無線感測網路截取 ZigBee/802.15.4 封包分析工具實作

張豈嘉、吳坤熹
國立暨南國際大學通訊工程研究所

摘要—本論文敘述一個無線感測網路的封包截取分析工具架構設計，使輕巧方便攜帶型的 Freescale MC1322x USB Dongle，搭配自行開發的軟體程式以及開放原始碼 Wireshark 網路封包分析軟體，即可於桌上型電腦或筆記型電腦上，分析區域範圍內的 IEEE802.15.4 ZigBee 網路封包。[1]

關鍵詞：IEEE802.15.4、ZigBee、封包分析、無線感測網路。

一、 簡介

近年來無線感測網路盛行，已逐漸擴展到居家控制、醫療照護、生態環境監控等領域。因此，提升無線感測網路中的傳輸品質、 增進保密資料的安全、排除網路故障的問題等議題越來越顯重要。然而要能夠達成這些目標，首要的第一步就是分析網路中所傳送的封包。了解各個封包中，每個欄位的數值為何。傳輸的封包於傳遞的過程中，又有哪些欄位被刪除、添加或修改。藉此才能一步一步清楚地分析出問題的癥結。

本研究開發出 ZigBee/IEEE802.15.4 封包分析的工具，將硬體裝置 Freescale MC1322x USB Dongle，結合 Wireshark[1]這套開放原始碼軟體，達到分析封包的功能。

在 ZigBee 無線網路的產品中，也包含網路分析的硬體裝置；這些裝置有些需搭配公司原廠的軟體來接收分析 ZigBee 的訊號，但對於封包的分析較為簡略或不夠完備，對於軟體的更新或升級支援也較缺乏。例如 Microship 公司的 ZENA Network Analyzer、BzWorks 公司 的 WiSens Packet Sniffer 等。

有些則是與其他軟體公司配合，本身並沒有開發軟體。例如以往強大的分析軟體 Daintree's Sensor Network Analyzer 雖支援 Texas Instrument、Freescale、Jennic 等多種硬體平台，也由於商業因素考量，已經於 2010 年 3 月 31 日停止販售。並刪除連結停止下載服務，因此，網路分析硬體若完全仰賴其他公司的分析軟體，則可能遭遇這類的情形。

另外，有些硬體裝置則是搭配開放原始碼的軟體來達成封包的截取與分析。近來有一套廣為流行的網路封包協定分析軟體 Wireshark（前身為 Ethereal），其功能為擷取網路封包，並且進行細部的分析與判讀，顯示出詳細的封包欄位；一般常用在網路故障排除、監聽異常封包、封包問題檢測等用途。有別於過去市面上昂貴的網路封包分析軟體，Wireshark 是一套在 GNU General Public License 的保障範圍下，使用者可以免費取得這套軟體與其程式碼的軟體。因此，Wireshark 是目前全世界最被廣泛使用的網路封包分析軟體。 Wireshark 支援了多種作業系統，在 Windows、 UNIX、Mac OS 下都有相對應的版本。因此，在 Wireshark 廣泛應用在 Ethernet 及 WiFi 等網路後，市場上也出現公司針對 Wireshark 開發搭配的 ZigBee 網路分析硬體產品來使用，例如 Exegin 公司的 Q51 PANalyzer。但這款設備並非 USB 裝置，如**圖 一**所示，較不方便攜帶，需另外搭配網路線使用，適用於固定場所的網路分析，而且分析儀器的售價較為高昂，售價美金 500 元。如**表 一**所示：

表 一：市售產品比較分析表

硬體產品	封包分析軟體	裝置韌體需求	參考價格
Freescale─ Sniffer USB Dongle	Wireshark (自由軟體)	原廠隨插即用	USD 100
Exegin─ Q51 PANalyzer	Wireshark (自由軟體)	原廠隨插即用	USD 500
Atmel─ AVR Microcontrollers	Wireshark (自由軟體)	需燒錄韌體另購燒錄配件	USD 200
Atmel─ AVRRZ541 AVR Z-Link 2.4 GHz Packet Sniffer Kit	IEEE 802.15.4 MAC	─	─
Microship─ ZENA Network Analyzer	ZENA™ Packet Sniffer	─	─
BzWorks ─ WiSens Packet sniffer	WiSens® Classic sniffer software	─	─
Texas Instruments─ CC2531	TI Packet Sniffer	原廠隨插即用	─

[1]本研究由國科會贊助，計畫編號 NSC 99-2218-E-029-001 及 NSC99-2221-E-260-012。

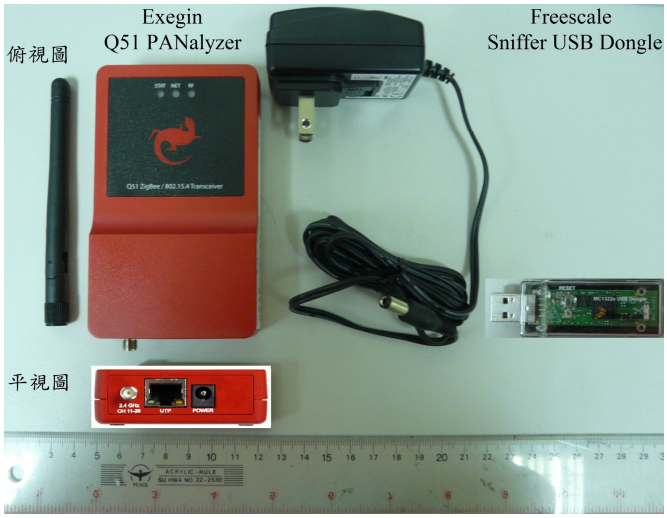


圖 一 :Q51 PANalyzer(未含網路線)與 Sniffer USB Dongle 實體

因此若希望解析 ZigBee/IEEE802.15.4 的網路封包，必須要結合硬體裝置與分析軟體。本研究主要開發出軟體模組，將 USB Dongle 裝置包裝成虛擬網路卡，使 Wireshark 能夠辨識出該項介面卡，並利用此裝置來擷取 2.4GHz 中 ZigBee 的訊號，進行封包擷取與分析的動作。

二、 背景知識

2.1 IEEE802.15.4 通訊協定

IEEE802.15 Working Group[2]定義無線個人區域網絡(Wireless Personal Area Networks, WPANs)為小覆蓋範圍、短距離(100M)、非視線傳輸(Non-Line of sight, NLOS)的無線傳輸標準。其中包含了 IEEE802.15.1 (Bluetooth)、IEEE802.15.3 (UWB)、IEEE802.15.4 (ZigBee)等幾種通訊標準。

IEEE802.15.4 通訊協定主要定義媒體存取層(Medium Access Control layer, MAC)與實體層(Physical layer, PHY)通訊協定。網路設備可以分為兩類：1.完整功能設備（Full Function Device, FFD)支持所有的網路功能，是網路的核心部分；2.部分功能設備（Reduced Function Device, RFD)只支持較少選擇和必要的網路功能，減少功能以降低成本，網路中大部分是此類設備。

2.2 ZigBee 通訊協定

ZigBee 是一種無線網路協定，主要由 ZigBee Alliance 所制定，底層採用 IEEE 802.15.4 標準規範的媒體存取層與實體層。其架構如**圖 二**下所示。

ZigBee 主要有下列特點：

1. 依設備角色不同可分為三類：協調器(Coordinator)、路由器(Router)、終端設備(End-Device)。
2. 低傳輸速率：最高傳輸速率 250Kb/s。
3. 低耗電：裝置可選擇是否開啟休眠功能。
4. 低成本：使用免費公用頻帶 2.4GHz。
5. 高網路擴展性：最多可支援高達 65535 個節點。
6. 高可靠度：採用直序展頻(DSSS)通訊方式，具有較高的抗干擾性。
7. 高安全性：支援 AES-128 加密。

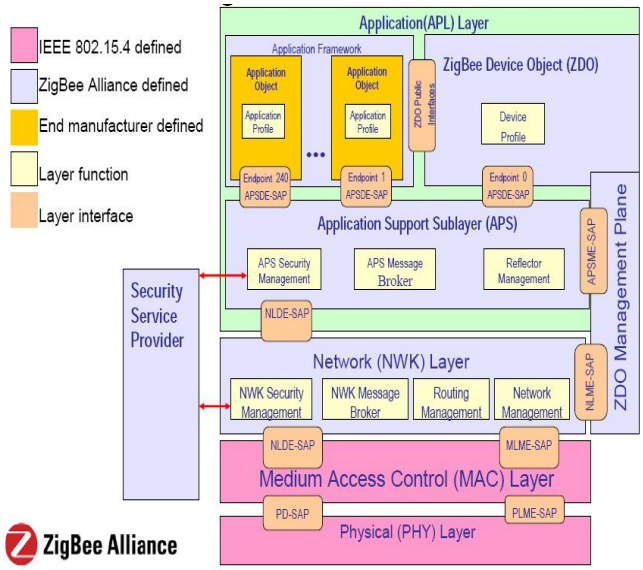


圖 二：ZigBee/802.15.4 網路架構

2.3 Wireshark Protocol Analyzer

Wireshark 主要的架構可以分為四個部分：使用者介面(User Interface)、協定分析(Protocol Analyzer)、封包擷取(Packet Capture)、裝置介面(Device Interface)。[3]協定分析為 Wireshark 的主體核心，可分為通訊協定直譯器(Protocol Interpreter)、解析器(Dissector)。另外，擷取核心(Capture Core)、竊取(Wiretap)負責將數據封包擷取和儲存。如**圖 三**所示。

擷取核心將會採用 WinPcap 中不同網路介面卡所擷取到的數據封包，竊取是將擷取到的二進制的數據封包存入 PcapFile，因為數據是二進制，所以需要由網路協定直譯器和解析器來分析。

解析器的設計是 Wireshark 最大的特點之一，不但可以支援許多網路協定而且相當完整，更因為開放原始碼的關係，允許使用者將新的協定製作成 Plug-in 加掛於軟體中。不同封包擷取軟體，例如 tcpdump、Microsoft Network Monitor captures、Novell LANalyzer capture[4]所產生的檔案亦可在 Wirehsark 中讀取檢視。。此外，在介面使用上，Wireshark 圖形化的介面相當容易上手，豐富的過濾語言，可以輕鬆判別出封包的種類，是一套整合度完整的軟體。

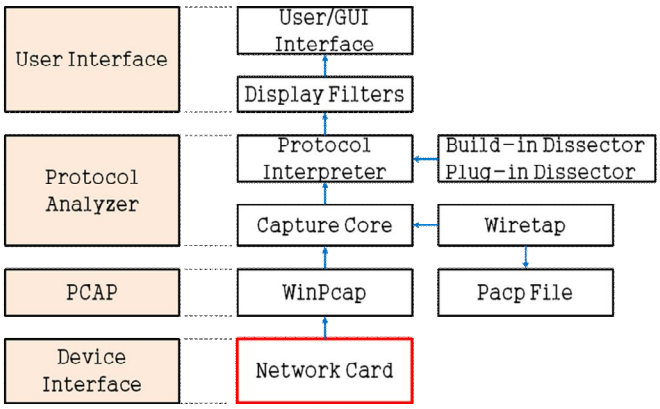


圖 三： Wireshark Architecture

網路封包分析的動作，若以 Wireshark 分析網路封包，首先要選擇適當的網路介面卡裝置。隨著使用網路介面卡裝置的不同，可以擷取不同的網路封包。例如選用 WiFi 無線網路卡擷取 IEEE 802.11 的網路封包、選用乙太網路卡擷取 IEEE 802.3 的網路封包。而 ZigBee/802.15.4 的網路封包，則必須仰賴 USB Dongle 為硬體的網路介面卡裝置。可惜的是，USB Dongle 並不是 Wireshark 所能正確判讀的網路介面卡裝置。若希望讓 USB Dongle 所擷取的封包可以利用 Wireshark 強大的功能予以解析，必須將 USB Dongle 包裝為虛擬的網路介面卡裝置。如**圖 四**所示。

圖 四：Wireshark 為軟體，USB Dongle 為硬體的網路封包分析架構

2.4 Freescale USB Dongle

Freescale USB Dongle 以 ZigBee Test Client(ZTC) [5][6] 這套檢測工具的架構為核心，定義了 Data Frame 及其他資料傳輸的格式，並且有 USB 介面可以做為連接埠。

ZigBee Test Client (ZTC)是 Freescale 自行設計的一套架構，適用於以 ZigBee Coordinator(ZC)、ZigBee Router(ZR)、ZigBee End-Device(ZED) 這三種裝置為元件之網路架構。ZTC 的架構如**圖 五**所示。

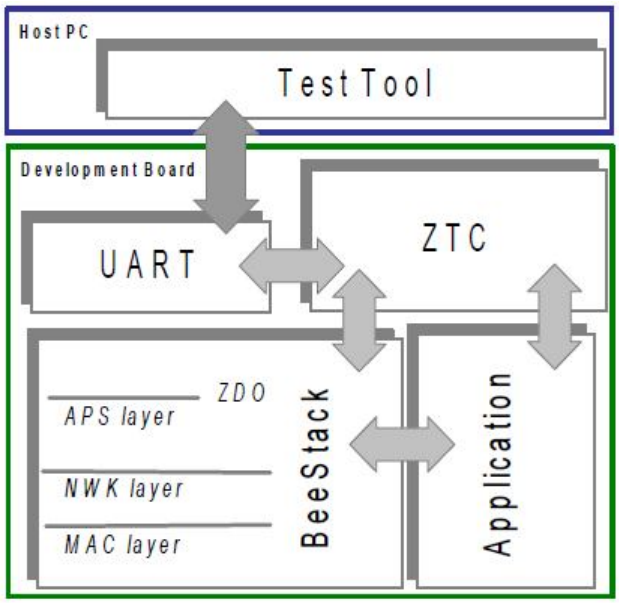


圖 五：ZTC Design Architecture

三、 提出方法

3.1 程式架構

為實現 Virtual Interface，程式架構如**圖 六**所示，將程式分為三個部分：1.Capture Freescale data、 2.Packet capture library、 3.User option。

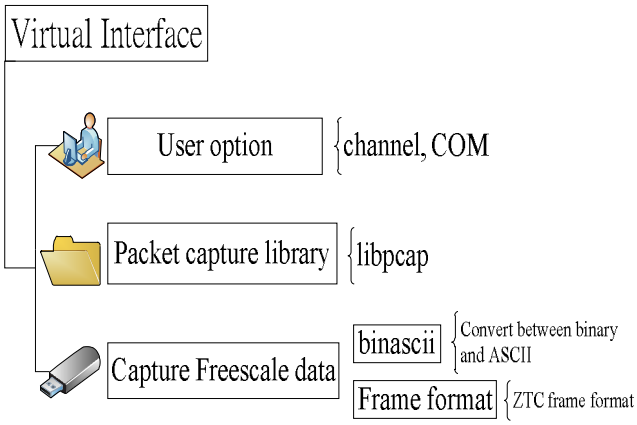


圖 六：程式架構圖

3.1.1 第一部分：Capture ZigBee data

將 Freescale 所制定 ZTC 架構下的資料格式依照其規則定義函式類別及物件名稱，並利用 Binascii API 將 USB 所接收到的二位元資料轉換為 ASCII 的格式。

3.1.2 第二部分：Packet capture library

將 802.15.4 的資料轉入 libpcap，這裡利用了 Wireshark CaptureSetup/pipes[7]的概念，導入 Serial API 以及重新改寫 Win32pipe API、Win32file API

3.1.3 第三部分：User option

這部分主要提供使用者可以依照 ZigBee/802.15.4 通道及 USB 連接埠不同，做適當的選擇及調整。

3.2 問題遭遇及解決

在第一部分將 Freescale USB Dongle 所擷取到的資料，嘗試並參考了許多種針對 USB 傳輸設計定義的方式，程式卻仍然無法判讀出正確的資料。因此，多方求證並找尋資料後，發現這套開發版引入了 Freescale 特有的 ZTC 架構，必須遵循其所特定的格式和規範。在詳讀過後，重新定義了類別和物件，才得以結合 Binascii API 將資料進行二位元和 ASCII 之間的格式轉換。

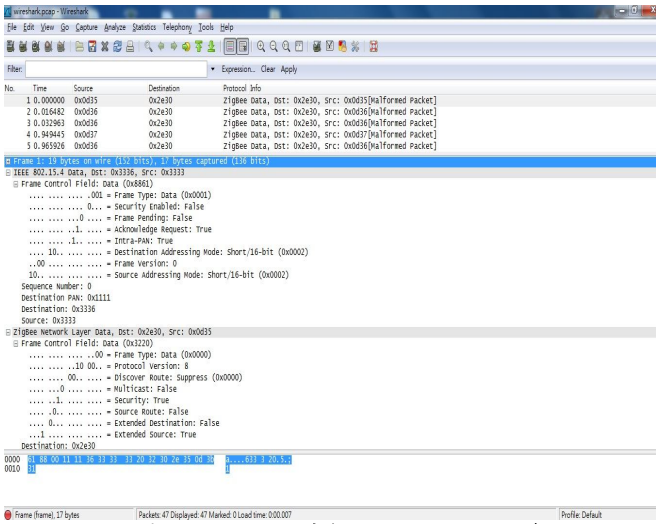
在介面的選擇上，應以 USB 或 RS-232 的函式庫為主，是花費最多時間進行研究與探討的部份。最後結論是以 RS-232 的函式庫進行撰寫，因為 USB 可以向下相容 RS-232，使用上可有更多的彈性。此外， RS-232 所找尋到相關的參考文獻也較為豐富。因此，放棄了原先因為此裝置為 USB 連接埠而撰寫的程式，重新改寫以 RS-232 函式庫為主的程式。

雖然最後採用 RS-232 的格式，但在研究的過程中，學習到 USB、RS-232 兩者之間的差異，以及 USB 傳輸控制的各種型態，資料訊框各個欄位和封包的型式，還有所對應函式庫的呼叫及運用。對這些格式都有更深入的了解。

這篇論文所撰寫程式是利用 Python 來完成，除了使軟體有更好的相容性以外，自己也從中學到除了 C/C++ 以外的程式語言，以及程式語言間的差異性，還有了解到 Python 在國外是被廣泛的使用，也藉此機會也向許多外國的程式設計者請益。不僅程式設計能力獲得了增進，在英文書信也較之前更熟練。這些都在這篇研究時自己所額外獲得的能力提升。

3.3 實作結果

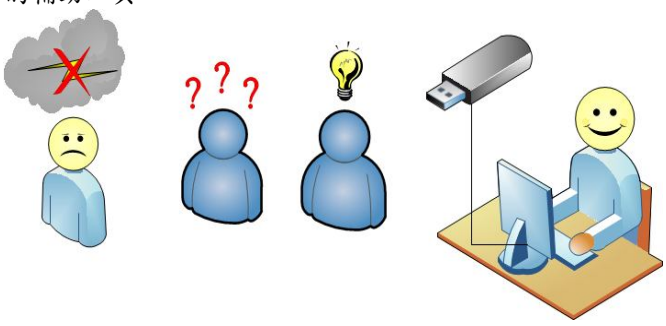
預期完成後的程式，將可由使用者自行設定 USB 所使用之連接埠，以及設定欲分析 ZigBee/802.15.4 無線網路之頻道，再開啟 Wireshark ，即可將所選擇需分析的封包進行分析。如圖五所示。



圖五：Wireshark 分析 ZigBee/802.15.4 封包

結論

目前無線感測網路的應用越來越為廣泛，然而這類的應用，包括效能及安全仍有很大的進步空間。在做本研究期間，曾經目睹廠商工程人員為了除錯但苦無工具煩惱，僅靠臆測來做為裝置除錯的判斷，沒有科學的作法相當曠日費時且出錯率極高。所謂「工欲善其事，必先利其器。」藉著這篇論文所提供的工具，希望使得往後從事 ZigBee 網路佈建與除錯的人，多了一種可以利用的輔助工具。



參考文獻

[1] Wireshark software, [http://www.wireshark.org/download.html]
[2] IEEE 802.15 Working Group for WPAN,[http://www.ieee802.org/15/]
[3] Angela Orebaugh, Gilbert Ramirez, Josh Burke ,and Jay Beale , “Wireshark and Ethereal network protocol analyzer toolkit “ , Syngress, Jan. 2007
[4] 蔡一郎「網路封包分析的好幫手—Wireshark 擷取分析、防範攻擊無所不包」，網管人技術專欄，[http://www.netadmin.com.tw/article_content.asp?sn=0808050013]
[5] Freescale”Freescale ZigBee Test Client(ZTC)”Reference Manual,Document Number:ZTCRM Rev. 1.4 10/2008 ,[http://application-notes.digchip.com/314/314-67711.pdf]
[6] Freescale”BeeSatack BlackBox ZigBee Test Client(ZTC)” Reference Manual,Document Number:BSBBZTCRM Rev. 1.4 02/2011 ,[http://www.freescale.com/files/rf_if/doc/ref_manual/BSBBZTCRM.pdf]
[7] Wireshark CaptureSetup/pipes,[http://wiki.wireshark.org/CaptureSetup/Pipes]