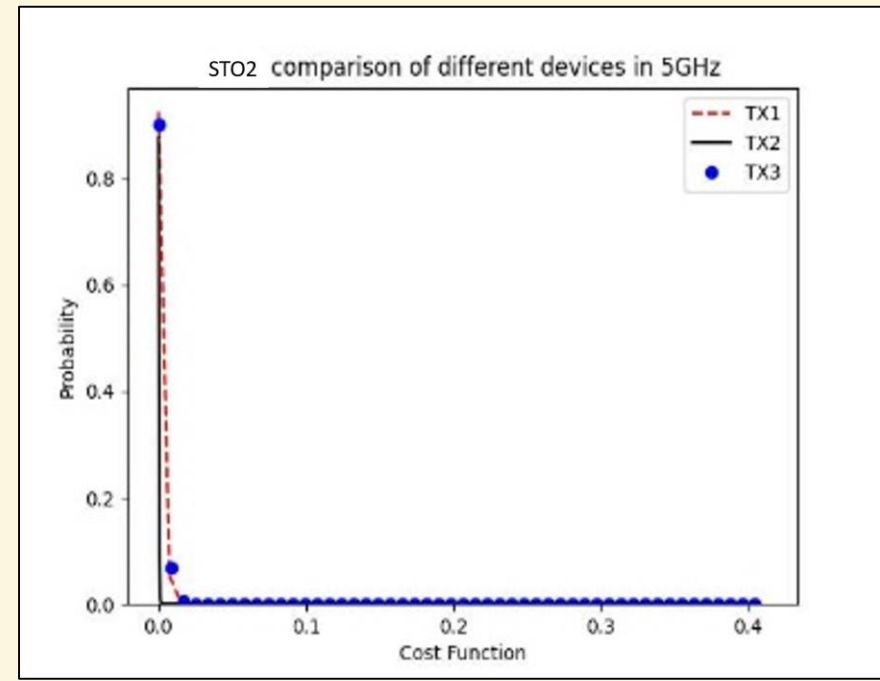
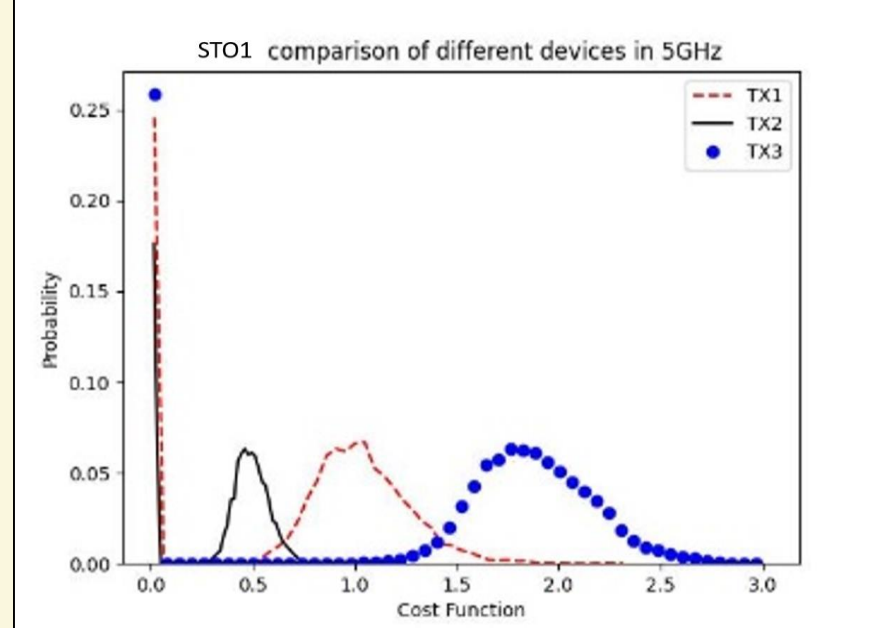
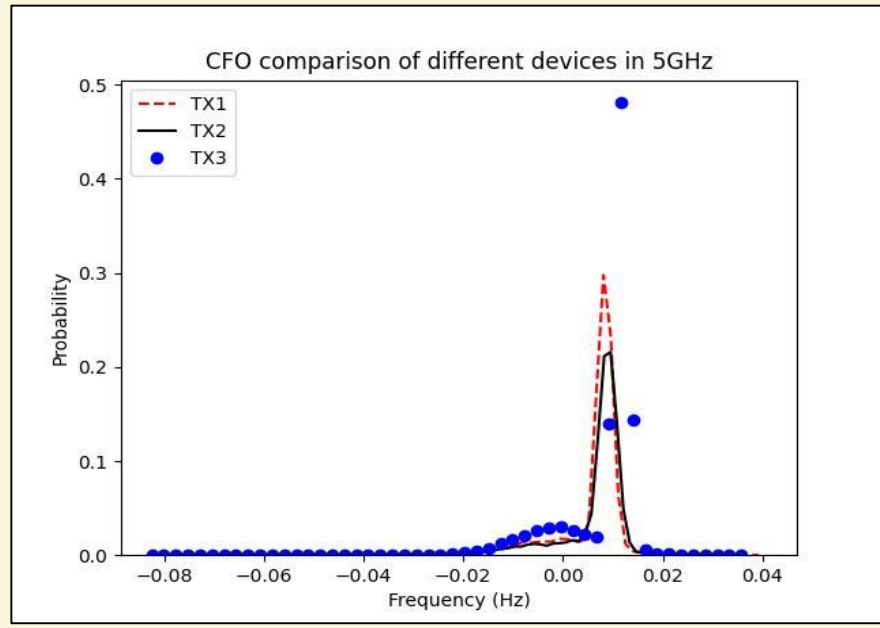
**IQ Amplitude=  $\alpha$**

**IQ Phase= $\phi$**

## 實驗結果

本次專題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。

以下為三台傳送裝置在5GHz頻段中所抽取的各特徵分佈圖



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STOI為主並配合其餘特徵值的判斷，可見指紋辨識的可行性。

## 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。

## 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 4<sup>th</sup>”.

[4] Yong Soo Cho, Jaekwon Kim, Won Young Yang and Chung G. Kang, "MIMO-OFDM WIRELESS COMMUNICATIONS WITH MATLAB".

[5] S.W. Ellingson, "Correcting I-Q imbalance in direct conversion receivers," 13 February 2007.