IEEE 802.15.3 簡介

交通大學資訊工程所　王友群 著

Section 1 前言

隨著無線通訊技術的蓬勃發展，無線網路的使用逐漸深植在我們的日常生活中，從居家環境、辦公場所、乃至於戶外移動時對數據/多媒體資訊的傳輸需求；也因此，針對多樣化的網路環境與使用者需求，IEEE(Institute of Electrical and Electronic Engineers，電氣和電子工程師協會)組織分別制定了 802.16、802.11、以及 802.15 系列的通訊標準(Standard)以應映都會型的長距離無線網路(Wireless Metropolitan Area Network，簡稱WMAN)、區域間的中距離無線網路(Wireless Local Area Network，簡稱WLAN)、以及個人化的短距離無線網路(Wireless Personal Area Network，簡稱WPAN)，如圖 6.1所示。

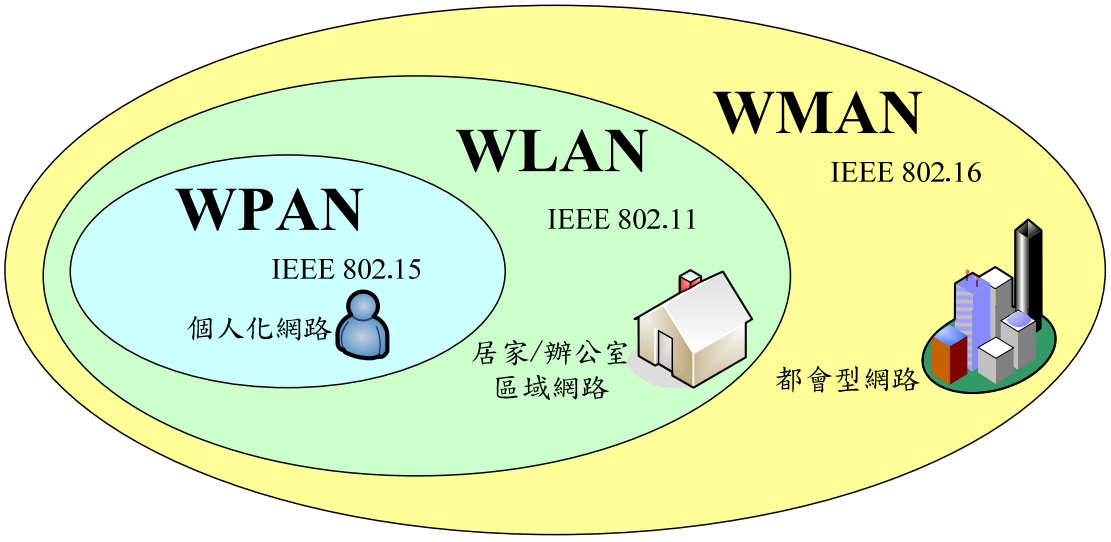


圖 6.1: 無線網路的層級架構示意圖

其中，針對 WPAN 所提出的 IEEE 802.15 系列又再根據使用者省電、高/低速傳輸與多媒體週邊應用上的需求而細分成四個通訊標準：

- IEEE 802.15.1：針對藍芽(Bluetooth)無線技術所提出的通訊標準。
- IEEE 802.15.2：主要討論 802.15 系列與其他無線通訊標準在 2.4GHz 公用頻帶上共存與互通性的議題。
- IEEE 802.15.3：又稱為 WiMedia，主要針對短距離、寬頻高速的要求所提出的無線通訊標準。
- IEEE 802.15.4：又稱為 ZigBee，主要著重在短距離、低功率(低速)的特性所提出的無線通訊標準。

在這個章節當中，我們將針對IEEE 802.15.3[1]這項通訊標準做一個整體性的介紹，在 6.2 節中，我們會先介紹這項通訊標準的著重目標以及發展狀況，6.3 節則是以網路的架構來探討 802.15.3 協定的運作，6.4 節將介紹 802.15.3 封包(Packet)傳輸的格式，最後，在 6.5 節中，我們將針對 802.15.3 的安全機制做一個深入的探討。

Section 2 IEEE 802.15.3 的初步認識

Section 2.1 應用與著重目標

WPAN 主要是界定個人範圍內的小型網路，其網路規模一般是定義在 10 到 100 公尺以內，而網路中的裝置可以是隨身攜帶、穿戴式、或是鄰近身體等具通訊能力的電子產品，例如：手提式電腦(Notebook)、個人數位助理(PDA)、數位式攝影機(DV)、藍芽耳機、手機、以及個人電腦等。而 IEEE 802.15.3 通訊標準則是針對這些裝置在短距離的範圍內提供高速寬頻的無線傳輸服務，其定位的應用主要包含兩個層面：

(1) 提供個人網路的多媒體傳輸服務，諸如聲音以及影片的串流(Stream)傳輸。
(2) 提供消費性多媒體裝置(Consumer multimedia devices)的無線傳輸服務，以取代傳統需透過有線(Cable)的方式在裝置間傳輸大量資料。

雖然 IEEE 802.11 也能提供裝置間的無線傳輸，然而其提供的傳輸速率無法滿足裝置間所傳送的大量資料，另外，由於 IEEE 802.11 的傳輸範圍較大，在 WPAN 的短距離範圍內所造成的干擾也相對增大，因此 IEEE 802.15.3 即為解決此問題而被提出。此外，為了滿足 WPAN 的網路特性，IEEE 802.15.3 制定了以下需求：

- **高速率的傳輸**：至少要能提供 110 與 200Mb/s 的傳輸速度。
- **服務品質**(Quality of service，即 QoS)：由於 IEEE 802.15.3 是著重在多媒體的傳輸，因此必需考量即時性網路流(Real-time flow)的延遲(delay)問題。
- **低電源消耗**：在 WPAN 網路下的裝置多半是利用電池來提供電源，因此需要考量省電的議題。
- **低成本**：如此才能廣泛應用在消費性多媒體裝置。
- **快速組態**(Fast configuration)與**隨意網路拓樸**(Ad-hoc topology)：由於 IEEE 802.15.3 是著重在 WPAN 內裝置間的資料傳輸，因此簡化繁複的網路設定並提供隨意的網路拓樸也是該通訊標準所著重的目標之一。
- **安全性考量**：由於無線訊號是透過空氣傳遞，導致網路的傳輸內容容易被他人所截取，因此 IEEE 802.15.3 也提供了一套安全機制以防止資料外洩。

Section 2.2 IEEE 802.15.3 參考模型

圖 6.2顯示出IEEE 802.15.3 的參考模型(Reference model)，也就是一般所稱呼的網路協定堆疊(Protocol stack)。類似其他IEEE 802 無線系列的通訊標準，IEEE 802.15.3 也只有定義實體層(Physical layer)與媒體存取層(MAC layer)的架構，至於和網路層(Network layer)協定的溝通則必需透過聚合子層(Frame convergence sublayer，簡稱為FCSL)的協定。為了能和一般通用的TCP/IP協定作溝通(即網路層的協定是使用Internet protocol)，802.2 FCSL為基本必需的FCSL協定；至於其他可選擇(Optional)的FCSL協定則包括有IEEE 1934 FCSL以及USB(Universal serial bus) FCSL，如此一來，此裝置將能實作Wireless FireWire或是Wireless USB的功能。

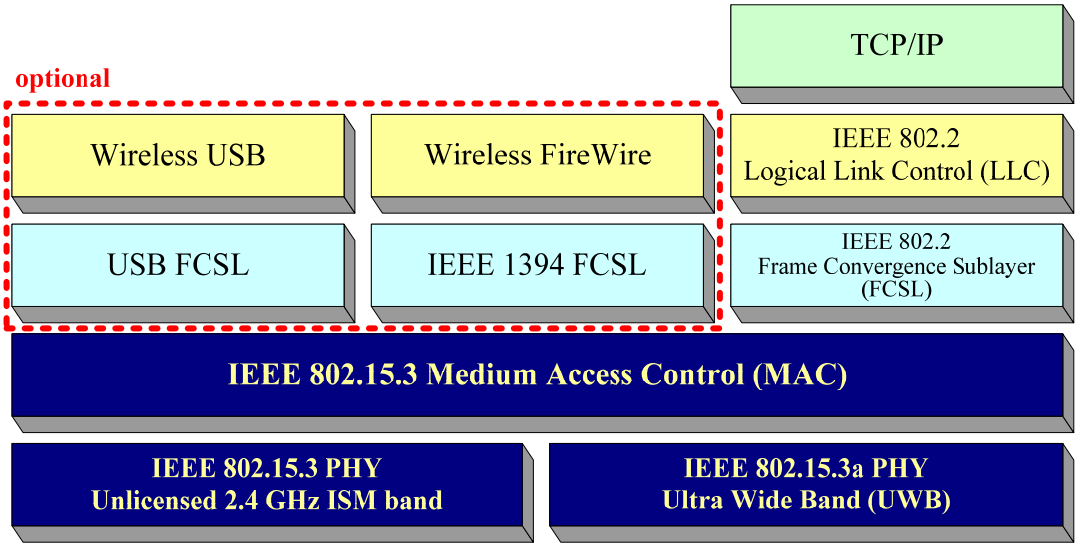


圖 6.2: IEEE 802.15.3 的參考模型

Section 2.3 標準演進與發展狀況

在圖 6.2的參考模型中，我們可以發現到實體層的部份包含兩個部份：IEEE 802.15.3 PHY(運作在 2.4GHz的公用頻帶上)以及IEEE 802.15.3a PHY(採用UWB的通訊技術)，這和IEEE 802.15.3 對高速寬頻的需求有關。仔細來講，原先IEEE 802.15.3 的標準制定是開始於 1999 年 11 月份，而到 2003 年六月份則正式公開此通訊標準，而這份標準就是我們所提到的IEEE 802.15.3 標準；然而，在這項通訊標準制定的時候，原先是考量使用 2.4GHz這段全球公認的免註冊(Unlicensed)頻帶(以美國為例，這段頻帶位於 2.4~2.4835GHz，總長為 83.5MHz)，如圖 6.3所示；而在這段頻帶上共分成 5 個頻道(Channel)，每個Channel的長度為 15MHz，其中第 1、3、5 個Channels和IEEE 802.11b 共用，而使用者可以選擇使用High-density mode(即採用Channels 1、2、4、5)或是 802.11b co-existence mode(即採用Channels 1、3、5)；雖然這段頻帶是全球公認的免註冊頻帶，但基於目前編碼(Coding)的技術僅能提供 11、22、33、44、以及 55Mb/s的傳輸速率，而這很顯然無法滿足IEEE 802.15.3 制定的高速寬頻之目標。

也因此，為了提升傳輸速率，IEEE 802.15.3 將目光轉向 UWB(Ultra wide band)這項通訊技術，並於 2002 年 12 月開始著手制定 IEEE 802.15.3a 通訊標準，在這項新標準中，媒體存取層的部份大致上仍遵循原先 IEEE 802.15.3 通訊標準所規範的原則，至於在實體層的部份則是著重在如何使用 UWB 來提升傳輸速率(至少要能提升到 110 以及 200Mb/s)。然而，由於 UWB 是運作在 3.1~10.6GHz 的頻帶上，並非全球公認的免註冊頻帶，因此需要各國在頻帶管理上作協調，另外，由於制定通訊標準的工作小組(Task group)意見上的分歧，使得原先預計在 2004 年完成的 IEEE 802.15.3a 通訊標準一再受到延遲。

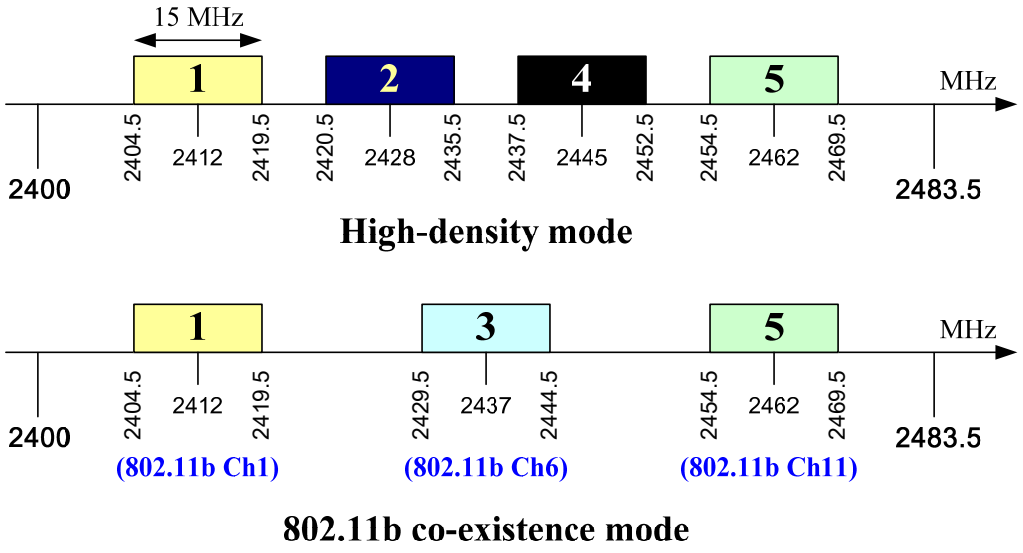


圖 6.3: IEEE 802.15.3 使用在 2.4 GHz 頻帶之 Channels

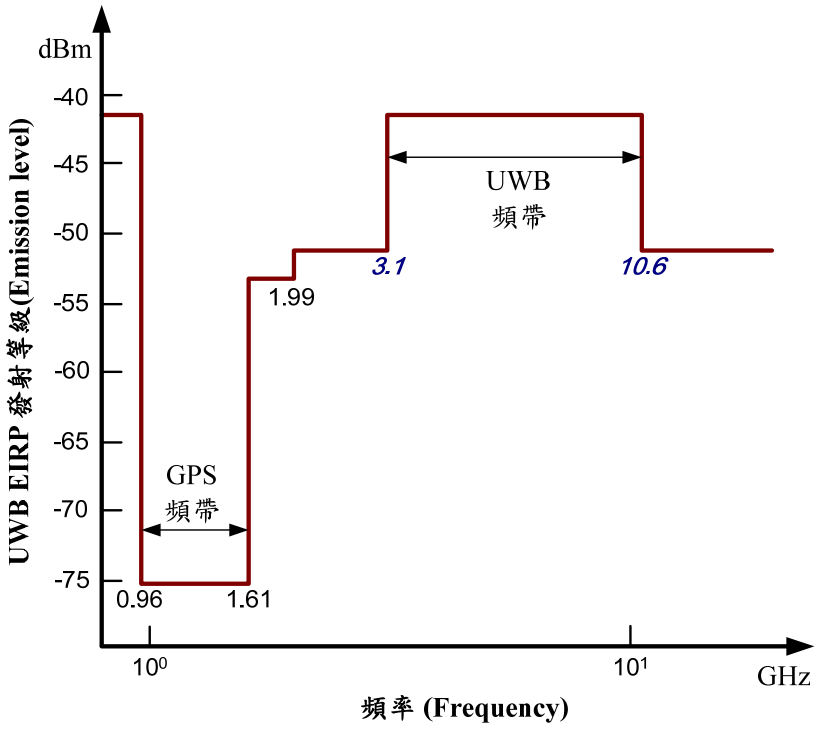
有鑑於UWB技術具備發展潛力，許多業者因此組成非官方的特殊聯盟團體以加速UWB應用的普及化，目前主要是以WiMedia-MBOA[4]和UWB Forum[5]兩大團體為主要陣營。WiMedia-MBOA聯盟的成員包括有HP、Intel、Microsoft、Nokia、TI、Panasonic、Philips、SONY等廠商，在技術方面，WiMedia-MBOA於實體層的技術是採用MB-OFDM (Multi-band orthogonal frequency division multiplexing)的方式，也就是採取多頻帶的方式，將現有的頻譜切割成 14 個 528MHz頻道，以避免干擾較大的頻段，這樣不但可以使既有不同頻段之無線傳輸技術得以並存，同時又可以因應不同國家對頻段的控管，因此擴展性較佳。另一方面，UWB Forum主要參與業者包括有Freescale、Motorola、SONY等廠商。在技術方面，UWB Forum於實體層的技術則是採取原先使用在手機與個人通訊系統產品上的DS-CDMA(Direct sequence code division multiple access)方式，也就是多用戶共享既有頻譜的整體頻寬，DS-CDMA主要的優勢在於利用最大頻寬形成的極短脈衝，可以使各裝置清楚偵測出其他裝置的所在位置，因此能夠大幅提升連接效率和服務品質，此外，DS-CDMA在整個頻段使用一致性的處理技術，因此能夠充份降低對其他無線網路技術的干擾。然而，WiMedia-MBOA和UWB Forum兩大聯盟在IEEE 802.15.3a標準的設計上並沒有太大的共識，所以造成該通訊標準一直無法定案。

另一方面，IEEE 802.15 WPAN Task Group 3b (TG3b)[6]也於 2005 年推出IEEE 802.15.3b-2005 的修定標準[7]，此標準為針對 2003 年所制定的IEEE 802.15.3[1]標準之MAC層所提出的修定版本(Amendment)，該標準的提出主要是要改善現有MAC層的實作(Implementation)以及跨廠商硬體溝通(Interoperability) 方面的問題；而本章節的敘述則是以 2003 年所制定的標準為主，並以IEEE 802.15.3b-2005 的修定內容作為輔助。

Section 2.4 UWB 的介紹

UWB嚴格來講並不是指通訊上的特定技術或是協定，根據美國聯邦電信委員會(Federal communications commission，簡稱FCC[2])對UWB的定義來看，UWB是指在3.1~10.6GHz頻帶下佔有超過 500MHz頻寬的「任意」訊號(Signal)，而且這個訊號必需要能達到圖 6.4所顯示的頻譜遮罩(Spectral mask)規範；換句話說，不管你是採用哪種技術來產生訊號，例如：脈衝無線電(Impulse radio)或是高速展頻技術(High-speed spread-spectrum)，只要所產生的訊號能夠達到上述FCC所定義的要求，都能稱做UWB訊號。此外，相對於IEEE 802.15.3 原先的通訊標準(運作在 2.4GHz頻帶上)，每個Channel僅佔 15MHz的窄頻(Narrow band)而言，500MHz的Channel寬度可以說是非常的寬敞，這也就是為何符合上述FCC所規範的訊號會被稱做UWB訊號的緣故。

以美國的情況而言，FCC 將 3.1~10.6GHz 這段長達 7,500MHz 的頻帶開放給 UWB 裝置使用，而且這段頻帶是毋需註冊的；然而，在其他國家諸如台灣、歐洲等國，3.1~10.6GHz 這段頻帶並未開放作為免註冊的區段，因此 UWB 裝置是否能運作在這些頻帶上還需其他各國的協調；此外，由於 UWB 訊號會佔據至少 500MHz 寬度的頻帶，因此對其他的通訊系統(亦作用在 3.1~10.6GHz 或鄰近區段者)會造成不小的干擾，因此如何和其他通訊系統協調還需進一步的研究。



[註] EIRP: Equivalent Isotropically Radiated Power，等效全向輻射功率

圖 6.4: 美國 FCC 單位針對室內通訊系統所提出的 UWB 頻譜遮罩規範
(摘錄至參考文獻[3])

Section 3 IEEE 802.15.3 的網路架構與運作

Section 3.1 Piconet 概念與裝置角色

為了因應WPAN的特殊網路環境，IEEE 802.15.3定義了「微網」(Piconet)作為網路架構的基本單位，所謂的Piconet指的是一個無線隨意的通訊系統(Wireless ad hoc data communications system)，而在這個系統中容許數個獨立的網路裝置(data devices，簡稱為DEV)彼此能夠互相溝通，如圖 6.5所示；值得注意的是，Piconet和一般WLAN甚至WMAN所定義的大範圍網路不同，它主要是針對大約10公尺範圍內的個人網路，且在這個網路內是可以容許網路裝置移動的。

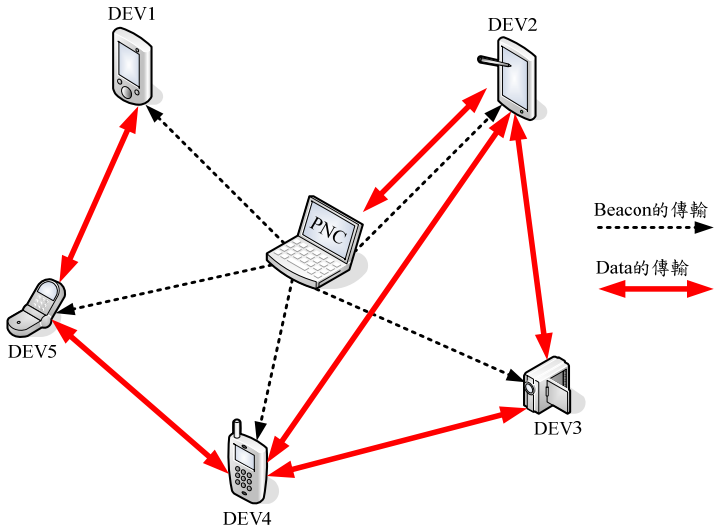


圖 6.5: IEEE 802.15.3 的 Piconet 與裝置角色

圖 6.5顯示一個IEEE 802.15.3 的Piconet，在這個Piconet中基本單位是DEV，而其中有一個DEV則是扮演「微網協調者」(Piconet coordinator，簡稱為PNC)的角色。PNC主要的目的在管理整個Piconet的運作，它的責任包括有：

- 定期廣播(Broadcast)Beacon 訊息給其他 Piconet 的成員，而 Beacon 中則包含了整個 Piconet 運作所需的的重要資訊。
- 調控整個 Piconet 的時間(Timing)機制，使得整個 Piconet 成員的時間能夠同步(Synchronize)，而這個 Timing 機制則可以透過 Beacon 訊息的傳送來達成。
- 管理 QoS、電源節省機制(Power saving mechanism)、以及 DEV 的存取控制(Access control)。
- 分配時槽(Time slot)給 DEV 以供其傳輸；然而要注意的是，兩個 DEV 彼此間可以直接做溝通(Peer-to-peer communication)而不用透過 PNC，如此一來，將可以減少不必要的傳輸與延遲(Delay)。
- 將金鑰(Payload protection keys)分配給各個 DEV。

每個 Piconet 都有一個「微網識別碼」(Piconet identifier，簡稱為 PiconetID)用來分辨不同的 Piconet，此外，為了簡化硬體設計以及達成低成本的目標，IEEE 802.15.3 容

許部份裝置不用實作 PNC 的功能。

Section 3.2 Piconet 的種類

由於不重疊(Non-overlapping)的 Channel 之數量有限，因此倘若找不到可用的 Channel 時，裝置間可能會形成所謂的「依存性微網」(Dependent piconet)。當有兩個 Piconet 是運作在相同的 Channel 上時，則最早形成的 Piconet 稱為「父微網」(Parent piconet)，而另外一個較晚形成的 Piconet 則就是 Dependent piconet；要注意的是，儘管 Dependent piconet 是和別的 Piconet 共享 Channel，它仍然具有自主性(Autonomous)，此外它也擁有自己的 PiconetID，然而由於 Channel 是共用的，為了避免和 Parent piconet 互相干擾，Parent Piconet 會特別保留一部份的 Time slot(稱為 Channel time assignment，簡稱 CTA，此部份會在 6.4 節中敘述)給 Dependent piconet 使用。

Dependent piconet會再根據和parent piconet的關係細分成兩種類型：鄰居微網(Neighbor Piconet)以及子微網(Child Piconet)，如圖 6.6所示。其中Neighbor piconet除了單純和Parent piconet共享Channel外，兩者間並不存在任何關係，而且兩個Piconet間的裝置也無法互相傳輸資料；另一方面，Child piconet可以看成是Parent piconet的涵蓋延伸(Coverage extension)，以Parent piconet的觀點來看，Child piconet中的PNC(亦稱為Child PNC)是被視為其Piconet中的裝置成員之一，因此，Parent piconet中的PNC(亦稱為Parent PNC)就可以和Child PNC做資料的傳輸，至於Parent piconet和Child piconet間的其他成員裝置則可以透過Parent PNC和Child PNC來做溝通。

至於兩個鄰近的 Piconets 若是運作在不同的 Channel 上，或是兩個運作在相同 Channel 上的 Piconets 彼此位在干擾範圍以外，則這兩個 Piconets 稱為「獨立微網」(Independent piconets)。

在接下來的章節中，我們將針對 Piconet 的運作做一個介紹，包括 Piconet 的建立、裝置成員的加入與離開、PNC 的換手、以及 Piconet 的終結等議題。

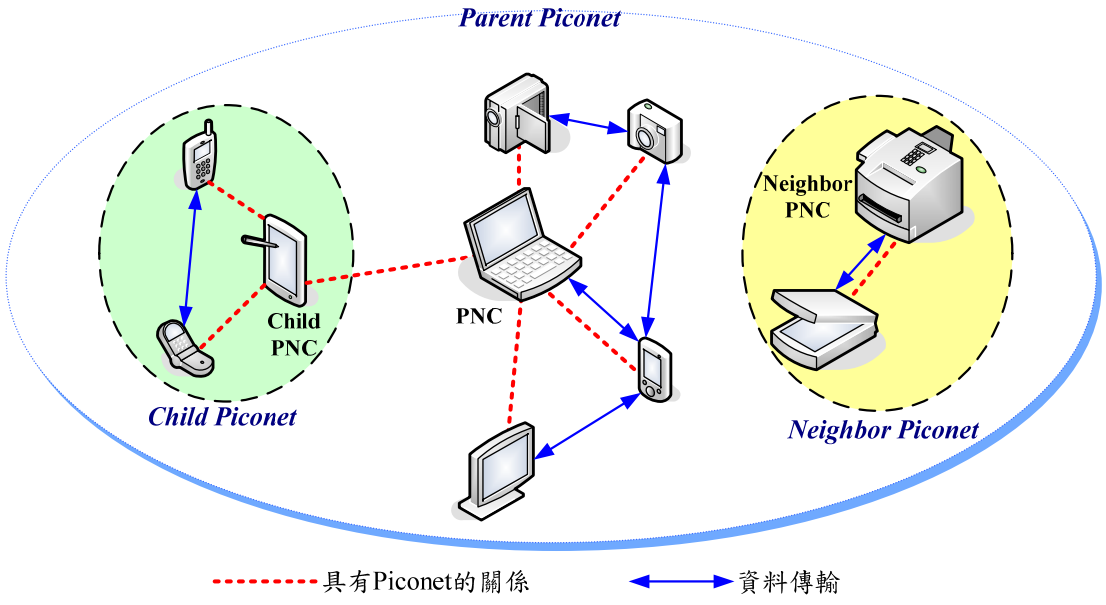


圖 6.6: IEEE 802.15.3 的 Piconet 種類

Section 3.3 Piconet 的建立

當一個裝置想建立 Piconet 時，它會先嘗試尋找可使用的 Channel，為了儘可能不和已存在的 Piconet 發生衝突(也就是儘量形成 Independent piconet)，這個裝置可以透過以下機制來判斷某個 Channel 是否已經被他人所使用：

- 利用被動式掃瞄(Passive scanning)的方式偵測是否存在其他的 Piconet。
- 藉由實體層的機制掃瞄所有的 Channel。
- 聆聽(Listen)來自其他 PNC 所發送出的 Beacon 訊息。

倘若這個裝置可以找到一個未被使用的 Channel，則它就可以藉由廣播 Beacon 訊息的方式建立一個 Piconet 並佔據該 Channel；若是該裝置找不到任何可以使用的 Channel 時，則它可以選擇加入現有的 Piconet，或是自行建立一個 Dependent piconet(亦即 Neighbor piconet 或是 Child piconet)。

值得注意的是，一開始建立Piconet的裝置不一定是最適合作為PNC的裝置，因此IEEE 802.15.3允許PNC換手(handover)的機制，即讓後來加入的裝置成員成為這個Piconet新的PNC。

Section 3.4 Piconet 的成員加入與離開

當一個裝置想加入已存在的Piconet時，它會執行聯結的程序(Association process)，如圖 6.7所示。一開始，這個裝置會先接收來自PNC所發出的Beacon訊息，之後該裝置會向PNC發出一個Association Request的訊息以要求加入這個Piconet，在圖 6.7我們可以看到Association Request訊息中包含兩種位址(Address)：DEV address以及DEVID，其中DEV address是用來辨識該裝置的位址，長度共有8bytes，且位址是廣域唯一的(globally unique)，另外的DEVID則是這個裝置在此Piconet的識別代號，長度僅有1個byte，而且只有在此Piconet是唯一的(至於兩個Piconet則可能會有相同的DEVID)，簡單來講，我們可以把DEV address視為這個裝置的身分證字號，而DEVID則就是這個裝置的臨時代號；DEVID的採用可以降低裝置在傳輸時的負擔(Overhead)，而一開始由於這個裝置尚未加入此Piconet，因此它的DEVID會被設成UnassocID，而當PNC收到Association Request後，它會立即回應一個ACK訊息，並在下一個訊息中夾帶PNC指定這個裝置的DEVID；之後該裝置會再發送一個Association Request訊息作為確認，最後PNC會在下一個Beacon訊息廣播這個新裝置加入的訊息，如此一來，Piconet中的其他裝置成員就會知道這個新裝置的存在。

另外，當新裝置要加入該Piconet時，它會和PNC交換自己的能力資訊(Capability information)，例如：實體層的資料傳輸速率支援狀況、電源管理機制的狀態、緩衝區的空間(Buffer space)、以及是否有能力擔任PNC等資訊，如此一來，PNC才能根據此新裝置的能力做調配管理的動作。

當一個裝置想離開Piconet、或是PNC想移除Piconet中某一個裝置成員時，此時去聯結的程序(Disassociation process)將會被啟動，如圖 6.8所示，要注意的是PNC也必需在Beacon中夾帶離開裝置的訊息，如此一來，Piconet中剩餘的裝置成員才會知道該裝置的

離開；此外，離開裝置的DEVID也會被設成無效，除非PNC再次將該DEVID設給其他新來的裝置。

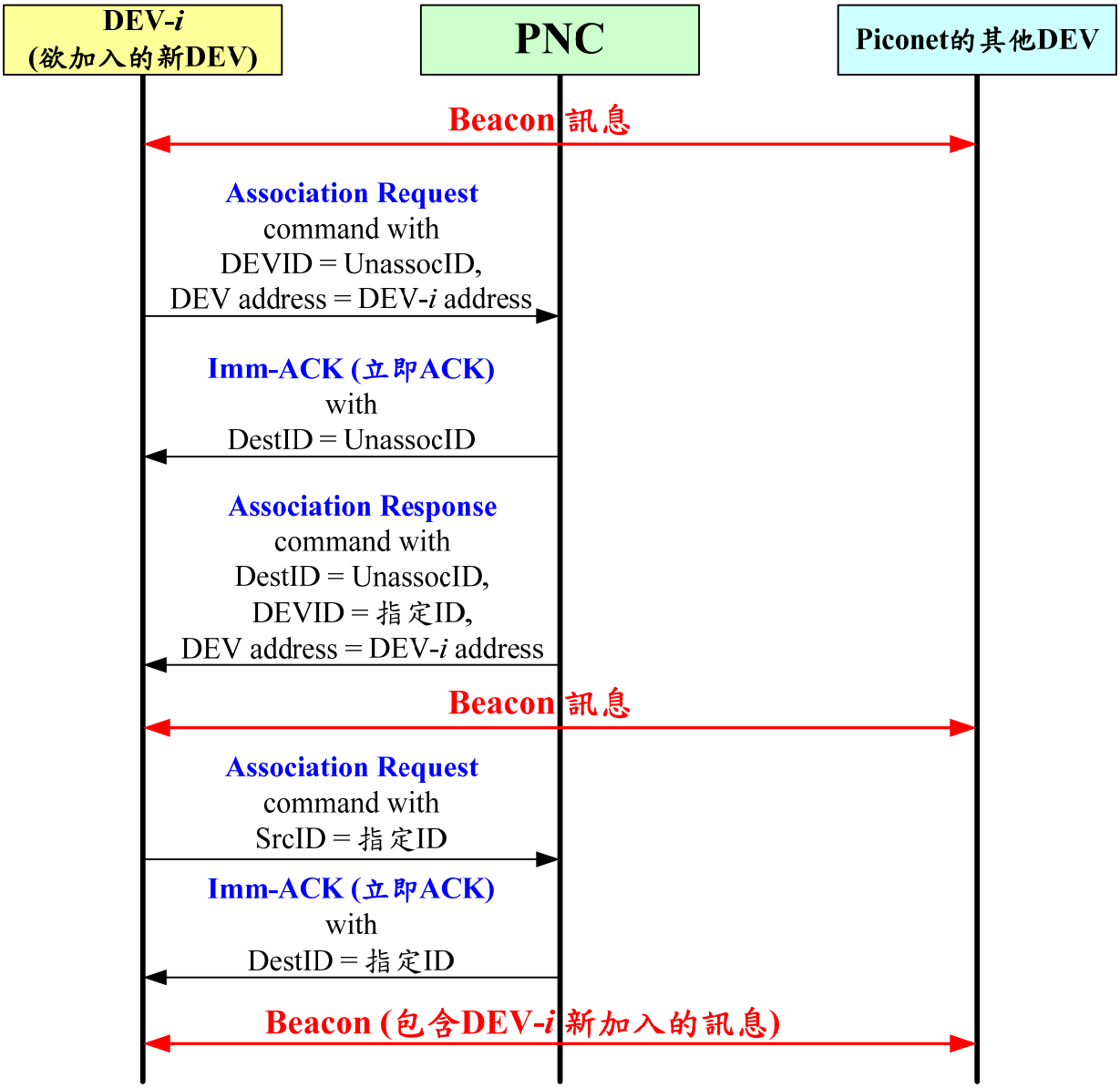


圖 6.7: 新裝置(DEV-*i*)加入 Piconet 所需的訊息交換流程

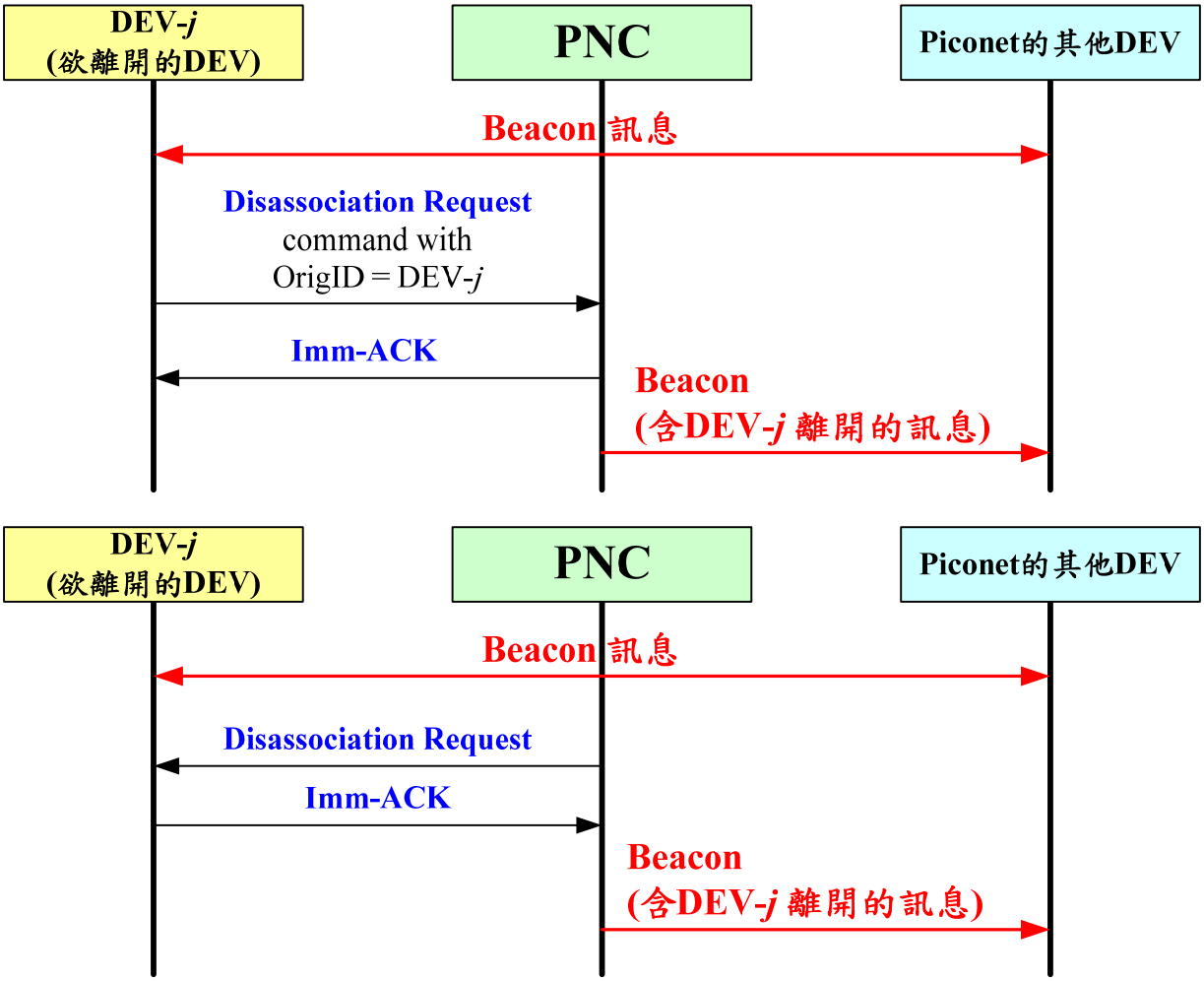


圖 6.8: 原裝置(DEV-*j*)離開 Piconet 所需的訊息交換流程
(上圖) DEV-j 主動要求離開 Piconet；(下圖)PNC 強制要求 DEV-j 離開 Piconet

Section 3.5 PNC 的換手

在 Piconet 運作的過程中，PNC 的角色是可以改變的，而這就稱為 PNC 的換手(PNC handover)，這個行為會在兩個情形下發生：

- 目前運作的 PNC 離開這個 Piconet，或是它的電源已快用盡。
- 當有新的裝置(能夠勝任 PNC 角色者)加入這個 Piconet。

其中在第二個情況下，倘若新加入的裝置能力較強，而且目前的安全策略(Security policy)允許下，則 PNC handover 才會發生。

當 PNC handover 發生時，原有的 PNC 會從 Piconet 中選擇可勝任 PNC 角色裝置中能力最強者作為新的 PNC(裝置能力的相關資訊在它加入 Piconet 時會告知 PNC，而原有的 PNC 這可以根據這些資訊來選擇新的 PNC)，同時原有的 PNC 會將其所記錄的資訊(例如：Time slot allocation)交給新的 PNC，以維持 Piconet 的正常運作。

Section 3.6 Piconet 的終結

當目前的PNC準備停止運作(或是離開)，而且Piconet中剩餘的裝置無人可以勝任PNC的工作時，則該PNC會在Beacon中包含一個「PNC終止資訊元件」(PNC Shutdown information element)以告知Piconet其他裝置成員該Piconet將要終結。倘若原有的PNC突然離開Piconet(因此未選擇接任的PNC)，則經過一段時間(該段時間稱為Association timeout period，簡稱為ATP)後，該Piconet自動解散，此時若有裝置可以勝任PNC的工作，則它會自行建立新的Piconet。

另外，若是Parent piconet終結時，則其他依存在這個Piconet的Dependent piconet也會跟著解散；另一方面，若是Neighbor Piconet要求解散，則它的PNC會向其Parent piconet的PNC發送一個Disassociation Request的命令以終結雙方的關係，若是Child Piconet要求解散，則Child PNC會使用一個Channel time request command通知Parent PNC終止關係。要注意的是，一個Dependent piconet的解散並不會對其所依存的Parent piconet造成影響，至多只是釋放資源而已。

Section 4 IEEE 802.15.3 的傳輸模式

IEEE 802.15.3的傳輸是以「超級訊框」(Superframe)為基本單位，Superframe內部的配置是由PNC來決定，基本上可以分成三大部份(如圖 6.9所示)：

(1) **Beacon**：用來註明一個Superframe的起始，PNC會在Beacon中包含這個Superframe所有相關的訊息，包括Piconet內各裝置成員的能力資訊(Information elements)以及同步用之訊息(Piconet synchronization parameters)，如圖 6.1所示；其中各裝置的訊息內容如表 6. 1所示(長度可變動，但長度至多為255bytes)，而同步用之訊息則規範了後續CAP以及CTAP的相關參數，例如是否採用SEC加密模式、CTAP時段是否含有MCTA時段、以及CAP時段的參數規範。

(2) **CAP** (Contention access period)：這段時間基本上是採用CSMA/CA(Carrier sense multiple access with collision avoidance)的競爭機制，也就是每個裝置會偵測Channel是否被他人所使用，以決定是否可以存取(Access)這個Channel。CAP這段時間除了可以用來交換PNC與其他裝置的命令(Command)外，還主要提供裝置間無需提出要求(Request)的資料傳送，例如非即時性一類的資料流(Non-real-time flows，這些資料由於沒有Delay限制，因此無需透過事先保留頻寬的方式來保障其傳輸)。

(3) **CTAP** (Channel time allocation period)：這段時間基本上則是採用TDMA(Time division multiple access)的存取機制，因此若有裝置想在這段時間傳送資料的話，則它必需向PNC提出申請(Reservation)，而PNC也會在Beacon中指定哪些Time slot是給哪個裝置使用。另外，CTAP又再分成兩部份：CTA(Channel time allocations)以及MCTA(Management CTA)，其中MCTA是用來傳輸PNC的命令，而CTA則是讓裝置傳送其資料。

藉由上述的Superframe架構，IEEE 802.15.3可以針對不同QoS需求提供服務，仔細

來講，Best effort的資料(例如：FTP的傳輸)是在CAP時段傳送，因為這類似的資料沒有時效性的需求(Delay requirement)，因此可以透過競爭的模式來傳送；另一方面，具有即時性(Real-time)的資料，例如：聲音或影片，則可利用CTAP的時段傳送，由於PNC會幫裝置保留Time slot，因此這類型的資料可以保障其傳輸。

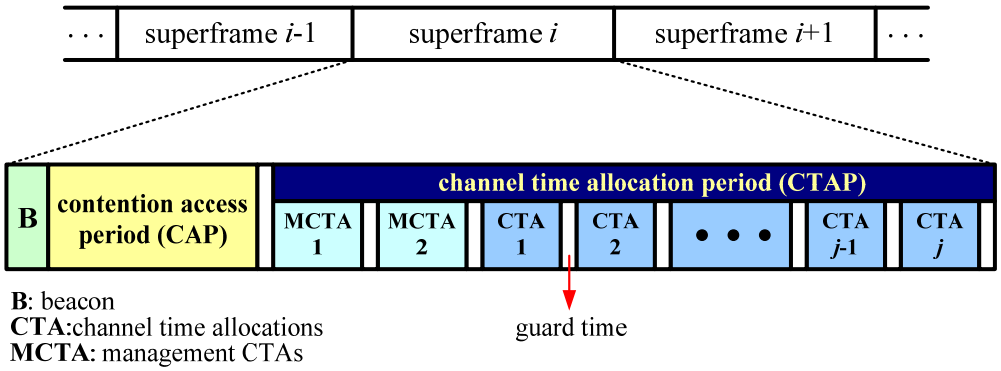


圖 6.9: IEEE 802.15.3 superframe 架構圖

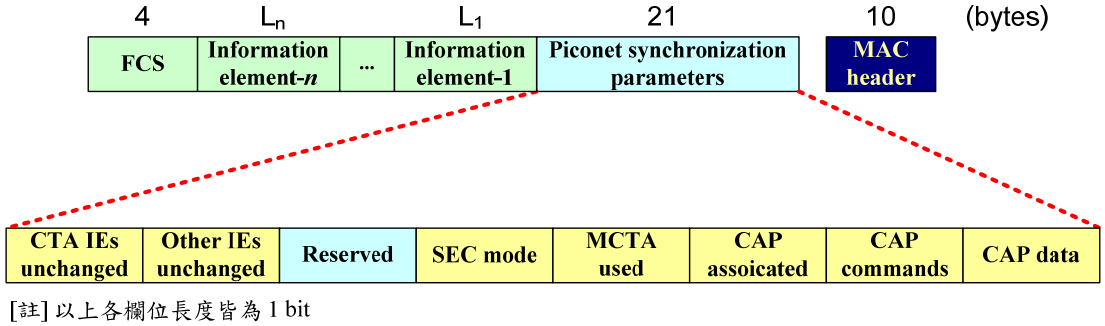


圖 6. 10: IEEE 802.15.3 Beacon 封包格式

位址	Element	說　　明
0x00	Channel time allocation	提供該裝置在 CTA 時段的相關參數
0x01	BSID	用來辨識該 Piconet
0x02	Parent piconet	用來辨識 Parent piconet 以及該裝置在 Parent piconet PNC 的位址(DEV address)
0x03	DEV association	該裝置 Associate 到 Piconet 的相關訊息
0x04	PNC shutdown	目前 PNC 是否要關機(shutdown)
0x05	Piconet parameter change	指定 Piconet 參數的變更
0x06	Application specific	讓使用者輸入自定的訊息(custom information)
0x07	Pending channel time map (PCTM)	讓裝置切換至 Active mode
0x08	PNC handover	提供 PNC 換手的訊息
0x09	CTA status	說明這個 Superframe 的 CTA 時段之相關訊息
0x0A	Capability	該裝置的能力

0x0B	Transmit power parameters	指定該裝置傳輸電力的參數
0x0C	PS status	說明裝置省電模式(Power-saving mode)狀態
0x0D	Continued wake beacon (CWB)	指定 CWB 所需的相關參數
0x0E	Overlapping PNID	說明一個裝置在目前的 Channel 或其他 Channel 中被偵測到
0x0F	Piconet services	說明裝置在應用層(Application layer)所提供的能力
0x10-0x7F	Reserved	保留用
0x80-0xFF	Vendor specific	各硬體製作廠商所制定之訊息

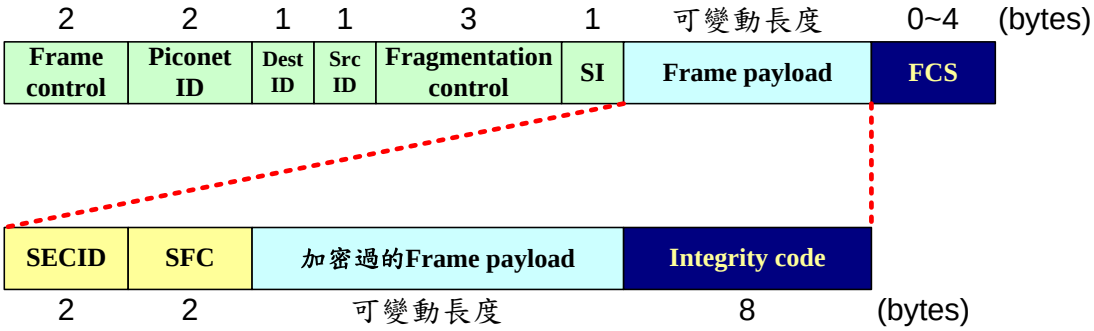
表 6. 1: Information elements 相關欄位資訊

Section 5 IEEE 802.15.3 的安全機制

目前 IEEE 802.15.3 支援兩種 Secuirty 模式，分別為：

- Mode 0 (基本)：基本上就是不提供任何安全機制，裝置間彼此無需透過認證(Authentication)，且所傳輸的資料並未加密；然而在這個模式下，裝置仍可選擇使用 Access control list(ACL)。
- Mode 1 (可選擇)：封包(Packet)加密的方式是採用 128 bits金鑰(key)長度的 AES(Advanced encryption standard) [8]方式，其中加密封包的的部分是採用 AES-CTR(Counter mode)的演算法，而封包完整性(Integrity)的驗證則是藉由 AES-CCM (Counter with CBC-MAC mode) 的 64 bits Integrity code。

一個完整的IEEE 802.15.3 封包格式如圖 6.11所示，其中封包的標頭(Header)包括有 2 個bytes的Frame control欄位、2 個bytes的Piconet ID欄位、1 個byte的目標裝置位址(即Destination的DEVID)、1 個byte的來源裝置位址(即Source的DEVID)、3 個bytes的Fragmentation control的欄位、以及 1 個byte的Stream index，總長共有 10 個bytes；之後緊接著一段長度可變動的封包內容(Frame payload)，最後會再加上 4 個bytes的Frame check sequence(FCS)以確保封包的完整性。



[註] SI: Stream index; SFC: Secure frame counter

圖 6.11: IEEE 802.15.3 加密後的封包格式

兩種 Security mode 的封包差異主要是 Frame payload 的部份，若是採用 Mode 0，則該封包只會包含 10 bytes 的 IEEE 802.15.3 Header、長度不定的 Frame payload、以及該 Frame 結尾的 FCS 欄位。若是採用 Mode 1，則 Frame payload 的部份將會透過 AES-CTR 演算法做加密的動作，並且會透過 AES-CCM 方法來產生 8 個 bytes 的 Integrity code 以作為驗證使用，除此之外，在加密後的 Frame payload 之前還會加上 2 個 bytes 的 SECID (Secure session ID)以及 2 bytes 的 SFC(Secure Frame Counter)，其中 SECID 是用來判別這次加密所使用的金鑰(金鑰長度為 128 bits)，而 SFC 則是用來區別同一把 128 bits 的 AES 金鑰在不同時間加密過程中所產生的加密封包與 Integrity code。而在 SECID 欄位中，前一個 byte 是記錄該金鑰發行者(Key originator)的識別碼，而後面的另一個 byte 則是代表相對於此金鑰發行者所發行的每把金鑰之專屬 8 bits 識別碼，要注意的是，對於同一個金鑰發行者而言，此 8 bits 的金鑰識別碼是不能重複的。

由於兩種Security mode的主要差異在Frame payload的部份，因此為了讓接收端(Receiver)得已判斷此封包是否有被加密，傳送端(Sender)會設定該封包的SEC欄位(位於封包標頭的Frame control部份，如圖 6.12所示)，若是封包有被加密，則該欄位會被設成 1，反之，則會被設成 0；藉由這個欄位，接收端將可以輕鬆判斷此封包是否有被加密過。

3 bits	3 bits	1 bit	2 bits	1 bit	1 bit	1 bit	1 bit	1 bit	2 bits
Protocol version	**Frame type**	**SEC**	**ACK policy**	**Retry**	**More data**	**IAR**	**IAN**	**CR**	**Reserved (尚未定義)**

[註] **IAR**: Implied ACK request
IAN: Implied ACK negative acknowledgement
CR: CAT relinquish

圖 6.12: Frame control 的欄位

最後，在一個 Piconet 中，每個 PNC-DEV 與 DEV-DEV 之間認證加密用的金鑰都是各自獨立的，換句話說，同一個裝置對於其他不同裝置所需要的加密金鑰將會是不同的。除此之外，PNC 會有一把群組資料加密金鑰(Group data key)用來加密廣播的訊息，要注意 Group data key 和 PNC 用來和其他裝置個別溝通用的金鑰是不同的。

Section 6 結語

在這個章節當中，我們整體性地介紹 IEEE 802.15.3 的通訊標準，這個標準是針對 WPAN 環境下提供高速寬頻的傳輸，因此可以提供個人化的多媒體傳輸應用，此外，它亦結合了 UWB 的技術以提升資料傳輸的速率；雖然目前標準的制定受到頻帶分配的限制與參與廠商的爭議而尚未制定完成，但 IEEE 802.15.3 所制定的目標將會是未來重要的發展應用之一。

參考文獻

[1] IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific

requirements “Part 15.3: wireless medium access control (MAC) and physical layer (PHY) specifications for high rate wireless personal area networks (WPANs)”, 2003.
[2] Federal Communications Commission (FCC). http://www.fcc.gov/
[3] G. R. Aiello and G. D. Rogerson, “Ultra-wideband wireless systems,” IEEE Microwave Magazine, vol. 4, pp. 36-47.
[4] WiMedia Alliance. http://www.wimedia.org/en/index.asp
[5] UWB Forum. http://www.uwbforum.org/
[6] IEEE 802.15.3b WPAN Task Group, http://www.ieee802.org/15/pub/TG3b.html
[7] IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements “Part 15.3: wireless medium access control (MAC) and physical layer (PHY) specifications for high rate wireless personal area networks (WPANs) - Amendment 1: MAC sublayer”, 2005.
[8] US National Institute of Standards and Technology, “Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication 197, November 2001.