IoT M2M 熱衷「開放、共享、混搭」之餘……

■文：任芷萍

產業多元化發展使物聯網 (IoT) 業者得以擁有盈利空間，不少企業正試圖增加市場覆蓋、以適當方式共同創造並獲取經濟價值。IBM 豪砸逾 300 億美元收購開源先驅 Red Hat 以及電信商轉向網路功能虛擬化 (NFV)，似乎正在為此做出最佳時代註解。大眾熟知的無線局域網 (WLAN) 為搶食 IoT 商機，近幾年亦在連線設定操作與傳輸技術本質做出不少變革；去年夏天新出爐的 IEEE 802.11ax 對此有諸多修正，更適合用於 IoT 部署，Wi-Fi Easy Connect 功能就是一例，可簡化 Wi-Fi 設備與「無顯示器」裝置配對的過程。

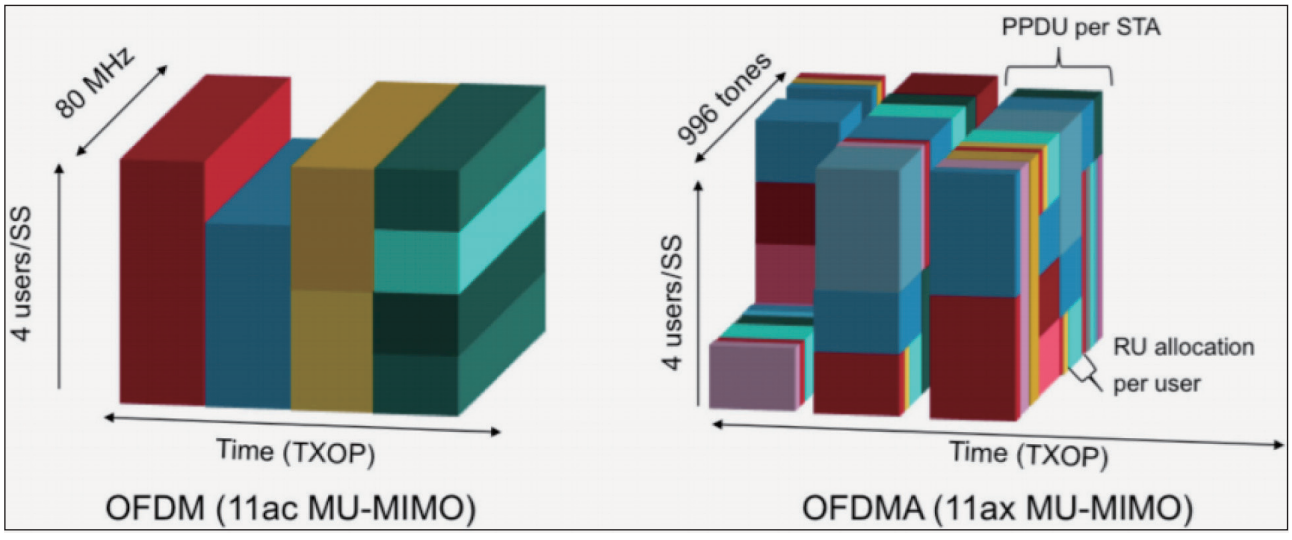
802.11ax、BLE mesh，與 IoT 更親近了！

這是個很實用而親民的舉措，因為很多物聯網裝置並未配備顯示螢幕。從此，用戶可透過類似保護設置 (WPS) 按鈕或從智慧手機掃描設備 QR Code 輕鬆連線。另為解決大量設備連接到現有網路導致壅塞，必須部署更多接入點可能出現干擾、增加分組錯誤率的問題，802.11ax 還具備以下特點，對環境中障礙物的抵抗力或優於 5G 網路：

1. 空間重用：CSMA / CA 具有衝突避免的載波偵聽多路訪問、保守 CCA (清除信道評估) 和高傳輸速率的組合使用允許在某些場景有限的空間重用；
2. 時間效率：CSMA / CA 可縮短節點每次訪問信道的時間；
3. 頻譜共享：引入動態混淆和 MU-OFDMA，改善頻譜佔用分散、相鄰 WLAN 效率低下和干擾；
4. 多個天線：上、下行鏈路皆支援 MU-MIMO (多用戶多輸入多輸出)，允許多個用戶同時下載和上傳數據。

除了廣域網路，歷史悠久的

圖 1：OFDM (11 ac MU-MIMO) vs. OFDMA (11ax MU-MIMO)



資料來源：https://www.cisco.com/c/dam/en/us/products/collateral/wireless/white-paper-c11-740788.pdf

藍牙 (Bluetooth)，因為已從最初單純的點對點傳輸，進化到一對多、多對多連接，亦入列 IoT 無線傳輸主要技術之一，在小範圍的消費電子尤具競爭力；2009 年問世的藍牙低功耗 (BLE)，即是針對小型物聯網應用而來。藉由增加調製指數和限制負載密集型／功耗密集型數據，將功耗降低 95 ～ 99%；訊息加密升級到 128 位元 AES-CCM，是將 BLE 拓樸結構推向低功率節點的先決條件；而藍牙技術聯盟 (SIG) 於 2017 年頒佈網狀網路 (Mesh) 規範後，其「自我修復」特性更成為多對多連接的關鍵轉捩點。

考慮到家電等消費產品更為形色不一、更難達到互操作性，日前藍牙技術聯盟宣佈成立「智慧家庭小組」(Smart Home Subgroup)，旨在為智慧家庭及其相關應用開發更多元的藍牙 mesh 模型規格，以構成網狀網路應用層並定義連接至藍牙 mesh 網狀網路中的裝置行為，促進跨廠牌的互通性。全球已有 60 家以上的企業會員加入新成立的智慧家庭小組，包括：阿里巴巴、GCT 半導體、利爾達科技、聯發科技、美的集團 IoT 公司、Nordic 半導體、Novel Bits、S-Labs、泰凌微電子、新思科技、UL 檢測服務以及小米等。

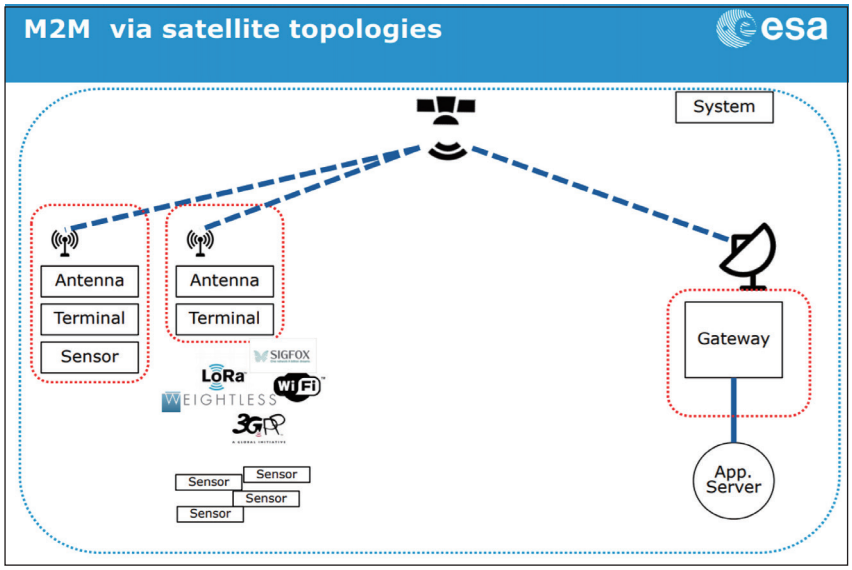
衛星通訊爲 M2M 挹注能量，資訊整合更全面

自推出以來，至少有 105 款由各大晶片、堆疊、零組件和終端產品供應商所推出具備藍牙 mesh 連網的產品已經認證合格。相對的，超遠距、超大頻寬、超廣覆蓋的衛星通訊市場亦值得留意；ResearchAndMarkets 統計，在天氣資訊、科學研究、電信、多媒體通訊、娛樂和導航帶動下，2017 年全球衛星機器對機器通訊 (M2M) 物聯網市場產值為 6.173 億美元，美國因衛星發射次數最多、為服務提供商帶來豐厚營收，市佔最高。預計 2018 ～ 2023 年，衛星 M2M 市場的 CAGR 為 32.58%，成長動能將從北美移至亞太區。

聯網汽車、銀行和零售終端為增長主力。在 L、Ku、Ka 和 S (含 X 和 C 波段) 四大頻段中，L 波段產值最高，未來五年 CAGR 亦最高。與此同時，第三方商業 IoT 平台正快速增長，企業和公共部門是最大客戶。技術研究公司 ReportLinker 將平台服務分為三類：設備管理和控制、應用啓用和網路連接管理平台。伴隨技術進步，多數供應商逐漸轉向水平模組化平台，可集成為一個完整的端到端解決方案，將在商業和工業物聯網 (IIoT) 廣泛應用，包括：醫療保健、汽車、車隊管理和地方政府的智慧城市計畫，市場正逐步從新概念原型轉向「需求實現」階段。

然而，去中心化的 IoT 世界讓資訊整合更趨複雜，促使開發者積極利用開發軟體套件 (SDK) 或應用程式介面 (API) 消弭互操作性隔閡。開放互連基金會 (OCF) 一直在這條路上努力不懈，而他們所發佈的 1.0 規範亦在去年 11 月獲得 ISO / IEC JTC 1 認可，將 OCF 標準列入 ISO / IEC 30118 (第 1-6 部分)。OCF 最新的 2.0 規範更進一步將公鑰基礎結構 (PKI) 和雲端管理功能結合，為生態系統定義一系列安全和原生網路協定；當中兩個開源標準——IoTivity 和 IoTivity Lite，稍

圖 2：衛星通訊 M2M



資料來源：歐洲太空總署 (ESA)：https://docbox.etsi.org/Workshop/2016/201611_M2MIoTWS/00_WORKSHOP/S07_LOWPOWERTECHNO/EuropeanSpaceAgency_Zeppenfeldt.pdf

晚亦將提交 ISO / IEC JTC 1 認證。

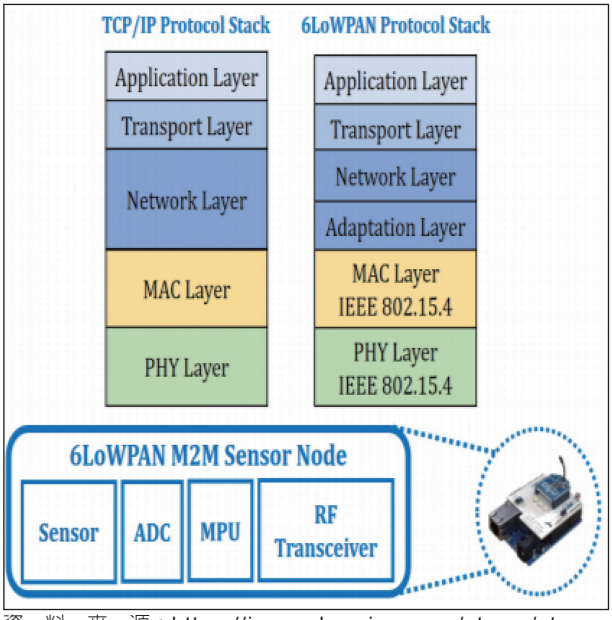
6LoWPAN 不需「轉譯」，就能直通 IP 網路

不過，要讓 M2M 對接互聯網協定 (IP)，對有限的電池容量和低功耗感測器／設備來說仍是一大負荷，因而促成「6LoWPAN」標準的興起——望文生義，它是最新版 IPv6 和低功耗無線個人區域網路 (LoWPAN) 的複合字，以確保 ZigBee(IEEE 804.15.4)、BLE、Z-Wave 等任何低功率無線電可與互聯網通訊。在 6LoWPAN 問世前，這些低功耗感測設備須借助閘道器 (Gateway) 的複雜應用程式「轉譯」、在 IP 堆疊的鏈路和開放系統互連 (OSI) 模型的網路層之間額外添加適配層，才能進行 IP 傳輸、連到雲端平台。

6LoWPAN 將 TCP IP 報頭壓縮成小封包，藉由用戶封包協定 (UDP) 消除感測網路上各種設備之間、IP 報頭中的冗餘或不必要的網路級訊息，借助邊緣路由器的協定堆疊，允許 IEEE 802.15.4 網路發送及接收 IPv6 分組，讓所有智能設備都可直接連接到 IP 網路並透過行動裝置控制。IEEE 802.15.4 承載 2.4GHz 無線電收發器訊息，近似 Wi-Fi 頻段、但傳輸和接收功率只需它的 1% 左右，低功耗感測器通常可訪問少於 1mW 的無線電；且這些通訊協定乃是基於 IP 開放標準堆疊，節點設備之間的無線訊號干擾將大幅減少。

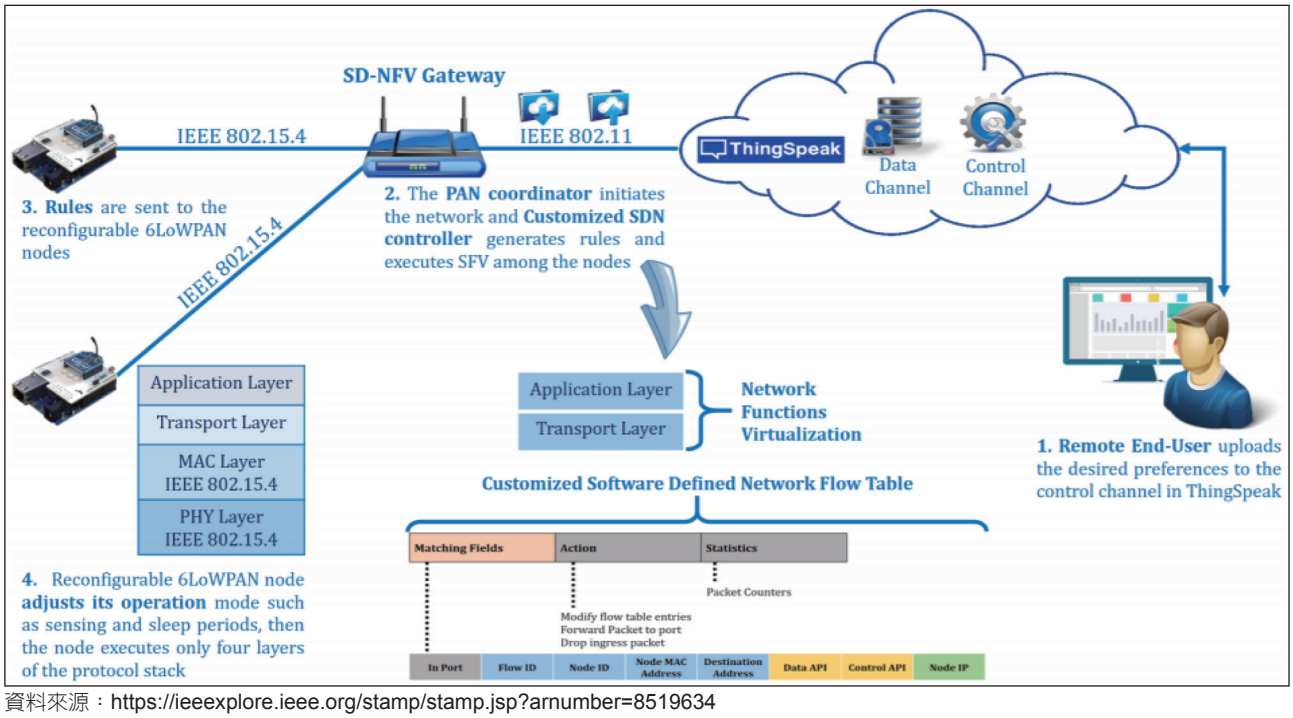
為確保 6LoWPAN 應用程式的安全性，在 TCP 之上運行的傳輸層安全性 (TLS) 亦是基於 UDP

圖 3：理想的 M2M 感測節點架構



資料來源：https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8519634

圖 4：可直接連接雲端之 6LoWPAN 感測器網路的可編程方案



資料來源：https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8519634

協定。然須留意的是，這需要有製作 OSI 模型、調整應用層，以及在網域新增、移除、移動感測器節點的能力奧援，以正確配置並應對後續更新。相中上述需求缺口，有半導體供應商祭出可編程 IPv6 通訊模組和整合平台因應，供開發者選擇 IPv6 韌體堆疊。以往，許多 IoT 解決方案供應商著眼於商業考量，會刻意採取專有的技術架構；但各式底層協定、感測器、設備乃至邊緣／雲端應用的百花齊放，「開放、共享、混搭」已然勢不可擋。

凡聯網必有風險，資安需求有增無減

緊接著，就是資安風險；趨勢科技日前即揭露 MQTT (消息隊列遙測傳輸) 和 CoAP (約束應用協定) 兩個當紅 M2M 協定的設計缺陷和漏洞——短短四個月內就有超過 2 億條 MQTT 和 1,900 萬條 CoAP 訊息經由管理器／伺服器外洩！雖然 MQTT 可一對多通訊並確保服務品質及訊息傳遞、適用於任務關鍵型 (mission critical) 通訊，而 CoAP 是從微型感測器等低功率終端節點收集遙測數據的首選，但實測發現，惡意攻擊者只需使用簡單的「關鍵字搜索」就能獲得想要的生產數據、識別資產／人員／技術等隱私，甚至發動針對性的攻擊行動。

市調公司 Grand View Research 預測到 2025 年，IoT 安全市場規模將達 98.8 億美元，此間年複合成長率為 29.7%。其中，專業服務將保持市場主導地位、達到 21.1 億美元的水準，應用安全類型的成長率最高、達 33.5%。採用雲端儲存機密數據、自帶設備 (BYOD) 正在增加數據安全隱憂。例如，駭客攻擊太陽能電池板系統企圖控制電力供應、入侵企業／居家監控系統窺探隱私或醫療保健裝置竊取敏感數據，或惡意干擾、關閉高速行駛中的智慧車等；企業／組織資料庫若不慎遭駭，更可能因洩密數據而導致重大損失。

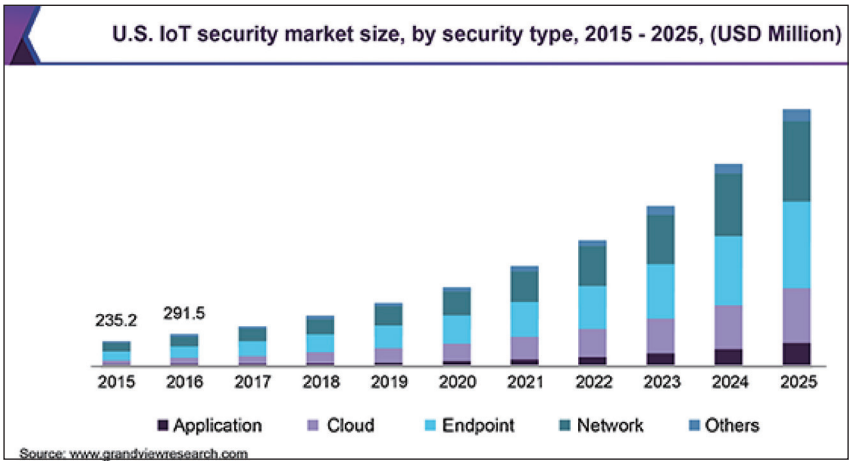
系統整合商建議：

1. 安全設計應追溯至基礎的微控制器 (MCU) 元件設計；
2. 每個開放端口都是潛在的攻擊點，應避免不必要的開啓、或適時主動關閉每個開放端口和可用協定；
3. 設備和雲端平台之間的所有通訊皆須加密，以確保機密性、完整性和真實性；
4. 主動監控設備韌體和雲服務中已知漏洞的依存關係，GitHub 和其他服務提供商可協助完成此過程；
5. 使用網路分段和不可變的基礎架構保護雲端平台，亦便於快速替換可疑伺服器；
6. 啓用或要求多重身份驗證。

善用加密、認證、安全分析防微杜漸

新一代 Wi-Fi 無線網路加密通訊協定 WPA3 亦為以前開放、未加密的 Wi-Fi 網路賦予更高的安全性，讓使用者獲得高級加密標準 (AES) 好處並實施「同步身份驗證」(SAE)。Wi-Fi 聯盟於去年 6 月推出 WPA3-Personal 認證計劃，提供更為個性化的加密，即使用戶擁有 Wi-Fi 密碼並已成功連接，網域用戶仍無法窺探另一 WPA3-Personal 流量；且具流量前向保密特性，無法解密破解前所捕獲的任何數據；而 WPA3-Enterprise 版本亦提升了傳輸敏感

圖 5：防止源於應用、雲端、終端、網路等詐欺和破壞之高漲需求，為 IoT 資安市場注入動力



資料來源：https://www.grandviewresearch.com/industry-analysis/internet-of-things-iot-security-market

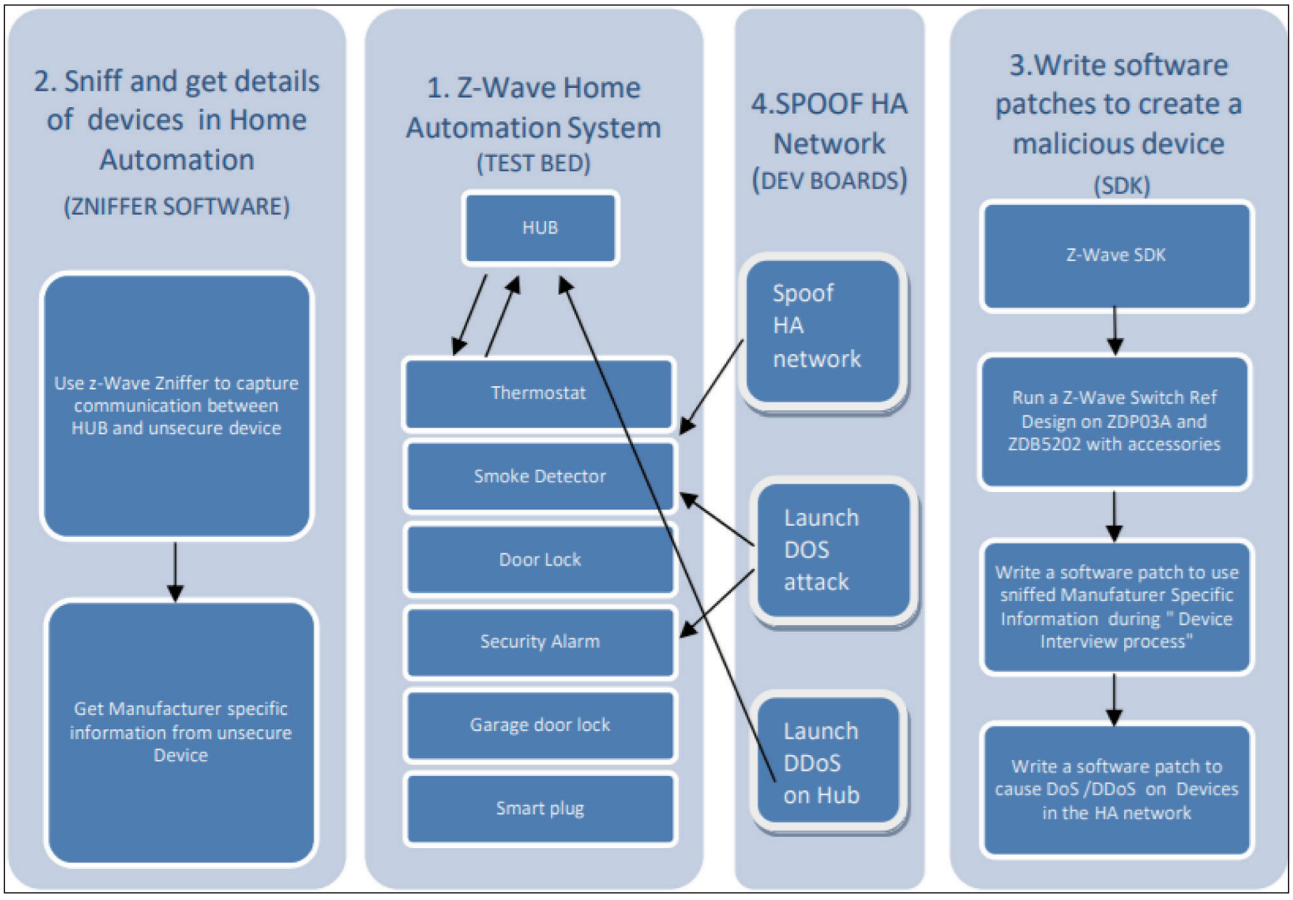
數據的網路加密強度，添加 192 位元的安全加密選項。

另 Wi-Fi Enhanced Open (增強型開放) 可選功能，則允許在開放式 Wi-Fi 熱點網路進行無縫加密——「機會無線加密」(OWE)，在接入點和單一用戶端之間進行唯一加密，以防止用戶窺探彼此的網路流量或執行其他攻擊。然須留意的是，Wi-Fi Enhanced Open 並不像 WPA3 網路經過身份驗證，仍有一定風險存在。惡名昭彰的「未來」(Mirai) 殭屍網路，即是利用互聯網傳播惡意軟體，早在 2011 年就曾傳出發生公用事業系統攻擊。2016 年 9 月，更爆發首起由 Mirai 殭屍網路引發的大規模物聯網攻擊，僅短短兩個月就感染超過 60 萬台 IoT 設備。

複製模組藉掃描整個互聯網查找易受攻擊的設備，多從互聯網路由器或聯網攝影機下手，發動「分佈式拒絕服務」(DDoS) 攻擊。2018 年，駭客矛頭則轉向 Z-Wave 無線協定，多達 1 億個智能家居設備存在漏洞。看似無害的智能揚聲器，就是絕佳駭客入口；有人預估 2021 年，此類網路犯罪成本可能高於 6 兆美元。語音駭客只需一個語音樣本回放，就能以假亂真、偽裝成設備所有者發號施令。更麻煩的是，智能語音助理能聽到人耳無法感知的白噪聲中所隱藏的聲音命令，駭客可在後台執行訂購或竊聽。

IoT 還有一個資安挑戰是：沒有製造標準，這反讓 IoT 設備成了駭客眼中的軟肋。有鑑於特定攻擊未必能被傳統防火牆識別，技術專家提醒：善用加密、認證、安全分析來防範，有助於增加機器學習 (Machine Learning)、大數據 (Big Data) 和人工智慧 (AI) 的複雜性，協助異常檢測和建模。此外，API 安全性對於保護數據完整性非常重要，以確保只有被授權的開發人員／應用程序可與 API 通訊。 CTA

圖 6：以 DDoS 攻擊 Z-Wave 家庭自動化系統



資料來源：http://www.hostsymposium.org/host2017/hwdemo/HOST_2017_hwdemo_14.pdf