物聯網和你我的生活

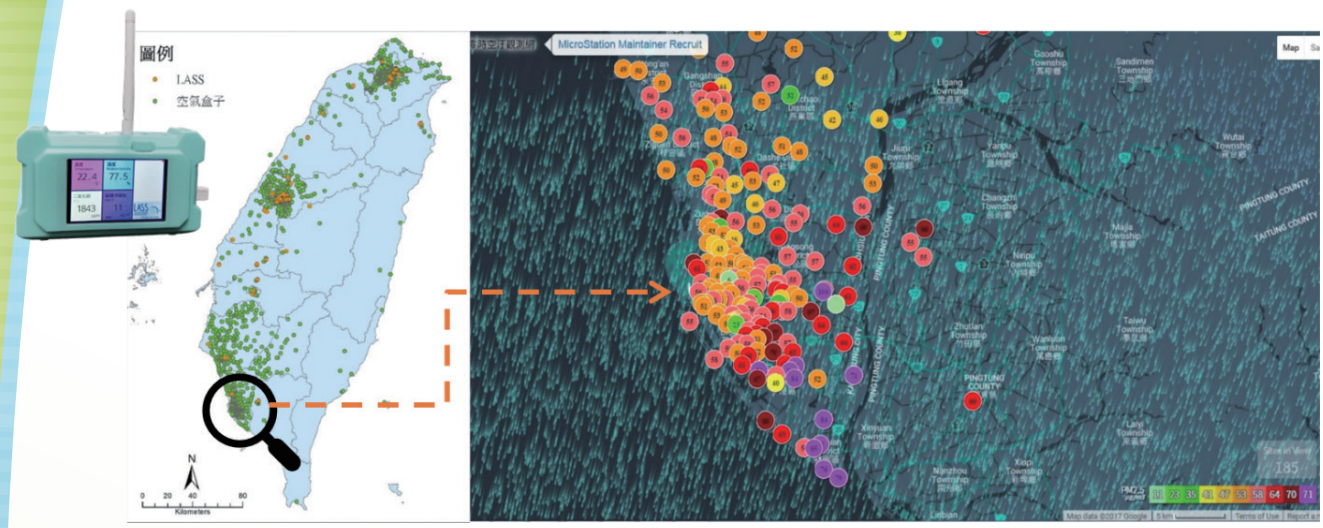
文・圖／廖婉君　林宗男　施吉昇　吳沛遠（臺灣大學電資學院物聯網中心）

物聯網（Internet of Things, IoT），奠基於萬物皆可聯網，舉凡能上網的裝置及應用皆在IoT的範疇之內，如監視器、水電錶、自駕車，甚至連智慧路燈等，這也是為何國際研究暨顧問機構 Gartner預測2020年全球物聯網裝置將達到240億美元如此龐大數字的原因。

物聯網系統有三個主要的元件，剛好就是「物」、「聯」、「網」。「物」是感測器或制動器。感測器的角色是蒐集資料，例如：溫度計、雷達測速器；制動器則是能改變系統狀態的電子裝置，例如冷氣控制器。「聯」是資訊傳遞的網路，透過它可將感測到的資料傳到他處，制動器也能透過它接收到不同的指令。「網」則是決策邏輯的網路，透過從網路蒐集而來的感測資料進行智慧分析而做成決策判斷，再把判斷之後產生的指令送到制動器，這樣才會產生物聯網。凡是能利用這三個元件的應用，都算是物聯網的應用。

以中央研究院聯合多位民間同好所發起的空氣品質監測系統為例，臺灣目前有76個空氣品質的政府測站，約2千個民間測站。政府環保單位的儀器是執法的依據，需要使用高精準度儀器，但費用也高，因此佈點較少。民眾自行安裝的「空氣盒子」，其目的是了解空氣品質的變化，精準度要求較低，費用少，自然數量比較多，可以構成一個空氣品質的資訊網路，不但能提供即時的空氣品質，還能透露污染源來自何處。這一類的物聯網系統著重在資料的收集，而這正是大數據以及機器學習的基本元素。有了散佈全臺灣的微型感測器，專家學者可以據此分析空氣污染的來源，讓空氣污染的罪魁禍首無法遁形。然而，此空氣品質監測目前僅止於搜集資料，發布訊息，但無法啟用制動器，因此改善空氣品質的目標尚難達成，無法發揮物聯網系統的最大功效。

漁產養殖也可以是IoT有效的應用。傳統蝦池在施放飼料的時候，因為無法近距離觀察，沒有辦法掌控蝦子到底吃了多少的飼料，以此常常造成過度投放飼料，不僅提高成本，也影響蝦池的水池，最終影響草蝦的成長。國立中山大學就有AI養殖團隊，將過去傳統的蝦池，變成了AI蝦池，可將蝦子養得又大又肥美。團隊將攝影機放入AI養殖池，



空氣盒子PM2.5感測網（資料來源：g0v零時空汙觀測網）

觀察蝦子的活動力，了解有沒有死蝦的狀況；另外透過水質監測器了解酸鹼度、溶氧量、溫度和鹽度，進而透過AI技術，控制餵餌量。傳統的蝦池育成率大約3到4成，而這樣的AI養殖池，育成率則高達7成。

機器學習與物聯網是相輔相成的。一方面，物聯網所蒐集到的資料，經由機器學習技術加以歸納，從而達成特徵識別與異常檢測，並協助使用者進行決策。舉例而言，工廠在生產過程中蒐集了諸如溫度、壓力、濕度、氣壓等製程量測資料，搭配品管部門的良率檢測結果，可透過機器學習技術，以歸納製程量測資料與良率之關聯性，如此不但可及早發現產品缺陷，以爭取出貨時效並減低成本，且可作為未來製程改良之決策參考。

機器學習技術需要大量資料以歸納出重要特徵與判斷準則。物聯網所持續蒐集之大量資料，配合群眾外包（crowd sourcing）將資料進行標籤化，可作為機器學習技術之養分。然而，物聯網所蒐集之資料可能會因感測器異常而造成資料缺失、資料本身可能是非結構性的、且需將眾多感測器量測資料格式進行整合。另外群眾外包亦可能有標示錯誤的問題。因此，如何經由適當的預前處理，使機器學習技術可有效予以分析，是一個看似無趣卻十分重要的工作。

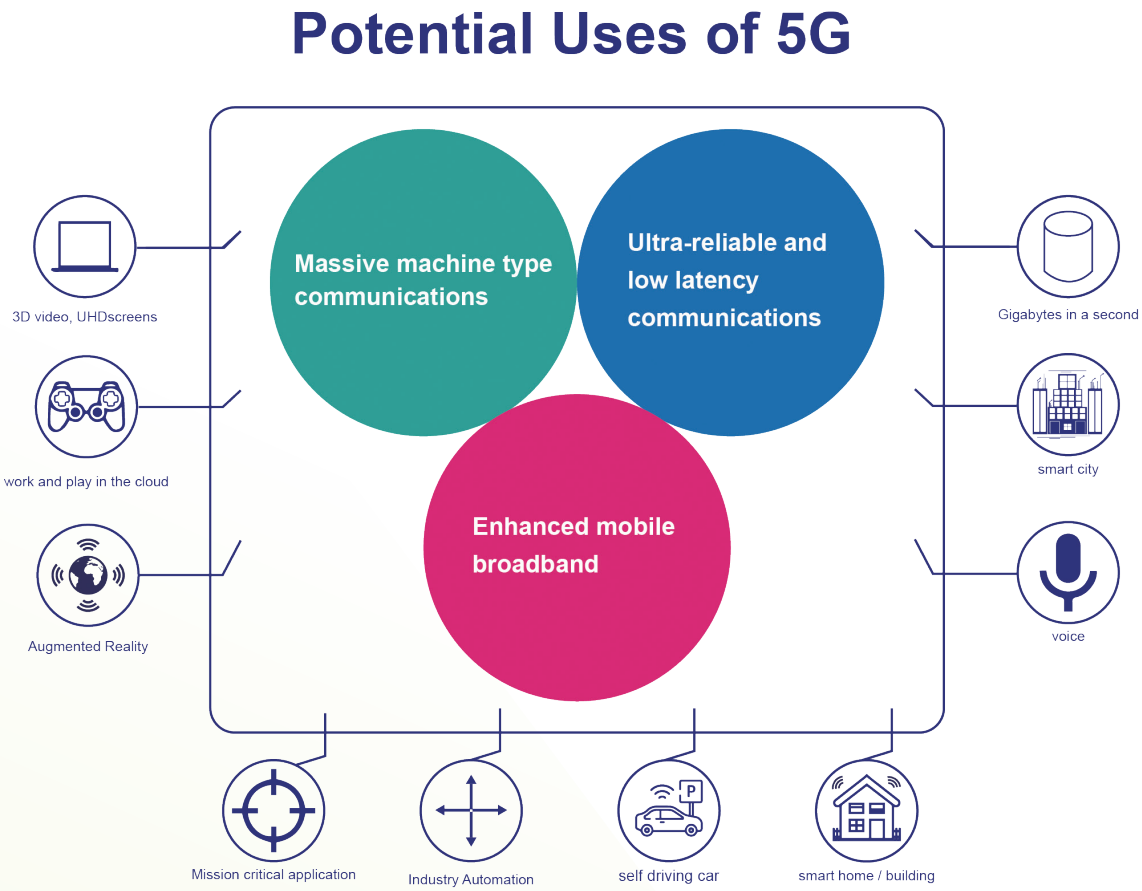
機器學習與物聯網亦應用於野生動物保育。據統計，每年約有27,000頭非洲象遭盜獵，約占非洲象族群的8%。有鑑於巡邏員任一時刻的巡守範圍有限，難以有效遏阻盜獵，南加大的PAWS（野生動物安全保護輔助）團隊，利用巡邏員在巡邏途中，以智慧型手機的Cybertracker App所回報的偵查資料，透過機器學習與賽局理論，預測盜獵可能發生

地點，並考慮當地地形，自動規劃具隨機性之巡邏路線。如此，不但能更有效偵查盜獵，且同時避免巡邏路線為被盜獵者所預測。PAWS團隊所開發之技術已應用於烏干達、馬來西亞等地。其於烏干達進行八個月的測試結果顯示，機器學習技術所預測之盜獵高可能性區域，其實際盜獵活動為低可能性區域之十倍。此外PAWS並與Air Shepherd合作，利用無人機搭載紅外線攝影機，搭配影像辨識技術，協助巡邏員偵測夜間盜獵活動。由此可見機器學習與物聯網的結合，是有無限多的可能性的。

物聯網的感測信號需透過通訊網路技術傳到後伺服器作智慧化判斷。根據不同的物聯網應用需求，傳輸技術有不同選擇。若用於家電或室內應用，常使用的連網技術包含有WiFi、藍芽、ZigBee等短距離無線通訊協定。WiFi傳輸速率高，適合用在傳輸影音，但缺點是耗電量高；而藍芽與ZigBee功耗低，應用在個人裝置。此三者均為短距離傳輸技術，應用範圍被侷限在10~300公尺以內。

若應用在智慧城鄉，包括智慧農業（土壤、農作物監控）、民生公共物聯網（自來水管路、瓦斯、水電錶等）、智慧城市（停車位管理、智慧路燈）、智慧交通（交通流量、交通號誌）、及智慧能源等，則需要長距離傳輸技術。更由於感測器裝置佈署範圍廣，且須避免頻繁更換電池，傳統的短距離無線傳輸不再滿足這些新興應用。取而代之的是低功耗廣域網路（Low Power Wide Area Network, LPWAN），因其傳輸資料量小、長距離傳輸、省電等特性，可大幅降低布建成本，擴展了物聯網應用場景，代表技術有LoRa、Sigfox以及3GPP主導的NB-IoT（Narrow Band IoT）。

正在制定中的5G三大應用場景：增強型行動寬頻通訊（Enhanced Mobile Broadband）、超可靠度和低延遲通訊（Ultra-Reliable and Low Latency Communications, URLLC）與海量機器型通訊（massive Machine Type Communication, mMTC），而實現這些應用場景的關鍵技術有軟體定義網路（Software Defined Network, SDN）與網路切片（Network Slicing）。利用網路切片技術可使營運商不必為了三大應用場景各自準備一份網路資源，讓未來的5G網路能夠更彈性分配資源給不同的應用場景。例如，海量物聯網中大量佈署感測器，這樣的物聯網是密集且靜止的，而另一種以任務關鍵導向的物聯網主要用於無人駕駛、自動工廠、智能電網等，需要的是高可靠與低延遲。兩種截然不同的應用情境經由網路切片技術，讓營運商在5G網路中能夠使用同樣網路資源，加上軟體定義網路使得對於網路規劃能夠有效且簡單的實現。



5G三大應用場景及相關IoT設備

此外，資安問題一直是物聯網的重要議題，物聯網設備往往負責簡單的資訊傳遞且價格低廉，可視為功能較差的電腦，以智慧路燈為例，只要路燈能在設定的時間開關燈，便會被當成正常產品，也就不會有人員遠端存取路燈來檢查，物聯網產品就像是防備措施簡陋又無人看管的電腦，這就是資安危機潛藏所在。

美國電信商Verizon於2017年揭露美國某大學遭到DDoS攻擊，攻擊者竟是校內能聯網的自動販賣機與智慧路燈。DDoS為分散式阻斷式攻擊的縮寫，可用當紅明星開演唱會導致售票網站當機來理解，導致售票網站當機的原因是熱情的歌迷，而導致學校網站當機的原因是數量龐大的物聯網設備。另一個例子是英國知名資安公司Darktrace執行長 Nicole Eagan於2018年揭露美國某賭場由於魚缸溫度監測器被駭客攻破，而溫度監測器又連到賭場內部網路，導致賭客資料外洩，此例子可提醒許多公司即使其內部網路沒有連到外網，也會有資安疑慮。

鑑於資安的考量，最後有幾點建議：首先，現今政府持續推動「數位匯流/IoT資安威脅防禦機制暨資安實驗室」，消費者無法控制物聯網產品的資安防護能力，要求製造商製造符合資安規範之產品需要政策面的協助。另外，消費者應修改物聯網產品的預設密碼，網路上時有所聞網路攝影機被輕易入侵，將個人隱私曝露在入侵者面前，甚至被用來挖礦或成為疆屍網路的一份子，這些往往肇因於使用產品的預設密碼。此外若密碼設定過於簡單，易遭字典攻擊法破解，即使產品提供再好的防護也是枉然，就像沒設定密碼的保險箱，討論其外殼堅固程度是沒有意義的。因此，物聯網應用要普及，良好的資安防護是非常重要的。（本期專題策畫／電機系林清富教授）

廖婉君小檔案

現於臺大電機工程學系擔任教授及臺灣大學電資學院物聯網中心主任。交通大學資訊科學系學士（1990）、資訊科學研究所碩士（1992），美國南加州大學電機通訊博士（1997）。主要研究領域包含：無線多媒體網路、行動邊緣運算暨雲端虛擬化、區塊鏈技術、物聯網。

林宗男小檔案

現任臺大學電機工程學系教授及臺灣大學資訊安全技術中心主任。臺灣大學電機工程學系學士（1989），普林斯頓大學電機工程學系碩（1993）博士（1996）。主要研究領域：深度學習、機器學習、網路資訊安全、資料科學、區塊鏈技術。

施吉昇小檔案

現任臺大資訊工程學系及資訊網路與多媒體研究所教授。伊利諾大學（香檳）電腦科學博士（2003）。主要研究領域：即時系統、排程理論、資源管理、嵌入式系統。

吳沛遠小檔案

現任臺大電機工程學系助理教授。臺大電機工程學系學士（2009）、普林斯頓大學電機工程碩（2012）博士（2015）。主要研究領域：機器學習、主動辨識、估計理論、智慧製造。