國立暨南國際大學通訊工程研究所

碩士論文

具有群播功能的 ZigBee/802.15.4 和 IPv6/802.3 閘道器之設計與實作

Design and Implementation of a Translator Between ZigBee/802.15.4 and IPv6/802.3 with Groupcast/Multicast Support

指導教授：吳坤熹 博士

研究生：葉俊克

中華民國：一◯◯年七月

國立暨南國際大學通訊工程研究所

碩士論文

具有群播功能的 ZigBee/802.15.4 和 IPv6/802.3 閘道器之設計與實作

Design and Implementation of a Translator Between ZigBee/802.15.4 and IPv6/802.3 with Groupcast/Multicast Support

指導教授：吳坤熹 博士

研究生：葉俊克

中華民國：一〇〇年七月

國立暨南國際大學碩（博）士論文考試審定書

通 訊 工 程 研 究 所

研究生　**葉俊克**　所提之論文

具有群播功能的 ZigBee/802.15.4 和 IPv6/802.3 閘道器之設計與實作

Design and Implementation of a Translator Between ZigBee/802.15.4 and IPv6/802.3 with Groupcast/Multicast Support

(中、英文題目)

經本委員會審查，符合碩（博）士學位論文標準。

學位考試委員會

溫志彥　委員兼召集人

王忍成　委員

吳坤熹　委員

中　華　民　國　100　年　7　月　29　日

致謝

在暨大這片好山好水的美麗校園中，不知不覺已經度過了二年的研究生生活。然而美好且令人憧憬的校園生活終究要告一段落，此刻即將離開校園，踏上新的旅程，迎接新的挑戰。

能夠在兩年內順利的完成碩士論文，首先要感謝我的指導教授吳坤熹老師對於我在碩士班兩年以來的指導與照顧。除了學術方面的研究之外，更不斷地教導我在面對難題或困境該有的態度及解決的方法，使我在專業領域與為人處世上都收穫良多。另外要感謝實驗室的所有成員，不管是去年已畢業的學長姊、今年一同畢業的同學、以及即將要升上碩二的學弟妹；每當我研究遇上困惑時，大家都能夠給予我適時的幫助，使我看清自己研究時的盲點，並且讓我的碩士生涯更加多采多姿。

最後要感謝我的家人，一直在背後默默付出並且給予我最大的支持與照顧，讓我能無後顧之憂地順利完成碩士的學業。

論文名稱：具有群播功能的 ZigBee/802.15.4 和 IPv6/802.3 閘道器之設計與實作

校院系：國立暨南國際大學科技學院通訊工程研究所　　頁數：41

畢業時間：一百年/七月　　學位別：碩士

研究生：葉俊克　　指導教授：吳坤熹博士

中文摘要

本論文實作一個轉換器，讓 ZigBee 節點能透過此轉換器和 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。過去的轉換器多半將 ZigBee 資料直接封裝在 IP 封包內傳送到 Internet 上，也因此侷限了 ZigBee 設備透過此一轉換器僅能與一部伺服器通訊的限制。此外，過去的設計缺乏群播的功能；當伺服器要送出指令給多個 ZigBee 節點時，必須由伺服器送出一個指令給轉換器；轉換器理解這個命令後，再逐一送出指令給各個 ZigBee 設備。為了改善以上缺點，本論文中設計了一個新的轉換器，採用位址映射和協定轉換的方式，讓兩端裝置進行溝通，並且善用 ZigBee 網路中的群播機制，讓伺服器端具有發送 Broadcast、Multicast、Groupcast 封包的功能。

關鍵字：IPv6、ZigBee、位址映射、協定轉換、轉換器

Title of Thesis: Design and Implementation of a Translator Between ZigBee/802.15.4 and IPv6/802.3 with Groupcast/Multicast Support

Name of Institute: Institute of Communication Engineering, College of Science and Technology, National Chi Nan University Page : 41

Graguation Time : 7/100 Degree Conferred : Master

Student Name : Jyun-Ke Ye Advisor Name : Dr. Quincy Wu

Abstract

This thesis describes the implementation of a translator between a ZigBee/802.15.4 network and an IPv6/802.3 network, so that the two networks can communicate through this translator. The data collected from the ZigBee sensor network are transmitted to an IPv6/802.3 server. Existing translators which allow ZigBee/802.15.4 devices to communicate with IPv6/802.3 devices usually encapsulate ZigBee data as the payload of IP packets, thus limit the destination to a single server on the Internet. Moreover, past design of translators did not incorporate the multicast mechanism. If a server wants to send a command to multiple ZigBee devices, it must send a command to the translator; after the translator recognizes the command, it will then send commands to individual ZigBee devices. To solve the aforementioned problems, our approach adopts address mapping and protocol translation to reduce the overall packet size. Furthermore, by elaborating the multicast mechanism in ZigBee, our translator allows IPv6/802.3 servers to send Multicast and Groupcast packets to reach a group of ZigBee devices.

Keywords: Address Mapping, IPv6, Protocol Translation, Translator, ZigBee

目錄

致謝 ..... **I**

中文摘要 ..... **II**

Abstract ..... **III**

目錄 ..... **IV**

圖目錄 ..... **VII**

表目錄 ..... **IX**

第一章　緒論 **1**

1.1　簡介 1

1.2　研究動機與目的 2

第二章　背景知識及相關研究 **4**

2.1　轉換器 4

2.2　IEEE 802.15.4 4

2.3　ZIGBEE 7

2.4　INTERNET PROTOCOL - IPV4 AND IPV6 8

2.5　IP/ZIGBEE 轉換器 10

2.6　SOAP/REST 轉換器 12

2.7　傳播機制和服務發現 14

2.7.1　Unicast 14

2.7.2　Broadcast 14

2.7.3　Multicast 15

2.7.4 Groupcast 16
2.7.5 服務發現機制（Service Discovery） 17
2.8 IPv6/ZigBee 轉換器 18
第三章 Message Control Multicast Translator 21
3.1 MCMT 設計需求 21
3.2 位址轉換 22
3.3 Broadcast 位址/群組位址 22
3.4 負載大小不相同 23
3.5 訊息型別（Message Type, MT） 24
3.6 與現有方法比較 24
第四章 系統架構與實作 26
4.1 系統架構 26
4.2 系統平台 27
4.3 運作流程 28
4.3.1 ZigBee 節點加入網路 28
4.3.2 封包傳送過程 30
4.3.3 群播封包傳送過程 31
4.4 實作結果 32
4.4.1 Unicast 33
4.4.2 Broadcast 34
4.4.3 Multicast/Groupcast 35
第五章 結論及未來方向 38
5.1 結論 38

5.2 未來方向 38

參考文獻 40

圖目錄

圖 1 ZIGBEE 透過通訊介面示意圖 3
圖 2 ZIGBEE 透過 ETHERNET 傳送資訊 3
圖 3 ZIGBEE/IP 轉換器示意圖 4
圖 4 ZIGBEE 協定架構圖[1] 5
圖 5 GENERAL MAC 標頭格式 7
圖 6 網路拓撲圖 8
圖 7 IPV4 封包格式[6] 10
圖 8 IPV6 封包格式[6] 10
圖 9 定義標頭格式[7] 11
圖 10 ZIGBEE 和 ETHERNET 封包[7] 11
圖 11 SOAP/REST 轉換器示意圖 12
圖 12 REST 機制的 XML 封包[8] 13
圖 13 MULTICAST 控制欄位 15
圖 14 THE EFFECT OF RADIUS IN ZIGBEE MULTICAST 16
圖 15 ZIGBEE GROUPCAST 17
圖 16 IPV6 位址分配至 ZIGBEE[10] 18
圖 17 從 ZIGBEE/802.15.4 傳送資料至 IPV6/802.3[10] 19
圖 18 利用兩台轉換器橋接 ZIGBEE 網路的傳輸流程[10] 20
圖 19 MCMT 系統圖 21
圖 20 MCMT 模組圖 27
圖 21 平台與系統模組對照圖 28
圖 22 (A) DEVICES JOIN THE ZIGBEE NETWORK (B) MAPPING TABLE ON THE COORDINATOR 29

圖 23 ZIGBEE 裝置 IPV6 定址方式 30
圖 24 UNICAST 傳輸過程 31
圖 25 MULTICAST/GROUPCAST 傳輸過程 32
圖 26 裝置位址示意圖 33
圖 27 伺服器接收與發送畫面 33
圖 28 UNICAST ETHERNET 封包截取圖 34
圖 29 UNICAST ZIGBEE 封包截取圖 34
圖 30 伺服器 發送 ZIGBEE BROADCAST 畫面 35
圖 31 BROADCAST ETHERNET 封包截取圖 35
圖 32 BROADCAST ZIGBEE 封包截取圖 35
圖 33 伺服器 發送 ZIGBEE MULTICAST/GROUPCAST 封包 36
圖 34 MULTICAST ETHERNET 封包截取圖 36
圖 35 MULTICAST ZIGBEE 封包截取圖 36
圖 36 GROUPCAST ETHERNET 封包截取圖 37
圖 37 GROUPCAST ZIGBEE 封包截取圖 37
圖 38 伺服器發送 MULTICAST 給多個 ZIGBEE 網路 39

表目錄

表 1　802.15.4 的頻譜特性 6

表 2　GROUP TABLE 17

表 3　ZIGBEE 裝置對應的 IPV6 位址 22

表 4　轉換表中特定 IPV6 位址 23

表 5　MESSAGE TYPE 24

表 6　各方法比較表 25

第一章　緒論

1.1　簡介

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 ZigBee/IEEE 802.15.4 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，需具備自行重建網路功能。
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（infrastructure）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）。

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，是值得深入研究的議題。

1.2 研究動機與目的

目前在實務上，大多數採用較簡單的方法，直接將資料儲存在負責收集的裝置，再將資料透過其它通訊方式轉傳（如 FTP、RS232、USB 等），容易造成佈建上的限制。

圖 1 說明負責收集資訊的網路節點 ZigBee Data Collector，透過通訊介面送至資料庫。此做法直接讀取 ZigBee 封包的內容，但會有幾個功能上的限制。首先採用 FTP 傳送的方式，需先將資料存成檔案，再透過 FTP 傳送到伺服器，因此無法達到即時通訊的功能；其次若是採用 RS232、USB 這類的傳送方式，則資料庫伺服器和 ZigBee Data Collector 之間的距離，不可超過傳輸線所能連接的距離（通常在 15 公尺以內），因此造成佈建網路時的擺放限制。

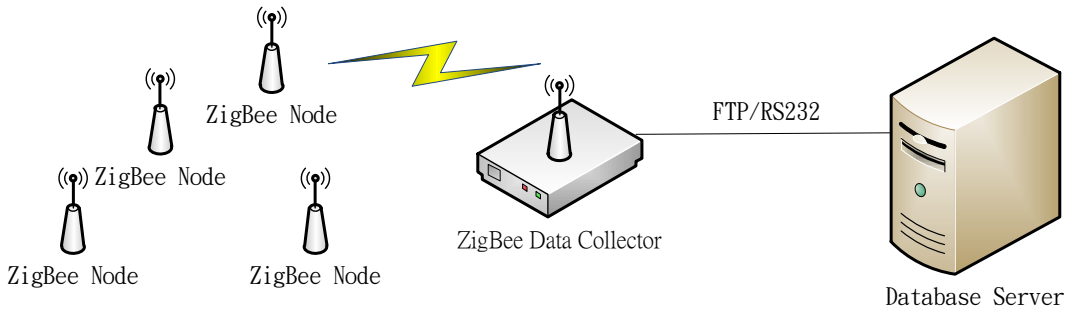


圖 1　ZigBee 透過通訊介面示意圖

且不談在戰場上的應用，即使在一般社區及住宅佈建無線感測網路時，負責收集資料的伺服器通常不會擺放在用戶家中，而是擺在較為安全且外人不能輕易接觸的地方，再藉由通訊網路接收感測器所傳回的資料。由於許多的建築或是大樓，大多早已建置 Ethernet 網路。因此較佳的設計方式，是透過既有的 Ethernet 網路進行通訊。如此可使佈建無線感測網路時能有更大的彈性，而且能與 Internet 上的網路應用結合。如何讓無線感測網路節點和網際網路中的資料庫伺服器互相通訊，便是本篇論文探討的重點。

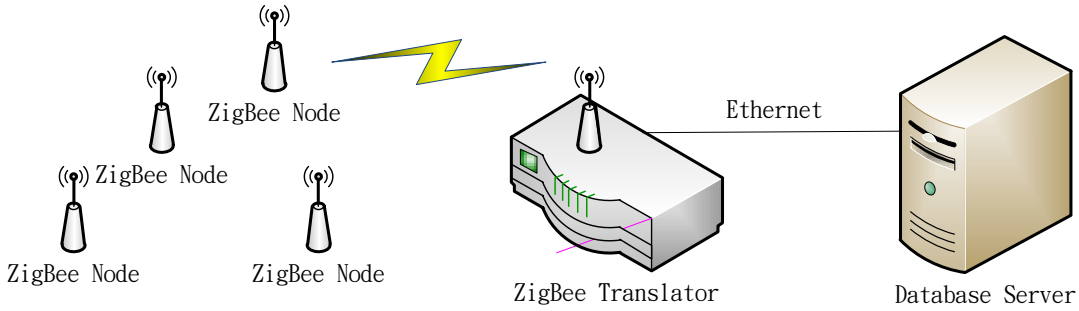


圖 2　ZigBee 透過 Ethernet 傳送資訊

第二章　背景知識及相關研究

2.1　轉換器

因為 ZigBee 與 TCP/IP 採用完全不同的通訊架構，所以這兩種不同的通訊協定無法直接溝通。為了使異質網路能互相通訊，需要透過一個機制，將不同的通訊協定互相轉換，一般稱有此功能的裝置為轉換器或閘道器。

圖 3 左半邊框框中所標示的部份為 ZigBee 網路，如果希望 ZigBee 網路節點能和圖中右邊位於 TCP/IP 網路中的伺服器通訊，則需要藉助轉換器；透過轉換器將兩邊的協定轉換後，即可讓 ZigBee 裝置和伺服器通訊。

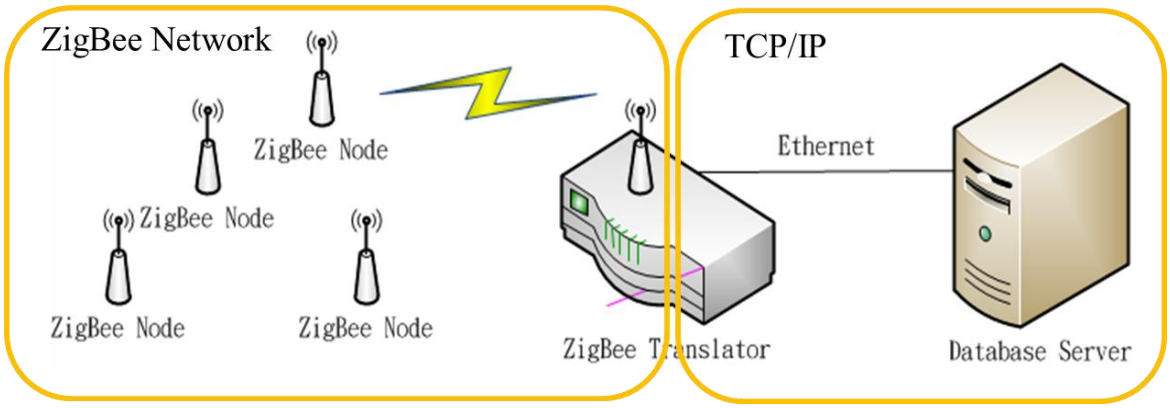


圖 3　ZigBee/IP 轉換器示意圖

2.2　IEEE 802.15.4

IEEE 802.15.4 是 IEEE 對於低速率、低功率傳輸的無線個人區域網路所訂定的標準，此標準定義了在 OSI 七層中的實體層和資料鏈結層。ZigBee 則是由 ZigBee Alliance 所提出，位於 IEEE802.15.4 通訊標準的上層。其架構略如圖 4 所示。主要的特色有：低功率、低速率、低成本、容易佈建。

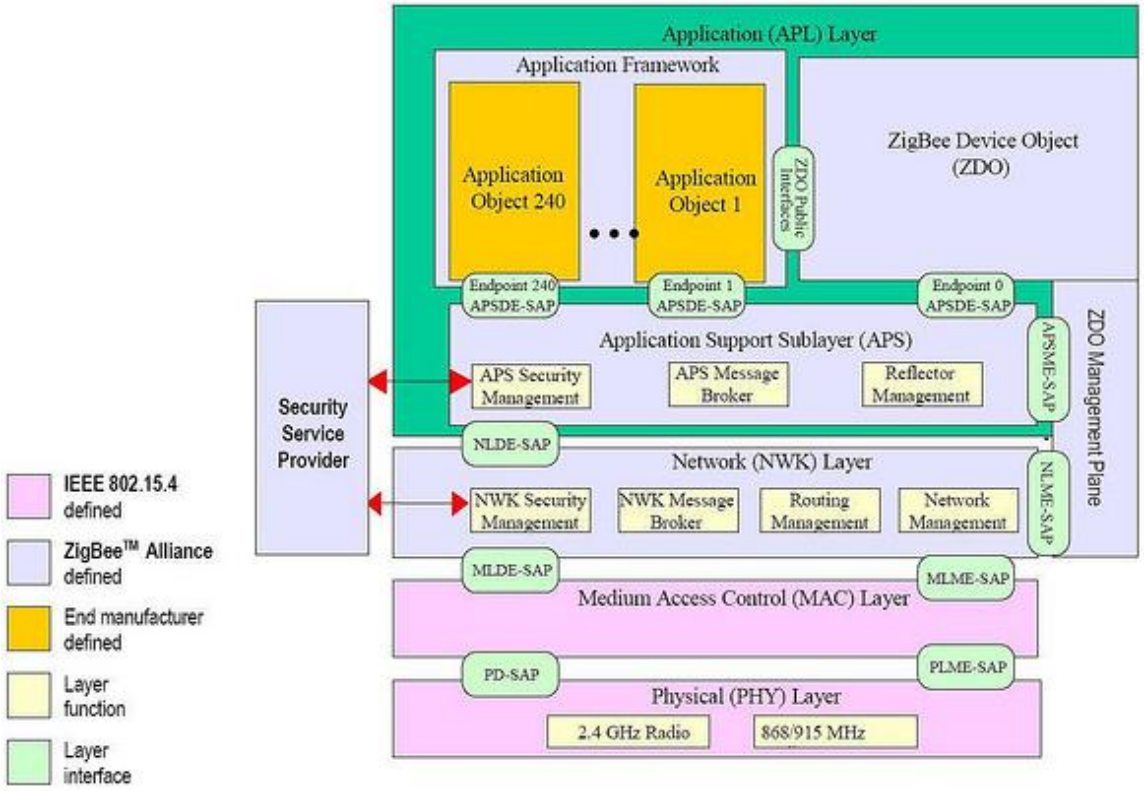


圖 4　ZigBee 協定架構圖[1]

實體層定義了物理特性、使用頻段、傳輸速度、傳輸距離等。表 1 說明可使用的頻段主要分為三種，分別為歐洲所使用的 868MHz 頻段、美國所使用的 915MHz 頻段、臺灣和世界通用的 2.4GHz 頻段。而各個頻段所使用的通道數量與傳輸速率為：868MHz 提供一個通道，傳輸速率為 20Kbps；915MHz 提供十個通道，傳輸速率為 40Kbps；2.4GHz 提供 16 個通道，傳輸速率為 250Kbps，理想傳輸距離為 100 公尺。實體層的協定並且提供下列功能：1. 計算連線品質 （Link Quality Indication）、2.能量偵測（Energy Detection）。

表 1　802.15.4 的頻譜特性

頻帶 MHz	頻率範圍 （使用地區）	通道數目	DSSS 調變	傳輸速率 bits per second
868	868~868.6MHz （歐洲）	1	BPSK	20
915	902~928 MHz （美國）	10	BPSK	40
2450	2400~2483.5MHz （全球）	16	OQPSK	250

資料鏈結層（或稱媒體存取控制層）提供了通道選擇機制、裝置種類、框架結構、安全機制。

IEEE 8022.15.4 提供了偵測頻道內各通道訊號強度的功能，讓最初建立網路時，能夠選擇較不易受其它訊號干擾的通道，以增加傳輸的穩定性。

IEEE 802.15.4 定義了兩種裝置種類：(1) 全功能裝置 FFD（Full Function Device），此裝置能夠成為此無線個人區域網路的協調者（Coordinator）或是路由器 (Router)。協調者負責建立此無線網路，並允許其它裝置加入此網路；路由器則負責尋找、建立以及維護路由並轉發封包。(2) 精簡功能裝置 RFD（Reduced–Function Device），一般為網路中的末端裝置，並無建立網路的功能。

IEEE 802.15.4 定義了四種框架結構：信標框架（Beacon Frame）、資料框架（Data Frame）、許可框架（Acknowledgment Frame）、命令框架（Command Frame）。 安全機制則提供了 AES-CBC-MAC-128、AES-CTR、AES-CCM-128 等加密機制。圖 5 所示為 MAC 標頭格式；值得注意的是其封包總長度限制為 127 位元組。

127 Octets							
Octets:2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	Frame check sequence
		Addressing fields					
MAC header						**MAC payload**	**MAC footer**

圖 5　General MAC 標頭格式

2.3 ZigBee

ZigBee 建立於 IEEE802.15.4 之上，定義主要的兩層：網路層和應用層。分成三種網路節點：ZigBee 協調者 （Coordinator）負責建立 ZigBee 網路，並設定各項網路參數；ZigBee 路由器 （Router）負責維護路由和轉發封包；ZigBee 末端裝置 （End Device）不會轉發封包，具有休眠功能。

ZigBee 網路最先由 ZigBee 協調者建立，在建立網路的同時，會指定一組十六位元的個人區域網路識別號（Personal Area Network Identifier, 簡稱 PAN ID）來代表此網路；同一個 ZigBee 網路中只允許存在一個協調者。其它 ZigBee 裝置則向協調者發出加入網路的請求；加入後，會取得 PAN ID 和由協調者配置的十六位元短位址（short address），ZigBee 裝置彼此間藉由此位址互相通訊。

ZigBee 提供三種拓撲方式：星狀拓撲 （Star）、樹狀拓撲（Tree）、、網狀拓撲（Mesh），如圖 6 所示。

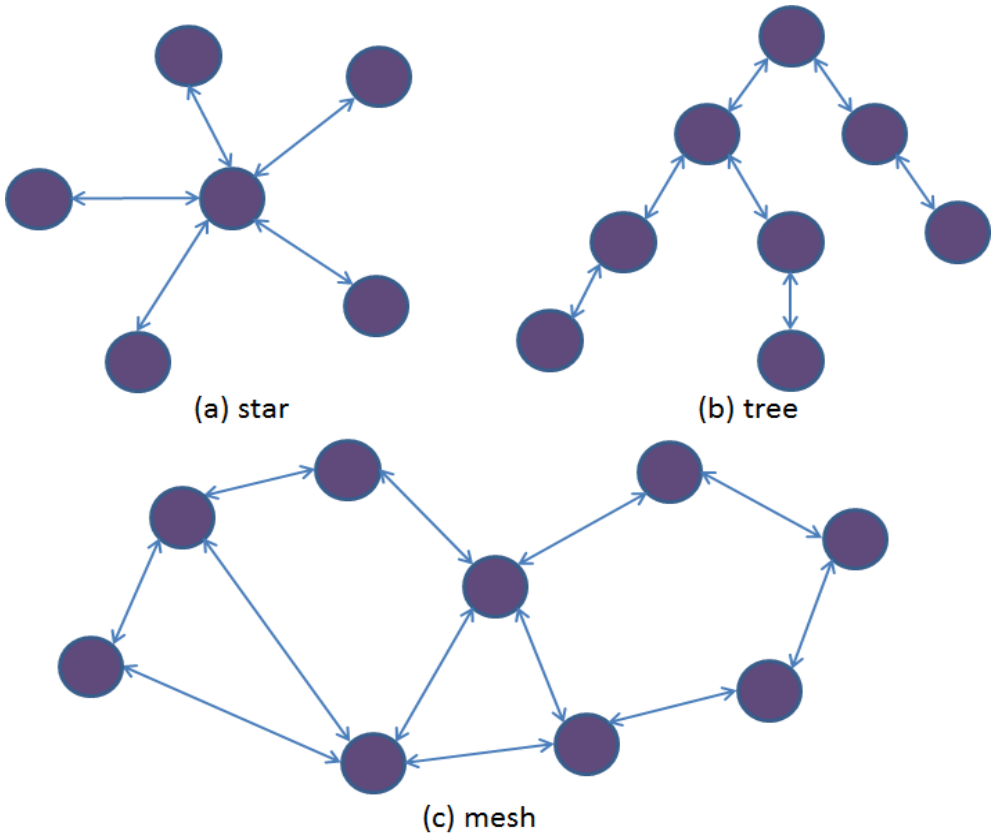


圖 6　網路拓撲圖

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、找尋且維護節點的繞徑路線、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, APS）、應用程式框架（Application Frame, AF）、ZigBee 裝置管制物件（ZigBee Device Object, ZDO）。

APS 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。

AF 提供 1-240 的 Endpoint（類似 TCP 協定中的 port）。

ZDO 提供 Device Discovery、Service Discovery、保密控管、網路控管等服務。

2.4　Internet Protocol - IPv4 and IPv6

在 TCP/IP 架構中，無論使用有線或無線網路，只要指定一個 IP 位址，即可正確地將資料送達目的地。在圖 2 的轉換器設計中，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。在這個原則下，我們分配給每個 ZigBee 節點一個對應的 IP 位址，反之資料庫伺服器亦配有一個 ZigBee 網路位址。如此一來，從資料庫伺服器的觀點，每個感測器節點看起來都像個 IP 裝置；而從感測器節點的觀點來看，伺服器就像是個它們可以直接通訊的 ZigBee 裝置。

網路層相對應的通訊協定有 IPv4 和 IPv6 新舊兩種版本。由於 IPv4 位址長度僅 32 位元，若在網路層選用 IPv4，要和 ZigBee 的 16 位元位址對應就較無彈性空間。為了讓大量 ZigBee 網路節點能對應全球位址，在本論文的設計中，網路層採用 IPv6 協定。下一段簡介 IPv6 的起源和特色。

由於現今網際網路的規模不斷成長，且成長速度超過設計之初所預期，加上近年來許多新的網路應用和行動通訊的蓬勃發展，導致 IP 位址的數量快速耗盡。根據 Internet Assigned Numbers Authority (IANA)的統計，IPv4 位址已於 2011 年 2 月發放完畢，因此新一代的 IP 協定—Internet Protocol Version 6 在未來預料將會取代 IPv4 成為網際網路的主流通訊協定[5]。

IPv6 除了要解決位址空間的不足之外，更簡化了過去 IPv4 未使用的標頭，如圖 7 所示。IPv6 有以下的特點：

1. 位址長度由 32 位元延伸為 128 位元，提供了大量的地址。
2. IPv6 將 IPv4 的基本標頭從可變長度轉變為固定 40 位元組（如圖 8 所示），可增加硬體處理封包速度。
3. 提供無狀態自動配置（Stateless Auto-configuration）機制，管理上更容易。
4. 加入 IPsec 以增加傳輸安全性。

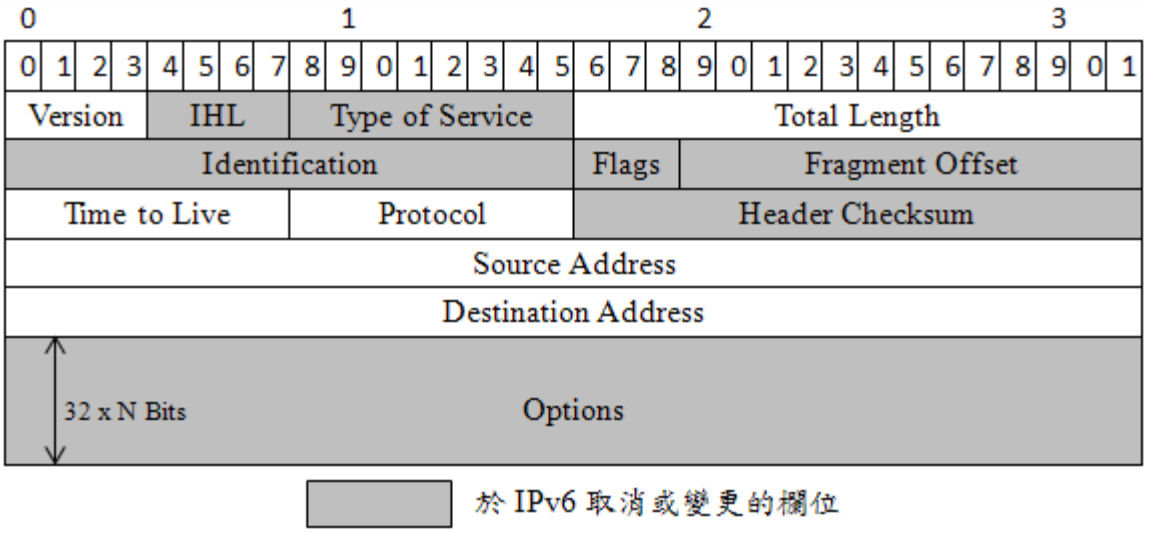


圖 7　IPv4 封包格式[6]

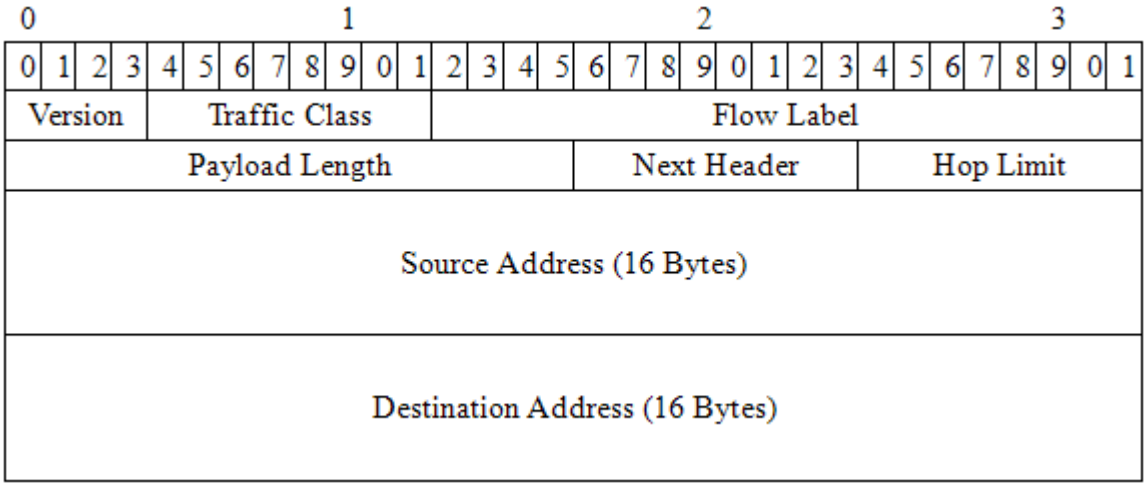


圖 8　IPv6 封包格式[6]

2.5　IP/ZigBee 轉換器

過去有不少 IP/ZigBee 轉換器的設計。論文[7]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。透過將 ZigBee 裝置的短位址填入自己定義的 Payload 格式（圖 9 的 Short Address 欄位），使轉換後的 UDP Payload 也能包含此資訊。但由於暫無提出 IPv4 裝置對應 ZigBee 短位址的方式，目前只能達到 ZigBee 裝置和單一的 IPv4 裝置互通。此論文的優點為只要標頭定義明確，是一個易於實現的方法；但也因為封裝標頭，在有限的 ZigBee Payload 中，占用了太多空間。

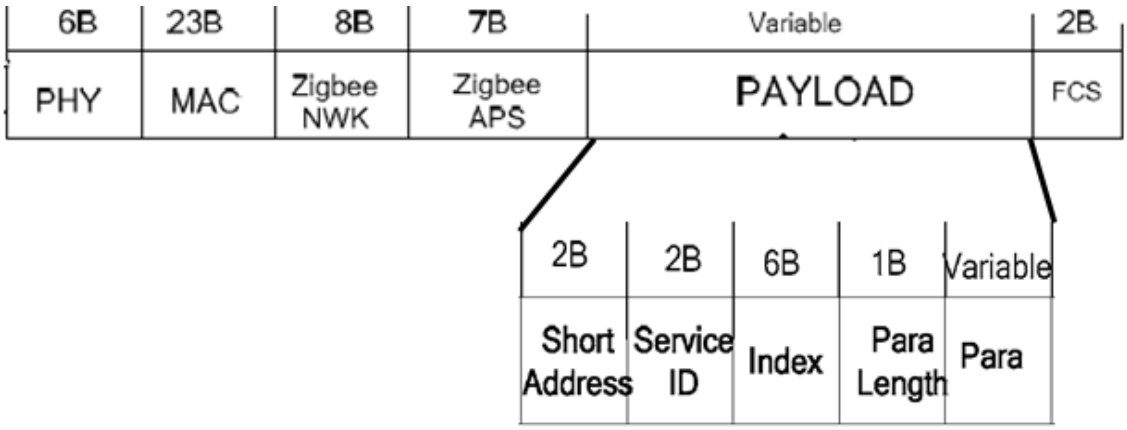


圖 9　定義標頭格式[7]

此外該論文提出位址映射的機制，是將 ZigBee 的短位址對應成 8 位元的裝置物件識別符(device object identifier, ObjectID)，轉換器依據不同的 ObjectID 管理不同裝置。在此機制下，外頭的伺服器只能藉此管理 256 個 ZigBee 網路節點，因此無法適用於較大型的 ZigBee 網路。最後比較轉換前後測試封包可發現，相較於 ZigBee 封包的 Payload 中自行定義的標頭，UDP 的 Payload 多出了無定義的資料，如圖 10 所示，紅色圈選處分別為 ZigBee APS Payload 和 UDP Payload。根據論文中所定義的轉換方式，兩邊 Payload 應當相同，所以是否能將兩邊封包正確轉換並通訊，還有待驗證。

NWK Dest. Address	NWK Src. Address	Broadcast Radius	Broadcast Seq.num	NWK payload
0x0000	0x1699	0x09	0x3B	00 02 00 FF FF 01 21 E5 0D 16 99 14 01 00 04 01 00 01 09 08 02 00

(a)ZigBee封包

```
User Datagram Protocol, Src Port: 35004 (35004), Dst Port: 35004 (35004)
    Source port: 35004 (35004)
    Destination port: 35004 (35004)
    Length: 36
    Checksum: 0x0000 (none)
  Data (28 bytes)

0000  ff ff ff ff ff ff 00 11  22 33 02 ca 08 00 45 00   ........ "3....E.
0010  00 38 00 02 00 00 20 11  96 e9 80 80 02 ca 80 80   .8.... . ........
0020  ff ff 88 bc 88 bc 00 24  00 00 14 00 20 20 00 1c   .......$ ....  ..
0030  16 99 14 01 00 04 01 00  01 09 08 02 00 00 00 00   ........ ....t...
0040  00 01 80 80 02 ca                                 ......
```

(b)Ethernet 封包

圖 10　ZigBee 和 Ethernet 封包[7]

2.6 SOAP/REST 轉換器

另一種作法則是在 ZigBee 轉換器的應用層中，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的程式轉成 XML 的格式[8]，如圖 11、圖 12 所示。將資料轉成 XML 的格式，轉換成可讀的資訊，容易和資料庫結合；但此方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。

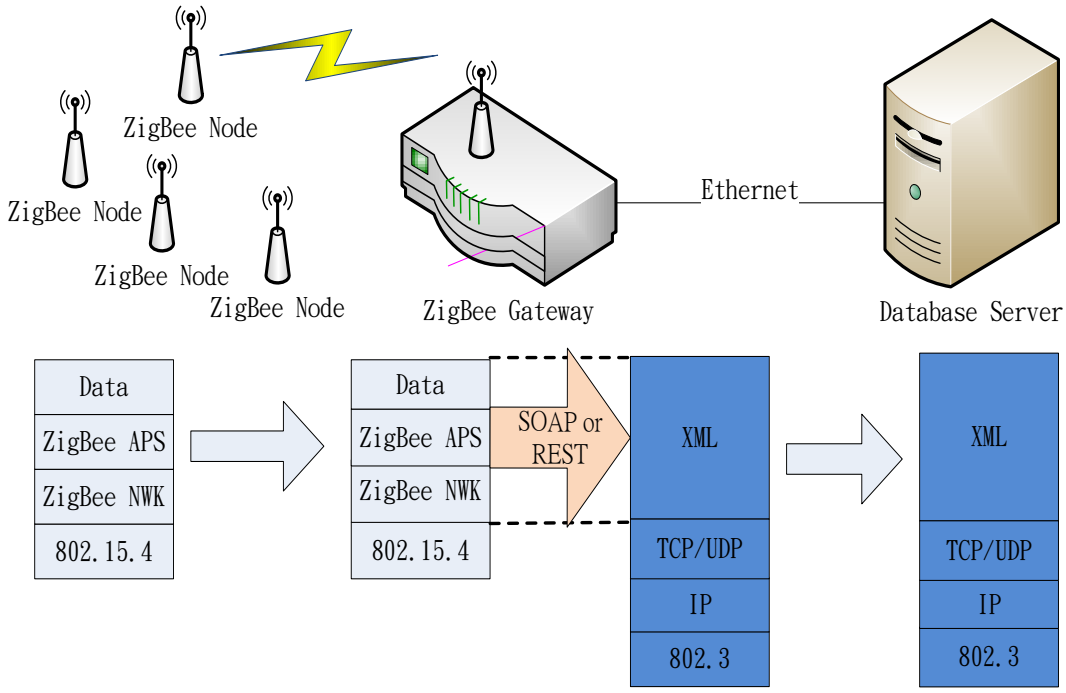


圖 11　SOAP/REST 轉換器示意圖

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

圖 12　REST 機制的 XML 封包[8]

上述（2.5 節和 2.6 節）兩個方法的共同缺點是，沒有服務發現機制（Service Discovery）和群播機制（Multicast/Groupcast）。然而，這兩個機制在 ZigBee 應用服務的建立上是非常重要的。

假設原先網路中只有一台伺服器收集透過轉換器傳送的 ZigBee 資料，ZigBee 節點只需發送資料給特定位址即可讓伺服器接收。但之後若新加入了一台伺服器，並希望 ZigBee 節點將資料改發送給新伺服器，則需要改變目的地位址。若無服務發現機

制，就只能在建立網路前，預先將伺服器位址，設定在 ZigBee 裝置中；若有服務發現機制，只要在 ZigBee 節點發送資料前，先詢問網路中誰是負責收資料的裝置，即可得知伺服器的位址，因此能夠很彈性地調整網路中伺服器的數量，並且無需預先在所有 ZigBee 裝置中設定伺服器的位址。

在群播機制實際應用上，假設目前需要監控的設備為一棟大樓各辦公室的電源，每一層分別有五十間辦公室。現在希望關掉某一層樓的電源時，若沒有群播機制，則需要發送五十次關閉電源命令分別給五十間辦公室的控制開關。每個開關所收到的內容是相同的一個關閉指令，因此在網路中連續發送相同內容的封包本質上是一種頻寬的浪費。若使用群播機制則可以將同層辦公室設定為同一群組，只需要發送一次關閉電源命令給指定群組，即可讓所有屬於此群組的辦公室關閉電源。如此一來，對於監控者來說，只需要發送一次命令即可達到相同的結果，可大幅降低網路頻寬的佔用。

因此 ZigBee 網路和 IPv6 網路的轉換器中，若能擁有服務發現和群播機制，則能提供更完善的應用。下一章節將會更進一步說明 ZigBee 各種傳播機制的運作和服務發現的功能。

2.7 傳播機制和服務發現

2.7.1 Unicast

每個 ZigBee 裝置加入 ZigBee 網路後，都會取得獨立的一組十六位元短位址，並透過此位址互相通訊。Unicast 是使用短位址來指定傳送封包給單一裝置的傳送機制。

2.7.2 Broadcast

此機制是用來傳送封包給所有 ZigBee 網路節點的機制。在 ZigBee 的標準文件中已定義三個特殊 Broadcast 位址：

0xFFFF：會傳送給 ZigBee 網路中所有的裝置。若有休眠的裝置，訊息則會

暫存在它的父節點直到休眠裝置醒來或是等待一定時間後把封包丟棄。

0xFFFD：會傳送給 ZigBee 網路中無線接收端有空的所有裝置。

0xFFFC：會傳送給 ZigBee 網路中所有的路由器和網路協調者。

2.7.3 Multicast

此機制用來傳送封包給 ZigBee 網路中的群組。ZigBee 網路中，可將裝置加入特定的群組（群組編號為 0x0000 至 0xFFFF，共十六位元）。當發送封包給指定群組時，所有屬於此群組的裝置都會收到此封包。使用 Multicast 時，網路層的標頭會額外增加 Multicast 控制欄位，如圖 13。Multicast Mode 用來決定來源節點是否為群組成員，分為 NonMember Mode 和 Member Mode。

Bits: 0 – 1	2 – 4	5 – 7
Multicast mode	NonmemberRadius	MaxNonmemberRadius

圖 13 Multicast 控制欄位

圖 14 說明 Multicast 傳送時，其控制欄位的運作方式。當來源端為非成員節點時，發送的 Multicast 封包為 NonMember mode，直到遇到第一個成員節點時，會將封包改變為 Member Mode；反之，Member Mode 封包並不會因為經過非成員節點而轉為 NonMember Mode。而在 Member Mode 中，當接收端為非成員節點時，NonMember Radius 值會減 1 後再轉發封包，而 NonMember Radius 被減為 0 時，會將封包丟棄。此外，當 Multicast 封包經過成員節點時，NonMember Radius 的值都會改成 Maximum NonMember Radius。由圖 14 可以看出，當 Radius 為 1 時，Multicast 只及於完全相鄰的群組。當 Radius 為 2 時，則中間可以允許隔一個 NonMember，以到達未直接相鄰的群組。

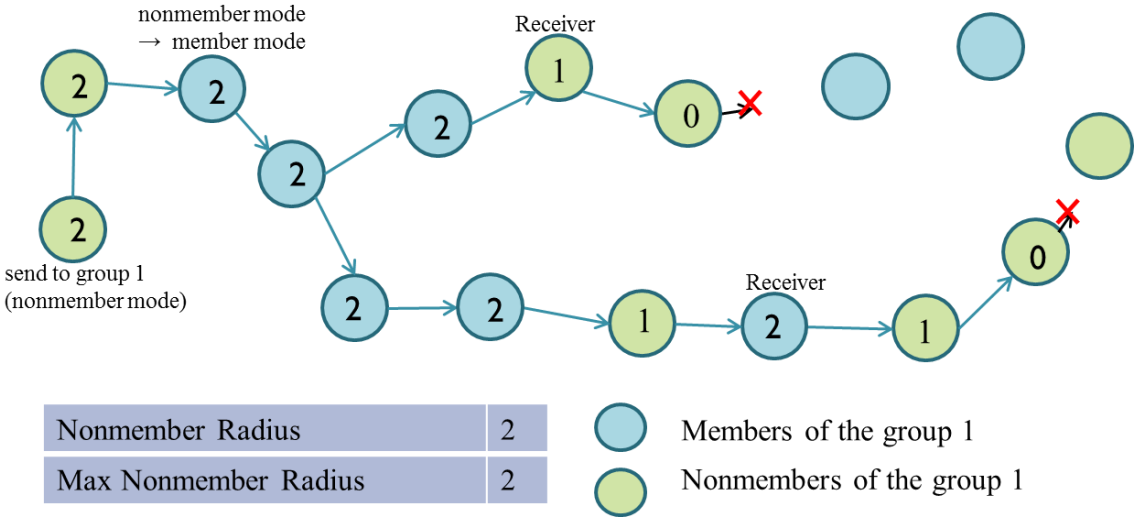


圖 14 The Effect of Radius in ZigBee Multicast

2.7.4 Groupcast

上一小節提到的 Multicast 是在 ZigBee 的網路層中實現，而 ZigBee 的應用層有另一套群播的機制。為了區分兩者，本文以群體播送（Multicast）和群組播送（Groupcast）分別表示網路層和應用層的群播機制，並以「群播」統稱兩個機制。使用 Multicast 有跳躍數的限制，在大規模網路中，跳躍數的限制可能會導致無法傳送到相距較遠的成員節點。而 Groupcast 則是透過網路層的 Broadcast 加上應用層中的群組位址過濾，實作出類似 Multicast 的傳播機制，所以無跳躍數的限制。因此在網路規模較大，且成員分散各地的 ZigBee 網路中，這兩種傳播機制有較明顯的差異。

Groupcast 提供了 Group ID 和 Endpoint(Ep)的對應表，如表 2 所示。透過裝置裡建立的 Group Table 可以將 Groupcast 封包傳送給裝置中對應的 Endpoint。Endpoint 相當於 TCP/IP 中所使用的 port，一般用來區分同一 ZigBee 裝置上對於不同設備的控制。以表 2 為例，假設 Endpoint 1~3 分別用來控制電燈 A~C 的開關，Endpoint 4~6 分別控制窗簾 A~C 的開闔，則 Group 1 可控制所有電燈，Group 2 控制所有窗簾，而 Group 3 控制電燈 A 及窗簾 A。每個 ZigBee 節點可以針對不同的應用來建立自己的 Group Table。

表 2　Group Table

Group ID	Endpoint
Group 1	Ep1, Ep2, Ep3
Group 2	Ep4, Ep5, Ep6
Group 3	Ep1, Ep4

圖 15(a)說明裝置發送 Groupcast 封包給 Group 1，由於在網路層是採用 Broadcast，因此每個裝置皆會收到封包，並根據裝置本身的 Group Table（如圖 15(b)），來決定封包如何處理。標示為藍色的裝置收到封包後會交由 Ep1 和 Ep2 處理，標示為橘色的裝置則是交由 Ep2 和 Ep3 處理，標示為綠色的裝置由於在 Table 中無法找到 Group 1 和對應的 Endpoint，因此僅將封包轉發。

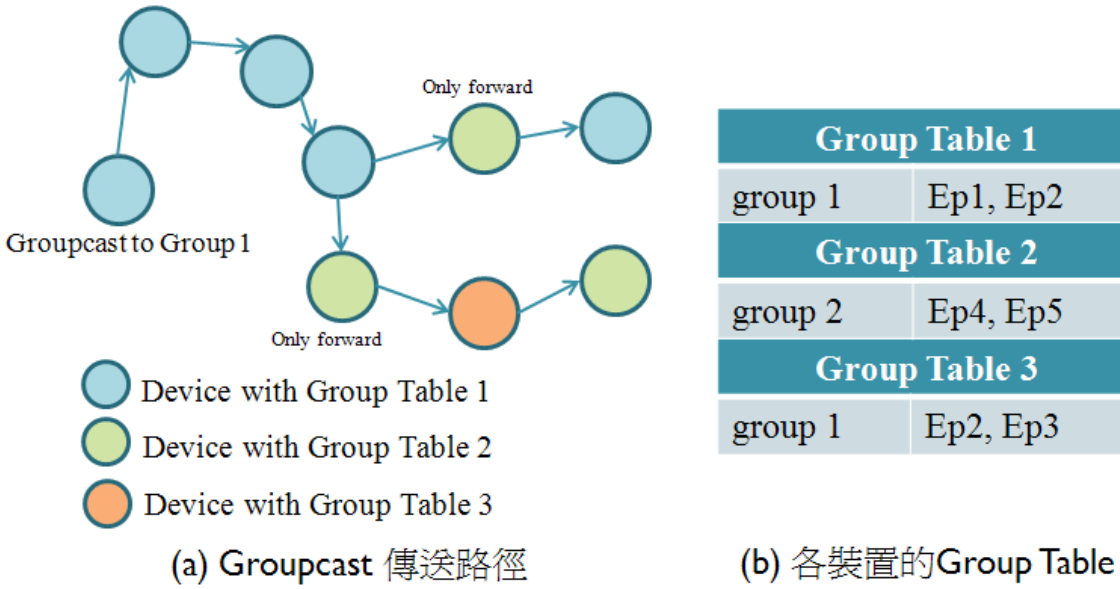


圖 15　ZigBee Groupcast

2.7.5　服務發現機制（Service Discovery）

Service Discovery 機制主要功能為提供網路中簡單的管理和維護服務設備的機制。透過此功能，可以尋找某種類型的服務和裝置，進而避免網路佈建時需預先配置

資訊(如伺服器的位址或轉換器的位址等)的麻煩。

ZigBee 和 IPv6 網路雖有各自的服務發現機制，如果沒有整合並轉換兩者的服務發現機制，則無法讓 IPv6 節點和 ZigBee 節點得知對方所提供的服務。

2.8 IPv6/ZigBee 轉換器

論文[10]設計一個轉換器讓 ZigBee/802.15.4 和 IPv6/802.3 能互相傳送訊息，其主要目標為：

1、 讓 ZigBee 節點和 IPv6 節點能分別被配置 IPv6 的全球位址和 ZigBee 短位址。

2、 在轉換器轉發封包時，盡量不要透過應用層轉換，以避免產生效能瓶頸。

3、 要在 ZigBee/802.15.4 和 IPv6/802.3 的網路中都能使用服務發現的機制。

4、 在 ZigBee 網路中的 Broadcast 封包，需要能夠傳送給適當的 IPv6 節點，且對 IPv6 的群播封包應有所限制。

為了能夠在傳送資料時有明確的目的地，透過位址映射表來達到 ZigBee 位址和 IPv6 位址的轉換。圖 16 說明 ZigBee 節點的 IPv6 位址表示方式，達成上述的第 1 點和第 2 點的目標。且整合簡單服務發現協定（Simple Service Discovery Protocol, 簡稱 SSDP）完成第 3 點的目標。

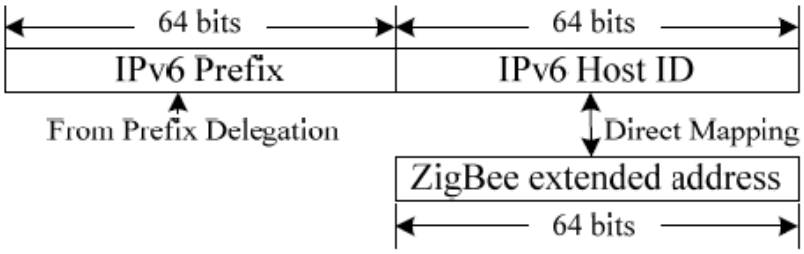


圖 16　IPv6 位址分配至 ZigBee[10]

第 4 點提到將 IPv6 群播封包做限制是因為，如果將 IPv6 所有的群播封包都轉送到 ZigBee 網路中，將會讓原本就屬於低速率傳輸的 ZigBee 網路癱瘓。所以應該利用 IPv6 群播中的群組功能，讓 ZigBee 網路只收到必要的群組封包。

論文[10]整合 SSDP 的機制來解決尋找裝置位址的問題。此外，若有兩部轉換器，可將兩個 ZigBee 網路互連， 讓 ZigBee 網路節點透過近距離轉換器，再經由 Ethernet，傳送資料至另一個轉換器所形成的 ZigBee 網路，進而延伸了同一個 ZigBee 網路的傳輸距離。圖 17、圖 18 分別說明封包如何傳送以及透過兩台轉換器傳送的流程。

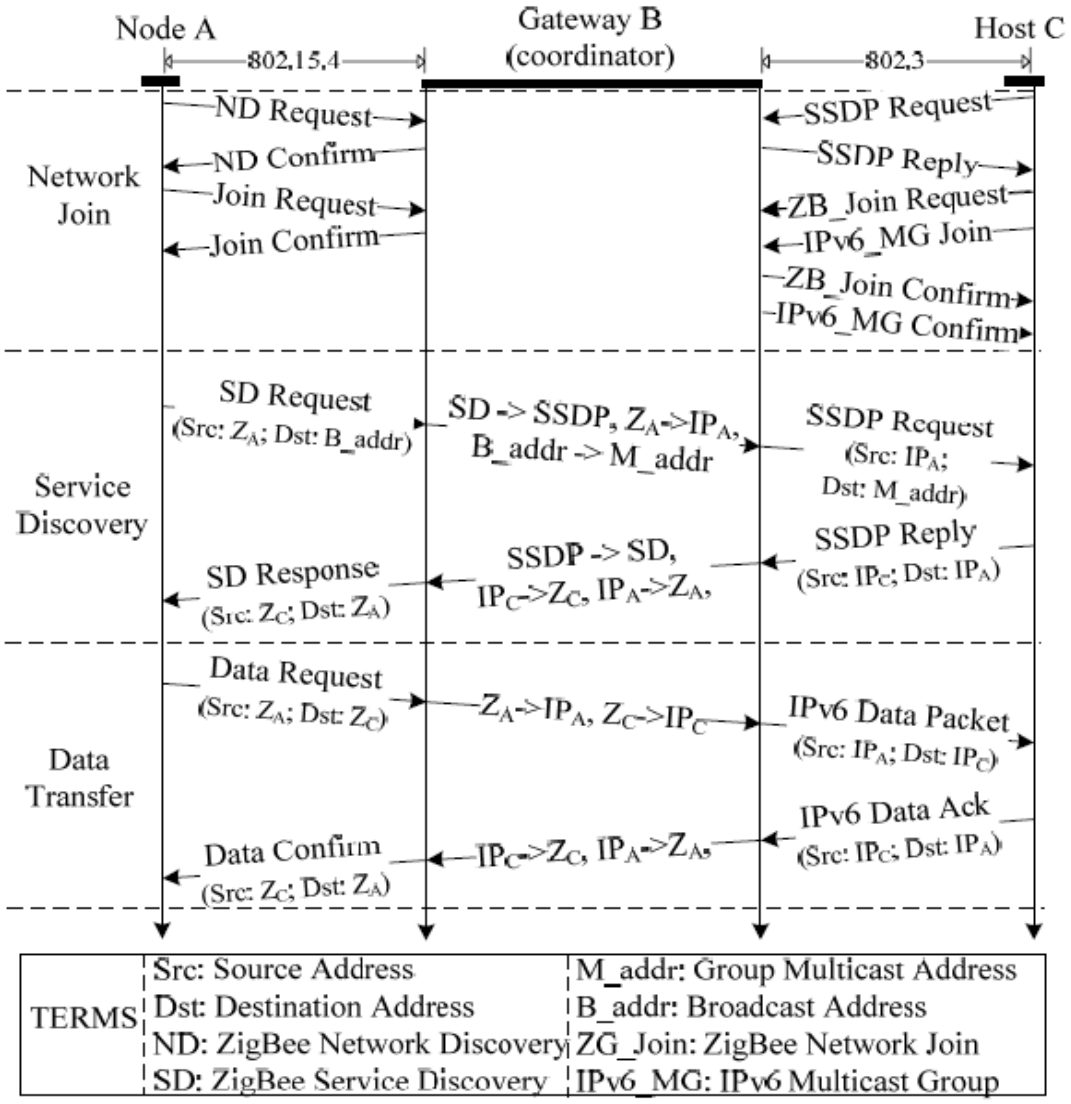


圖 17　從 ZigBee/802.15.4 傳送資料至 IPv6/802.3[10]

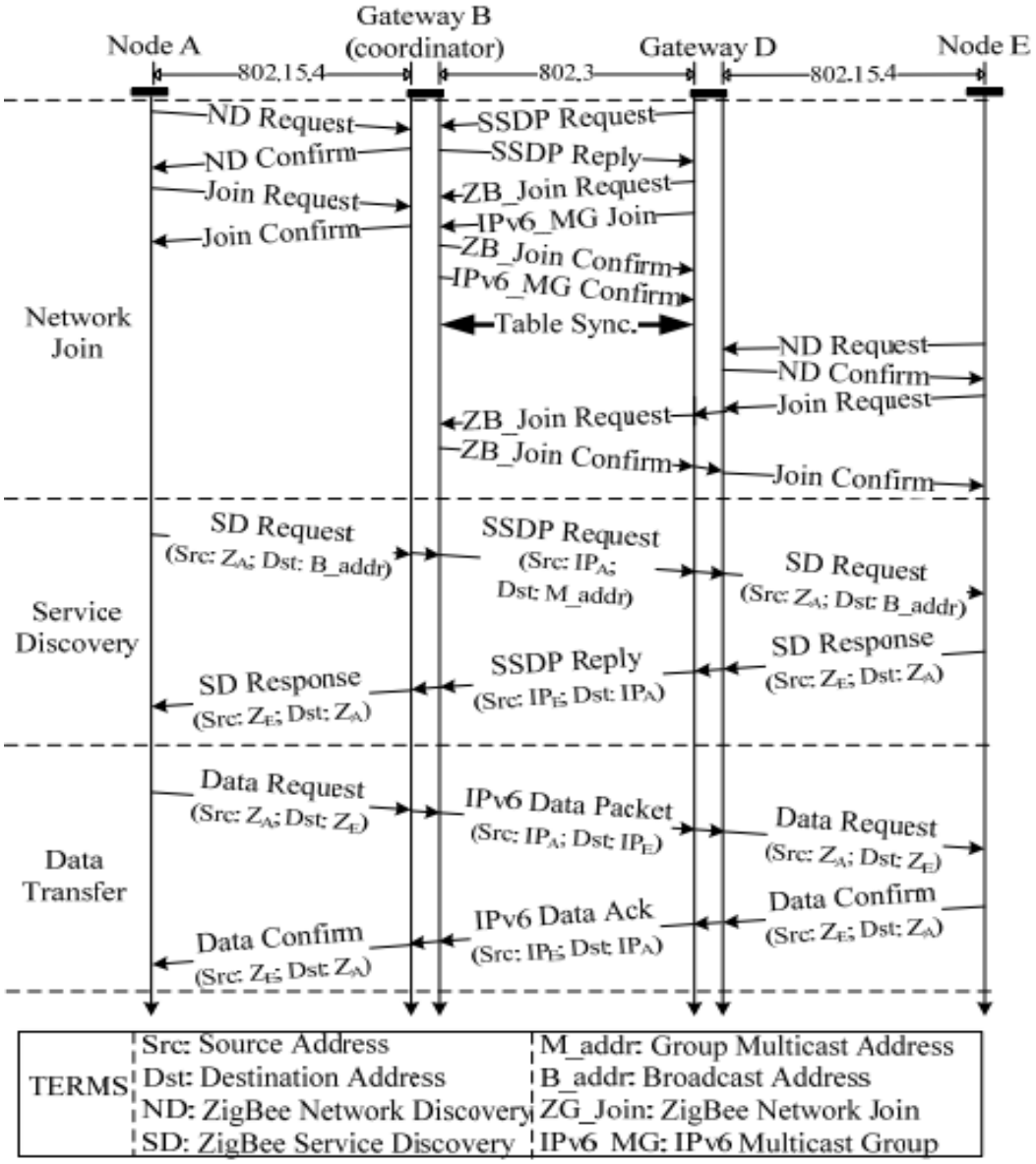


圖 18　利用兩台轉換器橋接 ZigBee 網路的傳輸流程[10]

第三章　Message Control Multicast Translator

為了解決前人所設計的轉換器不支援群播的問題，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 的轉換器，命名為訊息控制群播轉換器（Message Control Multicast Translator, MCMT），如圖 19 所示。

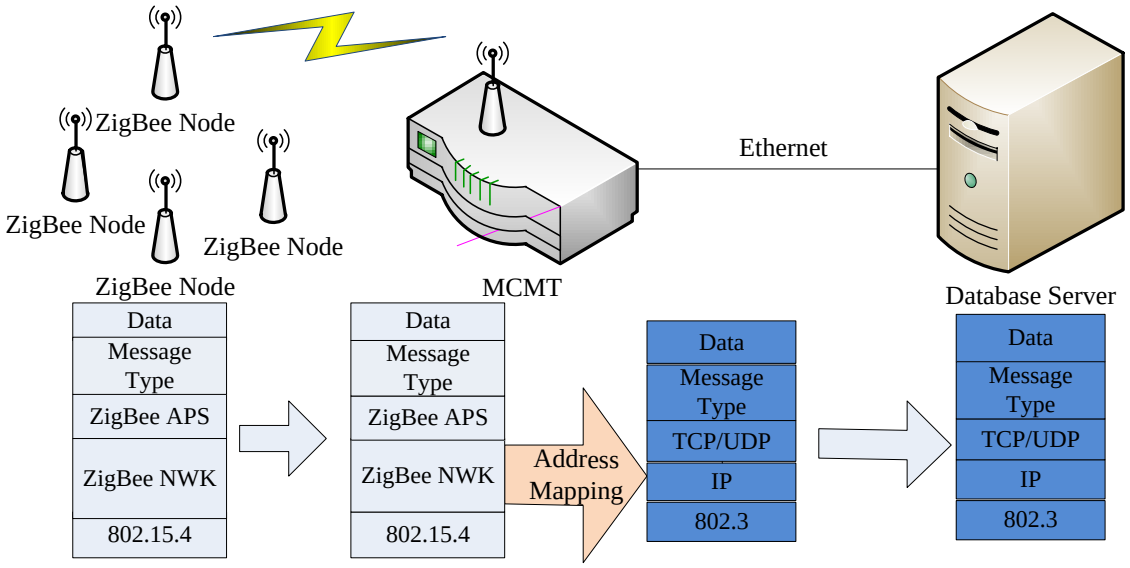


圖 19　MCMT 系統圖

設計此轉換器將會面臨以下幾個問題：位址如何轉換、兩個不同協定的群播封包如何發送和處理、802.3 和 802.15.4 的負載大小不相同等。

3.1　MCMT 設計需求

1. 讓 ZigBee 裝置能有相對應的 IPv6 位址。
2. 讓 IPv6 節點能有相對應的 ZigBee 短位址。
3. 阻斷來自 ZigBee 網路中的 Broadcast 及群播封包。
4. 阻斷來自 IPv6 網路中的群播封包。
5. 除了 ZigBee 節點和 IPv6 節點能互相收送 Unicast 封包之外，讓 IPv6 節點也能透

過轉換器發送 ZigBee 的 Broadcast/群播封包。

3.2 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[10]所提出的方法雷同，不同之處在 **3.3** 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）位址（即一般所謂的 MAC 位址）。我們根據 IPv6 網路中的位址前綴（Prefix）（64 位元）再加上 ZigBee 的延伸位址（64 位元），即可形成一個 IPv6 位址（128 位元）。如表 3 所示，所取得的 IPv6 Prefix 為 2001:e10:6840:409，而 ZigBee 裝置的 MAC 位址為 12:4b00:10a:2a75，即可產生一組代表 ZigBee 裝置的 IPv6 位址為 2001:e10:6840:409:12:4b00:10a:2a75。

表 3 ZigBee 裝置對應的 IPv6 位址

64 Bits	64 Bits
IPv6 Prefix	ZigBee Extended Address
2001:e10:6840:409	12:4b00:10a:2a75

3.3 Broadcast 位址/群組位址

ZigBee 和 IPv6 分別有 Broadcast（IPv6 無）、Multicast、Groupcast 的機制，為了避免 IPv6 中的 Multicast 封包造成 ZigBee 網路癱瘓，轉換器不適合將兩邊播送的封包全都轉傳。但 IPv6 節點若能妥善利用 ZigBee 各種播送機制，則可降低在通知大量 ZigBee 節點時所造成的網路阻塞。因此轉換器要如何讓 IPv6 節點傳送不同播送機制的 ZigBee 封包，對 ZigBee 網路相當重要。

故本論文提出的構想為，讓轉換器阻斷 IPv6 網路的群播封包及 ZigBee 網路內部的廣播與群播封包。當 IPv6 節點需要對 ZigBee 網路發送廣播與群播送封包時，則發

送目的地為特殊位址的 Unicast 封包；而轉換器根據各特殊位址所對應的播送機制，再轉發封包給 ZigBee 節點。

特殊位址轉換規則為，將 ZigBee 特定的廣播與群播位址，轉換成特定的 IPv6 位址，如表 4 所示。如此一來，IPv6 節點只要指定目的地為此特殊位址，即可達到對 ZigBee 網路發送廣播與群播封包的功能。

表 4　轉換表中特定 IPv6 位址

64 Bits	48 Bits	16 Bits	備註
IPv6 Prefix	0000:0000:0000:0000	FFFF	廣播位址
IPv6 Prefix	0000:0000:0000:0000	FFFD	廣播位址
IPv6 Prefix	0000:0000:0000:0000	FFFC	廣播位址
IPv6 Prefix	0000:0000:0000:0000	Group1	群播位址
IPv6 Prefix	0000:0000:0000:0000	Group2	群播位址

3.4　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，而 IEEE 802.3 所提供的 MTU 大小則為 1492，兩者差距甚大。因此轉換封包時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，封包長度通常低於 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，也是未來轉換器實作的重點之一。本論文主要先專注於 ZigBee 和 IPv6 網路的互通，故暫時將此問題留至未來改善。

3.5 訊息型別（Message Type, MT）

綜合 3.2、3.3，本論文已說明如何讓 ZigBee 擁有 IPv6 位址，並讓伺服器端發送資料給 ZigBee 單一節點、群組節點，甚至是所有節點。接下來說明如何區分各種播送機制封包，本論文在原先的傳輸資料中加入一個長度為 1 位元組的 Message Type（MT），根據此 MT 來決定所發送的封包為何種播送機制，例如 Unicast、Broadcast、Multicast、Groupcast 等，如表 5 所示。未來可加入新的 MT，以便使用 ZigBee 應用層的其它功能，如 Endpoint 等。

表 5 Message Type

Basic Message Type（MT）	Description	Example
Send packet（ZigBee to IPv6）	Send general packets	MT （0x10） + Server_Z + data
Unicast（IPv6 to ZigBee）	Send Unicast packets	MT （0x10） + data
Broadcast（IPv6 to ZigBee）	Send Broadcast packets	MT （0x11） + data
Multicast（IPv6 to ZigBee）	Send Multicast packets	MT （0x12） + data
Groupcast（IPv6 to ZigBee）	Send Groupcast packets	MT （0x13） + data

3.6 與現有方法比較

表 6 為本論文和先前所提到各種轉換器的比較表，從表格中最後三列可以看出，過去的論文皆尚無提出讓轉換器能發送 ZigBee Multicast 和 ZigBee Groupcast 的功能。並且在提出設計方法後，也鮮少將其實現，成為一套可實際運作的系統。

表 6　各方法比較表

	Design and Implementation of Industrial Wireless Gateway Base on ZigBee Communication[5]	SOAP/REST[6]	Internetworking Between ZigBee/802.15. 4 and IPv6/802.3 Network[10]	**Message Control Multicast Translator**
位址轉換方式	映射表	無	映射表	映射表
IPv4/IPv6	IPv4	IPv4/IPv6	IPv6	IPv6
主要方法	自定義標頭	轉換成XML格式	SSDP（Simple Service Discover Protocol）	MT（Message Type）
ZigBee Multicast	無	無	無	有
ZigBee Groupcast	無	無	無	有
實作	有	無	無	有

第四章　系統架構與實作

4.1　系統架構

由於 MCMT 需要發送來源位址不是本身 IP 位址的封包，無法使用一般的 Socket 撰寫發送封包程式，因此需使用 Raw Socket，而使用 Raw Socket 需要額外的設定並自行產生網路層和傳輸層的標頭檔。至於 MCMT 接收的部份，也需要接收目的地非 MCMT 本身 IP 位址的封包，使用一般的 Socket 無法做到，需要透過 Raw Socket 或其它方式。在[11]提到，接收端使用 libpcap，不但可攜性較高，也整合了過濾器的設定，故 MCMT 接收端部份使用 libpcap 撰寫。最後需透過 Multi-Thread 讓發送端的 Raw Socket 和接收端 libpcap 同時執行。

在 ZigBee 端則需要熟悉發送各種播送封包的 API，並了解封包的結構。另外，由於無法在 ZigBee 端使用 Multi-Thread 的函式，所以必須了解 ZigBee 處理事件的函式，以隨時處理無線收發端和序列傳輸介面收到的封包。最後再調整 ZigBee 和所連結的桌上型個人電腦（Personal Computer，以下簡稱 PC）兩邊的序列傳輸設定，使其一致，方能互相溝通。

根據上述實作的部份加上 Address Mapping Table 即完成系統模組圖，如圖 20。

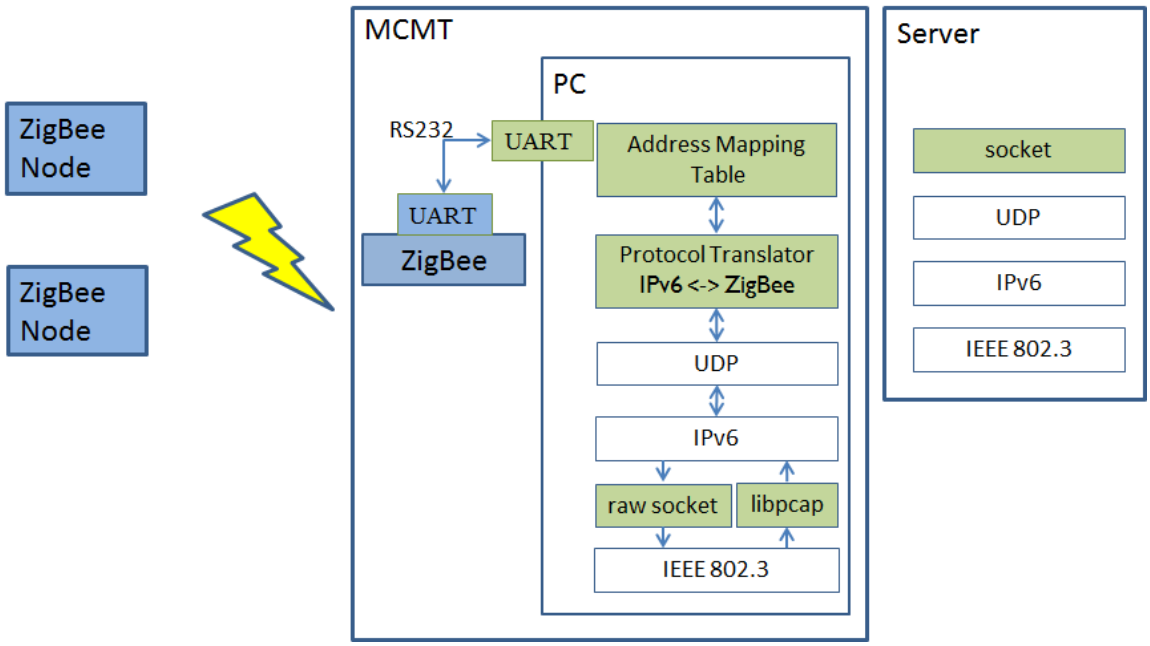


圖 20　MCMT 模組圖

4.2　系統平台

本研究所使用的開發平台分為兩部份，一端為個人電腦的部份(提供 Ethernet 介面)，作業系統採用 Linux CentOS 5.5；另一端為 ZigBee 裝置(提供 802.15.4 介面)，無線開發模組選用 Texas Instruments （TI）的 CC2530ZDK（ZigBee Development Kit）。TI 提供了免費的 Protocol Stack 和數個範例程式來簡單地說明 ZigBee 網路的運作機制，也提供 Packet Sniffer、Flash Programmer 等其它幫助開發的輔助軟體，讓我們能截取 802.15.4 封包以及將編譯完的程式碼下載至實驗板。在 MCMT 的設計上，目前是將 CC2530ZDK 的實驗板透過 RS232 傳輸介面和個人電腦通訊，形成一個同時具有 802.15.4 介面和 Ethernet 介面的轉換器，其實體照片如圖 21 所示。

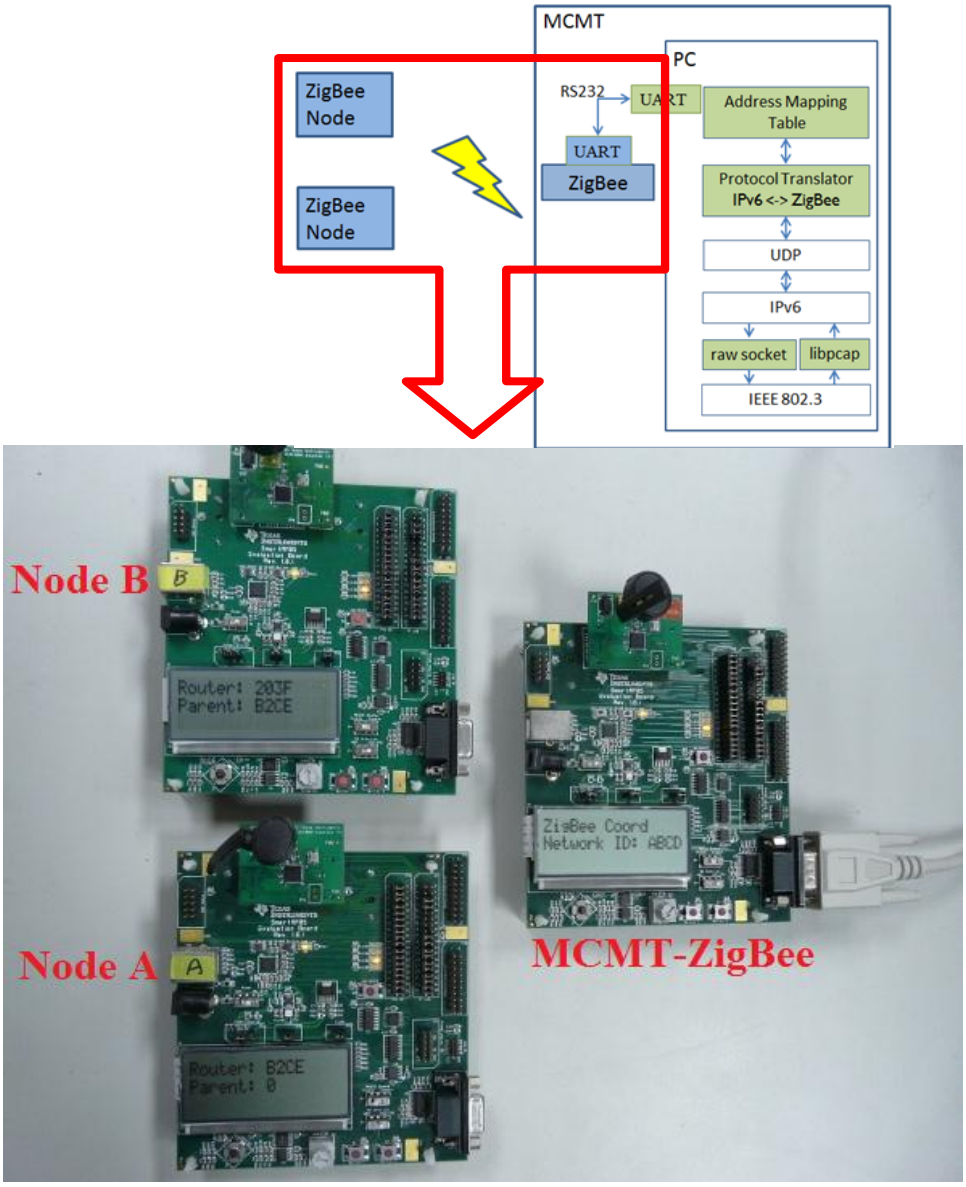
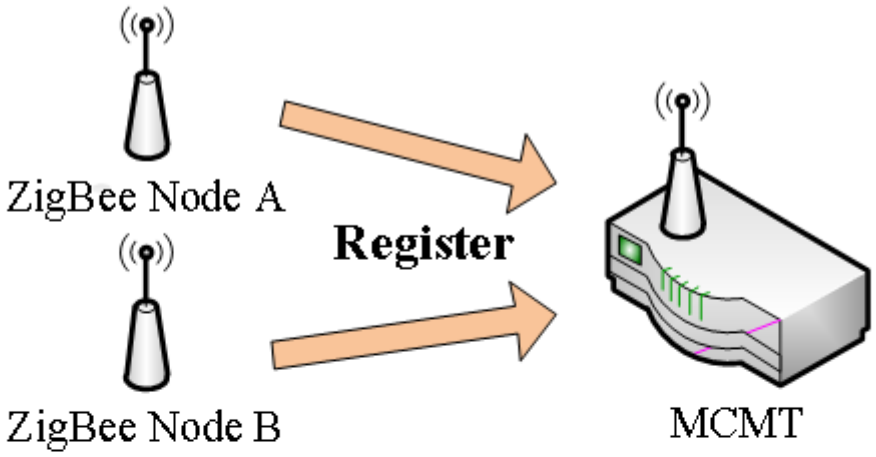


圖 21　平台與系統模組對照圖

4.3　運作流程

4.3.1　ZigBee 節點加入網路

圖 22 說明 ZigBee 裝置在加入網路後，轉換器會建立短位址和 MAC 位址的 Mapping Table。



(a) Devices Join the ZigBee Network

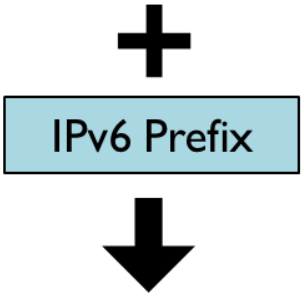
Mapping Table	Short address	ZigBee MAC (Extended address)
MCMT	M_Z	M_M
Node A	A_Z	A_M
Node B	B_Z	B_M

(b) Mapping Table on the Coordinator

圖 22 (a) Devices Join the ZigBee Network (b) Mapping Table on the Coordinator

透過 Mapping Table 中的 ZigBee MAC 和 IPv6 的 Prefix 結合後，即成為該 ZigBee 裝置的 IPv6 位址，最後加入預先已配置好的伺服器的短位址和對應的 IPv6 位址，即可讓所有裝置都具有 ZigBee 短位址和 IPv6 位址，如圖 23 所示。

Mapping Table	Short address	ZigBee MAC (Extended address)
MCMT	M_Z	M_M
Node A	A_Z	A_M
Node B	B_Z	B_M



	Short address	IPv6 address
MCMT	M_Z	M_6
Node A	A_Z	A_6
Node B	B_Z	B_6
Server	S_Z	S_6

圖 23　ZigBee 裝置 IPv6 定址方式

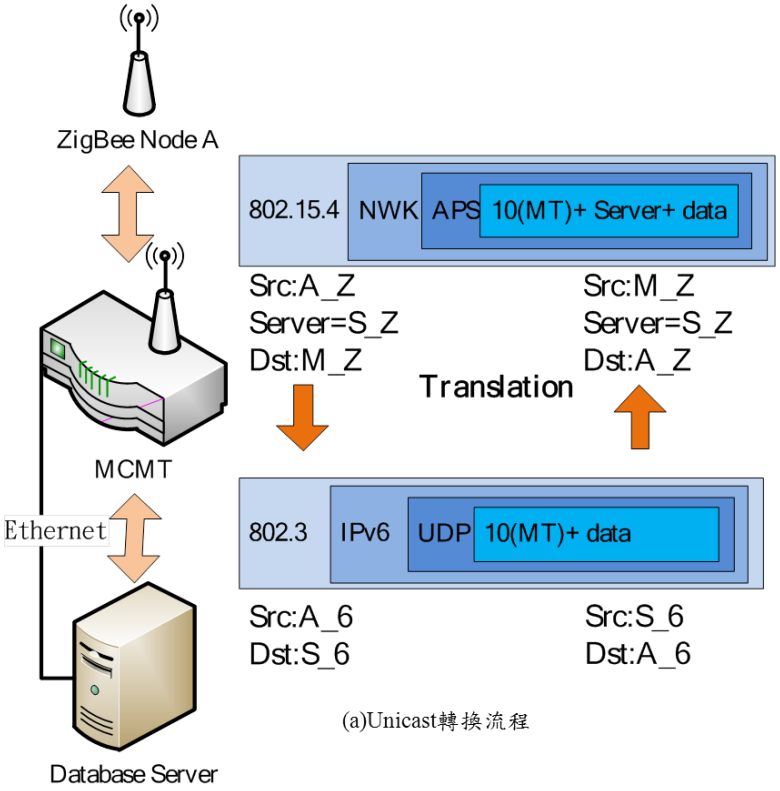
4.3.2　封包傳送過程

Unicast 傳輸過程如圖 24 所示。ZigBee Node A 要發送 Unicast 封包給資料庫伺服器時，Unicast 封包在 APS Payload 的 MT 欄位依據表 5 填入 0x10，Payload 的 Server 欄位則根據圖 24(b)填入伺服器 ZigBee 的位址 S_Z。當封包傳送到 MCMT 時，MCMT 會根據圖 23 之 Mapping Table 和 Prefix 將來源位址從 A_Z 轉成相對應的 IPv6 位址 A_6，目的地位址則是填入 S_Z 的 IPv6 對應位址 S_6。

由伺服器發送 Unicast 封包給 ZigBee Node A 時，亦根據表 5 在 UDP Payload 的 MT 欄位填入 0x10。當封包傳送到 MCMT 時，MCMT 依圖 24(b)將來源位址的 S_6 轉成相對應的位址 S_Z 後填入 APS Payload 的 Server 欄位中，並將來源位址改為

M_Z，而目的地位址則從 A_6 轉成 ZigBee 對應位址的 A_Z。

如此一來， Unicast 封包即可順利在 IPv6 伺服器與 ZigBee 裝置間收送。



(a)Unicast轉換流程

	IPv6 addr	ZigBee addr
Node A	A_6	A_Z
MCMT	M_6	M_Z
Server	S_6	S_Z

(b)位址對照表

圖 24　Unicast 傳輸過程

4.3.3　群播封包傳送過程

圖 25 說明伺服器若要傳送 ZigBee 的 Multicast 或 Groupcast 封包，則需要發送群組的 IPv6 特殊位址 GP_6（注意這並不是 IPv6 中 FF00::/8 的群播位址，而是表 4 中所定義的特殊位址），如圖 25(b)所示。當 MCMT 收到此封包後，會根據 MT 的值（12 or 13）來決定要發送 Multicast 封包或 Groupcast 封包給 ZigBee 網路中的 GP_Z 群組。若 MT 值為 12 則發送 Multicast，網路層的目的地位址填入 GP_Z；若 MT 值為 13 則發送 Groupcast，網路層的目的地位址填入 ZigBee 廣播位址 FFFD，GP_Z 則是填入 APS 層中的 Group Address 欄位。

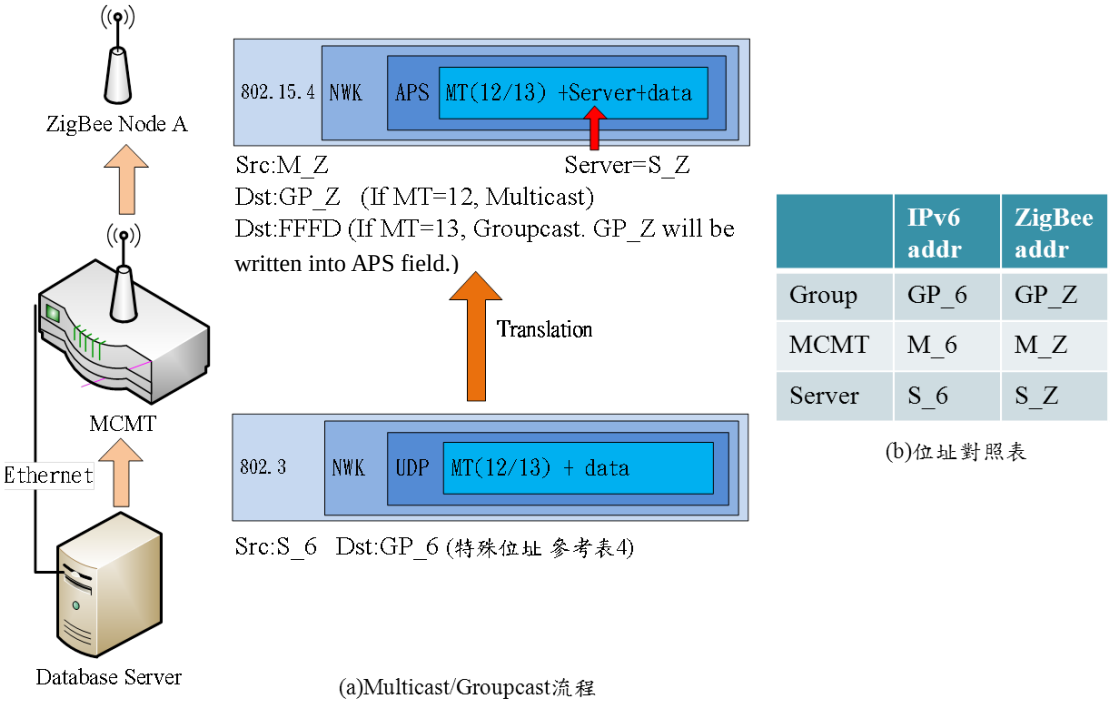


圖 25　Multicast/Groupcast 傳輸過程

4.4　實作結果

為測試各種傳播機制的運作是否正常，將進行 Unicast、Broadcast、Multicast、Groupcast 四種封包傳送。啟動 MCMT(包含 ZigBee 裝置和 PC 上的程式)後會自動建立網路，之後打開 Node A 和 Node B 裝置，兩個節點會自動加入網路並建立 Mapping Table。圖 26 顯示各個裝置的 ZigBee 位址和 IPv6 位址，此次實驗 Node A 所取得的短位址為 7773，Node B 為 F5F6，MCMT(ZigBee Coordinator)為 0000，伺服器預先配置的短位址為 00A1。

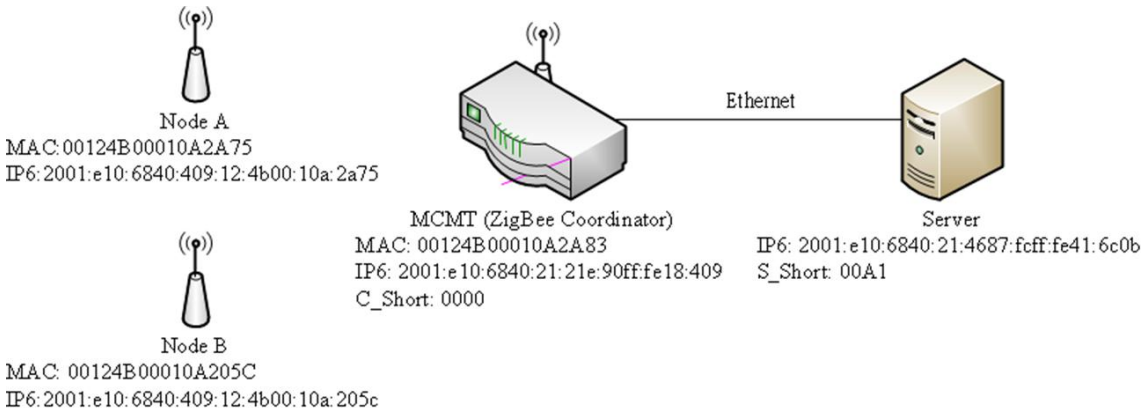


圖 26　裝置位址示意圖

4.4.1　Unicast

我們先由 Node A 和 Node B 分別發送 Unicast 封包給伺服器，之後再從伺服器端分別發送 Unicast 給 Node A 和 Node B。圖 27 所示為伺服器收到分別來自 Node A 與 Node B 之 Unicast 封包，並送出 hello word 訊息給 Node A 及 Node B。

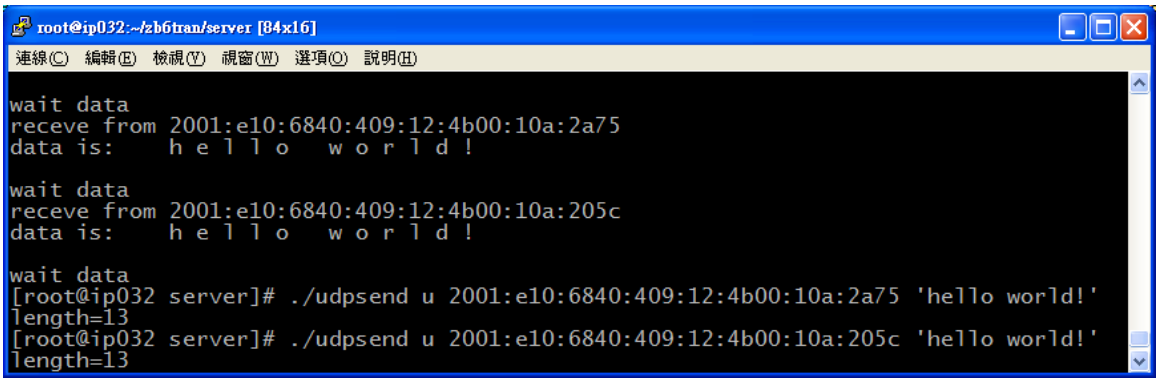


圖 27　伺服器接收與發送畫面[1]

圖 28 為伺服器端所截取的封包，從圖中可以得知封包承載（Payload）的第一個資料位元組為 Message Type 0x10（Unicast）。另外可從圖 29 觀察到轉換後的 ZigBee 封包，APS Payload 中多了兩個位元組的訊息（圖中以紅框標示），分別是第二個位元

[1] 伺服器端輸入以下指令：udpsend (u)nicast/(b)roadcast/(m)ulticast/(g)roupcast <IP address> <data>，即可發送封包。

組的 00 和第三個位元組的 A1，也就是代表伺服器位址的 00A1。除此之外，其餘資料內容皆與圖 28 的資料相同，由此可見伺服器和 ZigBee Node 能成功互相傳送 Unicast 封包。

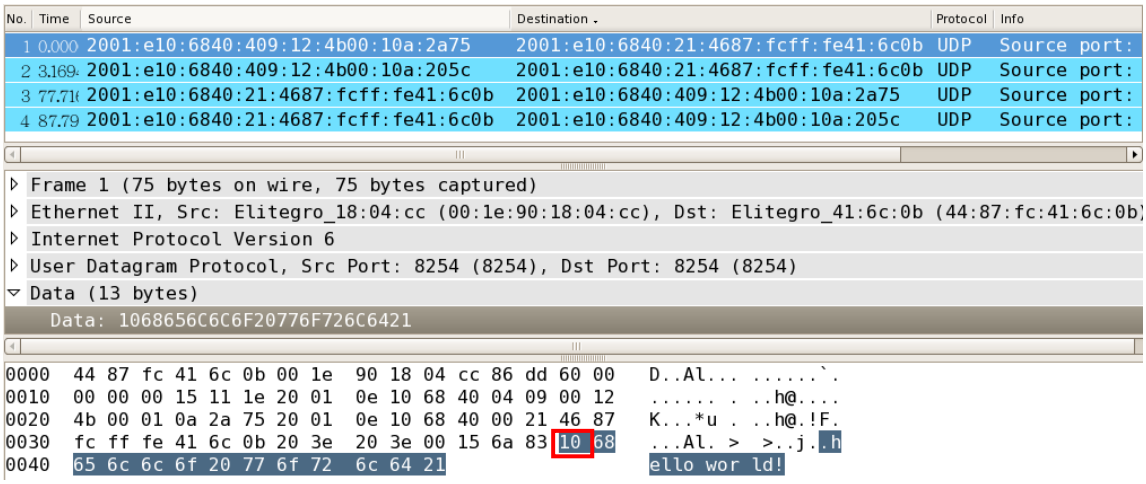


圖 28　Unicast Ethernet 封包截取圖

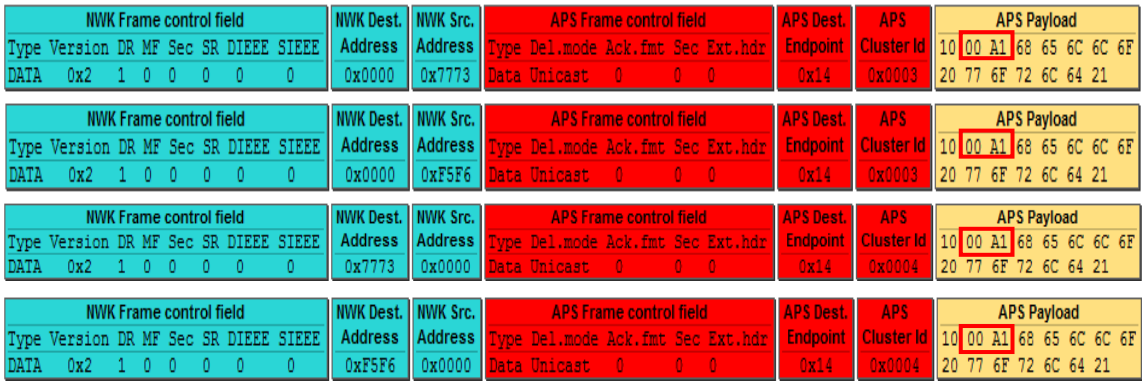


圖 29　Unicast ZigBee 封包截取圖[2]

4.4.2　Broadcast

伺服器指示 MCMT 發送 Broadcast 封包至 ZigBee 網路，如圖 30 所示。

[2]使用 Texas Instrument 公司之 SmartRF Protocol Packet Sniffer 擷取。與本論文相關性較低的欄位予以隱藏。

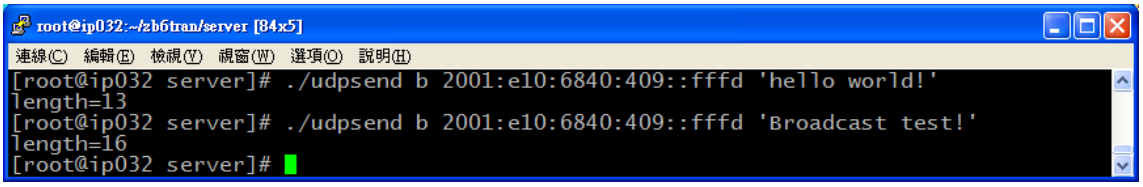


圖 30　伺服器 發送 ZigBee Broadcast 畫面

圖 31 是從伺服器端截取的封包，圖中可以得知此封包目的地為表 4 中 Broadcast 的特殊位址，且第一個資料位元組為 Message Type 0x11（Broadcast）。另外從圖 32 顯示的 ZigBee 封包可以得知，經轉換後，ZigBee 封包的目的地位址為 ZigBee 網路中的 Broadcast 位址 FFFD，驗證了伺服器能透過 MCMT 發送 ZigBee Broadcast 封包。

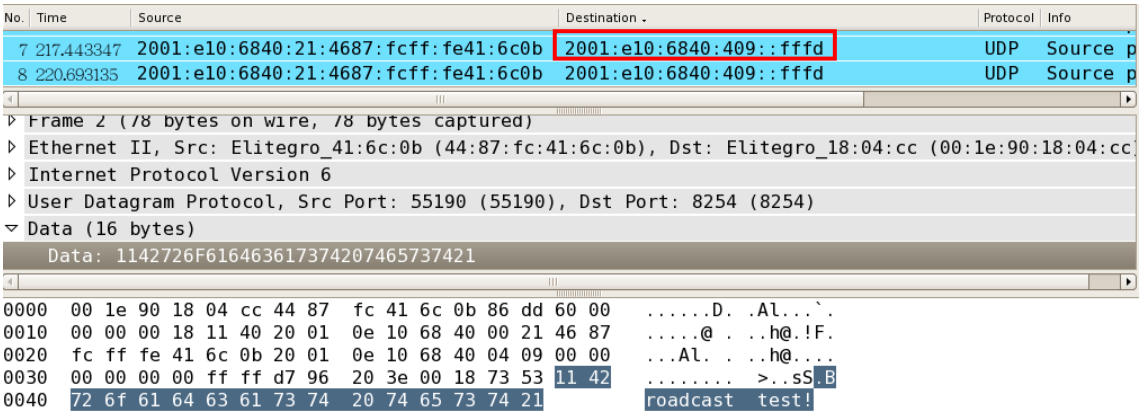


圖 31　Broadcast Ethernet 封包截取圖

NWK Frame control field								NWK Dest. Address	NWK Src. Address	APS Frame control field					APS Dest. Endpoint	APS Cluster Id	APS Payload
Type	Version	DR	MF	Sec	SR	DIEEE	SIEEE			Type	Del.mode	Ack.fmt	Sec	Ext.hdr			
DATA	0x2	0	0	0	0	0	0	0xFFFD	0x0000	Data	Broadcast	0	0	0	0x14	0x0005	11 00 A1 68 65 6C 6C 6F 20 77 6F 72 6C 64 21

NWK Frame control field								NWK Dest. Address	NWK Src. Address	APS Frame control field					APS Dest. Endpoint	APS Cluster Id	APS Payload
Type	Version	DR	MF	Sec	SR	DIEEE	SIEEE			Type	Del.mode	Ack.fmt	Sec	Ext.hdr			
DATA	0x2	0	0	0	0	0	0	0xFFFD	0x0000	Data	Broadcast	0	0	0	0x14	0x0005	11 00 A1 42 72 6F 61 64 63 61 73 74 20 74 65 73 74 21

圖 32　Broadcast ZigBee 封包截取圖

4.4.3　Multicast/Groupcast

伺服器指示 MCMT 發送 Multicast 和 Groupcast 封包至 ZigBee 網路中的群組 0001，並分別傳送 multi 訊息和 groupcast 1 訊息，如圖 33 所示。

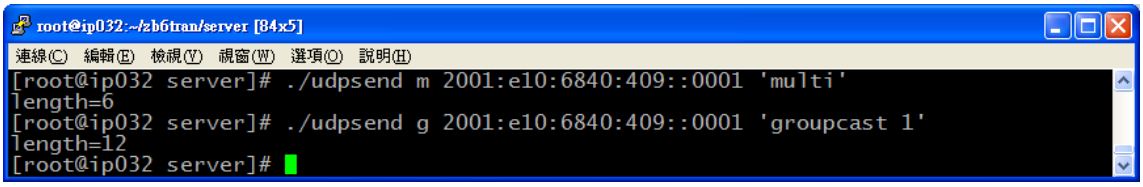


圖 33　伺服器 發送 ZigBee Multicast/Groupcast 封包

圖 34 顯示伺服器所發出的封包，目的地為 MCMT 所屬網路內，群組代號 0001 的 IPv6 特殊位址，且第一個資料位元組為 Message Type 0x12（Multicast）。另外圖 35 顯示在 ZigBee 無線網路中所擷取到的封包，NWK Frame control field 中的 MF(Multicast Flag)被設為 1，表示為 Multicast 封包，並額外增加 NWK Multicast control field。由此得知，伺服器能透過 MCMT 發送 ZigBee Multicast 的封包。

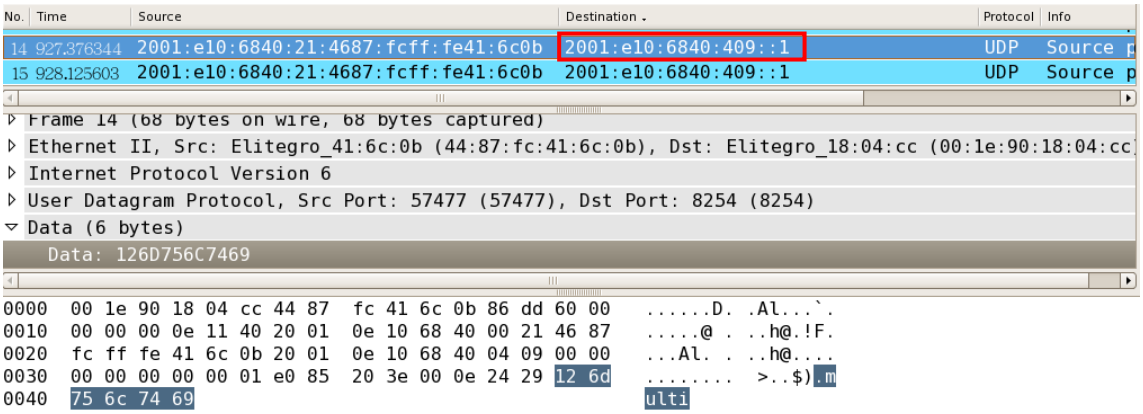


圖 34　Multicast Ethernet 封包截取圖

NWK Frame control field								NWK Dest. Address	NWK Src. Address	NWK Multicast control field			APS Frame control field					APS Dest. Endpoint	APS Payload
Type	Version	DR	MF	Sec	SR	DIEEE	SIEEE			Mode	Rad	MaxRad	Type	Del.mode	Ack.fmt	Sec	Ext.hdr		
DATA	0x2	1	1	0	0	0	0	0x0001	0x0000	Member	2	2	Data	Broadcast	0	0	0	0xFF	12 00 A1 6D 75 6C 74 69

圖 35　Multicast ZigBee 封包截取圖[3]

圖 36 顯示為以 Groupcast 發出的封包，目的地位址和伺服器發送 Multicast 封包給群組 0001 相同，但藉由第一個資料位元組為 Message Type 0x13（Groupcast）來區別兩種傳播機制。圖 37 顯示在 ZigBee 無線網路中所擷取到的封包，APS Frame control field 中的 Deliver mode 為 Group，表示此封包為 Groupcast 封包。Deliver mode 為 Group 時，裝置會根據 Group Table 來尋找相對應的 Endpoint，因此 Groupcast 封包格式有

[3] 由於封包顯示長度過長，為了方便觀看，關閉顯示 APS Cluster Id 欄位。

Group Address 欄位，而不像圖 35 中的封包具有 Endpoint 欄位。

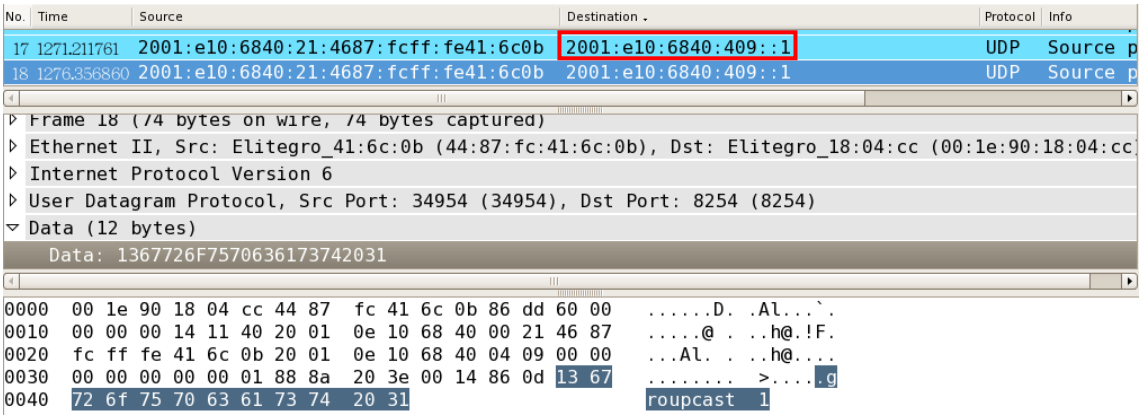


圖 36　Groupcast Ethernet 封包截取圖

圖 37　Groupcast ZigBee 封包截取圖

第五章　結論及未來方向

5.1　結論

MCMT 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，使伺服器端能直接發送 IPv6 address 的封包，經由 MCMT 轉送至 ZigBee 終端設備。並且伺服器端具有發送 ZigBee Broadcast、ZigBee Multicast、ZigBee Groupcast 的功能，讓伺服器通知所有或部份節點時，能透過這些機制，降低 ZigBee 的網路負擔，改善網路效能。

相較於市面上的轉換器做法，其封包是以轉換器為目的端，經由轉換器去分析封包中的 ZigBee 位址後再進行轉發，本論文直接以目的地位址判別，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，並能降低轉換器工作負擔。

5.2　未來方向

目前 MCMT 還有許多改進的方向，例如無法讓 ZigBee 裝置動態得知伺服器的短位址。未來需要整合 IPv6 和 ZigBee 網路的 Service Discovery 機制，讓任何節點都能尋找特定的節點或服務是否存在，並尋得其位址。如此一來加入新伺服器時，能讓所有網路節點得知新伺服器的位址及其提供的服務。

此外，未來亦需整合 ZigBee 和 IPv6 的群播機制，使伺服器發送 Multicast 時能同時送給多個不同 PAN ID 的 ZigBee 網路，如圖 38 所示。

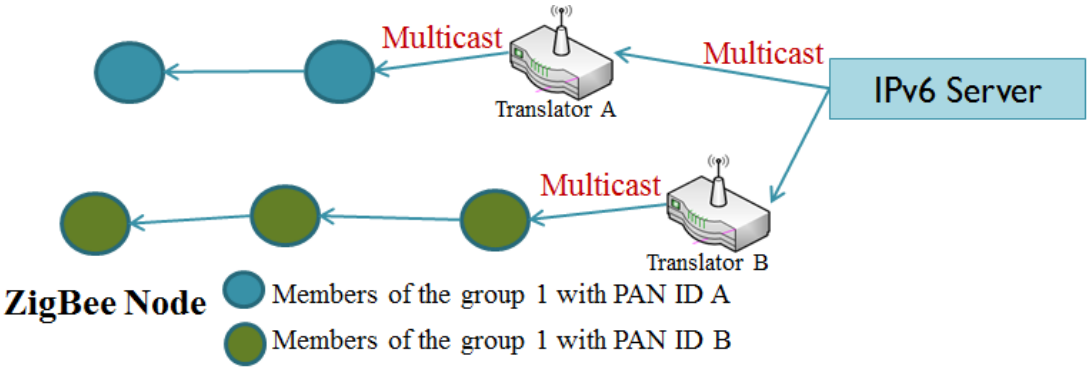


圖 38　伺服器發送 Multicast 給多個 ZigBee 網路

最後希望能將此轉換器移植到嵌入式 Linux 系統，運用最少的硬體資源達到更好的效能。

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] S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, IETF RFC 2460, December 1998.

[6] 張瑞雄、陳俊良、陳彥文、趙涵捷、賴威光、賴溪松、陳錦洲、陳懷恩，「IPv6 新世代網際網路協定暨整合技術」，台北：旗標出版社,2008。

[7] Guozhen Hu, “Design and Implementation of Industrial Wireless Gateway Base on ZigBee Communication”, the Ninth International Conference on Electronic. Measurement & Instruments （ICEMI’2009）, October 2009, pp.684-688, Beijing, China.

[8] ZigBee Alliance, “Understanding ZigBee Gateway”, ZigBee Document 095465r13, September 2010.

[9] R. Vida, L. Costa, “Multicast Listener Discovery Version 2 (MLDv2) for IPv6”, IETF RFC 3810, June 2004.

[10] Reen-Cheng Wang, Yao-Chung Chang, Ruay-Shiung Chang, “Internetworking Between ZigBee/802.15.4 and IPv6/802.3 Network”, SIGCOMM Data Communication, August 2007, pp.362-367, Kyoto, Japan.

[11] W. Richard Stevens, Bill Fenner, Andrew M. Rudoff, “Unix Network Programming, Volume 1: The Sockets Networking API”, 3rd Edition, Addison-Wesley Professional, 2003, pp. 815.