

物聯網的便利與危機

■ 趙志宏、劉川綱、李忠憲

物聯網讓生活周遭的物件與設備連結成一個大型的智慧網路，它們的資料提供生活上的便利，卻也可能成為個人隱私外洩的媒介，這些外洩的物件感測資料很可能成為網路犯罪的重要工具。

想像一下這樣的場景：

下午 6 點，下班走到停車場準備開車回家，車子感應到身上的識別物件自動解開中控鎖。坐上駕駛座後，用語音聲控發動引擎並說回家，行車電腦便執行引擎的啟動，導航電腦跟著顯示回家的路徑及交通狀況。中途出現某條道路塞車，導航電腦會重新計算回家路線以避開塞車路段，也顯示有哪些路口的紅綠燈故障，提醒經過時要小心往來車輛與行人。

離家只剩 10 分鐘車程時，家裡的智慧中控電腦與行車電腦互相交換資訊，並經由行車電腦通知目前室內溫度是 30 度，是否需要預先開啟客廳空調，並詢問是否想知道冰箱裡有什麼菜色，中控電腦則可依據冰箱裡的菜色建議晚餐的菜單。

什麼是物聯網

上述的例子主要是透過物聯網系統讓真實世界的物件具備智能與聯網能力，提供更方便與更有效率的居家生活。這一切好像電影情節，但這樣的生活已悄悄在我們的周邊逐漸實現了。

在這一個例子中，我們看見智慧車輛、智慧城市與智慧家庭的互聯，看到人和物件的連結與溝通，也看到了物件和物件的連結與溝通。這就是物聯網的基本概念，透過賦予物件智能與聯網的能力，運用網路的連接甚至雲端運算，建構出更便利的生活方式與環境。

**透過賦予物件智能與聯網的能力，
運用網路的連接甚至雲端運算，可建構更便利的生活方式與環境。**

2005年，國際電信聯盟就發表了一篇國際網路報告，深入探討物聯網與其技術細節，以及對全球商業和個人生活的影響。事實上，物聯網並不是一個獨立的網路，而是一個賦予物件智能與聯網能力，建構出人與物件、物件與物件、物件與人之間的通訊網路。也就是透過物聯網和一般網路的資訊交換與傳遞，讓虛擬世界與實體世界完美地連接。

物聯網已非科幻小說的情節，也非商業騙局。目前已經有許多成熟的關鍵技術及相關技術的應用，也讓人們勾勒出物聯網的發展願景，如智慧生活、智慧醫療、智慧物流、智慧城市，甚至於所謂的智慧國家、智慧地球等概念。

物聯網的應用

近期以來，物聯網一直受到產業界的關注與期待。在資訊盛事「2014台北國際電腦展」中，國內外廠商也把物聯網視為未來資訊技術的重要趨勢，不約而同地爭相預估其相關產值會持續呈爆炸性成長。大量的文章評述也無不吸引著大眾關注這個新興的名詞。

然而，物聯網到底要如何應用在一般大眾的生活中，卻依舊讓一般人感到好奇又陌生。物聯網是各種物件連結而成的網路，這些物件就在我們周遭，如家中的冷氣機、冰箱、電視、電腦、洗衣機、汽車、機車等。

當這些物件有管道與其他物件連結溝通時便形成網路，這個網路若與目前使用的網路連結，世界各地人們周遭的物件便在網路世界連結在一起，形成一個超大型網路。一旦這網路成形，各種智慧科技生活都成為可能，人們可遠端控制各種物件設備，全自動化的生活模式讓世界更便利，這也是物聯網所勾勒的美好前景。



智慧家庭裡，家人可以透過智慧型手機控制電視、電話、電腦、微波爐與戶外監控器。

如何讓這些物件互相連結呢？拜感測與晶片技術進步所賜，只要在各式物件設備上配置小型感測器與控制晶片，就可感知物件周遭的環境資料，再利用互聯網把資料蒐集到處理中心，提供給各種應用領域控制利用。

以一般大眾家中常用的冷氣機為例，若冷氣空調公司在出售的冷氣機上都安裝感測網路裝置，家中冷氣機就可把溫度感測資料與冷氣運作狀態上傳至資料處理中心，公司便可利用這些資料達到以下目標。

首先，維修更便利。當冷氣機把運作資料傳回冷氣空調資料中心時，公司可準確掌握運作狀態，在發生問題的第一時間進行維護排程，顧客不需自己反映故障情形，冷氣機維護會更快速，服務品質更高。其次，冷氣機銷售資料更準確。當冷氣機銷售地點、數量、運作時間都回傳到資料中心時，公司可更準確地掌握客戶的使用習性、銷售熱點及備貨情形，對於冷氣空調產業的幫助不言可喻。

再者，顧客可得到更便利的智慧生活。冷氣空調公司提供顧客一個便利手機 APP 小幫手程式，顧客便可利用手中的智慧型手機控制冷氣機運作，出門不再擔心忘了關，回家前也可先讓它運轉，利用物聯網，有網路的地方就可以監視控制。再其次，空調產業也可與其他領域結合，例如在冷氣機上安裝紅外線或其他監控裝置，顧客便可以順便監控家中的狀況。

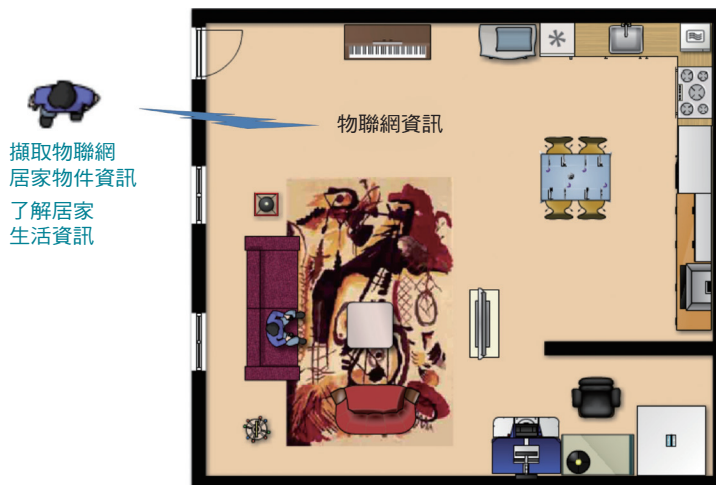
物聯網的安全危機

物聯網讓大眾生活周遭的物件與設備連結成一個大型智慧網路，它們的資料提供生活的便利，卻也可能成為個人隱私外洩的媒介，這些外洩的物件感測資料很可能成為網路犯罪的重要工具。更甚者，還可能損害大眾與國家的安全。試想，假如公路系統的控制資料被外部有心人士盜取，他可以完全控制整體公路系統的交通號誌，屆時如同電影般的國家安全災難就可能發生。

若是一般民眾的家內設備資料，如冷氣、電視、電腦與各式電器的使用紀錄外洩，外人便很輕易地知道哪些戶沒人在家，甚至何時到家。一切生活習性與行為都被他人所知，再無所謂個人隱私與安全可言，物聯網便會成為犯罪的溫床。因此，物聯網推廣運用的最大疑慮就是安全問題。

一般網路上的安全機制大抵以資料本身加密或外加其他安全機制為主，如防火牆、

由於物聯網更貼近我們的日常生活，若只留意其便利性而忽略了安全性，將帶來可怕的災難。



當外部居心不良的人透過網路擷取到居家資料時，民眾的資訊安全將無保障。

系統更新、防毒軟體安裝等。然而，把資料加密的複雜度愈高，需要的技術就愈難，對於小型感測器而言，勢必無法承擔這麼大的加密工作。

若是要外加其他安全機制，到底何種規格的安全等級才能合格？尤其未來物聯網上的物件數量會是現在的百倍，各區域間的安全機制都不相同，安全漏洞將更難以防堵。一旦一個區域被駭客擊潰，就如同一個城池被攻破一隅，整座城池也會不保，這樣的風險確實令大眾難以信服物聯網的安全。因此，在安全的物聯網確實實現時，智慧科技生活的前景才會是美好且真實的。



物聯網的安全由居家到國家甚至到國際層級，層層都需要把關，當其中一層被破壞時，整體的網路安全就會潰堤。

整體來說，物聯網的發展可望達成「一物一智能，萬物為我所用」的目標，進而讓生活與環境更便利。然而，由於物聯網更貼近我們的日常生活，因此不論在私領域或公領域的應用，若只留意其便利性而忽略了安全性，物聯網將帶來可怕的災難。水能載舟亦能覆舟，在發展物聯網技術的同時，其安全性的考量是眾人必須面對且重視的一大課題。

趙志宏

高雄大學圖書資訊館

劉川綱

嘉南藥理大學資訊多媒體應用系

李忠憲

成功大學電機工程學系

