# 無線感測網路 ZigBee/802.15.4 和 TCPIP/802.3 之協定轉換器實作

**葉俊克*、吳坤熹**
國立暨南國際大學電機工程學系通訊工程碩士班

**摘要 —本論文實作一個閘道器，讓 ZigBee 節點能透過此閘道器和 IPv6/802.3 的伺服器進行溝通，使 ZigBee 感測網路中所收集到的資訊能夠透過 Ethernet 網路將資料送至伺服器端。此閘道器將採用位址映射和協定轉換的方式，讓兩端裝置進行溝通。[1]**

**關鍵詞**：IPv6、ZigBee、位址映射、協定轉換、閘道器。

## 一、 研究背景

隨著感測、無線通訊等技術的成熟，近幾年來無線感測網路(Wireless Sensor Network)的應用愈趨普遍。在 2004 年由 IEEE (Institute of Electrical and Electronics Engineers) 802.15.4 工作小組和非營利組織 ZigBee Alliance 提出的 IEEE802.15.4/ZigBee 標準[1]，就是針對無線感測網路應用，所發展出的一套通訊標準。其特色為低功率、低速率、低成本。發展至今，無線感測網路的應用也越來越多，例如：人體健康監測、工業自動化、溫度感測、燈光控制、自動計量裝置等[2][3]。愈來愈多的工作，都可以透過無線感測網路的支援，而達到智慧控制的目的。

無線感測網路起源於美國加州伯克萊大學的一個研究計畫[4] ，此計畫是由美國國防部先進研究計畫局(Defense Advanced Research Projects Agency, DARPA)所資助，其目的為開發出一套無線感測系統應用於軍事用途，例如透過無人飛機將數千甚至數萬個感測器，散佈在需要監控的戰場上收集資訊。一段時間後，再透過無人飛機去將散佈在戰場上的感測器所收集的資訊透過無線網路傳送回飛機。如此一來，就不需要派出人員冒著危險去收集戰場上的資訊。

無線感測網路相較於其它無線網路，例如 WiFi、WiMAX (Worldwide Interoperability for Microwave Access)、藍牙(Bluetooth)、超寬頻(Ultra-Wideband, UWB)等。有以下幾點特色：

1. 無線感測網路的節點數量相當多，往往有數千到數萬節點。
2. 因網路拓撲(topology)無法事先預測，需具有自行重建網路功能。
3. 無線感測網路節點的感測環境，通常處於無電力供應或電力供應不便的地方，大多時候採用電池來提供電力。希望僅透過電池，節點便能工作長達數個月甚至半年。因此，為了降低能源損耗，無線感測網路節點的體積、記憶體、運算能力、功率有較大的限制。
4. 無線感測網路基於減少成本和動態拓撲的特色，希望在無任何基礎建設時，也能彼此傳送訊息，而為了確保每一個節點都能互相溝通，需要支援多點跳躍傳輸(multi-hop)。

上述這些特性，與 WiFi、Bluetooth 等其它無線網路架構相較都有明顯的不同。

現在許多關於無線感測網路的應用，都著重於監控的功能；不論是家庭監控、工業監控、醫療監控、環境監控等。為了與更多的網路應用結合，都必須先把收集的資訊傳送至一部伺服器的資料庫中，以便之後能對這些資料做分析，甚至進一步去控制各個網路節點。如何將無線感測網路節點中收集到的資訊，傳送到資料庫中，是本篇論文探討的重點。

目前已有數種將資訊送到資料庫的方法，分別是通道機制、將封包轉變為 XML 格式的機制、協定轉換機制，或是將收集到的訊息存成檔案，再透過 ftp 進行傳送的機制。其中，協定轉換機制雖已被提出，但實際在市面上所販賣的閘道器，大多是採用其它三種方法，尚未看到使用協定轉換機制的閘道器商用成品。下一段落會分別說明各種機制的基本架構和優缺點。

一種常見的閘道器設計是通道機制，ZigBee 閘道器將 ZigBee 無線網路端收到的 802.15.4 封包負載，加上 TCP/IP 標頭後，透過 Ethernet 傳送到後端的資料庫伺服器，最後再由後端的伺服器負責處理封包內容，如**圖一**所示。此做法，後端的服務器需要有一個對應的特定程式來負責解析封包。此外，並不是所有的 ZigBee 封包資訊在 Ethernet 網路都是必要的（例如 ZigBee 網路中的封包序號、跳躍限制數等），所以將整個 802.15.4 封包的負載直接以 Ethernet 傳出，會造成頻寬的浪費。

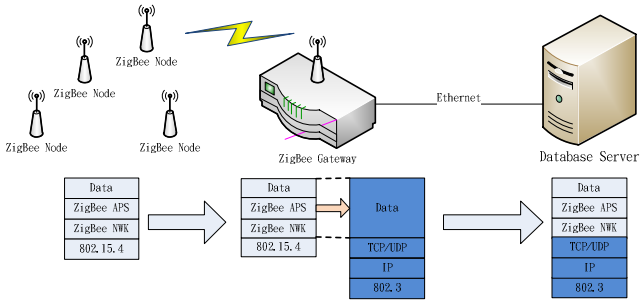


**圖 一：通道機制示意圖**

另一種作法則是在 ZigBee 閘道器的應用層中設計符合簡單物件存取協定(Simple Object Access Protocol, SOAP)或表象化狀態轉變(Representational State Transfer, REST)的應用程式，將 802.15.4 的封包資料透過應用層

[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。

的程式轉成 XML 的格式[5]，如**圖 二**、**圖 三**所示。將資料轉成 XML 的格式，會讓封包變得相當大，造成頻寬的浪費。此外，透過應用層將封包轉換成 XML，勢必需要比較多的記憶體去處理。

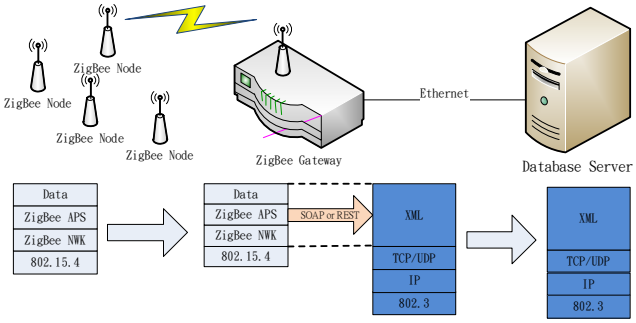


**圖 二：SOAP/REST 機制示意圖**

| | |
|---|---|
| Request XML message | <?xml version="1.0" encoding="UTF-8"?><br><tns:APSMessage<br>xmlns:tns="http://www.zigbee.org/GWGRESTSchema"<br>xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"<br>xmlns:gal="http://www. zigbee.org/GWGSchema"<br>xsi:schemaLocation="http://www.zigbee.org/GWGRESTSchema/<br>rest/rest.xsd http://www.zigbee.org/GWGSchema/rest/gal.xsd "><br><gal:DestinationAddress><br><gal:NetworkAddress>0x0001</gal:NetworkAddress></gal:Desti<br>nationAddress><br><gal:DestinationEndpoint>0x02</gal:DestinationEndpoint><br><gal:SourceEndpoint>0x01</gal:SourceEndpoint><br><gal:ProfileID>0x0104</gal:ProfileID><br><gal:ClusterID>0x0000</gal:ClusterID><br><gal:Data>0102030405060708090a0b0c0d0e0f</gal:Data><br><gal:TxOptions><br><gal:SecurityEnabled>true</gal:SecurityEnabled><br><gal:UseNetworkKey>true</gal:UseNetworkKey><br><gal:Acknowledged>true</gal:Acknowledged><br><gal:PermitFragmentation>true</gal:PermitFragmentation><br></gal:TxOptions><br><gal:Radius>3</gal:Radius><br></tns:APSMessage> |
| Response XML message | <?xml version="1.0" encoding="UTF-8"?><br><tns: APSMessageResult<br>xmlns:tns="http://www.zigbee.org/GWGRESTSchema"<br>xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"<br>xmlns:gal="http://www. zigbee.org/GWGSchema"<br>xsi:schemaLocation="http://www.zigbee.org/GWGRESTSchema/<br>rest/rest.xsd http://www.zigbee.org/GWGSchema/rest/gal.xsd "><br><gal:ConfirmStatus>0x00</gal:ConfirmStatus><br><gal:TxTime>0x01234567</gal:TxTime><br></tns:APSMessageResult> |

**圖 三： REST 機制的 XML 封包**

除了上述兩種常用的作法，還有一種已提出概念但尚未有詳細定義細節的方法為閘道遠端介面協定(Gateway Remote Interface Protocol, GRIP)[5]，如**圖 四**。不同於 SOAP 和 REST 利用文字去進行存取控制，GRIP 主要的運作方式為在傳輸層上訂定一個透過位元轉換的協定，用來轉換 ZigBee 封包的內容。因為轉換部份是利用位元來定義，所以相對於利用文字來控制，能節省較多的頻寬。

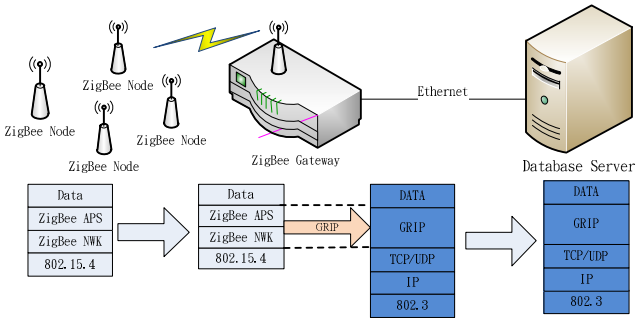


**圖 四：GRIP 機制示意圖**

因此，本論文仿照 GRIP 的設計，提出一個閘道轉換器的架構設計如**圖 五**，藉由此轉換閘道器讓 ZigBee 網路和資料庫伺服器能夠互相傳送資訊。它的運作的方式偏向上述的第三種方式，透過一個映射對照表來轉換 ZigBee/802.15.4 和 TCPIP/802.3 兩者之間的協定。透過此方法，將本來 ZigBee 的封包轉換成 Ethernet 封包之後，就能將封包透過已經佈建好的 Ethernet 網路設施傳送到資料庫伺服器。此方法和第一種相比，優點為在 ZigBee 閘道器將需要保留的資訊存入映射對照表中，然後將原先存在於 ZigBee 網路但在 Ethernet 中不必要的資訊移除，以節省頻寬的使用。而和第二種方法相比，第二種方法無論是採用 SOAP 或是 REST，因為將資料轉換為 XML 格式，其封包大小都會比原先的資料量大上很多，佔用比較高的頻寬；同時讀取 XML 格式，也需要花費比較高的運算能力。故本論文所提出的方法可節省較多頻寬。

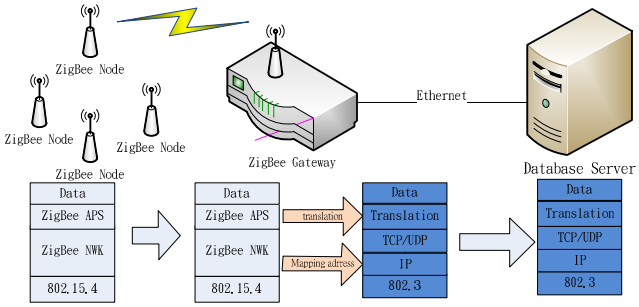


**圖 五：閘道器示意圖**

## 二、 背景知識

### 2.1 ZigBee

ZigBee 建立於 IEEE802.15.4 之上，定義主要的兩層通訊協定：網路層和應用層。分成三種網路節點：ZigBee 協調者(coordinator)、ZigBee 路由器、ZigBee 末端裝置。提供三種拓撲方式：星狀拓撲(star)、樹狀拓撲(tree)、網狀拓撲(mesh)。

網路層主要的工作為：加入或離開某個網路、提供封包安全性的處理、傳送封包到目標節點、找尋且維護節點的最佳路徑、搜尋鄰居節點並儲存其資訊、建立網路(協調者工作)、設定網路參數(協調者工作)、分配網路位址(協調者工作)。

應用層則可細分為應用程式支援子層(Application Support Layer)、應用程式框架(Application Frame)、ZigBee 裝置管制物件(ZigBee Device Object)。APS 子層

主要負責上層應用程式與下層網路層的協調，並維持物件之間的連結表。

### 2.2 IPv6

為了讓 Ethernet 和 ZigBee 網路互通，我們需要建構一個彼此都能通用的網路位址，所以每個 ZigBee 節點都需要一個對應的 IP 位址，而資料庫伺服器則需要一個 ZigBee 網路位址。因為 ZigBee 的網路節點相當多，加上 ZigBee 網路位址為 16 位元，若在網路層選用 IPv4，在位址的對應上較無彈性，所以在我們的設計中，網路層採用 IPv6 協定， 在此節略為說明 IPv6 的起源和特色。

由於現今網際網路的規模不斷成長，且成長速度超過當初所預期，加上近年來許多新的網路應用和無線網路的推陳出新，導致 IP 位址的數量明顯不足。根據 IANA 和 RIR 的統計，IPv4 位址將於 2011 年發放完畢，因此新一代的 IP 協定—RFC 2460 (Internet Protocol Version 6)因應而生。

IPv6 除了解決位址空間的不足之外，更簡化了過去 IPv4 未使用的標頭。IPv6 有以下的特點：

1. 位址長度由 32 位元延伸為 128 位元
2. 基本標頭從可變長度轉變為固定 40 位元組
3. 無狀態自動配置(Stateless Auto-configuration)
4. 加入 IPsec 以增加傳輸安全性
5. 新加入 Anycast

## 三、 現有方法

先前已有數個如何讓 IPv6 和 ZigBee 互相轉換的設計方法[6]，論文[7]則是將 ZigBee 的資料，自行定義一個標頭，將 ZigBee 的部份資訊放入此標頭，利用此方式來達到 ZigBee 和 IPv4 的互通。該論文雖有提出位址映射的機制，但在標頭中卻無轉換後位址的欄位，且由其測試數據中可以發現，實際上 ZigBee 和 IPv4 互通的方法並不是使用位址映射機制。此外，測試過程和結論都未提及是否能夠支援多個 IPv4 節點。

另一篇論文[8]最主要的解決方法是透過一個類似動態網域名稱的系統，讓所有 802.15.4 節點和 IPv6 節點都分別得到相對應的 IPv6 位址和 802.15.4 位址，使 IEEE 802.15.4 節點和 IPv6 節點能夠互相存取。但此論文僅說明了如何利用此系統得到相對應的位址，至於轉換器收到 IPv6 的群播封包會如何處理，以及 IPv6 節點如何向 ZigBee 的網路調節者發送註冊封包等問題，都未被提及。

論文[9]提出了 802.15.4 和 IPv6 的位址映射表和映射規則如**圖 七**，並加入簡單服務發現協定(Simple Service Discovery Protocol, SSDP)的機制，來完成 802.15.4 節點和 802.3 節點的互通。對於 IPv6 節點如何加入 ZigBee 網路同樣沒有詳細的說明，也沒有說明是否能使用 ZigBee 應用層中群組播送的功能。

## 四、 提出方法

本論文提出一個透過位址映射、協定轉換、訊息型別 (Message Type)，且支援 ZigBee 網路中 Groupcast/Multicast 的閘道器。

設計此閘道器將會面臨以下幾個問題：位址轉換、兩個不同的協定如何發送和處理群播封包、802.3 和 802.15.4 的負載大小不相同等。

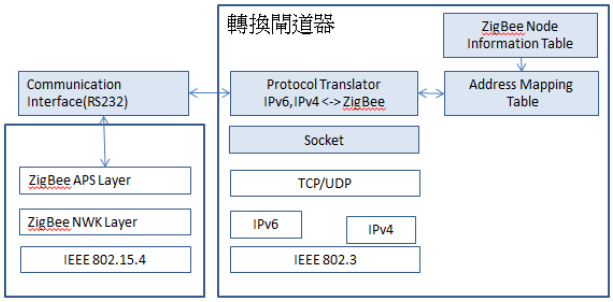


**圖 六：轉換閘道器系統架構圖**

### 4.1 位址轉換

為了讓 ZigBee 的網路節點和 IPv6 節點能夠互相溝通，需要設計一個機制，讓 ZigBee 節點能擁有對應的 IPv6 位址。位址轉換機制大致上和**錯誤！找不到參照來源。**所提出的方法雷同，不同之處在 **4.2** 小節會加以說明。

每個 ZigBee 裝置出廠時，都會擁有一個唯一的、由 IEEE 組織所規範及發配的 64 位元 ZigBee 延伸位址(Extended Address)/MAC 位址，我們根據 IPv6 中的位址前綴(prefix)(64 位元)再加上 ZigBee 的延伸位址(64 位元)，即可成為一個 IPv6 位址(128 位元)。如**圖 七**所示。

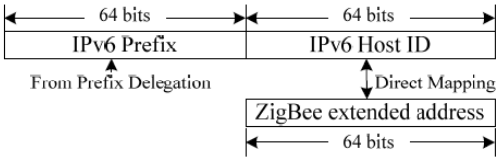


**圖 七：IPv6 位址分配至 ZigBee 節點**

### 4.2 群體播送(Multicast)

ZigBee 和 IPv6 各自有群體播送的機制，為了避免互相干擾，且避免讓 IPv6 中的過多的群體播送封包造成 ZigBee 網路癱瘓，此閘道器不適合將兩邊群體播送的功能直接轉換並傳送，故本論文提出的構想為，讓兩邊的功能獨立，當 IPv6 節點需要發送 ZigBee 群體播送封包時，則發送到一個特定位址，閘道器辨認此封包為本文定義的特定位址，再轉發群體播送封包給 ZigBee 節點。而 IPv6 網路中的群體播送封包則不進行轉換。

實際的位址轉換規則，也是雷同 **4.1** 的方法，將 ZigBee 特定的群體播送位址如：FFFF、FFFD…等，進行位址轉換。如此一來，IPv6 節點就能透過發送封包給此位址達到發送 ZigBee 群體封包功能。

| 64bits | 32bits | 32bits |
|---|---|---|
| IPv6 Prefix | 0..0 | PANID:FFFF |
| IPv6 Prefix | 0..0 | PANID:FFFD |
| IPv6 Prefix | 0..0 | PANID:FFFC |

。

**圖 八：特定 IPv6 位址**

### 4.3 負載大小不相同

根據 IEEE 802.15.4 標準，802.15.4 的 MTU(Maximum Transmission Unit)為 127 位元組，再扣掉 ZigBee 各層所使用的基本標頭大小，所剩下的負載空間最長也僅有 102 位元組。而 802.3 所提供的 MTU 大小為 1492，兩者差距甚大。因此會有分割和組合封包的問題，雖然在目前的應用中，伺服器端也就是 IPv6 端所發送的訊息大多為控制訊號，封包長度並不會超過 127 位元組，但難保未來不會有其它應用的封包長度會超過 127 位元組。所以如何將封包有效地分割並重組，也是未來閘道器所需要的功能之一。本論文主要專注於先讓 ZigBee 和 IPv6 網路能夠互通，故暫時將此問題留至未來改善。

### 4.4 訊息型別

綜合 4.1、4.2，ZigBee 已經有了 IPv6 位址，伺服器端也已經可以發送資料給 ZigBee 節點，甚至是 ZigBee 群體播送封包。接下來說明如何讓 ZigBee 節點認識 IPv6 節點，本論文在原先的傳輸資料中加入一個長度為 1 位元組 MT(Message Type)，根據此 Message Type 來決定所發送的封包為何。透過此方式，除了原先閘道器預設的伺服器之外，可以透過命令讓其它伺服器加入，並分配一個 2 位元組長度的位址給伺服器，讓 ZigBee 以此位址來分辨不同的伺服器。並擁有較彈性的空間供 ZigBee 支持應用層的其它功能，如 Group、Endpoint 等。

**表 I： Basic Message Type**

| Basic Message Type | Description | Example |
|---|---|---|
| add short & extended address | Add a new address in the a mapping table | MT + Short addr. + extended addr. |
| Add Server | Add a new server in gateway | MT + Server addr(2Byte) |
| Send packet | Send general packet | MT + Server addr + data |
| Send Groupcast | Send Groupcast packet | MT + Group + Server addr + data |

### 4.4 封包傳遞

**圖 九**和**圖 十**分別說明封包如何透過閘道器在 ZigBee 和 IPv6 裝置之間傳送，我們假設 ZNA(ZigBee Node A)的 802.15.4 短位址(Short address) 為 ZNASA、IPv6 位址為 ZNAV6，ZG(Zigbee Gateway)的 802.15.4 短位址為 ZGSA、IPv6 位址為 ZGV6，DS(Database Server)的 802.15.4 短位址為 DSSA、IPv6 位址為 DSV6，**圖 十**中的 FFFDV6 為 **4.2** 所提到的特殊位址，用來發送 ZigBee 群體廣播封包，若 MT 設定為 Send Groupcast 如**表 I**，可讓伺服器發送群組廣播封包。

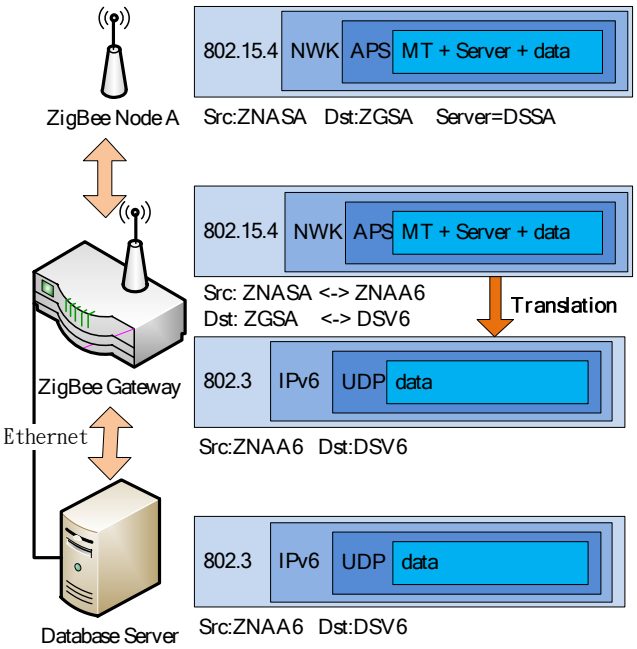


**圖 九: ZigBee 節點和 IPv6 伺服器傳送封包流程**

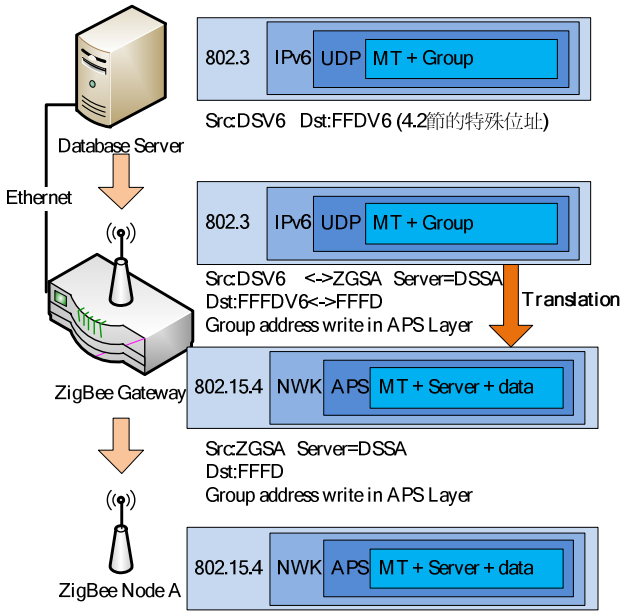


**圖 十：伺服器發送群組播送封包至 ZigBee 網路**

## 五、 結論及未來展望

### 5.1 結論

實驗所使用的平台為德州儀器的 CC2530ZDK (ZigBee Development Kit)和作業系統為 Linux 的電腦。將 CC2530 的無線射頻模組透過 RS232 介面和電腦作為溝通介面。協定轉換器主要會在 Linux 系統上開發，ZigBee 的部份，例如發送 802.15.4 封包的動作則在 CC2530ZDK 的實驗模組板上修改。

現階段尚在 Linux 系統上進行協定轉換器的實作，預計轉換器完成後，此轉換器能夠自動分配一個 IPv6

位址給每一個加入此網路中的 ZigBee 設備，而伺服器端能直接發送目的地為 ZigBee 設備的 IPv6 address 的封包，完成互相溝通的管道。相較市面上的閘道器做法，其封包是以閘道器為目的端，經由閘道器去分析封包中的 802.15.4 位址後再進行轉發，傳送效率可大幅改善。更可進一步改善使用通道機制或是 SOAP、REST 機制所造成頻寬浪費的問題，並能降低閘道器工作負擔。未來希望能將此轉換閘道器整合為嵌入式 Linxu 系統，運用最少的硬體資源達到更好的效能。

## 5.2 未來展望

由於現階段在 Linux 系統上，尚未有完全支援 ZigBee 協定的開放源碼，使得開發閘道器上部份功能有所限制，未來如有更完善的資源，讓 ZigBee 整套協定在 Linux 系統上運作，就能更方便解決目前尚未處理完善的問題，例如在 4.3 節所提到的分割重組的問題、支援更多 ZigBee 應用層的功能、或是讓單一 ZigBee 節點接受多個不同目的端位址的封包…等。

無線網路和有線網路的結合，不管應用於哪一種無線網路，閘道器都扮演著舉足輕重的角色，希望藉由此論文，能啟發後人對於閘道器更多功能的設計與應用。

## 參考文獻

[1] ZigBee Alliance, “ZigBee Specifications”, ZigBee Document 053474r17, November 2009.
[2] 藍浩益「無線感測網路百家爭鳴 傳輸品質與分工架構」，新通訊元件雜誌，2006，第 61 期，53-57
[3] 雲漢，「善用 ZigBee 雙向溝通特性 智慧電網加速普及」，新通訊元件雜誌，2010，第 108 期，25-31
[4] Smart Dust - Autonomous sensing and communication in a cubic millimeter, http://robotics.eecs.berkeley.edu/~pister/SmartDust/
[5] ZigBee Alliance, “Understanding ZigBee Gateway”, ZigBee Document 095465r13, September 2010.
[6] Md. Sakhawat Hossen, A. F. M. Sultanul Kabir, Razib Hayat Khan, Abdullah Azfar, “Interconnection between 802.15.4 Devices and IPv6: Implications and Existing Approaches”, International Journal of Computer Science Issues, IJCSI, Vol. 7, Issue 1, No. 1, January 2010
[7] Guozhen Hu, “Design and Implementation of Industrial Wireless Gateway Base on ZigBee Communication”, The Ninth International Conference on Electronic Measurement & Instruments (ICEMI’2009), Beijing, China.
[8] S Sakane, Y Ishii, K Toba, K Kamada, N Okabe, “A translation method between 802.15.4 nodes and IPv6 nodes”, International Symposium on Applications and the Internet (SAINT) Workshops, 2006.
[9] RC Wang, RS Chang, HC Chao, “Internetworking Between ZigBee/802.15. 4 and IPv6/802.3 Network”, SIGCOMM Data Communication, 2007