



運用無線射頻指紋辨識技術於 5G 專網之剖析

林俊霖^{1,*} 楊信宏² 王子嘉² 楊依茹² 王若耘² 劉馨勤³

¹ 國家中山科學研究院資訊通信研究所天頻計畫專案組長

² 國立臺灣科技大學電機工程系碩士

³ 國立臺灣科技大學電機工程系教授

摘要

隨著物聯網（Internet of Things, IoT）技術的發展和開放無線接入行動網路（如第五代無線通信系統 [5th Generation Wireless Networks, 5G]、新無線電 [New Radio, NR]、Long Term Evolution [LTE]、Wi-Fi 等）的快速部署，越來越多的設備會使得在訊號傳播範圍內的所有用戶影響其他用戶之信號，甚至對其他用戶造成惡意攻擊或攔截。因此在無線通訊帶來方便的同時，用戶私人資訊之安全性也面臨了巨大的挑戰。

因通信機發送波形帶有唯一的「射頻指紋」，可茲以識別及驗證通信發射裝置。故本文從 Wi-Fi 設備所發送之波形切入，來探討如何減少接收端設備對發射端之射頻指紋特徵之影響。本研究提出了接收機校正法及加權分類結合判斷演算法，以提升射頻指紋特徵之辨識能力，並希望可推廣到 5G 複雜的電磁環境。預期未來若能導入無線射頻指紋辨識技術，將可對這些 5G 設備有效降低設備間自我干擾現象，同時發揮統一管理、節省成本之功能，這對電信營運商而言，將有降低營運成本之莫大助益。

關鍵詞：第五代無線通信系統、行動通信、無線射頻指紋辨識、物聯網、接收機校正法

* 通訊作者：林俊霖

電子郵件：C6ALSL@ncsist.org.tw

（收件日期：2021 年 8 月 19 日；修正日期：2021 年 10 月 3 日；接受日期：2021 年 11 月 5 日）



The Anatomy of Using Radio Frequency Fingerprint Identification Technology in Private 5G Networks

Chun-Lin Lin^{1,*}, Hsin-Hung Yang², Tzu-Chia Wang², Yi-Ju Yang²,
Jo-Yun Wang², Hsin-Chin Liu³

¹Chief, Tien-Ping Program Office Project Management Section, Division for Information Communication Research
Communication Section, National Chung-Shan Institute of Science and Technology

²Master, Department of Electrical Engineering, National Taiwan University of Science and Technology

³Professor, Department of Electrical Engineering, National Taiwan University of Science and Technology

Abstract

With the development of the Internet of Things (IoT) technology and the rapid deployment of open wireless access mobile networks (such as 5th Generation Wireless Networks [5G], New Radio [NR], Long Term Evolution [LTE], Wi-Fi, etc.), more and more devices result in multi-user interference (MUI) within the signal transmission range, and may even suffer attacks or interceptions from some malicious users. Therefore, while wireless communication brings convenience, the security of users' private information is also facing a huge challenge.

As a communication signal waveform sent from a transmitter has its unique radio frequency fingerprint (RF fingerprint), which can be used to identify and authorize the transmitter device. In this article, we investigate the RF fingerprint of waveforms sent from a Wi-Fi transmitter, and discuss how to reduce receiver influence on the RF fingerprint associated with a transmitter. In this work, we propose a receiver calibration method, and a weighted classifier combining decision algorithm to improve the RF fingerprint identification rate. We hope this research can be extended to a more complex electromagnetic environment like 5G networks. It is expected that the self-interference phenomenon between these 5G devices can be mitigated if RF fingerprint identification technology can be adopted. Additionally, the RF fingerprint technology can be helpful for the functions of unified management and cost-saving of telecommunication operators.

Keywords: 5th Generation Wireless Systems (5G), mobile communication, radio frequency fingerprint recognition, Internet of Things (IoT), receiver calibration method

* Corresponding Author: Chun-Lin Lin
E-mail: C6ALSL@ncsist.org.tw

壹、何謂第五代無線通信系統 (5th Generation Wireless Systems, 5G) 技術

5G 英文全稱 5th Generation Wireless Systems，中文翻譯成「第五代無線通信系統」，是現有第四代無線通信系統（4th Generation Wireless Systems, 4G）通訊技術的延伸，主要設計能有效提升資訊傳輸速度、減低傳輸延遲，並改善無線服務彈性而研發出來。一般而言，5G 技術的速度最快可達 20 Gbps，而 4G 的最高速度僅 1 Gbps，以傳輸速度而言，兩者差了將近 20 倍；對於實已邁入各項裝置均可互聯互通的物聯網（Internet of Things, IoT）時代而言，通信系統的吞吐容量將越來越顯得重要，因為各項電子設備和物品將擁有了它們從未有過的智能化、互通性的能力，這也是為何需要 5G 通信技術來為物聯網時代的數百萬計設備提供無縫隙、無時延的連接；但隨著物聯網技術的發展和 5G 無線的快速部署，越來越多的輻射設備出現在日益複雜的電磁環境中；為了能夠統一管理這些設備，無線信號準確識別技術就顯得日益重要，因為除了可確認同質性系統彼此相容互通外，還能濾除其他異質通信系統所造成的干擾現象，所以「無線射頻指紋辨識技術」就是為了有效解決這個問題，而在近幾年發展出來的應用技術；另根據數位雜誌整理分析的預估，到了 2020 年以後，每個人平均聯網的裝置數量將高達 6.5 個設備，全世界將有 500 億臺聯網設備（如圖 1），這些應用可從目前現有的技術，如智慧型手機、平板電腦和智能手錶，到未來冰箱、未來汽車、擴增實境（Augmented Reality, AR）／虛擬實境（Virtual Reality, VR）眼鏡，甚至是智能服裝，相信在不久的將來，都有可能予以實現。

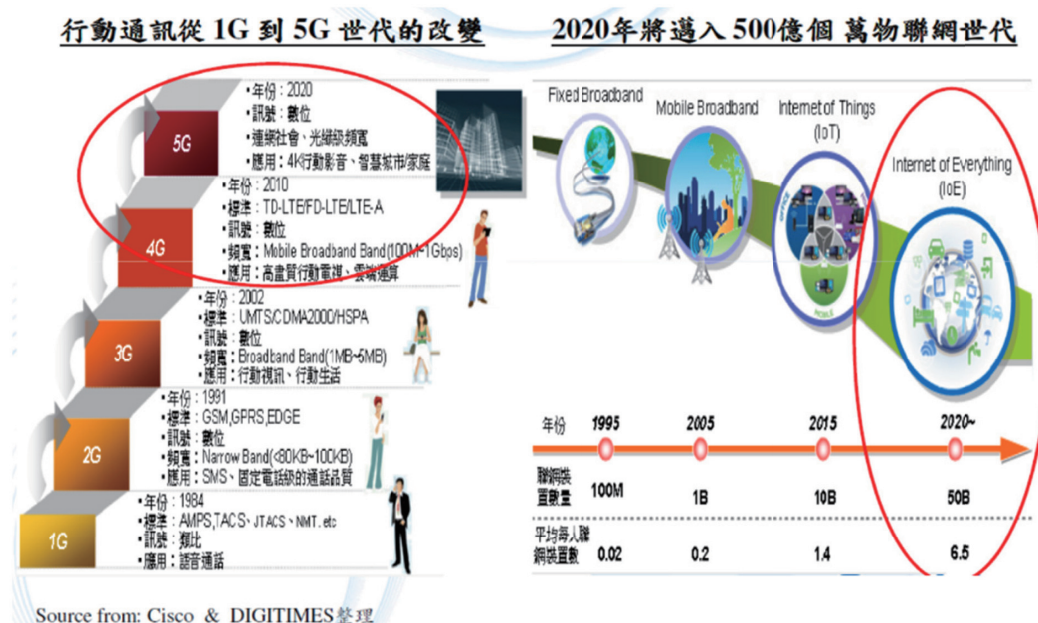


圖 1 4G 滿足人的需求、5G 實現萬物的聯網溝通

資料來源：吳伯軒（2014）。

5G 不僅是行動通信技術的升級，也將促進大數據分析、人工智慧與雲端運算再進化，更是面向全新服務、智慧生活、智能生產的網路變革；簡言之，如果把 4G 比喻成一條鄉間的普通馬路，那 5G 就可說是立體的高速公路；又拿另一個例子比喻，就像以前人類使用馬車代步要走三天三夜的路程，但現在出遠門可坐高鐵、坐飛機一樣，一天之內就能來回，以上皆是對 5G 提供生活便利性及影響性的最好形容；所以，5G 所擁有的八大關鍵性能（最大傳輸速度 20 Gbit/秒、使用者平均傳輸速度 1 Gbit/秒、頻譜使用效率為 4G 的 3 倍、通訊機移動速度高達 500 公里/小時、傳輸延遲小於 1 毫秒、服務覆蓋密度 10^6 個/平方公里、網路能量效率為 4G 的 100 倍、通道容量密度 10 Mbit/秒/公尺²）將推廣到三大應用主軸（超高速、超低時延、超大連接）的關鍵能力和萬物互聯的七大應用場景（公共安全、智慧醫療、工廠自動化、智慧交通、智慧製造、智慧物流、物聯網），如圖 2；將開啟人類社會的新一輪變革，對社會各領域的影響與衝擊也前所未有，三大應用說明如後。

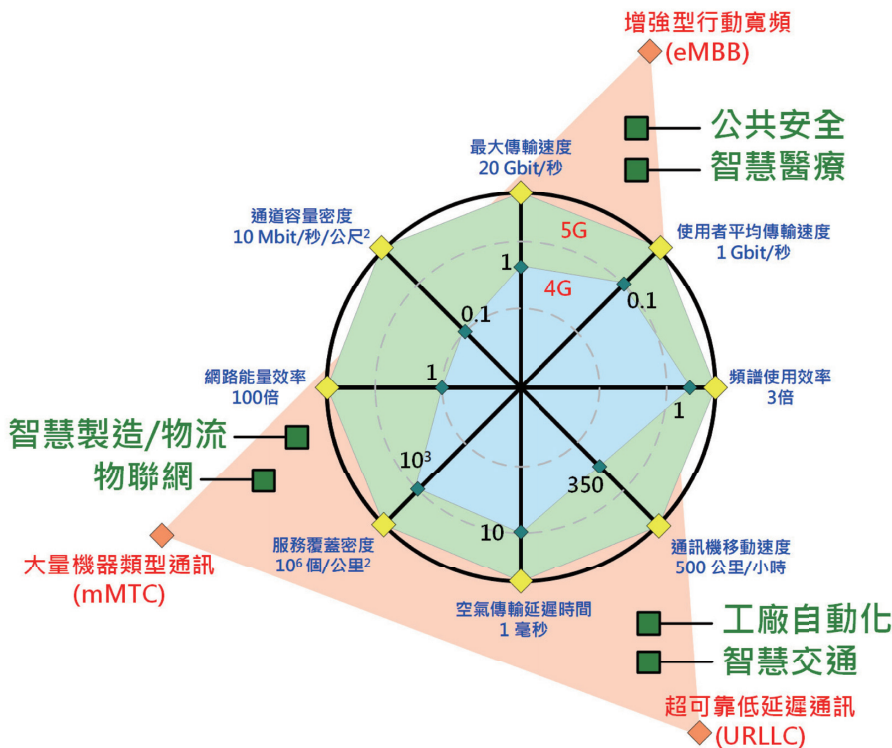


圖 2 5G 三大應用主軸

資料來源：作者研究整理。

一、增強型行動寬頻（Enhance Mobile Broadband, eMBB）

透過 eMBB 技術，可大幅度增強傳輸信號所需的頻寬效益，亦可涵蓋不同的傳輸範圍和應用領域，包含無縫覆蓋和熱點通信，無縫覆蓋適用於高速移動的需求，同時，資料傳輸率亦須比現今 4G 系統還高，熱點通信則以高密度區域移動性低的用戶為主，其最快可達

資料傳送速度 20 Gbps 的目標（等於 2.5 GBytes／秒），所以能以更高的資料傳輸速度，傳送更大量的資料，這項技術能讓使用者在六秒的時間內，就可以下載 15 GB 完整長度的高清電影，比目前 4G 連線下載相同影片的速度，足足快了四分鐘；換句話說，一部兩小時的 HD 電影只要六秒鐘就可下載完成，更可提高達文西手術的切割點精準度，病人可少流 80% 的血；也就是說，對 eMBB 應用的關鍵能力而言，最關鍵的特性就是極低延遲性（Ultra-Low Latency）、高峰值資料傳輸率（Peak Data Rate）與單位區域內的傳輸容量（Area Traffic Capacity），其特性將可適用於公共安全及智慧醫療的場景（如圖 2）。

二、超可靠低延遲通信（Ultra Reliable and Low Latency Communication, URLLC）

此技術強調的是低於 1 ms 延遲時間及錯誤率低於 10^{-5} ，所以可以應用於對資料傳輸量之時間延遲和可靠度要求非常嚴格的場景；例如工業自動化製造、遠端醫療手術、無人駕駛、智慧交通等，這也是 5G URLLC 特性能應用於車輛聯網的最大優勢，5G 網路的時延性（Latency of Over-the-Air）低於 1 毫秒，且用戶間的時延性（Latency of End-to-End）低於 5 毫秒，簡單來說，車輛駕駛在極度複雜的交通環境中，假設處於自動駕駛狀態，採用 4G 網路技術的車輛，接受訊息可能慢半拍或遺漏訊息，無法與周遭環境即時同步與處置反應，便會出現車輛行駛安全性危險，只有 5G 以上的聯網能力，才能滿足自駕車聯網需求，舉例來說，在時速 100 公里／小時的行駛車輛，一旦偵測到任何危險，能以近乎零延遲（低於 1 ms 延遲時間）的速度接收剎車信號，當車輛自動偵測危險到完全剎車停住的那一段時間，汽車僅僅走了幾公分而已，在 4G 的時代裡，同樣條件下，車輛可能已經行駛了 1 公尺，這是超越 4G 的技術大躍進（如圖 2）。

三、大量機器類型通訊（Massive Machine Type Communication, mMTC）

mMTC 是 5G 的三大特性之一，網路營運商可以利用 mMTC 與邊緣運算（Multi-Access Edge Computing, MEC）等前瞻通訊技術，可同時提供百萬個以上眾多的設備連線；因此，mMTC 係透過蒐集和分析所有連網之感測器所產生的巨量資訊，來處理和掌控當下的使用環境；MEC 使這些大量資訊傳輸和資料分析可以在邊際網路處理，以降低整體網路處理資訊的負荷量，大大減少了通信設施和營運成本，使用 MEC 在行動網路的邊緣提供雲端運算設備產生的數據的能力，進而減少整個網路的頻寬和資源消耗，並且不需要通過雲端伺服器，而打造出滿足巨量物聯網網路需求的基礎設施，此外，mMTC 技術強調的是服務覆蓋密度 10^6 個／平方公里、網路能量效率為 4G 的 100 倍、通道容量密度 10 Mbit／秒／平方公里，所以可發揮「超巨量通訊」的願景，因此可同時間介接 100 萬臺物聯網裝置，規範每個設備本身僅可傳送少許的資料量，所以可獲得較小的符元時間長度（Symbol Duration），在既有的訊框架構與輪詢機制下，不僅可將整體傳輸信號所需的時間減少，還可降低信號延遲的效應、確保資料能正確接收，因此可有效提升通信品質及覆蓋範圍；此技術適用於智慧製造、智慧物流及萬物聯網的場景（如圖 2）。

貳、以指紋特徵辨識發射機之相關研究

因應 5G 行動通信的快速部署，特別是對於擁有更高資料傳輸率、更低延遲時間及介接更多用戶量的 5G 和開放無線接入網路（例如 5G 新無線電 [New Radio, NR]、Long Term Evolution [LTE]、Wi-Fi 等）行動通信而言，在不同的時間與設備間，越來越多的設備會使得在訊號傳播範圍內的所有用戶影響其他用戶之信號（如圖 3），甚至對其他用戶造成惡意攻擊或攔截，因此在無線通訊帶來方便的同時，用戶私人資訊之安全性也面臨了巨大的挑戰；本文探討射頻指紋可能受到通訊過程的各種影響，例如發射端、接收端設備之硬體缺陷與無線通道之多路徑之影響，這使得射頻指紋在分類與識別的過程中難以保障其穩定性與準確性。一般而言，特定接收端所提取之指紋辨識無法直接使用於其他接收端；因此射頻指紋識別可攜性成為資訊安全研究的一項熱門議題；並從 Wi-Fi 無線設備發送的波形在通訊的實體層中皆帶有唯一的「射頻指紋」特徵切入，其能夠識別用戶裝置並對授權用戶進行分類，來探討如何減少接收端設備對發射端之射頻指紋特徵之影響。

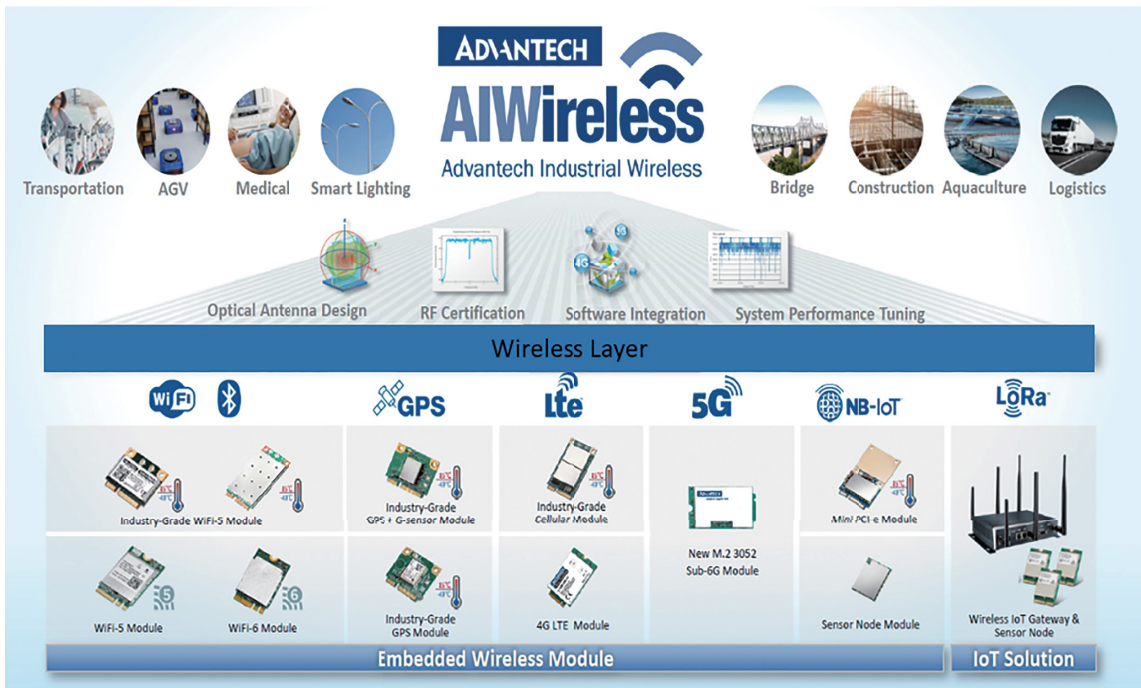


圖 3 5G 與開放型無線網路複雜設備共用情境

資料來源：Huang-Fu and Lin（2019）。

一、指紋特徵之成因

在無線通訊之過程中，人們利用電磁波作為媒介傳遞訊號，而電磁波通過反射、折射等物理現象在物理限制範圍內的任何地方傳播，這使得在範圍內的其他用戶都能夠輕易地參與

其中，甚至會遭受不明來源之惡意攻擊或攔截，因此在無線通訊帶來方便的同時，用戶私人資訊之安全性也面臨了巨大的挑戰；然而，設備在傳遞訊號的過程中，會因為電路上元件的微小誤差而導致訊號產生細微的變化，而此微小的變化就如同人的指紋一般獨一無二且無法仿冒，因此被稱為射頻指紋特徵。

二、指紋特徵之應用

承前述，我們能夠藉由無線設備發送的波形在通訊的物理層中夾帶此唯一且獨特之指紋特徵加以識別用戶，並且進一步對授權用戶進行分類，不僅帶給了用戶安全以及隱私上之保障，也讓無線通訊擁有了更多發展的可能性。然而，這些由發送端設備所產生之訊號卻會因為接收端設備、無線通道等的差異而無法提取其純粹的射頻指紋特徵，進而導致辨識率的下降，因此如何降低這些外在因素對指紋特徵的影響一直是值得研究的方向；而本研究所要探討的核心問題則是針對不同接收端產生的影響進行分析以及校正，進一步的提升指紋辨識之可攜性。

三、指紋特徵提取方法之相關研究

如圖 4 所示，表示了一般收發機之間無線通訊之過程，而射頻指紋特徵源於通訊過程中的各個方面。在收發機的影響因素中包括時脈抖動（Clock Jitter）、數位類比轉換器（Digital to Analog Converter, DAC）取樣誤差、混頻器（Mixer）、頻率合成器、功率放大器之非線性特性與設備天線等，最後經由類比電路與數位處理單元的處理，在訊號的各個部分依照特性提取不同的射頻指紋特徵，進而完成裝置之辨識，如圖 5（Wang, Sun, Piao, Zhu, and Ren, 2016）。

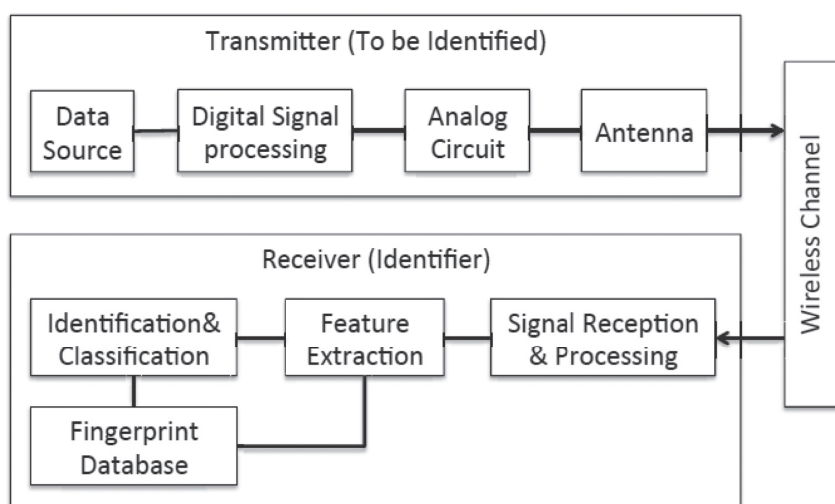


圖 4 無線物理層中識別之過程

資料來源：Wang et al. (2016)。

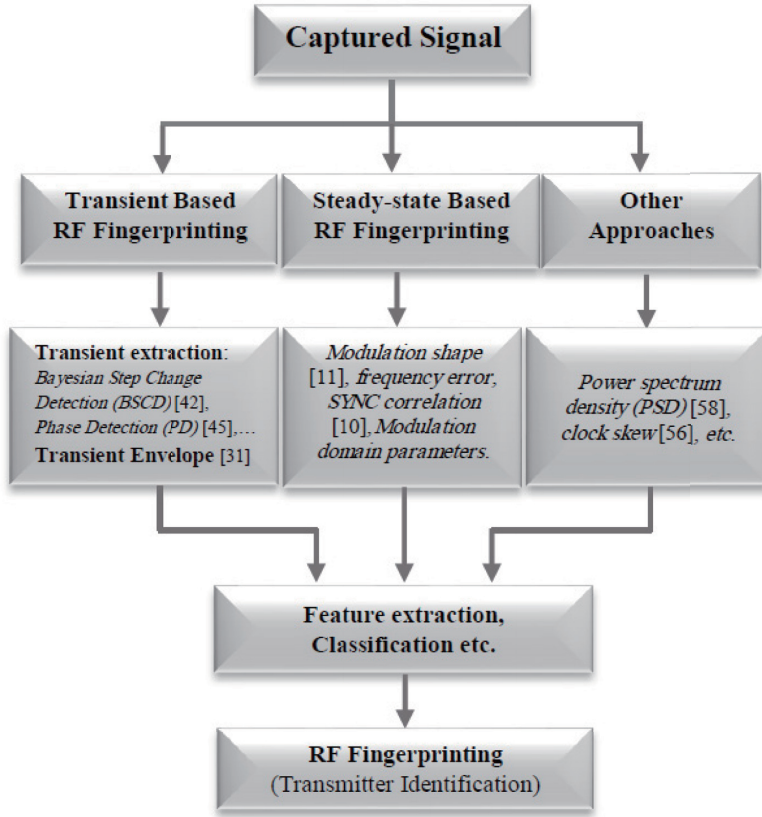


圖 5 無線發射端識別之結構與射頻指紋技術之分類

資料來源：Soltanieh, Norouzi, Yang, and Karmakar (2020)。

對於發射端之識別技術，可以依據是訊號的瞬態、穩態或是其他部分之特徵進行大致的區分 (Soltanieh et al., 2020)。而目前最受關注之識別類別為基於訊號瞬態之辨別技術，但由於瞬態訊號為射頻放大器從空閒狀態變為數據通訊時發射之短暫訊號，其瞬變之性質使得它們難以被檢測，因此本章節著重於介紹與本研究相關的穩態射頻指紋特徵的提取與分析。

頻率偏移特徵 (Frequency Offset Feature) 提取方法

載波頻率偏移 (Carrier frequency offset, CFO) 特徵是由收發端間之振盪器頻率差異所引起的，也是當前常用於指紋分類的參數之一 (Peng, Hu, Zhang, Jiang, Yu, and Yan, 2018)。在本文中，介紹了一種精確的頻率偏移估計方法來對 ZigBee 設備進行分類，且估計的頻率偏移資訊可以進一步用於提取第三節中的調變偏移特徵。

(一) 粗略頻率偏移估測

ZigBee 封包開頭的前同步碼序列可用於進行粗略頻率偏移估測，並且會在估測之前預先計算前同步碼序列 $z(n)$ 之 OQPSK 波形，並且通過逐步的頻率搜索進行頻率預補償，表示為 $\Delta f_{coarse} = f_{start} + f_{step}$ ，接著將產生相關峰值的頻率偏移選擇為粗略的頻率預補償值。該過程在數學上表示為：

$$\operatorname{argmax}_{\Delta f_{coarse}} \sum_{n=1}^{N_{preamble}} |y(t + nT_s) \cdot e^{j2\pi\Delta f_{coarse}nT_s} \cdot z^*(n)| \quad (1)$$

其中 $N_{preamble}$ 為前導序列波形的長度， T_s 為取樣率。

(二) 精密頻率偏移估測

首先，接收到的訊號會先被粗略頻率偏移補償，表示為：

$$y'(t) = y(t)e^{j2\pi\Delta f_{coarse}t} \quad (2)$$

接著，透過補償訊號 $y'(t)$ 與已知 OQPSK 展頻晶片 $z_i(n)$ 之間的互相關來獲得峰值相關值，其過程之數學式表示為：

$$\operatorname{argmax}_i \sum_{n=1}^{N_{chip}} |y'(N_{chip} \cdot (k-1)T_s + nT_s) \cdot z_i^*(n)| \quad (3)$$

其中 k 是 ZigBee 符號的指標。

由上式回傳的晶片指標表示為 i_{Coor} ，即可建構出訊號 $s(k)$ ：

$$s(k) = \sum_{n=1}^{N_{chip}} |y'(N_{chip} \cdot (k-1)T_s + nT_s) \cdot z_{i_{Coor}}^*(n)| \quad (4)$$

而 $s(k)$ 與相鄰訊號之間的差分值可以表示為：

$$d(k) = s(k) \cdot s^*(k+1) \quad (5)$$

最後，我們可以得到精密的頻率偏移估計 Δf_{fine} ，表示為：

$$\Delta f_{fine} = \operatorname{angle}\left(\frac{1}{K-1} \sum_{k=1}^{K-1} d(k)\right) \cdot \frac{1}{2\pi N_{chip} T_s} \quad (6)$$

其中 K 是估測中的符號總數。此外，相位偏移也可以由此估算為：

$$\psi = \text{angle} \left(\frac{1}{K} \sum_{k=1}^K s(k) \cdot e^{-2j\pi\Delta f_{\text{fine}k} N_{\text{chip}} T_s} \right) \quad (7)$$

四、以應用機器學習（Machine Learning）辨識發射機之相關研究

機器學習是人工智慧的一個分支，它從資料中得到複雜的樣本以用來訓練與學習，以創造演算法並利用來做預測最後達到人工智慧的方法。機器學習可以分為以下幾個大類：監督式算法（Supervised Algorithm）、非監督算法（Unsupervised Algorithms）、加強學習（Reinforcement Learning）與併合算法（Hybrid Algorithms）。根據 Baldini and Steri (2017) 與 Soltanieh et al. (2020) 中，最常用於指紋辨識也是最多文獻探討的演算法為監督式算法。

監督式算法中，不同的資料集需要各自資料集的類別（Label），並且不同類別要相互排斥才可以進行分類。若應用於射頻指紋特徵，我們在分類前除了不同網卡的指紋特徵資料集外也需要這些特徵屬於哪張網卡的類別資料集。

類神經網路是一組連接的輸入和輸出單元，每個連接都有相關權重，如圖 6。類神經網路在分類的方法是透過學習過程通過調整權重以預測輸入樣本的類別，常用的神經網路分類是倒傳遞演算法（Back Propagation Algorithm），它執行學習的方法是利用多層前饋神經網路（Feed-Forward Neural Network），通過處理迭代的方式訓練樣本數據集，其中每次迭代中比較每一個樣本的預測，用於實際目標值和調整對應每層中的權重。類神經網路的優勢是它們能夠忍受複雜的數據或離群的指紋，缺點是在分類前需要一段很長的學習時間。因為數據庫的建立可能需要相當大量的時間收集並提取指紋。神經網路的調整可能需要一些經驗的幫助以縮小參數列表，這些參數是特定於一種類型的組成（Baldini and Steri, 2017）。

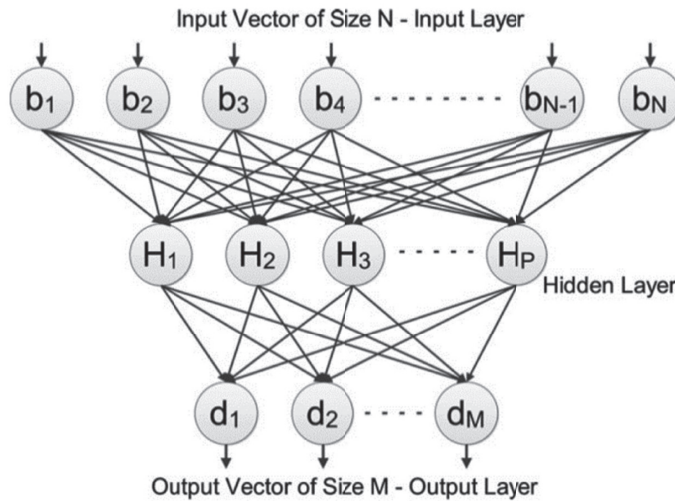


圖 6 類神經網路示意圖

資料來源：Uluagac, Radhakrishnan, Corbett, Baca, and Beyah (2013)。

Uluagac et al. (2013) 及 Radhakrishnan, Uluagac, and Beyah (2015) 使用量化共軛梯度後向傳播 (Scaled Conjugate Gradient Backpropagation) 為訓練函數，並且發現輸出神經元 (Output Neurons) 與 S 型隱藏 (Sigmoid Hidden) 是理想的圖型識別。Uluagac et al. 及 Radhakrishnan et al. 使用類神經網路中的前饋網路，前饋網路中參數從輸入層向輸出層單向傳播，與其它類神經網路不同的是它的內部不會構成有向環，其中也提到使用此種方法還需要圖型識別 (Pattern Recognition) 與非線性函數擬合 (Nonlinear Function Fitting)。O'Shea, Corgan, and Clancy (2016) 說明相比於傳統的機器學習分類，如 Support Vector Machine (SVM) 和 K-Nearest Neighbor (KNN)，使用卷積類神經網路 (Convolutional Neural Network, CNN) 和深度類神經網路 (Deep Neural Networks, DNN) 以提供更大的準確性，特別是在低 Signal-to-Noise Ratio (SNR) 條件下效果會更顯著，此文獻中 CNN 使用四層類神經網路，兩層為卷積層 (Convolutional Layer) 另兩層為密集全連接層 (Dense Fully Connected Layer)，其中三層使用的激活函數 (Activation Function) 是整流線性單位函數 (Rectified Linear Unit, ReLU) 另一層使用 Softmax 激活函數，如圖 7 所示。文中另外提到正則化 (Regularization) 可以預防過度擬合 (Over-Fitting)，而文中 CNN 使用 Dropout 以防止過度擬合的情況。

在 O'Shea et al. (2016) 中比較不同 SNR 的情況下使用不同分類方法，對於低 SNR 與較短的樣本數 CNN 與 DNN 具有較佳的分類效果，其中也說明 CNN 所需要花費的訓練時間比支援向量分類 (Support Vector Classification, SVC) 還要少，但相比於其他方法 (如 KNN) 多出許多訓練時間，相對的在分類上 CNN 比其他常用方法 (SVC、KNN) 省下更多分類時間。

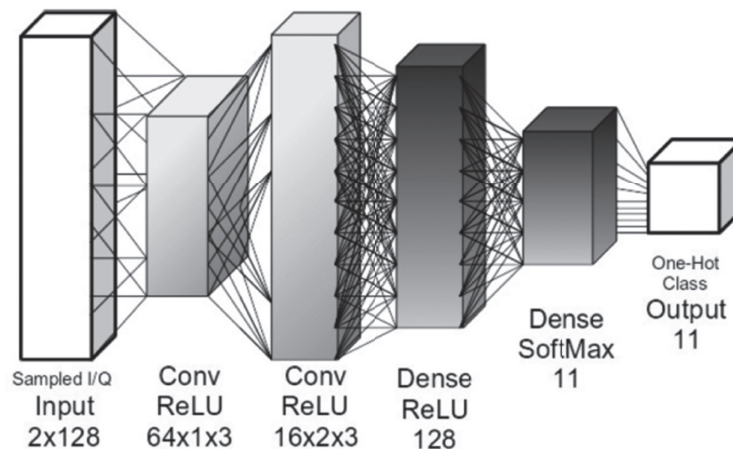


圖 7 CNN 的架構圖

資料來源：O'Shea et al. (2016)。

五、影響辨識成效之原因及其改善方法之相關研究

射頻指紋是無線通訊設備本身固有的特性，傳輸訊號會受到裝置硬體的影響 (Rehman,

Sowerby, Alam, and Ardekani, 2014; Rehman, Sowerby, and Coghill, 2012) 而同時包含發射端與接收端之射頻指紋特徵，因此每臺接收機提取的特徵不具備可攜性的性質。以下將回顧以往文獻研究進行介紹。

(一) 接收機之間的特徵可攜性探討

Rehman et al. (2014) 主要為探討不同接收端間的特徵可攜性效能表現，其第一部分以高端接收機取得之特徵進行辨識模型訓練，再使用此模型對低端接收機取得之特徵進行分類。而模擬結果顯示高低端接收機特徵數值分布差異明顯，因此兩者特徵可攜性極低。

第二部分研究則以七臺低端接收機進行七組辨識模型之訓練，並用各辨識模型分辨其餘低端接收機之特徵，如圖 8。

整體研究結果表示不論接收端的類型是否相似，都會因硬體缺陷不一而造成不同設備提取之特徵無法具有可攜性。

(二) 混合多種特徵增加辨識準確度

Peng et al. (2018) 研究為以通用軟體無線電設備 (Universal Software Radio Peripheral, USRP) X310 訓練 54 臺發射端的特徵辨識模型，並間隔 18 個月後由 USRP N210 以此辨識模型進行分類。

該文獻使用了四種特徵，分別為微分星座圖、載波頻率偏移、調製偏移和星座軌跡圖。並依據通道訊雜比不同預先計算其對應之權重，實際訊號再以相應權重混合四種特徵。收集數據之實驗在視距傳播 (Line-of-Sight) 情形下進行，結果顯示使用不同接收端分別進行訓練和分類的分類錯誤率為 0.1105，仍在可接受範圍內，同時也驗證了指紋特徵的穩定性。

校正函數方法為：

1. 訊號差異生成校準函數

Baldini, Giuliani, Gentile, and Steri (2018) 提出訂定一臺標準發射端，各接收端接收其訊號並以訊號差異建立裝置彼此間的校正函數，再用此函數校正其餘發射端之訊號。同時使用滑動窗口找出受接收端特徵影響較小的訊號段，最終以馬氏距離和與分辨正確率判斷校正效能。

2. 於轉換網路生成校準函數

Merchant and Nousain (2019a) 及 Merchant and Nousain (2019b) 使用了卷積神經網路進行分類器與轉換網路訓練，並以 Kullback-Leibler 散度比較每臺接收端所訓練之分類器所輸出的機率分布，進而觀察接收訊號經轉換網路校正後分布是否相似。

其中轉換網路架構使用了殘差神經網路 (Residual Neural Network) 模型概念提高性能和收斂時間，最終研究結果顯示此方法具有校正大部分偏差的能力。

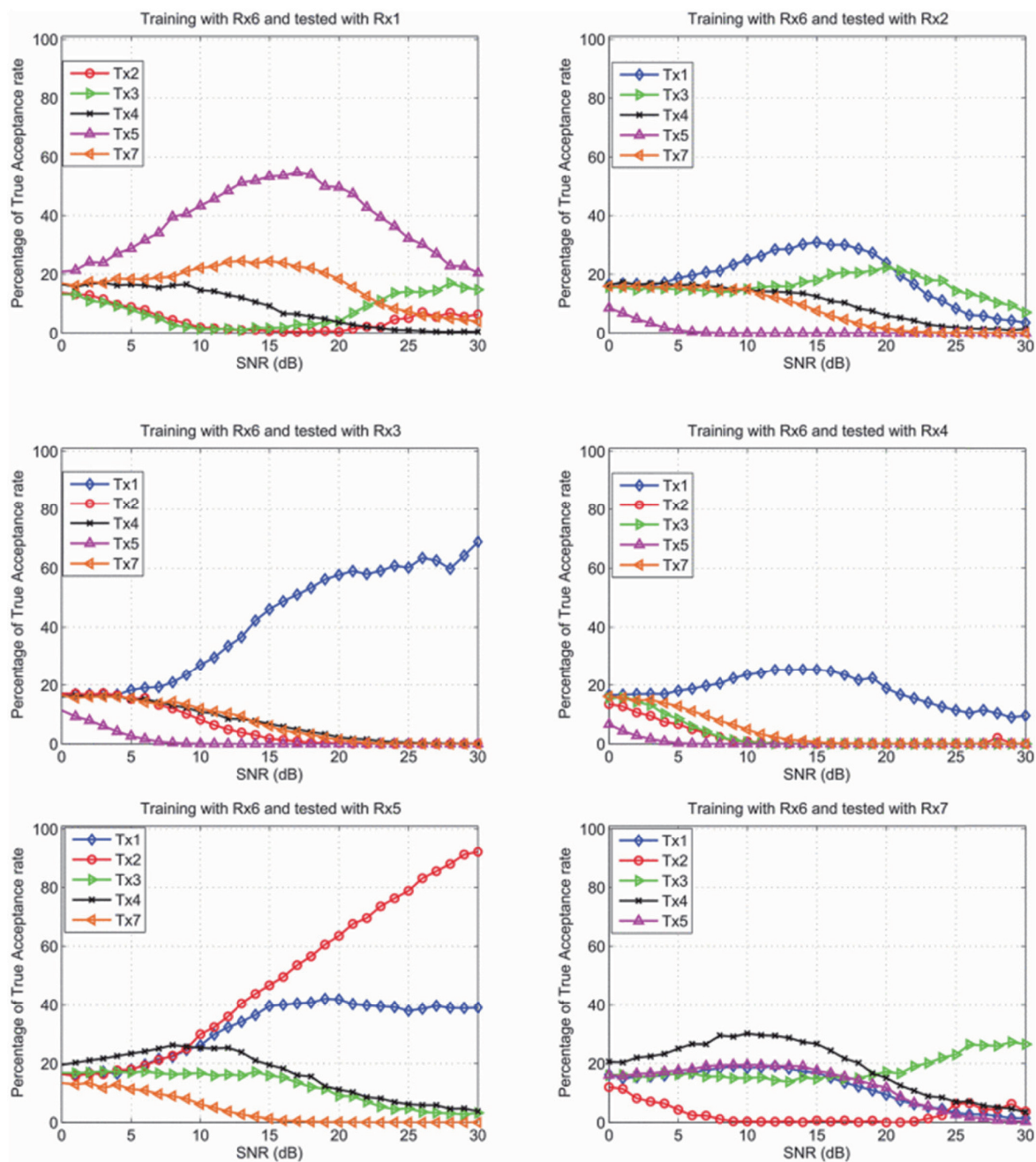


圖 8 低端接收機間特徵可攜性之比較

資料來源：Rehman et al. (2014)。

參、以指紋特徵辨識 802.11g Wi-Fi 網卡之研究

一、系統介紹

USRP 是由 Ettus Research 及其母公司 National Instruments 設計的一系列軟體定義無線電，大多數 USRP 通過其高速連結的主機之軟體來控制並且發送與接收數據，而此研究將與 GNU Radio 軟體套件一起使用，以創建複雜的軟體定義無線電系統。

雖然 USRP 之某些特性及規格因型號而異，但所有的 USRP 設備都使用相同的通用結構，因此本研究將會探討訊號在傳輸的過程中可能對訊號造成偏差之因素，並且利用接收端所產生之指紋特徵，對接收訊號進行研究與處理，以達成提升射頻指紋辨識可攜性之目的。

(一) 標準 802.11a/g 之調變與解調

802.11a/g 所使用之調變技術為 Orthogonal Frequency Division Multiplexing (OFDM)，是現今許多調變方法的基本組成部分；因此本章節將依序討論 OFDM 的基本概念與調變原理，並且介紹如何在 802.11a/g 調變中創建出 OFDM 符號，最後說明 PPDU 規範之下的訊框傳送格式以及訊框組成成分之生成。

OFDM 是一種利用大量且正交的子載波傳遞訊息以提高傳輸速率的調變技術，在一個簡單的 OFDM 系統中，會利用 N 個相互正交的正弦訊號來傳送 N 個位元的資料，而接收端則是利用相同的子載波頻率將接收訊號進行解調，進而得到原始之傳輸資料。

在 802.11a/g 的調變技術中，會將訊號組成 OFDM 符號進行傳輸，而詳細之 OFDM 訊號之生成過程則如圖 9 所示。首先，輸入之位元資料流會先經過卷積編碼與位元交錯等程序之處理，並且依據不同的調變方式 (BPSK、QAM 等) 將輸入資料分組並且映射到不同的子載波上，接著利用 Inverse Fast Fourier Transform (IFFT) 將 64 個頻域子載波訊號轉換為時域之 64 個取樣點訊號，其中只有 52 個子載波被用來傳遞資料，並且在這當中的 4 個子載波為固定之導頻子載波 (分別位於第 -21、-7、7、21 個子載波)。下一步會將轉換至時域之 64 個取樣點訊號之前加上一段防護區間 (Guard Interval) 以防止因為多路徑干擾而產生的 Inter-Symbol Interference (ISI) 與 Inter-Carrier Interference (ICI)，並且由此構成一個 OFDM 符號，接著即是重複以上步驟直至位元數量到達訊框所規範之最高容量亦或是輸入訊號皆被轉換為 OFDM 符號，最後則是在數個 OFDM 符號之前加上前導碼 (Preamble) 組成為一個符合 PPDU 訊框格式的 OFDM 訊框進行傳輸。

本研究之目的為利用 802.11a/g 規範之 Wi-Fi 訊號之指紋特徵來識別個別設備，因此本章節將針對規範 (IEEE, 1999) 中所定義之 PPDU 訊框格式進行介紹，並且更深入的探討其子訊號之組成。如圖 10 所示，表示封包中各個符元於時域上之表現，而一個標準之 PPDU 訊框包含了 PLCP Preamble (包含了短訓練符元與長訓練符元)、SIGNAL 與 DATA 的部分，以下便針對構成訊框之各種不同符元所承載之資料逐一進行介紹。

1. 短訓練序列

如圖 11 所示，短訓練序列是由 10 個短訓練符元所組成，頻域上包含了 12 個子載波，用於訊號偵測、訊號同步與粗略頻偏估測，並且由序列 S (如下所示) 調變而來：

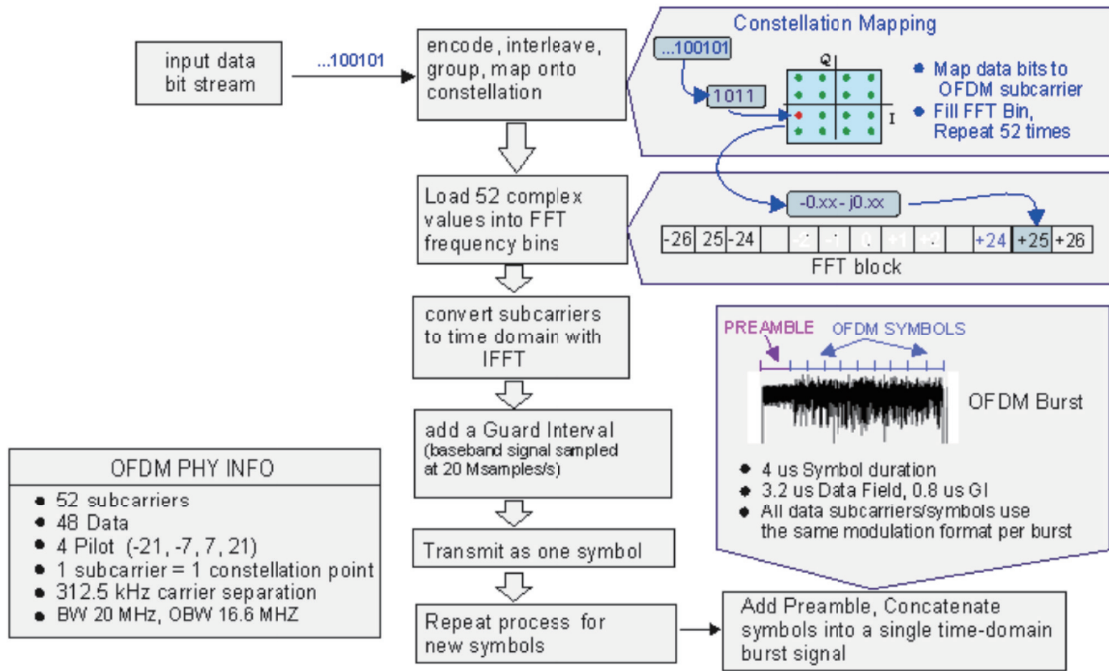


圖 9 OFDM 訊框之生成

資料來源：Keysight Technologies (n.d.)。

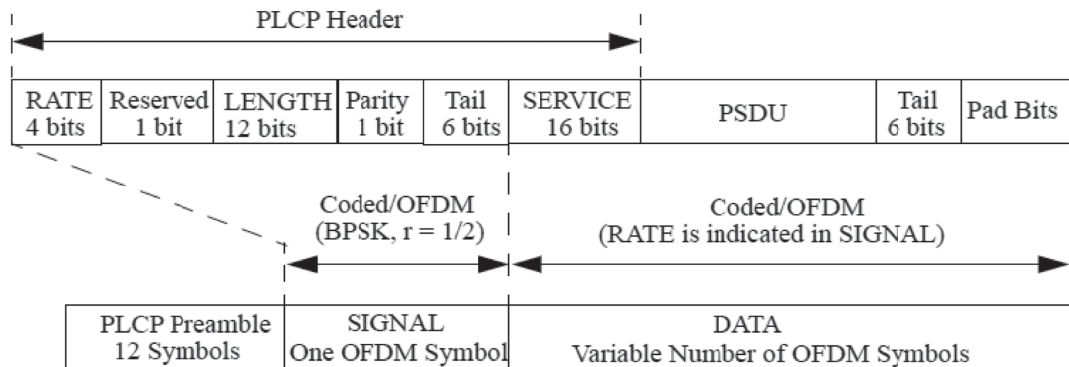


圖 10 PPDU 之訊框格式

資料來源：IEEE (1999)。

$$S_{-26,26} = \sqrt{(13/6)} \times \begin{Bmatrix} 0, 0, 1+j, 0, 0, 0, 0-1-j, 0, 0, 0, 1+j, 0, 0, 0, \\ -1-j, 0, 0, 0, 0, -1-j, 0, 0, 0, 1+j, 0, 0, 0, 0, \\ 0, 0, 0-1-j, 0, 0, 0, 0-1-j, 0, 0, 0, 1+j, 0, 0, \\ 0, 1+j, 0, 0, 0, 0, 1+j, 0, 0, 0, 1+j, 0, 0 \end{Bmatrix} \quad (8)$$

其中乘上 $\sqrt{(13/6)}$ 是為了將 OFDM 短訓練序列信號正規化，也就是將頻域上之平均載波資料功率固定為 1，因此短訓練序列於時域上之表示式為：

$$r_{SHORT}(t) = w_{TSHORT}(t) \sum_{k=-N_{ST}/2}^{N_{ST}/2} S_k e^{j2\pi k \Delta f t} \quad (9)$$

其中 N_{ST} 為總子載波之數量，此處為 52， $w_{TSHORT}(t)$ 為時域之窗口函數（Window Function），目的為平滑一連串 OFDM 符元之間的串連，並表示為下式：

$$W(k) = \begin{bmatrix} 0.5 & k = 0 \\ 1 & 1 \leq k \leq 16 \\ 0.5 & k = 60 \end{bmatrix} \quad (10)$$

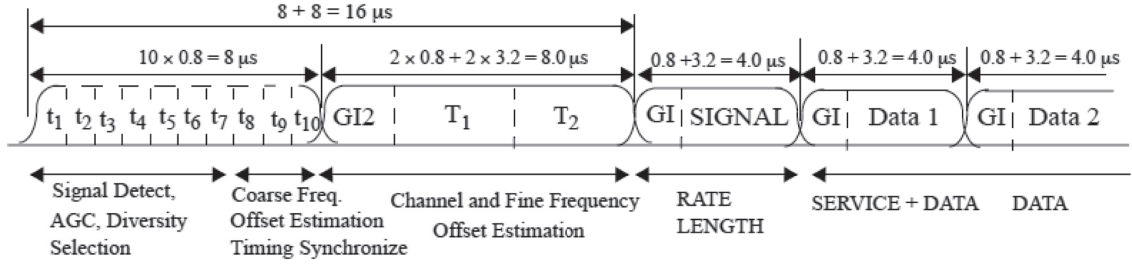


圖 11 OFDM 訓練序列之結構

資料來源：IEEE（1999）。

2. 長訓練序列

長同步訊號是由 2 個長同步符元所組成，頻域上由 53 個子載波所組成（包含載波中心頻之 DC 子載波），用於通道估計與精細頻偏估測，並且由序列 L （如下所示）調變而來：

$$L_{-26,26} = \begin{pmatrix} 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, 1, \\ -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 0, 1, -1, \\ -1, 1, 1, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, \\ 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1, 1 \end{pmatrix} \quad (11)$$

並且能夠將時域上之長同步訊號表示為：

$$r_{LONG}(t) = w_{TLONG}(t) \sum_{k=-N_{ST}/2}^{N_{ST}/2} L_k e^{j2\pi k \Delta f (t - T_{G12})} \quad (12)$$

其中 $w_{TLONG}(t)$ 為窗口函數， T_{G12} 為長同步訊號前方之訊號防護區間。

3. SIGNAL

緊接在 OFDM 同步訊號之後的即為 SIGNAL 訊號，由 24 個位元所組成，如圖 12 所示。其中 RATE 區塊包含了四個位元（位元 0 至位元 3），傳達了有關此訊框其餘部分中所使用的調變類型以及編碼率之訊息，而編碼之過程包括卷積編碼、位元交錯、調變映射、插入導頻子載波以及 OFDM 調變之過程。

位元 4 為保留位元，位元 5 至位元 16 則為 LENGTH 區塊，傳達了 MAC 層要求於 PSDU 所傳遞之八位元字節數，位元 17 為校驗位元，位元 18 至位元 23 則設置為 0。

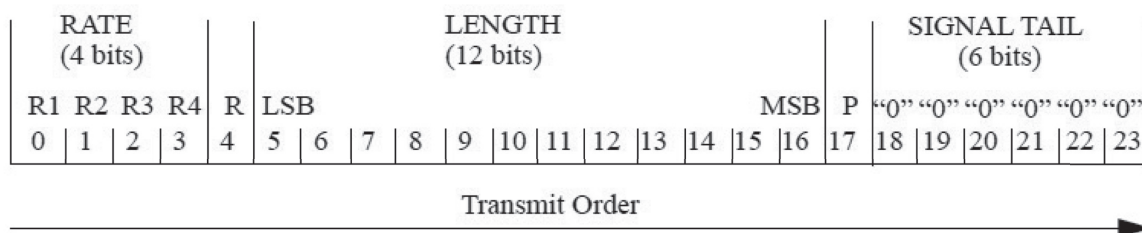


圖 12 SIGNAL 訊號之位元分配

資料來源：IEEE（1999）。

4. DATA

如圖 11 所示，DATA 區塊中之訊號以每 4 μs 定義為一個 OFDM 符號，並且每個 OFDM 符號在頻域皆由 52 個子載波進行資料之傳輸。其中 4 個子載波為導頻子載波以估測並補償頻率與相位偏移，而導頻子載波則由序列 P 的傅立葉變換所產生，序列 P 如下表示：

$$P_{-26,26} = \begin{pmatrix} 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \\ 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, \\ 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, \\ 0, 0, -1, 0, 0, 0, 0, 0, 0 \end{pmatrix} \quad (13)$$

因此可以得知導頻子載波的位置分別為 -21、-7、7、21。

此外，導頻訊號之極性（Polarity）是由序列 P_n 控制，為 $P_{0..126v}$ 的 127 個位元序列的循環延展，此極性將控制序列 P 是乘上 +1 或是 -1。

（二）傳輸端之指紋特徵介紹

本章節將探討本研究所提取之指紋特徵於傳送端裝置之生成原因，而傳送端設備之架構圖如圖 13 所示。傳送端在發送訊號時會先經由 DAC 將數位訊號轉換為類比訊號，並且藉由本地振盪器（Local Oscillator）與混頻器將基頻訊號升頻為帶通訊號以利無線傳輸。

首先，由於各個傳送端之 DAC 取樣頻率與標準 DAC 之取樣頻率的偏差將產生取樣頻

率偏移 (Sampling Frequency Offset, SFO) 特徵，本地振盪器之頻率誤差也將導致帶通訊號之載波頻率產生偏移，並且依據估計方式的不同可以再分別取得載波頻率偏移特徵、略載波頻率偏移 (Short CFO, SCFO)、精細載波頻率偏移 (Long CFO, LCFO) 與殘差頻率偏移 (Residual CFO, RCFO)，接著，由於移相器 (Phase Shifter) 的移相偏差以及 IQ 路徑之所有電路之細微誤差都將造成 IQ 不平衡，因而造成增益不平衡 (Gain Imbalance) 特徵、相位偏移 (Phase Offset) 特徵與振幅偏移 (Magnitude Offset) 特徵，而星座圖的偏移以及功率的變化能夠進一步提取誤差向量幅度 (Error Vector Magnitude, EVM) 特徵以及功率頻譜密度 (Power Spectral Density, PSD) 特徵。

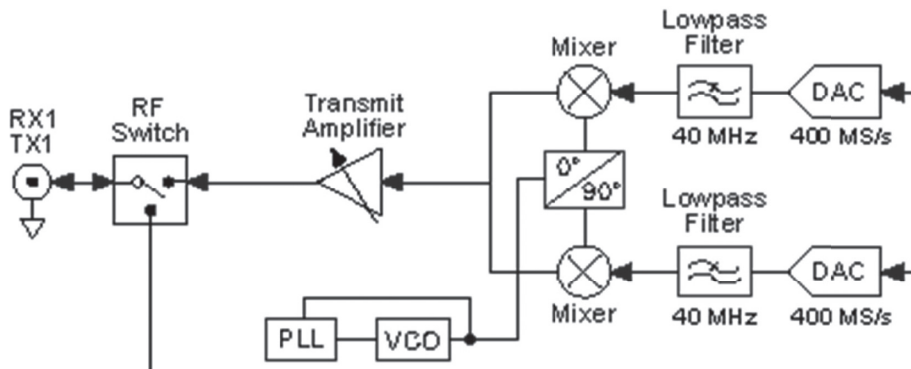


圖 13 傳送端設備之架構

資料來源：Ettus Research (2016)。

(三) 接收端對指紋特徵之影響

為了去除接收端設備對傳送端指紋特徵之影響，本章節將各別探討接收端指紋特徵之生成原因、提取方法以及對傳送端指紋特徵所造成之影響。如圖 14 所示，為接收端設備之架構圖，基於此架構我們可以針對各個接收端之特徵進行分析。

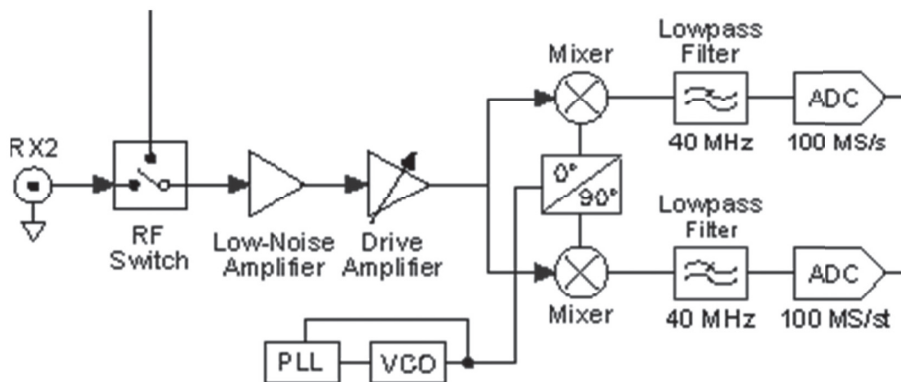


圖 14 接收端設備之架構

資料來源：Ettus Research (2016)。

1. 直流偏移 (DC Offset)

首先，本地振盪器與混頻器及低雜訊放大器的輸入端之間的隔離並不完美 (Razavi, 1997)，這將導致本地振盪器的訊號洩漏，而洩漏訊號若由低雜訊放大器與混頻器之輸入端流入，將會造成自混頻的現象，最後導致混頻器輸出之訊號含有直流準位之偏移，如圖 15 所示。

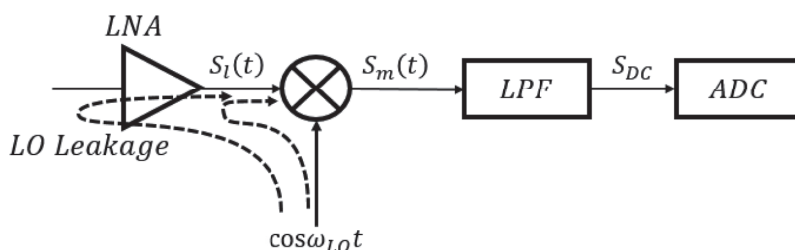


圖 15 本地震盪器之自混頻

資料來源：作者研究整理。

2. IQ 增益不平衡

由傳送端之 IQ 不平衡特徵可以得知，接收端 IQ 路徑之電路誤差以及移向器之移向誤差也將導致 IQ 不平衡之特徵，也就是 IQ 增益不平衡、相位偏移以及振幅偏移，進而影響接收端之 IQ 增益不平衡之特徵。而如圖 16 所示，其中圖 16 (a) 與圖 16 (b) 分別表示 I / Q 增益不平衡以及相位偏移在星座圖上所造成之影響，圖 16 (c) 與圖 16 (d) 則表示 I / Q 增益不平衡以及相位偏移於時域上影響之表現。

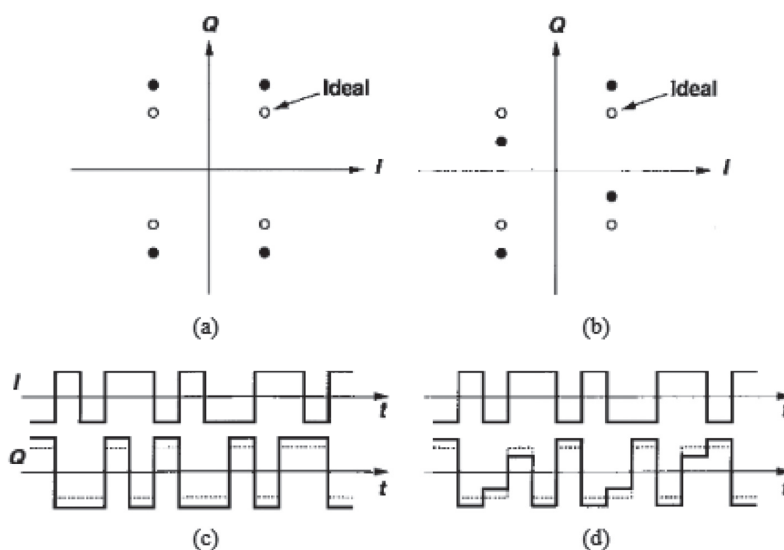


圖 16 I / Q 增益不平衡與相位偏移之示意圖

資料來源：Razavi (1997)。

3. 載波頻率偏移

載波頻率偏移為發送端本地振盪器之頻率與標準頻率之間的誤差，然而接收端之本地振盪器也會有頻率偏移，將影響傳送端之載波頻率偏移特徵，因此本節將利用粗略頻偏估測與精細頻偏估測分別得出 SCFO 特徵與 LCFO 特徵，進而得知接收端設備對載波頻率偏移特徵所產生之影響。

若假設理想傳送端之基頻訊號為 $x(t)$ ，則經由傳送端本地振盪器升頻後之訊號表示為 $x(t) \cdot e^{j2\pi f_t t}$ ，接下來訊號經由接收端本地振盪器降頻之後，由於 $f_t \neq f_r$ ，可以表示為：

$$x'(t) = x(t) \cdot e^{-j2\pi \Delta f t} \quad (14)$$

如圖 17 所示，由於短訓練序列是由 10 個相同的短訓練符元所組成，而長訓練序列則由 2 個相同的長訓練符元所組成，我們可以利用這個特性，將符元的其中一個取樣點與其 N （短訓練序列為 16，長訓練序列為 64）個取樣點後之訊號進行運算，估計出載波頻率偏移，如下式所示：

$$\begin{aligned} x'[n] &= \tilde{x}(nT_s) \cdot e^{-j2\pi \Delta f n T_s} \\ x'[n+N] &= \tilde{x}((n+N) \cdot T_s) \cdot e^{-j2\pi \Delta f (n+N) T_s} \end{aligned} \quad (15)$$

由此式可以得知，第 n 個取樣點之訊號將會有 $-2\pi \Delta f n T_s$ 的相位偏移，而第 $n+N$ 個取樣點之訊號將會有 $-2\pi \Delta f (n+N) T_s$ 的相位偏移，因此利用以下兩式我們可以估算出載波頻率偏移：

$$\angle(x'[n] \cdot x'^*[n+N]) = -2\pi \Delta f N T_s \quad (16)$$

$$\Delta f = \frac{-1}{2\pi N T_s} \angle(x'[n] \cdot x'^*[n+N]) \quad (17)$$

其中粗略頻偏估測之 N 為 16，精細頻偏估測之 N 為 64，並且分別得到 SCFO 特徵與 LCFO 特徵，最後將兩者相加即為載波頻率偏移特徵。

4. SFO 與 RCFO

接收端所提取之取樣頻率偏移特徵為傳送端的 DAC 與接收端的類比數位轉換器（Analog-to-Digital Converter, ADC）之間的取樣頻率偏差，由於 ADC 之取樣頻率偏移將會影響判斷 DAC 之取樣頻率偏移因此需要估算收發機之間的取樣頻率偏移，並且進一步去除



圖 17 訓練序列之取樣關係圖

資料來源：Lu (2018)。

其影響。RCFO 則為第二小節所述之粗略頻偏估測與精細頻偏估測之後補償不完全之頻率偏移，因此可以得知若存在收發機之間的 RCFO 也會影響到傳送端之 RCFO 特徵。

如圖 18 所示，橫座標為子載波之索引數，縱座標為每個子載波所對應之相位偏移，其中載波頻率偏移對於每個子載波都會造成相同之相位偏移，而取樣頻率偏移則會造成和子載波索引相關之相位偏移，因此我們可以藉由此特性，並且利用傳輸固定資料的導頻子載波來計算出中心子載波之頻率偏移，即為 RCFO 特徵：

$$\Delta f_R = \frac{1}{2\pi} \angle (x_i[-21] + x_i[-7] + x_i[7] - x_i[21]) \quad (18)$$

而 SFO 所造成的影響是每個子載波以固定的相位差進行偏移，進而導致相位旋轉，因此可以由下式得出 SFO 特徵：

$$\Delta S = \frac{\angle(x_i[-7]) - \angle(x_i[-21])}{14} \quad (19)$$

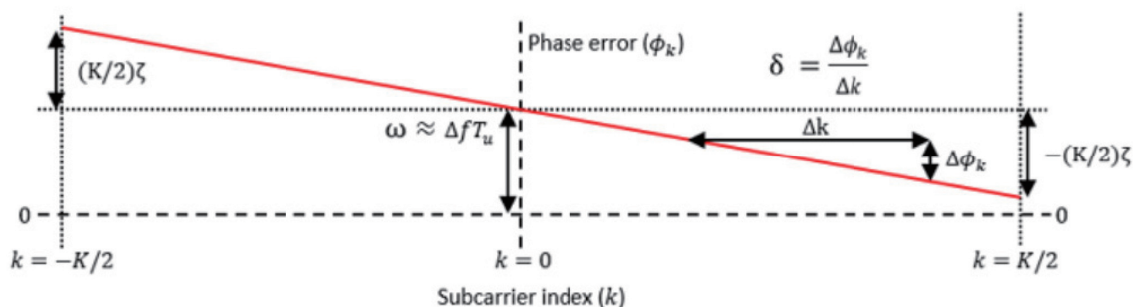


圖 18 取樣頻率偏移與殘差載波頻率偏移

資料來源：MathWorks (2020)。

二、指紋特徵提取方法

本節將根據實際程式的程序分別從時域以及頻域提取短訓練序列、長訓練序列以及 SIGNAL 符元的指紋特徵，並將在此章節依序介紹各別指紋特徵之提取方法；然而，由於 802.11a/g 訊號是由頻域調變訊號，又根據最後各別指紋特徵的辨識結果可以發現時域特徵的辨識表現遠遠不及頻域特徵，因此本研究最後方向為著重提取不同的頻域特徵。

（一）短訓練序列之特徵（Short Training Sequence）：SCFO

由接收端接收之訊號往往會混雜著雜訊，導致難以辨別訊號之起始點，因此需要進行粗略頻偏估計（Coarse Frequency Estimation），找出 802.11g 訊號段一次短循環的起始點。首先利用短訓練序列每 16 個取樣點為一次循環訊號之特性，將第 n 個取樣點訊號 $x[n]$ 和其 16 個取樣點後之訊號 $x[n+16]$ 進行相關性之運算。當相關值 $C_s[n]$ 高於設定之閾值，則可視為找到短訓練序列之訊號段，即第 n 個取樣點時之訊號位於短訓練序列段之中。

$$C_s[n] = \frac{x'[n]x'^*[n+16]}{x'[n]^2} \quad (20)$$

其中 $C_s[n]$ 為兩取樣點訊號之相關性， $x'[n]$ 為接收之時域訊號的第 n 個取樣點。

粗略頻偏估計採用 802.11a/g 訊號之短訓練序列部分進行估計，經由短同步可得第 n 個取樣點時訊號位於短訓練序列。而後由 n 個取樣點往後進行 16 次頻偏估計。

$$\Delta\tilde{f}_s = \sum_{m=0}^{16-1} \frac{\angle(x'[n+m]x'^*[n+m+16])}{2\pi \cdot 16} \quad (21)$$

其中 $\Delta\tilde{f}_s$ 為粗略頻偏估計值之總和， $x'[n]$ 為接收訊號的第 n 個取樣點。最終由 16 個頻偏估計值進行平均即可得粗略頻偏估計值 Δf_s ，即為特徵 SCFO。

$$\Delta f_s = \frac{\Delta\tilde{f}_s}{16} \quad (22)$$

（二）長訓練序列之特徵（Long Training Sequence）

1. LCFO

欲提取長訓練序列之指紋特徵，首先需找出長訓練序列之起始取樣點，進而對訊號進行處理並且提取指紋特徵。由於長訓練序列每 64 個取樣點循環一次，且循環兩次，因此可以透過規範中長訓練序列之理想數值，將輸入訊號以 64 個取樣點為一單位，與規範數值進行

相關性運算，並且以滑動窗口的方式，每次計算將接收訊號往後位移一個取樣點，同時記錄此次運算起始取樣點之位置，數學式如下所示：

$$C_l[n] = \sum_{m=0}^{64-1} \frac{x'[n+m]x_L^*[m]}{x_L[m]^2} \quad (23)$$

其中 $x'[n]$ 為接收訊號之第 n 個取樣點， $x_L[m]$ 為理想長訓練序列第 m 個取樣點， $C_l[n]$ 為第 n 個取樣點所得之相關性。

當選取之 64 個取樣點為一完整長循環時，會達到與規範數值最高之相關性，兩段完整循環將會依序得出兩項最高相關性數值。藉由尋找相關性數值最高的兩次運算結果 $C_l[n_{m1}]$ 、 $C_l[n_{m2}]$ ，則可以比較兩次運算之起始取樣點位置 n_{m1} 、 n_{m2} ，若 $n_{m1} < n_{m2}$ ，則可得知長訓練序列首次循環起始取樣點為 n_{m1} ，二次循環起始取樣點為 n_{m2} 。

精細頻偏估計採用 802.11g 訊號之長訓練序列部分進行估計，其估計方法與粗略頻率偏移之估計方法十分相似。由自相關數值得知長訓練序列兩次週期之起始位置 n_{m1} 、 n_{m2} 。而後由取樣點 n_{m1} 往後依序進行 64 次頻偏估計。

$$\Delta \tilde{f}_l = \sum_{m=0}^{64-1} \frac{\angle(x'[n_{m1}+m]x'^*[n_{m1}+m+64])}{64} \quad (24)$$

其中 $\Delta \tilde{f}_l$ 為精細頻偏估計值之總和， $x'[n_{m1}+m]x'^*[n_{m1}+m+64]$ 為接收訊號的第 $n_{m1}+m$ 個取樣點。最終由 64 個頻偏估計值進行平均即可得精細頻偏估計值 Δf_l ，即為特徵 LCFO。

$$\Delta f_l = \frac{\Delta \tilde{f}_l}{2\pi \cdot 64} \quad (25)$$

2. 載波頻率偏移

在此處所提取之載波頻率偏移即為上述之 SCFO 與 LCFO 之和，數學式如下所示：

$$\Delta f = \Delta f_s + \Delta f_l \quad (26)$$

3. 長訓練序列之取樣頻率偏移 (Sampling Frequency Offset on Long Training Sequence, SFO1)

取樣頻率偏移在頻域中對各個子載波所造成之相偏移會根據子載波索引數之不同而呈現線性變化，因此我們可以從長訓練序列的子載波在相位上的變化求得取樣頻率偏移，即為 SFO1 特徵，數學式如下所示：

$$\Delta s_l = \frac{\angle(x_l'[53]) - \angle(x_l'[11])}{42 \times 2\pi} \quad (27)$$

其中 $X_l[k]$ 為長訓練序列第二個符元的第 k 個子載波訊號。

4. 頻域之誤差向量幅度 (Error Vector Magnitude on Frequency Domain, f_EVM)

誤差向量幅度為星座圖上理想星座點與實際訊號星座點之間之向量幅度，而長訓練序列在頻域上是以 BPSK 調變，因此如圖 19 所示，我們可以計算實際接收之長訓練序列訊號在頻域上之星座點與規範之星座點之間的向量幅度，即為所謂的 f_EVM 特徵，然而一個長訓練符元在頻域上有 52 個子載波，因此一個長訓練符元我們可以求得 52 個 f_EVM 特徵，數學式如下所示：

$$evm[k] = evm[kX] = \sqrt{(X'_{I_l}[k] - X_{I_l}[k])^2 + (X'_{Q_l}[k] - X_{Q_l}[k])^2} \quad (28)$$

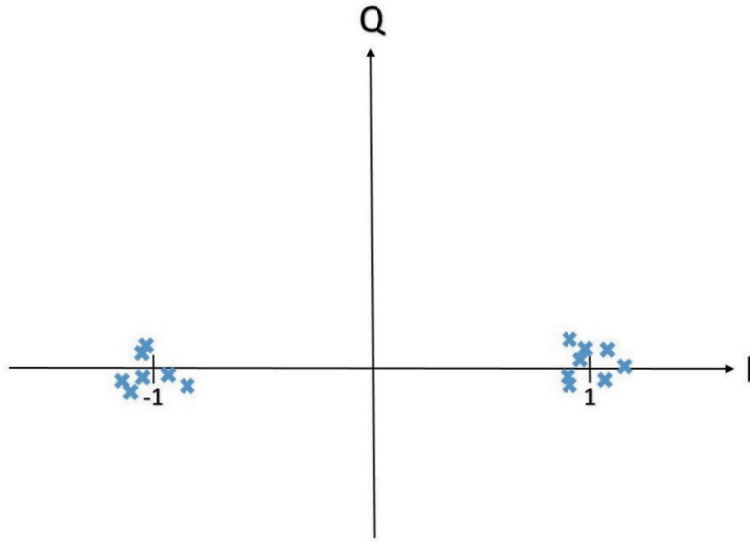


圖 19 頻域之長訓練序列於星座圖上之表示

資料來源：作者研究整理。

(三) SIGNAL 符元之特徵

1. PSD

PSD 特徵由 SIGNAL 符元進行估計，首先求取頻域訊號之功率，而後將之除以訊號頻寬便可得到功率頻譜密度，而為了觀察各個子載波的 PSD 特徵變化，此處也是提取 52 個子載波的 PSD 特徵，數學式如下所示：

$$P[k] = 10 \cdot \log_{10} \left(\frac{X'_{2I}[k]^2 + X'_{2Q}[k]^2}{B/64} \right) \quad (29)$$

其中 $X'_{2I}[k]$ 為 SIGNAL 符元第 k 個子載波之實際訊號 I 分量， $X'_{2Q}[k]$ 為 SIGNAL 符元第 k 個子載波之實際訊號 Q 分量， B 為訊號頻寬（20 MHz）。

2. RCFO

由前面章節可知補償載波頻率偏移後仍可能殘留些許載波偏移，因此要再以 SIGNAL 符元的導頻子載波所傳送的導頻訊號進行殘餘頻率偏差估計。

令 SIGNAL 符元之 64 個子載波中的四個導頻訊號相加後所估計之頻偏表示如下：

$$\Delta f_R = \frac{1}{2\pi} \angle (X_2[-21] + X_2[-7] + X_2[7] - X_2[21]) \quad (30)$$

其中 Δf_R 為殘餘頻偏估計值， $X_2[k]$ 為 SIGNAL 符元第 k 個子載波訊號。

3. SIGNAL 符元之取樣頻率偏移（Sampling Frequency Offset on SIGNAL Symbol, SFO2）

由於傳送端及接收端使用之取樣速率不盡相同，因此將會造成取樣點間的誤差。SFO2 以 SIGNAL 訊號中的導頻子載波進行每個取樣點間之頻偏估計，所有估計值之平均則為 SFO2 特徵估計值。

$$\begin{aligned} \Delta s_{21} &= [\angle(X_2[-7]) - \angle(X_2[-21])] \frac{1}{14 \times 2\pi} \\ \Delta s_{43} &= [\angle(X_2[21]) - \angle(X_2[7])] \frac{1}{14 \times 2\pi} \\ \Delta s_{42} &= [\angle(X_2[21]) - \angle(X_2[-7])] \frac{1}{27 \times 2\pi} \\ \Delta s_{32} &= [\angle(X_2[7]) - \angle(X_2[-7])] \frac{1}{14 \times 2\pi} \\ \Delta s_{31} &= [\angle(X_2[7]) - \angle(X_2[-21])] \frac{1}{28 \times 2\pi} \\ \Delta s_{41} &= [\angle(X_2[21]) - \angle(X_2[-7])] \frac{1}{42 \times 2\pi} \\ \Delta s_{41} &= \frac{1}{6} (\Delta s_{21} + \Delta s_{32} + \Delta s_{43} + \Delta s_{31} + \Delta s_{42} + \Delta s_{41}) \end{aligned} \quad (31)$$

其中 $X_2[k]$ 為 SIGNAL 符元的第 k 個子載波訊號， Δs_{ij} 為以第 i 個與第 j 個導頻子載波所估計之取樣頻率偏移， Δs 為導頻子載波估計之頻偏平均，即為 SFO2 特徵。

三、應用機器學習辨識 802.11g Wi-Fi 網卡之演算法

(一) 特徵縮放 (Feature Scaling)

在原始資料中，不同的指紋特徵會有各別的數值範圍，而特徵縮放是為了使特徵落於某個特定區間，另一個使用特徵縮放技術的優點為在使用梯度下降法求解最佳化問題時，特徵縮放可以加速梯度下降法的收斂速度。

特徵縮放主要分為兩種，分別為正規化 (Normalization) 與標準化 (Standardization)，但是正規化對於極值影響嚴重，所以標準化為較為理想的方法。標準化部分則是運用 Z 分數標準化 (Z-Score Standardization)：

$$Z = \frac{x - \mu}{\sigma} \quad (32)$$

當中 μ 為資料的平均值 (Mean)， σ 為資料的標準差 (Standard Deviation)，為轉換後的數值。標準化後的平均值為 1，標準差為 0。資料進行標準化可以提高演算法的收斂速度，降低運算所需的時間。

(二) 滑動窗口 (Sliding Window)

在 CNN 中無法使用單個封包的單筆特徵數值當作一筆資料進行訓練，因為數值太少而無法進行訓練，所以我們需要將多個數值整合成一筆資料作為訓練數據集，使用滑動窗口的方法可以將多個數值進行整合，如圖 20 所示，實驗中固定窗口大小以及每次滑動單位以取得更高的資料使用率。如圖 21 在進行滑動窗口方法進行整合前會先將資料集分為訓練資料集與測試資料集，以避免在訓練資料與測試資料具有重複之數值，致使在 CNN 分類中因為重複數值而影響分類效果。

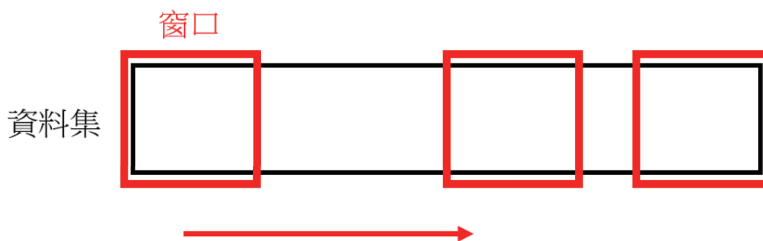


圖 20 滑動窗口

資料來源：作者研究整理。

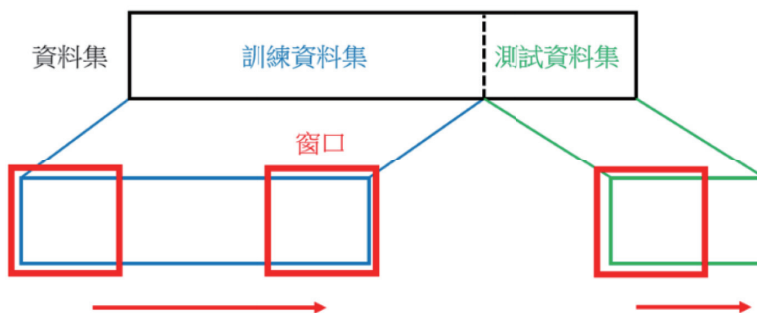


圖 21 滑動窗口的資料分割

資料來源：作者研究整理。

(三) CNN

O'Shea et al. (2016) 的演算法在 CNN 用四層卷積層與一層密集全連接層做為輸出層 (Output Layer)。實驗使用 CNN 的方法如圖 22 所示，四層卷積層使用 ReLU 做為激活函數，可以將非線性特性引入到 CNN 網路中，而密集全連接層則使用 S 型 (Softmax) 激活函數以於進行最後的分類，公式如下：

S 型激活函數：

$$f(z) = \frac{1}{1 + e^{-z}} \quad (33)$$

ReLU 激活函數：

$$f(z) = \begin{cases} 0 & \text{for } x < 0 \\ x & \text{for } x \geq 0 \end{cases} \quad (34)$$

除了卷積層與密集全連接層外其他分別加進了池化層 (Pooling Layer) 與 dropout 層已預防過度擬合的情形。此 CNN 模型中採用的損失函數 (Loss Function) 為交叉熵 (Cross Entropy)，若預測值越接近實際值，則損失函數得出的數值愈小，反之若差距越大，則函數數值愈大，優化器 (Optimizer) 則使用 ADAM 進行訓練。

(四) 辨識率與 F1 Measure

圖 23 是混淆矩陣，其中 TP (True Positive) 是預測值為 Positive，而真實值也為 Positive 的情形；FP (False Positive) 是預測值為 Positive，而真實值為 Negative；FN (False Negative) 是預測值為 Negative，而真實值為 Positive；TN (True Negative) 是預測值為 Negative，而真實值也為 Negative 的情形。而其準確率 (Accuracy) 公式為：

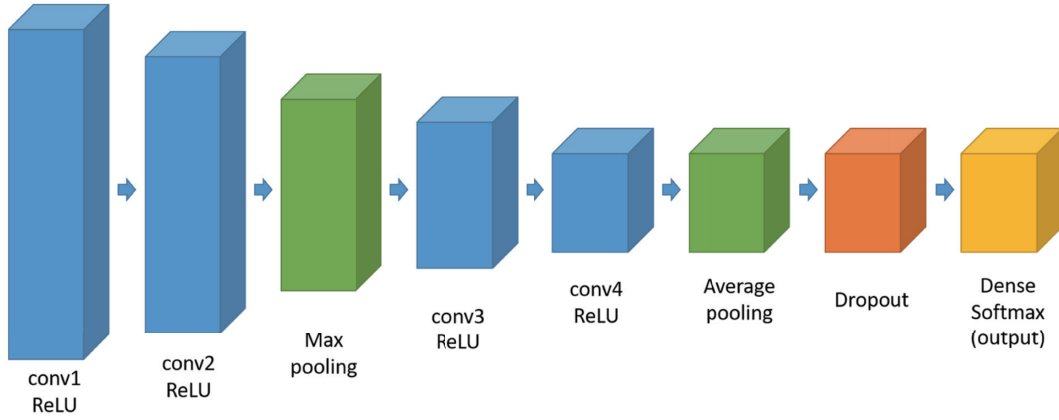


圖 22 CNN 演算法架構圖

資料來源：作者研究整理。

$$\frac{TP + TN}{TP + TN + FP + FN} \quad (35)$$

而精確率 (Precision) 為：

$$\frac{TP}{TP + FP} \quad (36)$$

而召回率 (Recall) 分別為：

$$\frac{TP}{TP + FN} \quad (37)$$

舉例而言，如圖 24 第一個類別為例（類別 0），三階混淆矩陣可以縮減至二階混淆矩陣，並可利用準確率公式進行計算其準確率，但直接計算準確率會考慮到 TN，使要觀察的 TP 比例相對下降許多，所以我們會將準確率改變為辨識率（Identification）再進一步計算，而辨識率的公式如下：

$$\frac{\sum_{all\ label} TP}{TP + TN + FP + FN} \quad (38)$$

		Predicted class	
		Positive	Negative
Actual class	Positive	TP (True Positive)	FP (False Positive)
	Negative	FN (False Negative)	TN (True Negative)

圖 23 混淆矩陣

資料來源：作者研究整理。

		Predicted class		
		0	1	2
Actual class	0	10	4	7
	1	1	8	3
	2	4	2	5



		Predicted class	
		0	非0
Actual class	0	10	11
	非0	5	18

 :TP
 :FP
 :FN
 :TN

圖 24 混淆矩陣舉例

資料來源：作者研究整理。

除了使用辨識率可以確認訓練的好壞外，F1 measure 也是一個方法，但跟辨識率不一樣的是 F1 measure 可以算出各個類別對此模型的好壞，比起對整個混淆矩陣進行數值化的辨識率，F1 measure 可以更加深入的探討各個類別，並對其進行數值化以利於之後加權。而 F1 measure 算法如下：

$$F1\ measure = \frac{2 \cdot precision \cdot sensitivity}{precision + sensitivity} \quad (39)$$

F1 measure 利用精確率與召回率進行調和平均計算，而調和平均比一般平均最大的差別在於其對極小值的敏感度，可以假設精確率與召回率的數值為 0 與 1，一般平均值為 0.5，但使用調和平均的 F1 measure 其值為 0，可見若有極小值發生，F1 measure 就會有較為明顯的下降。

（五）加權方法

在不同特徵當中，不是所有特徵都可以將不同類別都分類正確，這種情形下必須將穩定分類的特徵提取出來並優先考慮這些特徵，使用加權方法可以對較高正確分類的特徵加上更高的權重以利於提高辨識結果。

在實驗中主要使用兩種不同的加權方法，其中一種為平均辨識率加權，而另一種為平均 F1 measure 加權。如圖 25 為例，左半邊為無權重方法，因有兩個特徵判斷為網卡 1，所以最終結果也會分類為網卡 1，此方法下，當不可靠的特徵比可靠的特徵多很多時，無法有效的進行分類，因為可靠的特徵沒有占據比較高的權重；同樣的圖 25 右半邊為此次實驗加權方法，利用這些權重相加可以發現，因為特徵 3 的權重比其它兩者特徵高，也就是說特徵 3 比起其他兩種特徵具有更高的可靠度與正確度，所以經過加權後可以發現網卡 2 的分數比網卡 1 的高，所以最終選擇網卡 2 作為最終分類結果，使用此方法將可靠的特徵占有更高的比重，以提升其辨識率。

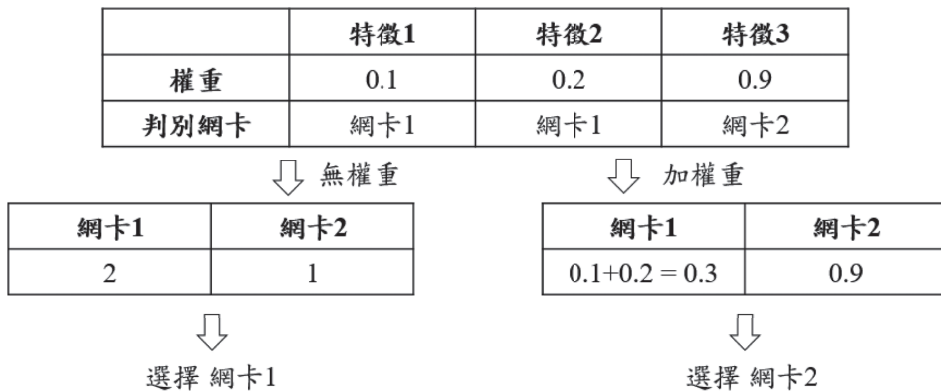


圖 25 加權方法範例

資料來源：作者研究整理。

四、改善相異接收機之辨識方法

接收端校正正在於去除接收端之間的差異，讓特徵只留下傳送端與通道的影響。令不同接收端提取出的特徵皆可使用相同的辨識模型進行分類，達成指紋特徵的可攜性。

首先訂定一臺接收端為標準，並在分類階段統一使用其訓練的辨識模型，下文將用於訓練模型的接收端稱為「訓練接收端」，其餘接收端則稱為「校正接收端」。

（一）指紋特徵分布之分析

透過分析不同接收端接收相同通道與相同傳送端訊號所提出的特徵之分布，可觀察到由接收端造成的分布差異，而校正的目標便是盡可能將此差異去除，令校正接收端與訓練接收端提取之特徵分布趨於相似。

分析結果顯示特徵 SCFO、LCFO、載波頻率偏移、PSD 皆呈現高斯分布（Gaussian Distribution），此分布有數值集成的特性，因此使用均值平移校正法，將校正接收端特徵分布之平均值移至訓練接收端特徵分布之平均值。

透過圖 26 可觀察在理想狀況之下校正後校正接收端與訓練接收端提取之特徵分布更為

相似。另外對於 PSD 特徵提取之 52 個數值，我們視為 52 個獨立特徵並對每個子載波進行各自的校正。

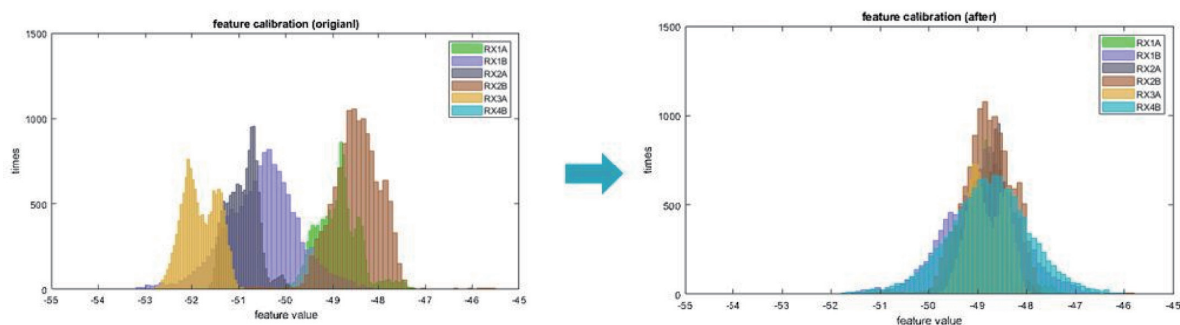


圖 26 第二個子載波之 PSD 分布理想校正前後對比

資料來源：作者研究整理。

(二) 接收端校正流程

由於實際上使用的校正數值應能通用於該校正接收端所接收的任何訊號，因此以該校正接收端與訓練接收端差異之均值作為最終校正數值，如圖 27。

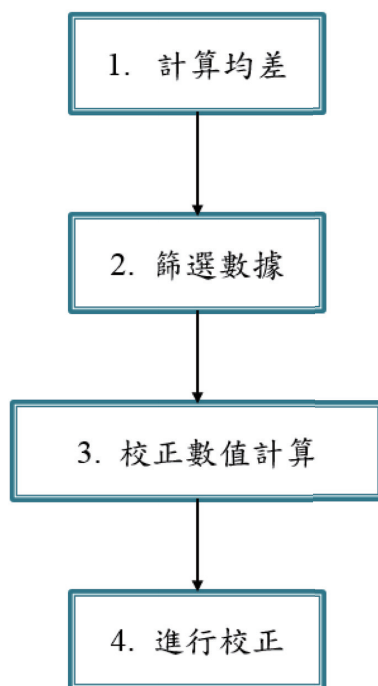


圖 27 校正流程

資料來源：作者研究整理。

1. 計算均差

首先計算各接收端接收相同通道和傳送端訊號取出之同特徵間彼此的平均值，而後求出各均值之差，此均差值則可視為是接收端之間的差異值。實驗中共使用 15 張網卡作為傳送端，因此每臺接收端將能夠求得各個特徵的 15 個均差值，如圖 28。

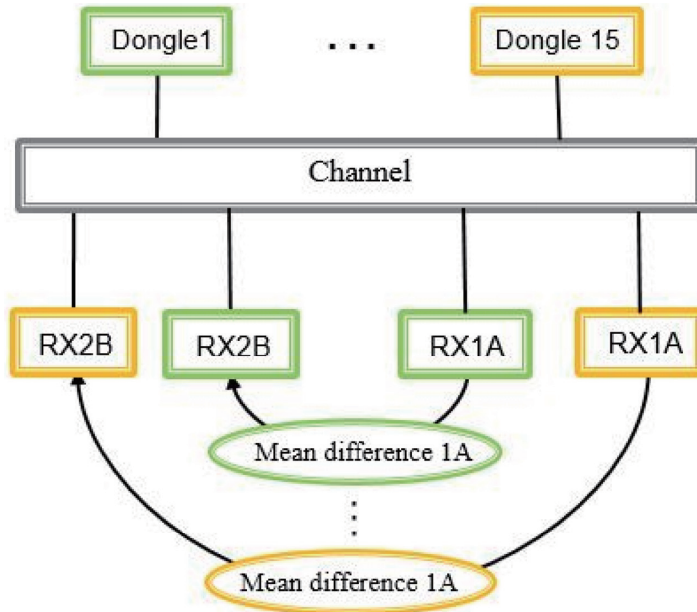


圖 28 各校正接收端與訓練接收端計算均差

資料來源：作者研究整理。

2. 篩選數據

由於每段數據求得之均差值偶有極端值，因此需要先去除極端值較多的傳送端數據。以圖 29 為例，RX1B 接收 Tenda3 網卡的訊號所求得之 SCFO 特徵均值差便是一個極端值。

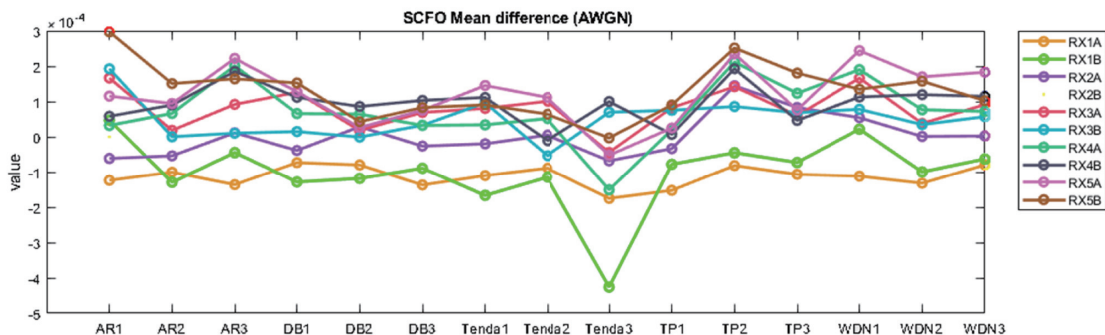


圖 29 各接收端接收各網卡訊號所求之 SCFO 平均值差值

資料來源：作者研究整理。

實驗最終去除最多次達到篩選標準的前四張網卡資料，並以其餘 11 張網卡資料計算最終校正數值。

3. 校正數值計算

經資料篩選後，每臺校正接收端重複計算均差流程，圖 30 (a)，求出校正接收端與訓練接收端的均差數值，而後將均差進行平均，圖 30 (b)，該平均均差值則為該接收端接收任何訊號的通用校正數值，圖 30 (c)。

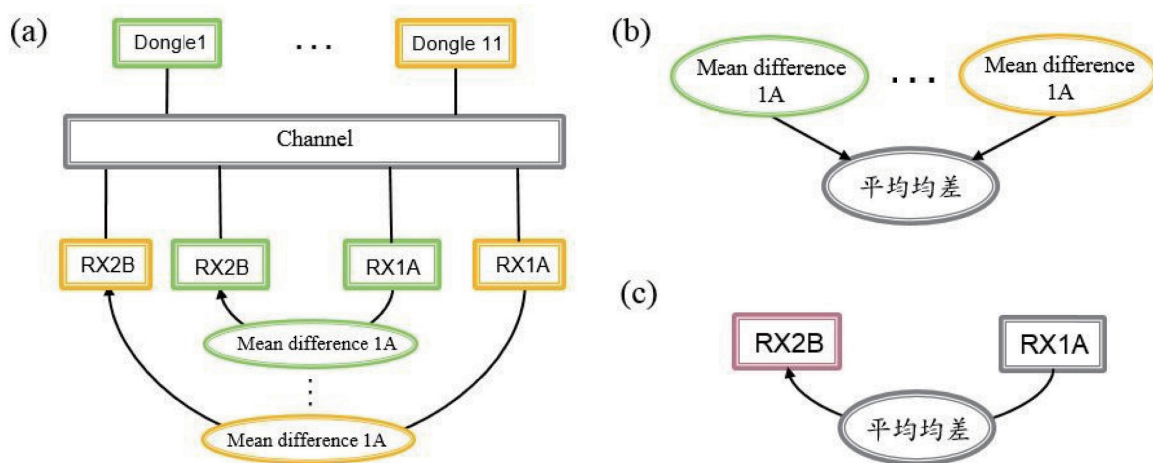


圖 30 校正數值計算示意

資料來源：作者研究整理。

(三) 校正結果分析

圖 31 為載波頻率偏移特徵使用均值平移校正法結果之前後分布對比，可知分布經過校正有集中之趨勢。由於最終校正數值期望對於接收任何數據皆有效，因此於單一傳送端特徵分布於校正後無法同理想情形一般完美重合，但會有分布集中之作用。

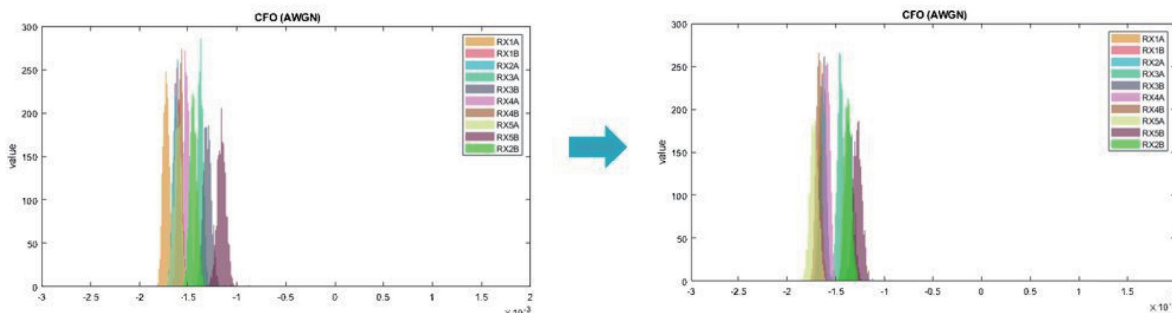


圖 31 載波頻率偏移特徵分布實際校正前後對比

資料來源：作者研究整理。

均值平移校正法為一種針對高斯分布的校正方式，由圖 32 可觀察出平均辨識率在校正後的載波頻率偏移、SCFO 特徵可提升 9%，PSD 特徵可提升 18%，而 LCFO 特徵由於其原始分布平均值已十分相近，較無改善空間。其餘無改善之特徵皆為均勻分布（Uniform Distribution）。

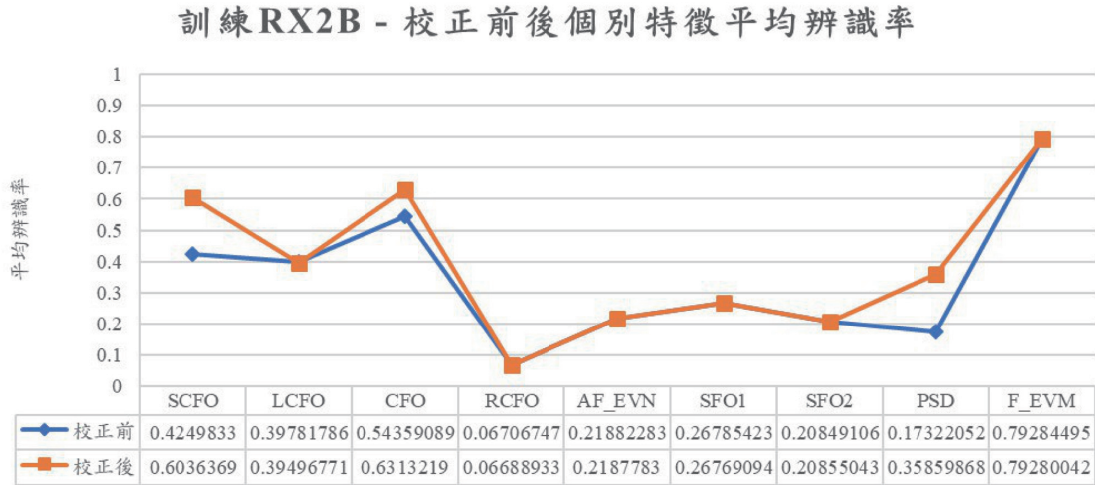


圖 32 校正前後個別特徵平均辨識率

資料來源：作者研究整理。

肆、具體研究成果

一、實驗量測方法

為了提供研究所需之數據，本研究根據三種不同通道（加性高斯白雜訊 [Additive White Gaussian Noise, AWGN]、Rician、Rayleigh）的定義而架設了三種實際量測的環境並進行了數據的量測與蒐集，以下將對三種通道各別進行介紹。

（一）AWGN Channel

AWGN 指的是一種功率譜函數為常數，並且振幅為高斯分布的雜訊訊號，一般來說 AWGN 通道便是指無其他訊號干擾的自然衰減通道，因此本研究之實驗方法為利用纜線連接，使接收訊號呈現自然衰減的現象，如圖 33 所示。

實驗方法為在 PC1 連接了傳輸端網卡、PC4 連接了路由器，並且從中擷取 PC1 與 PC4 之間無線傳輸的封包資料。為了加快量測的速度，我們將網卡以纜線連接至四路功率分配器，因此可以將網卡功率平分至四個輸出端，分別傳入多個 USRP 接收端以加快數據的量測，而未接上終端設備的輸出端口則為了阻抗匹配加上了終端阻隔器，實際量測圖如圖 34 所示。

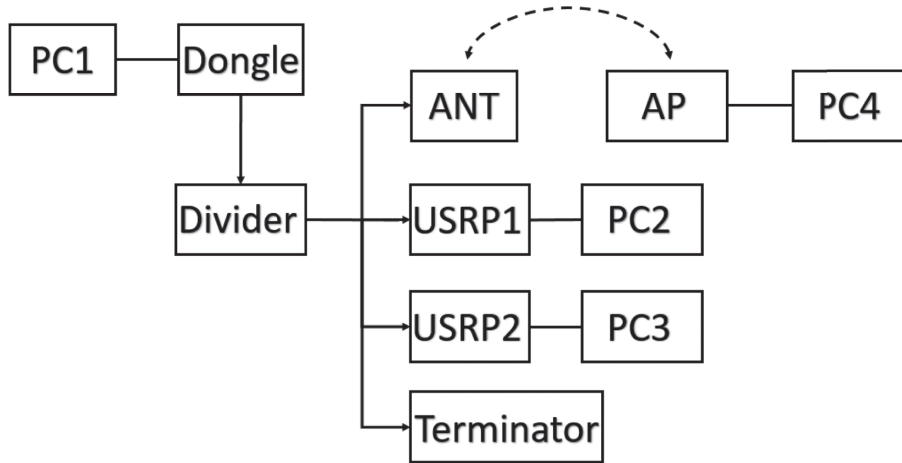


圖 33 AWGN 通道量測架構

資料來源：作者研究整理。

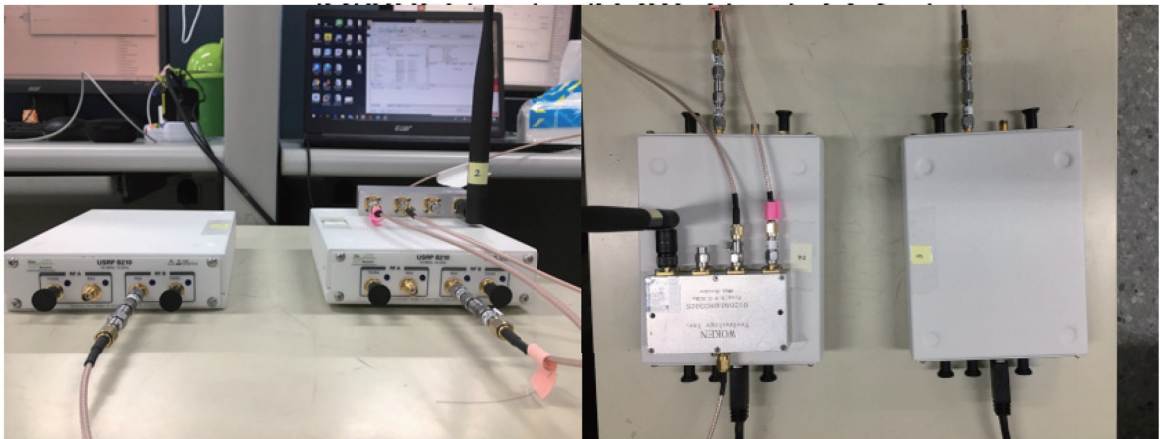


圖 34 AWGN 通道實際量測接線

資料來源：作者研究整理。

（二）萊斯衰落通道（Rician Fading Channel）

萊斯衰落通道可以模擬多路徑干擾的環境，比起 AWGN 通道更能模擬實際環境所造成的影響，而此通道的特點為傳輸端與接收端之間擁有直視路徑（Line of Sight），因此在此通道環境的建構中，必須讓傳輸端天線與接收端之間存在直視訊號，而實驗架構圖如圖 35 所示。

實驗架構大致與 AWGN 相同，是利用擷取 PC1 與 PC2 之間的無線訊號來完成量測，但是由於是監聽無線訊號的接線方式，因此改為監聽天線接至功率分配器的輸入端，並且在輸出端接上數個 USRP 與終端阻隔器，實際量測圖如圖 36 所示。

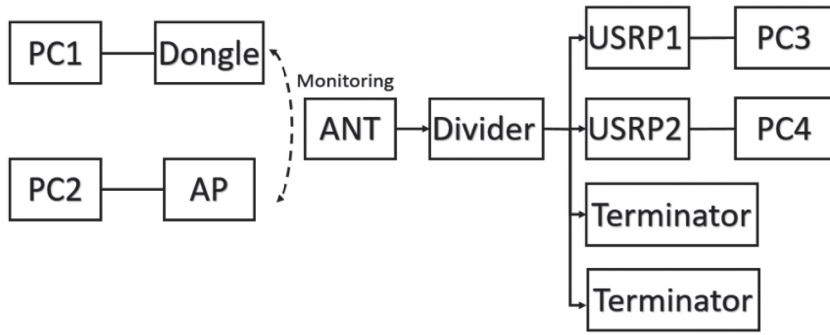


圖 35 Rician 通道量測架構

資料來源：作者研究整理。

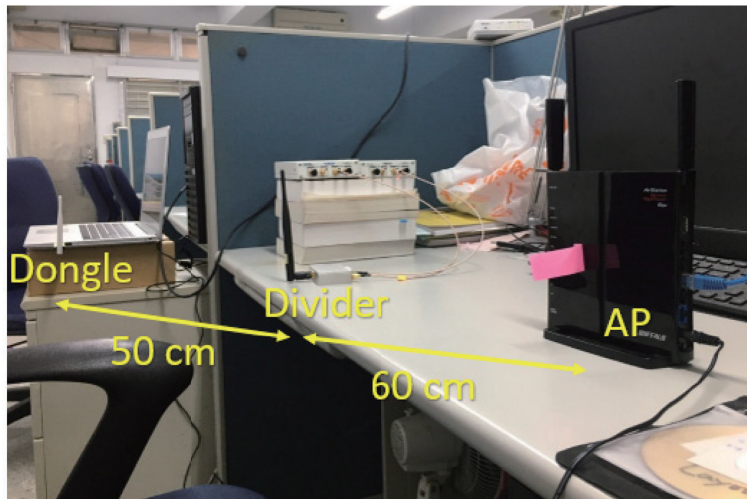


圖 36 Rician 通道實際量測接線

資料來源：作者研究整理。

（三）瑞利衰落通道（Rayleigh Fading Channel）

瑞利衰落通道與萊斯衰落通道不同的地方在於發射端與接收端之間不存在直視路徑，因此量測環境的架設上必須考慮網卡與路由器之位置，以保持此衰落通道之特性，其量測架構圖與實際量測環境接線圖分別如圖 37、圖 38 所示。

二、相同接收機之辨識成效

在經過特徵提取、特徵校正、窗口移動、CNN 演算法後，進行相同接收機的辨識，為了查看模型是否能正確辨別不同的，實驗使用 RX2 portB 的訓練資料進行訓練，RX2 portB 的測試資料集來評估辨識率，而訓練資料集與測試資料集是個別獨立的資料集，詳細實驗設定如表 1 所示，而結果如表 2 所示，在辨識率中 15 張網卡在 AWGN 通道還是 Rician 通道都有 96% 以上的辨識率，其結果證明此模型在相同接收端下分類不同發射端是可行的。

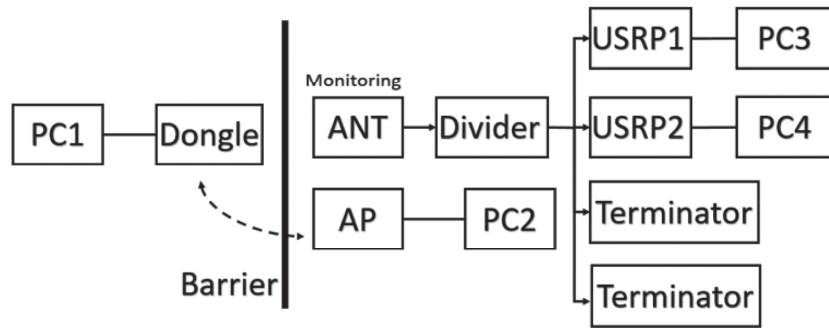


圖 37 Rayleigh 通道量測架構

資料來源：作者研究整理。



圖 38 Rayleigh 通道實際量測接線

資料來源：作者研究整理。

表 1 相同接收端之參數設定

參數	數值	
訓練接收端	RX2 portB (AWGN、Rician)	
測試接收端	RX2 portB (AWGN、Rician)	
指紋特徵	SCFO、LCFO、載波頻率偏移、RCFO、SFO1、SFO2、Average Frequency EVM (af EVM)、PSD、Frequency EVM (f EVM)	
網卡數 (個)	15	
滑動窗口大小	40	
每次窗口滑動數	20	
單一類別訓練集數量 (筆)	349 (7,000 個封包資料)	PSD、f EVM: 7,000 (7,000 個封包資料)
訓練集數量 (筆)	5,235	PSD、f EVM: 105,000
單一類別測試集數量 (筆)	99 (2,000 個封包資料)	PSD、f EVM: 2,000 (2,000 個封包資料)
測試集數量 (筆)	1,485	PSD、f EVM: 30,000

資料來源：作者研究整理。

表 2 相同接收端之辨識率詳細數據

Identification\Channel	AWGN	Rician
Equal Weight Identification	0.984512	0.962290

資料來源：作者研究整理。

三、相異接收機之辨識成效

在不同的接收機進行辨識中，利用特徵提取、特徵校正、CNN 演算法、平均辨識率加權與平均 F1 measure 加權等方法希望能有效提升在不同接收端的辨識率。其中因為使用 OFDM，所以實驗中只將頻率域的特徵提出來已期待有更高的辨識率，並利用接收端二 port B 進行資料收集進行訓練，然後在不同接收端中收集的資料進行辨識率測試，而詳細的實驗參數請參考表 3，其參數之中因為 PSD 與 f_EVM 有足夠的數據進行 CNN，因此就不進行窗口滑動。實驗結果如圖 39 與表 4 未校正特徵前的資料集進行辨識，在等權的情形下只有 63.7% 的辨識率，平均辨識率加權可以至 81.5%，平均 F1 measure 加權中平均辨識率可以至 83.3%，圖 40 與表 5 為特徵校正後的辨識率，可以發現在等權的情況下有 72.9% 的辨識率，接著平均辨識率加權則有 86.0%，最後平均 F1 measure 加權更可以達到 87.6% 的平均辨識率，由此得知相比於校正前的特徵，校正後的辨識率有更好的結果，而校正前經過加權的辨識率皆有 80% 以上，校正後更有 86% 的平均辨識率。

接著將 AWGN 通道的方法同樣運用於 Rician 通道中，如表 6 之參數設定，實驗中將 AWGN 通道換為 Rician 通道的數據集，並利用相同頻率域的特徵進行不同接收端的特徵校正，其實驗結果如圖 41 與表 7 所示，等權辨識率有 56.5%，而經過平均辨識率加權與平均 F1 measure 加權辨識率各別為 68.1% 與 71.5%。

表 3 特徵校正前之加權辨識率（AWGN）

參數	數值	
訓練接收端	RX2 portB (AWGN)	
指紋特徵	SCFO、LCFO、載波頻率偏移、RCFO、SFO1、SFO2、Average Frequency EVM (af EVM)、PSD、Frequency EVM (f EVM)	
網卡數 (個)	15	
滑動窗口大小	40	
每次窗口滑動數	20	
單一類別訓練集數量 (筆)	349 (7,000 個封包資料)	PSD、f EVM: 7,000 (7,000 個封包資料)
總共訓練集數量 (筆)	5,235	PSD、f EVM: 105,000
各個接收端測試集數量 (筆)	7,485 (10,000 個封包資料)	PSD、f EVM: 10,000 (10,000 個封包資料)

資料來源：作者研究整理。

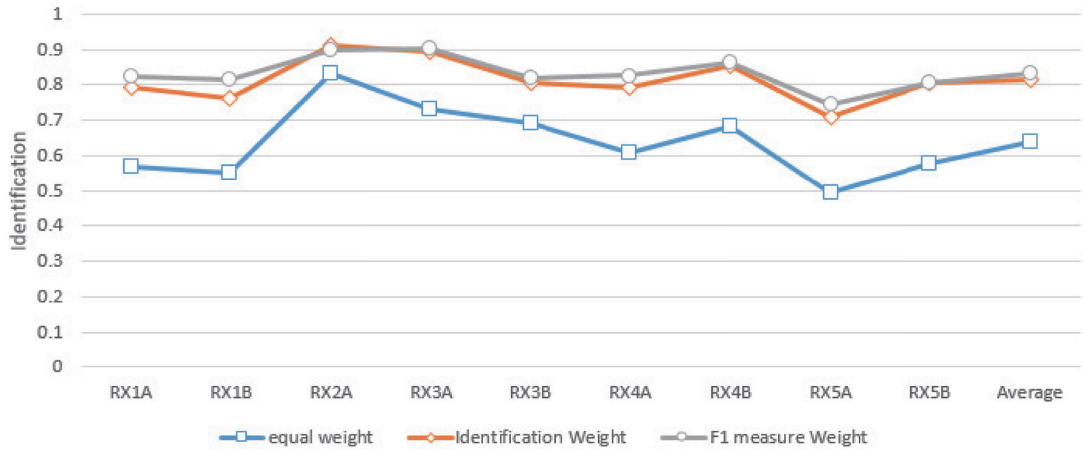


圖 39 特徵校正前之加權辨識率 (AWGN)

資料來源：作者研究整理。

表 4 特徵校正前之加權辨識率詳細數據 (AWGN)

Method/Receiver Number	RX1A	RX1B	RX2A	RX3A	RX3B
Equal weight	0.56927	0.54937	0.83113	0.73293	0.69152
Identification Weight	0.79345	0.76433	0.91142	0.89512	0.80828
F1 measure Weight	0.82391	0.81737	0.89753	0.90341	0.81764

Method/Receiver Number	RX4A	RX4B	RX5A	RX5B	Average
Equal weight	0.60695	0.6819	0.49446	0.57662	0.63713
Identification Weight	0.79158	0.85665	0.70795	0.80655	0.81504
F1 measure Weight	0.82619	0.86212	0.74402	0.80428	0.83294

資料來源：作者研究整理。

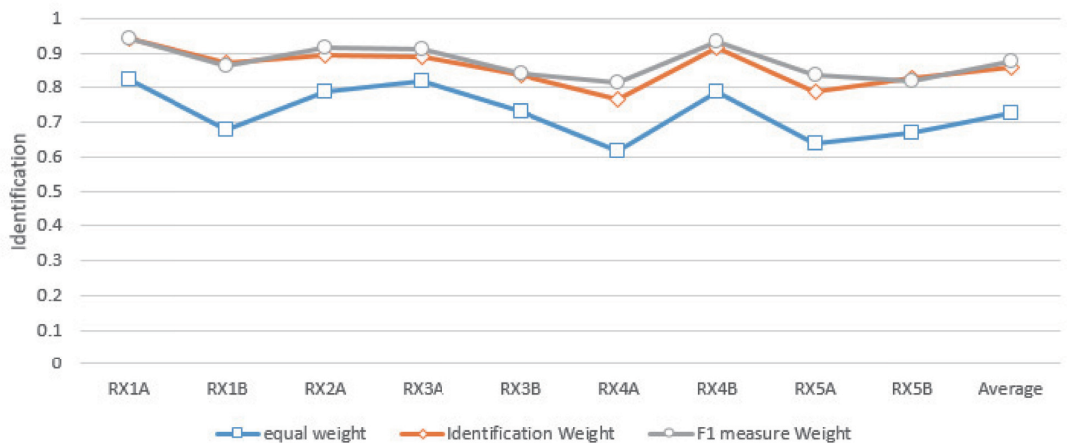


圖 40 特徵校正後之加權辨識率 (AWGN)

資料來源：作者研究整理。

表 5 特徵校正後之加權辨識率詳細數據 (AWGN)

Method\Receiver Number	RX1A	RX1B	RX2A	RX3A	RX3B
Equal weight	0.82365	0.67682	0.79065	0.82098	0.73039
Identification Weight	0.94188	0.87428	0.89566	0.88898	0.83914
F1 measure Weight	0.94469	0.86493	0.91757	0.91049	0.84355

Method\Receiver Number	RX4A	RX4B	RX5A	RX5B	Average
Equal weight	0.61539	0.78758	0.63995	0.67174	0.72857
Identification Weight	0.765	0.91637	0.79011	0.82953	0.86011
F1 measure Weight	0.81496	0.93373	0.83674	0.82017	0.87632

資料來源：作者研究整理。

表 6 接收端對不同射頻指紋特徵辨識之參數設定 (Rician)

參數	數值	
訓練接收端	RX2 portB (Rician)	
指紋特徵	SCFO、LCFO、載波頻率偏移、RCFO、SFO1、SFO2、Average Frequency EVM (af EVM)、PSD、Frequency EVM (f EVM)	
網卡數 (個)	15	
滑動窗口大小	40	
每次窗口滑動數	20	
單一類別訓練集數量 (筆)	349 (7,000 個封包資料)	PSD、f EVM : 7,000 (7,000 個封包資料)
總共訓練集數量 (筆)	5,235	PSD、f EVM : 105,000
各個接收端測試集數量 (筆)	7,485 (10,000 個封包資料)	PSD、f EVM : 10,000 (10,000 個封包資料)

資料來源：作者研究整理。

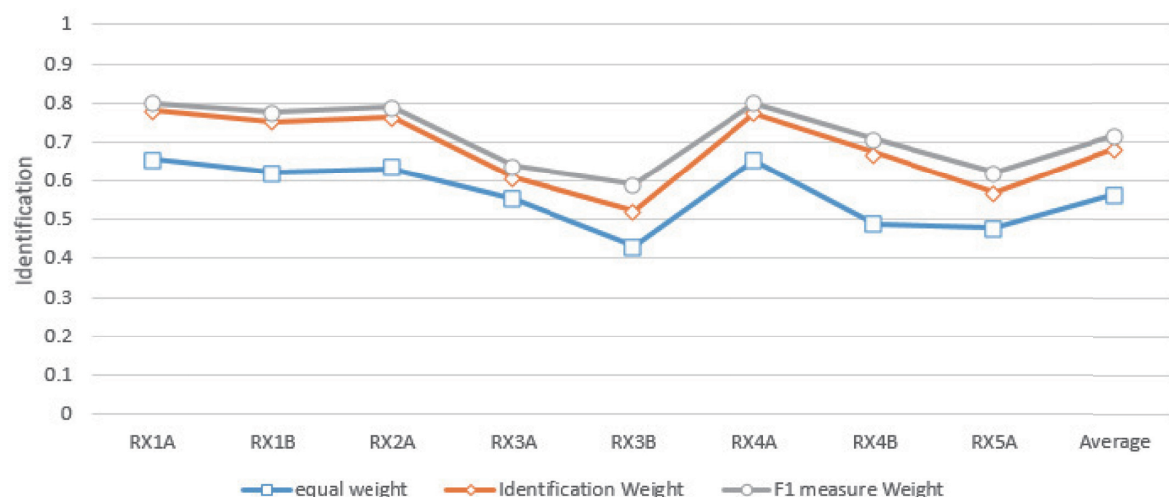


圖 41 特徵校正後之加權辨識率 (Rician)

資料來源：作者研究整理。

表 7 特徵校正後之加權辨識率詳細數據 (Rician)

Method\Receiver Number	RX1A	RX1B	RX2A	RX3A	RX3B
Equal weight	0.65678	0.622712	0.632599	0.553908	0.430327
Identification Weight	0.781697	0.752973	0.764729	0.607348	0.523313
F1 measure Weight	0.798397	0.776353	0.788377	0.637408	0.590782
Method\Receiver Number	RX4A	RX4B	RX5A	Average	
Equal weight	0.654242	0.488844	0.478424	0.564729	
Identification Weight	0.773681	0.671743	0.570474	0.680745	
F1 measure Weight	0.798798	0.70648	0.622979	0.714947	

資料來源：作者研究整理。

伍、5G 專網之應用與剖析

一、5G 物聯專網系統運用於國防之構想

在「5G 無線通信」是國家數位化戰略先驅的思維下，規劃結合雲端運算、大數據、物聯網及人工智慧等技術深度融合，並參考 3GPP 5G 規範 R15 版本，規劃發展可以滿足部分 5G 標準的「類 5G 無線通信系統」，並整合「物聯網感測網路系統」以形成異質網路系統，俾人與人、人與武器，及各武器系統間，得以讓彼此資訊相互感知，成為未來國軍數位化戰場轉型的關鍵基礎設施，提供未來國軍「智慧國防」與「軍用物聯網」能量奠基（如圖 42），發揮「保障態勢準確感知」、「後勤物資精確配送」、「武器裝備自主智能」及「指揮控制高效精準」等四項國防戰備效益。

二、5G 物聯專網系統運用於國防之技術

（一）AR／VR

1. eMBB 使得 AR 和 VR 實現，不再遙不可及，AR／VR 可以運用到人機操作訓練，搭配語音、視覺和觸摸等多種對話模式，提升人員訓練成效。
2. VR／AR 需要大量的資料傳輸、儲存和計算功能，這些數據和計算密集型任務如果轉移到雲端，就能利用雲端服務器的資料儲存和高速計算能力，來提高即時分析決策的效能。
3. 學員配掛可穿戴設備，透過人工智慧可針對每個學生的特點為其定製合適的學習安排課程。
4. AR／VR 提供國防預期效益（如圖 43～44）：（1）樽節訓練成本：VR／AR 訓練一個戰鬥機飛行員，僅需駕駛艙模擬設備，不必擔心飛機耗損與人員傷亡之問題；（2）提升訓練頻率：VR／AR 訓練不受天候影響，多位士兵可同時進行同一任務訓練，不互相影響；（3）適應戰爭環境：VR／AR 系統可模擬多樣戰爭環境，



圖 42 各作戰武器間彼此資訊相互感知

資料來源：作者自行整理。

以及各種突發狀況，讓受訓者鍛鍊並提高反應能力和心理承受能力；（4）啟發作戰思維：虛擬軍事演習可以較小的代價、較短的時間實施大規模戰略級演習，通過多次演習，可發現更多解決問題之方案。



圖 43 韓軍利用 VR 模擬射擊練習

資料來源：VR 界的搬磚小哥（2017）。

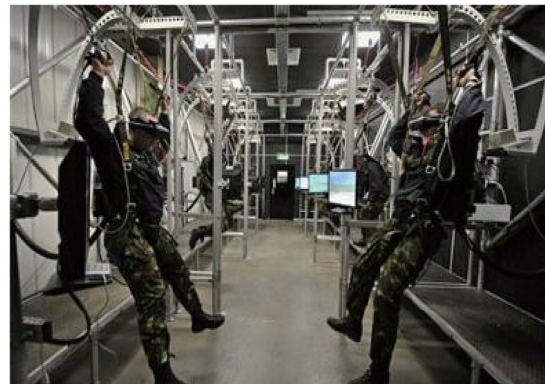


圖 44 美軍利用 VR 進行空降模擬訓練

資料來源：VR 界的搬磚小哥（2017）。

（二）數位戰士（如圖 45）

1. 數位戰士所配備之個人智慧型終端可透過 5G 自主專網，鏈結雲端伺服器，隨時可查看地圖、傳遞作戰命令及戰地情報，並能讀取 UAV 無人偵察機之即時偵蒐影像，供單兵運用。

2. 採用穿戴式生理監測裝置結合智慧醫療，透過 AI 模型對戰士進行生理分析，醫療中心可即時監控戰士生理狀況，進行健康管理。

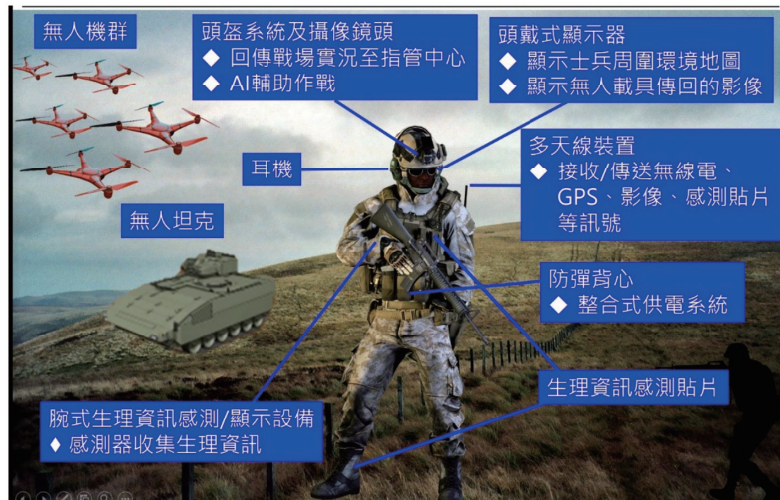


圖 45 數位戰士運用示意

資料來源：作者自行整理。

陸、結論

「5G 無線通信」是國家數位化戰略先驅，本案將結合雲端運算、大數據、物聯網及人工智慧等技術深度融合，期能建構出國軍專屬 5G 專網無線網路，俾人與人、人與武器、及各武器系統間，得以讓彼此資訊相互感知，將成為國軍數位化戰場轉型的關鍵基礎設施；另指紋特徵分別會受到不同接收端之影響，因此本研究期望利用資料校正的方法與特徵加權方法，對較不受影響的特徵給予高權重，希望進行轉移接收端時可以提升網卡分類的辨識率。

從分類結果可以發現，以相同方法進行 AWGN 與 Rician 通道辨識，在相同的接收端下其辨識率有些下降，說明了通道也會對此轉移接收端辨識方法產生負面影響，但是如果觀察在 AWGN 通道利用頻域特徵的辨識率可以發現資料校正可以改善其分類結果，不管是等權、平均辨識率或 F1 measure 加權皆有所提升，並且相比於等權方法，加權後辨識率也會有所提升，最終平均辨識率可以到達 87.6%。

本文從 Wi-Fi 無線設備發送的波形在通訊的實體層中皆帶有唯一的「射頻指紋」特徵切入，其能夠識別用戶裝置並對授權用戶進行分類，來探討如何減少接收端設備對發射端之射頻指紋特徵之影響，提出了接收端的平均值平移校正法、平均辨識率加權法之研究，以提升射頻指紋特徵之辨識能力，希望可推廣到 5G 複雜的電磁環境，預期若能導入 5G 無線射頻指紋辨識技術，將可對這些 5G 設備有效降低設備間自我干擾現象。

最後感謝資訊工業策進會在計畫「無線射頻資安晶片加速偵防應用」的支持。

參考文獻

- VR 界的搬磚小哥，2017 年 5 月 9 日，〈虛擬現實 VR 技術被用來訓練軍隊〉，《每日頭條》，<https://kknews.cc/tech/y6qbpjn.html>（瀏覽日期：2020 年 5 月 15 日）。
- 吳伯軒，2014 年 4 月 10 日，〈三大需求引領 5G 網路新標準，物聯網應用是最大亮點〉，《Digitimes》，https://www.digitimes.com.tw/tech/rpt/rpt_show.asp?v=20140410-142（瀏覽日期：2020 年 5 月 15 日）。
- Baldini G., and Steri G., 2017, “A Survey of Techniques for the Identification of Mobile Phones Using the Physical Fingerprints of the Built-In Components,” *IEEE Communications Surveys & Tutorials*, 19(3), 1761-1789. doi:10.1109/COMST.2017.2694487
- Baldini G., Giuliani R., Gentile C., and Steri G., 2018, “Measures to Address the Lack of Portability of the RF Fingerprints for Radiometric Identification,” in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France: IEEE, 1-5. doi:10.1109/NTMS.2018.8328703
- Ettus Research, 2016, “About USRP Bandwidths and Sampling Rates,” https://kb.ettus.com/About_USRP_Bandwidths_and_Sampling_Rates (accessed August 15, 2020).
- Huang-Fu C. C., and Lin A., 2019/12/26, “Tech Talks: Evolving Wireless Connectivity in the Age of IoT & 5G,” *ADVANTECH*, https://advcloudfiles.advantech.com/events/assets/21f83a87-a848-440c-ba79-f79eb3eaaab0/agenda-slides/08_Tech-Talks_Evolving-Wireless-Connectivity-in-the-Age-of-IoT--5G_JJ.pdf (accessed August 15, 2020).
- IEEE, 1999, *IEEE Standard for Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band*, New York, NY: IEEE. doi:10.1109/IEEESTD.1999.90606
- Keysight Technologies, n.d., “Concepts of Orthogonal Frequency Division Multiplexing (OFDM) and 802.11 WLAN,” https://rfmw.em.keysight.com/wireless/helpfiles/89600b/webhelp/subsystems/wlan-ofdm/content/ofdm_basicprinciplesoverview.htm (accessed August 15, 2020).
- Lu D., 2018/04/12, “IEEE 802.11 PHY and OFDM(4)—Synchronization,” *David's Notes*, <https://yungshengl.github.io/2018/04/12/WCSNotes3-4/> (accessed August 15, 2020).
- MathWorks, 2020, “Joint Sampling Clock and Carrier Frequency Offset Tracking,” <https://ww2.mathworks.cn/help/wlan/examples/joint-sampling-rate-and-carrier-frequency-offset-tracking.html#d120e6313> (accessed August 15, 2020).
- Merchant K., and Noursain B., 2019a, “Enhanced RF Fingerprinting for IoT Devices with Recurrent Neural Networks,” in *MILCOM 2019–2019 IEEE Military Communications Conference (MILCOM)*, Norfolk, VA: IEEE, 590-597. doi:10.1109/MILCOM47813.2019.9021080
- Merchant K., and Noursain B., 2019b, “Toward Receiver-Agnostic RF Fingerprint Verification,” paper presented at *2019 IEEE Globecom Workshops (GC Wkshps)*, Waikoloa, HI. doi:10.1109/

GCWkshps45667.2019.9024574

- O'Shea T. J., Corgan J., and Clancy T. C., 2016, "Convolutional Radio Modulation Recognition Networks," in C. Jayne and L. Iliadis (Eds.), *EANN 2016: Engineering Applications of Neural Networks*, Cham, Germany: Springer. pp. 213-226. doi:10.1007/978-3-319-44188-7_16
- Peng L., Hu A., Zhang J., Jiang Y., Yu J., and Yan Y., 2018, "Design of a Hybrid RF Fingerprint Extraction and Device Classification Scheme," *IEEE Internet of Things Journal*, 6(1), 349-360. doi:10.1109/JIOT.2018.2838071
- Radhakrishnan S. V., Uluagac A. S., and Beyah R., 2015, "GTID: A Technique for Physical Device and Device Type Fingerprinting," *IEEE Transactions on Dependable and Secure Computing*, 12(5), 519-532. doi:10.1109/TDSC.2014.2369033.
- Razavi B., 1997, "Design Considerations for Direct-Conversion Receivers," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 44(6), 428-435. doi:10.1109/82.592569.
- Rehman S. U., Sowerby K. W., Alam S., and Ardekani I., 2014, "Portability of an RF Fingerprint of a Wireless Transmitter," paper presented at *2014 IEEE Conference on Communications and Network Security*, San Francisco, CA. doi:10.1109/CNS.2014.6997481
- Rehman S. U., Sowerby K., and Coghill C., 2012, "Analysis of Receiver front End on the Performance of RF Fingerprinting," paper presented at *the 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sydney, Australia. doi:10.1109/PIMRC.2012.6362777
- Soltanieh N., Norouzi Y., Yang Y., and Karmakar N. C., 2020, "A Review of Radio Frequency Fingerprinting Techniques," *IEEE Journal of Radio Frequency Identification*, 4(3), 222-233. doi:10.1109/JRFID.2020.2968369
- Uluagac A. S., Radhakrishnan S. V., Corbett C., Baca A., and Beyah R., 2013, "A Passive Technique for Fingerprinting Wireless Devices with Wired-side Observations," paper presented at *2013 IEEE Conference on Communications and Network Security (CNS)*, National Harbor, MD. doi:10.1109/CNS.2013.6682720
- Wang W., Sun Z., Piao S., Zhu B., and Ren K., 2016, "Wireless Physical-Layer Identification: Modeling and Validation," *IEEE Transactions on Information Forensics and Security*, 11(9), 2091-2106. doi:10.1109/TIFS.2016.2552146