國立交通大學

資訊工程學系

碩士論文

IEEE 802.11i 無線網路快速換手之設計與實作

Design and Implementation of a Fast Handoff Mechanism for IEEE 802.11i-based Wireless Networks

研究生：蔡亞軒

指導教授：曾建超　教授

中華民國九十四年七月

IEEE 802.11i 無線網路快速換手之設計與實作

Design and Implementation of a Fast Handoff Mechanism for IEEE 802.11i-based Wireless Networks

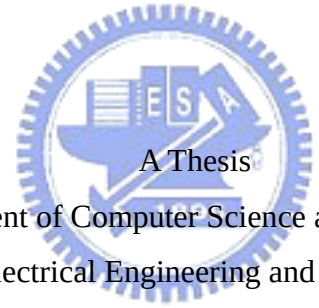
研 究 生：蔡亞軒　　Student：Ya-Hsuan Tsai

指導教授：曾建超　　Advisor：Chien-Chao Tseng

國 立 交 通 大 學 電 機 資 訊 學 院

資 訊 工 程 學 系

碩 士 論 文



A Thesis

Submitted to Department of Computer Science and Information Engineering

College of Electrical Engineering and Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer and Information Science

July 2005

Hsinchu, Taiwan, Republic of China

中華民國九十四年七月

IEEE 802.11i 無線網路快速換手之設計與實作

研究生：蔡亞軒　　指導教授：曾建超 博士

國立交通大學

資訊工程研究所碩士班

摘要

近年來無線網路的技術發展逐漸成熟，舉凡傳輸速度、傳輸距離都有大幅的進步，在各公共場合 (例如機場、車站及餐廳等等) 也佈建著許多熱點 (Hot Spot)，使用者可以透過這些熱點來連接上網際網路，使用網際網路上多元的服務。網路安全一直都是人們所關心的課題，無線網路帶給我們便利的上網服務，但也引出許多安全相關的問題，當我們使用無線網路時，有心人只要有電波接收的設備，就可以竊聽在空氣中傳遞的訊息，為此 IEEE 802.11 標準中規定使用有線等級私密 (Wired Equivalent Privacy) 來保護資料的安全性，但不幸的是，有線等級私密在設計上有重大瑕疵，其安全性已不足以被信賴，因此制定了 IEEE 802.11i 標準做為無線網路安全性的規範，IEEE 802.11i 使用更複雜的機制來達到資料的私密性和完整性，但也增加了行動節點 (Mobile Node) 在網路中換手 (Handoff) 的延遲時間。

為了加快換手的速度，讓上層應用程式能夠更順暢的進行，我們提出預先四訊息交換 (Pre-Four-Way-Handshake) 的方法避免 802.11i 四訊息交換的延遲。在我們提出的預先四訊息交換的機制中，行動節點在要執行換手之前，先透過目前所聯結的無線存取點 (Access Point) 和可能會換手到的目標無線存取點溝通，預先執行四訊息握手交換，並把成果用一特別的資料結構儲存起來，而此資料結構會擁有一唯一的識別名稱。配合著 IEEE 802.11i 中的預先認証程序 (Pre-Authentication)，行動節點在換手後僅需傳遞先前儲存的資料結構識別名稱，則無線存取點和行動節點雙方就可繼續進行一般資料的傳送，因換手而造成應用程式的暫時中斷也可以降到最低。

由於預先認証和預先四訊息握手交換行動節點都必須知道目標無線存取點的位址，所以我們提出一位置資訊交換架構來輔助快速換手的機制。在此架構中，設立有一台位置伺服器，此位置伺服器會有當地無線網路的基地台與認證伺服器的網路資訊及拓撲等知識，而行動節點會將本身目前的位置資訊告知位置伺服器，位置伺服器會

記錄下來並依行動節點過去的位置記錄，預測出行動節點可能會換手到的無線存取點，之後藉由雙方訊息的交換，讓行動節點得知目標無線存取點的位址，藉以輔助本論文快速換手的機制。

最後，我們實作出一套包含位置資訊交換及快速換手機制的系統雛型，以驗証我們所提出的方法。實作結果証明，我們的方法確實可行。

Design and Implementation of a Fast Handoff Mechanism for IEEE 802.11i-based Wireless Networks

Student：Ya-Hsuan Tsai Advisor：Dr. Chien-Chao Tseng

Department of Computer Science and Information Engineering
National Chiao Tung University

Abstract

With the advance of wireless internet technologies, the transmission rate of IEEE 802.11 networks increases significantly while the deployment cost decrease substantially. Many IEEE 802.11-based hot spots have been deployed in public areas, such as airports, transit stations, restaurants, and hotels, so that hot spots users can surf the Internet and subscribe services even when they are away from their home or offices. However one of the most important issues that remain to be solved in 802.11 networks is the security issue. The downside of using wireless technologies is that anybody can effortlessly eavesdrop messages in the air with a wireless network adapter. Therefore, IEEE 802.11 specification adopted wired equivalent privacy (WEP) to protect messages transferred in the air. Unfortunately, WEP has a significant flaw in security. Hence IEEE standard committees proposed 802.11i specification as the security enhancement for wireless environment. IEEE 802.11i employs more complex mechanism to achieve data confidentiality and integrity. However, it also increases the handoff delay time.

In this thesis, we adopted a new method, pre-four-way-handshake, to shorten the handoff delay of IEEE 802.11i four-way-handshake. Together with the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node (MN). Before commencing a handoff, an MN communicates with candidate target access points (APs), through the access point that the MN is currently associated with, to perform pre-authentication and pre-four-way-handshake.

Both the MN and each of the target APs store the results of pre-authentication and pre-four-way-handshake in a specific data structure, called security association (SA). Each SA has a unique identifier for identification purpose. The MN needs only send the corresponding identifier to the AP with which it newly associates. The AP then uses the identifier to find the MN's SA to retrieve the MN's authentication statuses and key materials. Because the MN have performed the authentication and key exchange procedures with the new AP before it starts a handoff process, the MN can continues transferring general packets immediately after it has associated with the new AP. Therefore the application interruption due to handoff can be reduced substantially by the pre-authentication and pre-four-way-handshake.

Because the MN needs to obtain the addresses of the candidate APs beforehand for pre-authentication and pre-four-way-handshake, we also proposed a location information exchange architecture to assist the fast handoff. In this architecture, there is a location server that maintains the configuration and topology information of APs. Besides, it also keeps track of MN's locations and predicts which APs the MN might handoff to. By exchanging messages with the location server, the MN can obtain the addresses of the candidate APs and perform pre-authentication and pre-four-way handshake when handoff is about to occur.

We have implemented a prototype that employs a location server for pre-authentication and pre-four-way-handshake in IEEE 802.11i-based networks. Experimental results show that our proposals are very effective.

誌謝

這篇論文能順利完成，首先要感謝我的指導教授—曾建超博士，在過去兩年之中提供良好的研究環境，並對於論文題目構思、內容撰寫及口試期間給予細心的指導以及實質的建議。感謝我的論文口試委員邵家健博士與紀光輝博士，感謝他們在百忙之中撥冗細心審查我的論文，並提供許多寶貴的意見，使我的論更加完善。我還要特別感謝實驗室所有同學、學長姐和學弟妹們的支持與鼓勵，讓我在兩年的碩士生涯中過得非常充實，謝謝你們。

此外，我還要感謝我的父母親、妹妹以及關心我的朋友們，在我遇到挫折和困難時，有你們的支持和鼓勵，讓我更能堅持地研究下去。

僅將此成果獻給我親愛的家人以及所有關心我的師長和朋友們。

目錄

圖目錄

表目錄

第一章　緒論

1.1　研究動機

近年來，各種無線傳輸技術蓬勃發展，在電信網路領域有 GSM、GPRS、3G 等，而在資料網路領域中則有藍芽、WiFi、WiMax 等技術，其中支援 WiFi 功能的設備數量以驚人的速度在成長，在許多公共場所也布有熱點 (hot spot) 提供民眾無線上網的服務。WiFi 是依據 IEEE 802.11[3]標準來運作的，其利用不需事先申請的頻段來傳輸資料，所以可以用較低的成本來架設出無線網路的環境，IEEE 802.11 無疑是當今最普及的無線網路技術。

由於無線網路會將資料在空間中傳遞，有心人士只要有電波接收設備，就可以截取到正在傳遞的封包，若被竊聽的是具高度機密性的資料，那後果可能不堪設想，因此 IEEE 802.11i[10]制定了一套安全性的規範，其中包含了加密演算法及資料完整性檢驗，可以保護訊息在空間中傳遞時的機密性 (confidentiality) 及完整性 (integrity)，也就是讓竊聽者無法取得訊息的本文或是修改訊息的內容。

在有線網路的環境下，我們必須將電腦和遠端網路孔用網路線連接才可以上網，而無線電波是在空間中自由放射，在沒有控管的情況下，只要持有電波的接送設備，任何人都可以使用無線網路，因此使用者的認証 (authentication) 和授權 (authorization) [1]就格外顯的重要，最終就是要達到只有合法的使用者才可以使用無線網路的資源。在 IEEE 802.11i 的標準裡也規定了認証和權限控管方式。

IEEE 802.11i 是一套附加於 IEEE 802.11 無線網路的安全性標準，其包含了 802.1x 連接埠網路存取控制 (Port-Based Network Access Control)[4]，用來達成使用者認証及連線存取控制的目的，及四訊息握手交換 (Four-Way Handshake) 用來導出加密金鑰，所產生的金鑰會用在 TKIP (Temporal Key Integrity Protocol) 或是 AES (Advance Encryption Standard) 等加解密演算法來保護封包的內容。

當行動裝置把連線從一無線存取點 (wireless access point) 交遞至另一基地台時，稱為換手 (handoff)，換手時行動裝置必須先切斷目前的連結，然後連結至新的基地台，之後再重新完成使用者認証和計算出加密金鑰的動作，而此時一般

的封包是無法正常傳送的，這段時間稱為換手延遲 (handoff delay)[8]。太長的換手延遲會造成網路應用程式的中斷，尤其目前當紅即時 (real-time) 服務對於中斷時間的要求更是嚴格，本論文就是研究在 IEEE 802.11i 網路下快速換手的方法，以期使得換手延遲對網路應用程式的影響降到最低，也讓使用者感受不到換手的發生，最後達到順暢換手 (smooth handoff) 的目的。

1.2 研究目標

在一個支援 IEEE 802.11i 安全性規格的無線網路環境中，換手的過程可以分為以下幾個步驟：

a、 行動節點 (Mobile Node，MN) 偵測自己和目前所聯結無線存取點的連線訊號，若訊號降低到某一門檻之下，則行動節點會選擇另一訊號較好的無線存取點做為換手的目標。

b、 行動節點切斷和目前無線存取點的連線，並和目標無線存取點聯結。

c、 行動節點和無線網路系統後端的認証中心 (authentication server) 進行 IEEE 802.1x 身份認証的動作。

d、 行動節點和無線存取點進行四訊息握手交換，計算出對應的加密金鑰。

e、 行動節點把金鑰安裝至加解密模組，開始繼續傳送正常的封包。

其中 a 和 b 的步驟需要的時間是根據網路卡上的晶片以及韌體運作來決定的，不同廠牌的網路卡和基地台也會有不同的數據，由於依賴硬體製造的因素太重，所以我們不由此方面來著手。步驟 e 所需要的時間則是依據行動節點的系統運算能力。

而 c 的步驟在 IEEE 802.11i 標準裡已定義了預先認証 (pre-authentication) 的方法，當行動節點在換手之前先對目標的無線存取點進行預先認証，使得在換手之後可以省略此認証動作而直接進行下一步驟。

在針對上述 d 的步驟，本論文提出了利用預先四訊息握手交換 (pre-four-way-handshake) 的方式來降低此階段所需要的時間，我們設計了一套新的訊息交換流程來達成。而為了能夠做到正常順利的換手，無線存取點必須能夠

知道行動節點是否已做過預先四訊息握手交換，對此我們將標準規格做了一些修改。

在原先的標準裡，四訊息握手交換可以檢查出行動節點和無線存取點預先認証是否成功，而在本論文裡使用預先四訊息握手交換來降低換手延遲，則必須有另一個機制來檢查預先四訊息握手交換是否成功，而此機制要符合簡單快速的原則，若此機制所需要的時間很長，則預先四訊息握手交換所增加的效能將會大打折扣。

在整個快速換手的機制中，我們建立一個位置伺服器 (location server)，用來記錄並管理行動節點目前的位置資訊，而行動節點也會週期性的向位置伺服器更新自己的連線狀況，當行動節點的連線訊號降低到某一門檻時，會向位置伺服器送出要求，而位置伺服器會回覆一個候選無線存取點列表，行動節點則可以依此列表來進行預先認証及預先四訊息握手交換的動作。而在位置伺服器上我們可以利用行動節點的位置資訊來做目標無線存取點的挑選，減少預先認証及預先四訊息握手交換所造成的負擔，讓整體的快速換手效能更加提升。

本論文的研究目標為下：

1. 利用預先四訊息握手交換建構出一支援快速換手的無線網路環境。
2. 設立一位置伺服器來記錄行動節點的位置資訊，並提供目標無線存取點列表給對應的行動節點。

1.3 章節簡介

本論文的章節內容簡述如下：

第一章：描述本論文的研究動機，以及本論文想要達到的目標。

第二章：簡介本論文中相關的研究背景，包括 IEEE 802.11 無線網路、IEEE 802.1x 認証及存取控管機制和 Robust Security Network 以及相關論文的研究探討。

第三章：介紹我們所提出快速換手機制的設計方法，包括預先四訊息握手交換設計方法以及利用位置資訊增加換手效能設計方法。

第四章： 介紹我們實作出整套系統的方式，包括使用的軟硬體架構，新增或是修改過的封包格式。

第五章： 以範例說明本系統和原先效能上的差別，並舉出實際操作的例子來顯示整個系統的運作狀況。

第六章： 總結整篇論文，並提出未來可繼續研究的方向。

第二章　背景與相關研究

2.1　IEEE 802.11 無線網路簡介

IEEE 802.11 標準是目前被廣泛使用的無線網路傳輸技術，在這標準中定義了無線網路的實體層 (Physical layer) 以及媒介存取控制層 (Media Access Control layer，MAC) 運作方式，由於 IEEE 802.11 無線網路所使用的無線電頻率是位於 ISM (Industrial、Scientific、Medical) 頻段，因此我們不必向政府機關申請執照，就可以自行架設出 IEEE 802.11 無線網路環境，這優勢加速了 IEEE 802.11 無線網路的發展，同時也產生了許多新的問題和考量，時至今日，許多相關標準仍然還在討論和制定當中。

IEEE 802.11 無線網路可以分為兩種運作模式：具基礎建設網路模式 (infrastructure mode) 以及無線隨意網路模式 (Ad-Hoc mode)，如圖 2.1 所示，具基礎建設模式下各行動節點的資料傳輸都必須要透過無線存取點 (access point)，而無線隨意網路模式則是由各行動節點自行負責資料傳輸的動作，本論文則著重於具基礎建設網路模式下的研究。

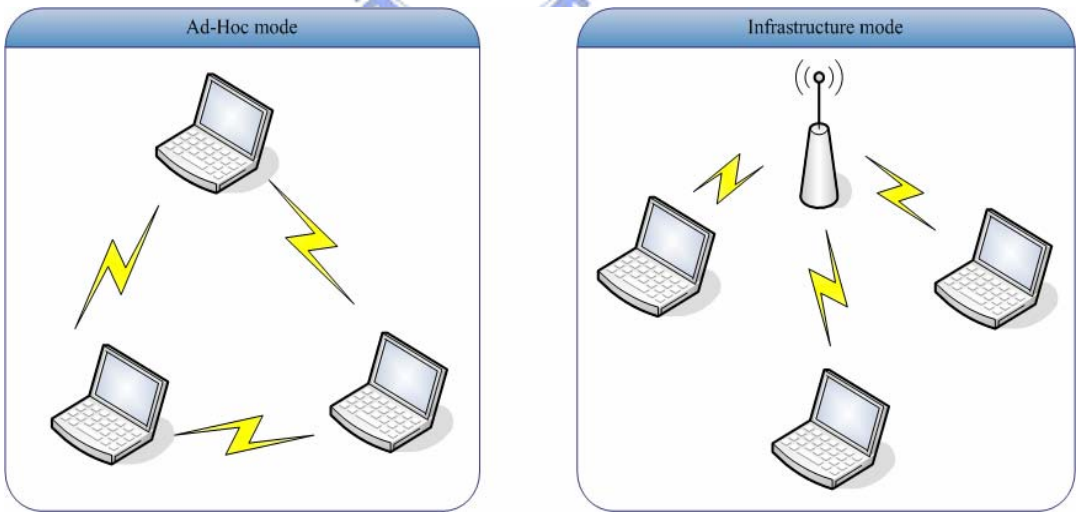


圖 2.1　具基礎建設無線網路及無線隨意網路示意圖

在具基礎建設網路模式下，行動節點想要透過無線存取點來連接上網際網路，必須依照 IEEE 802.11 無線網路的規定完成三個階段，並且和無線存取點達成聯結，之後才可以傳送一般資料封包。此三個階段依序為：探查 (probe)、身份

認証 (authentication) 以及聯結 (association)。茲將介紹於下。

探查的目的是要搜尋目前環境下是否有無線存取點的存在，可分為被動式掃描 (passive scan) 和主動式掃描 (active scan)。無線存取點會定時發出信標 (beacon)，某行動節點可以聆聽這些信標就可得知是否有無線存取點存在，這樣稱為被動式掃描。主動式掃描則是行動節點主動送出探查要求 (probe request) 的封包，無線存取點在收到探查要求後，會送出探查答覆 (probe response) 做回應，這樣行動節點也可以了解目前所處環境下無線存取點分布的狀況。

身份認証是為了驗証使用者的身份，也分為兩種：開放系統身份認証 (open system authentication) 和共享金鑰身份認証 (shared key authentication)。其中開放系統身份認証並不做任何的身份檢查，而共享金鑰身份認証則利用一事先取得的金鑰做為驗証身份的依據。

聯結為資料傳輸前的最後一個步驟，在此階段行動節點會取得一聯結識別碼 (Association ID，AID)，此識別碼是基地台用來分辨聯結到該基地台的行動節點所用。

圖 2.2 為整個 IEEE 802.11 連線狀態圖：

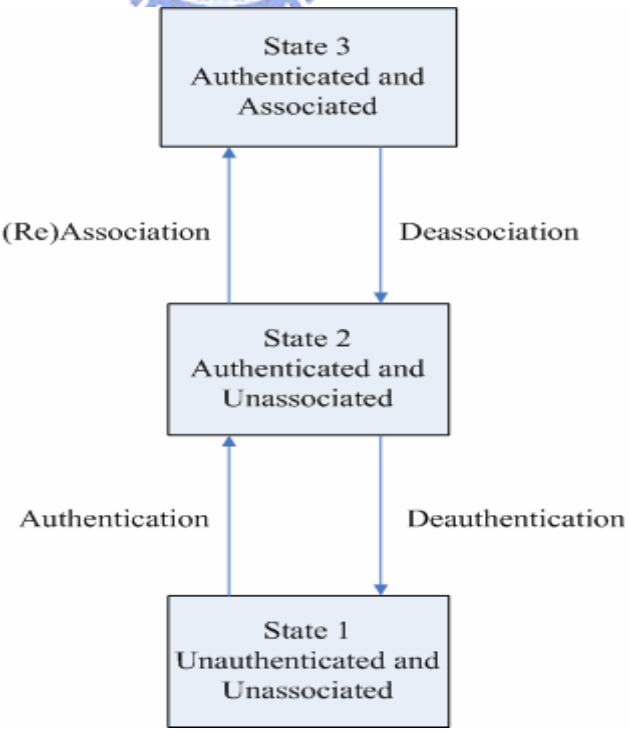


圖 2.2 IEEE 802.11 連線的整體狀態圖

無線網路利用電波訊號傳遞資料，有心人士只要有電波的接收設備即可以攔截在空氣中傳輸的資料，因此 IEEE 802.11 標準也規定了一套維護資料的安全性的機制，稱為有線等級隱私 (wired equivalent privacy，WEP)，有線等級隱私使用 RC4 演算法來加密傳遞的資料，使用 40 至 120 位元長度的加密金鑰，但不幸的是，有線等級私密已被証實在設計上的發現了重大瑕疵[5]。因此，IEEE 提出了一個新的安全性標準—IEEE 802.11i 標準，也就是所謂的 RSN (Robust Security Networks)，這將在之後的章節做介紹。

2.2 IEEE 802.1x 連接埠網路存取控制

近年來，網路安全的重要性漸漸的被人們所重視，尤其現今無線網路快速成長，由於電波可在空氣中自己傳送，行動節點只要有無線網卡，就可以透過無線存取點連結上網路，而系統端必須做好權限的控管，強制未經過身份認証的使用者先做一個認証的動作，這點對無線網路服務提供者 (wireless ISP) 是非常重要的，因為無線網路提供者會依據使用者的連線時間或封包傳遞大小來收費，若是身份認証的機制沒做好，會造成很多使用者與服務提供者的糾紛。即便是免費的無線網路環境，例如在大學的圖書館內，網路管理者也不會希望使用者未經身份認証就可以使用無線網路，由此可知身份認証及網路存取控制是環路安全中很重要的一環。

IEEE 802.1x 制定了身份認証及網路存取控制的架構，它是以一個類似連接埠 (port) 的概念，如下圖 2.3 所示，所有的服務存取動作都必須透過一個連接埠來完成，在未經過身份認証及授權之前，連接埠是關閉的，也就是除了身份認証的訊息之外，其餘的封包訊息都無法通過，此時必須先與後端的認証中心完成身份認証並取得授權，連接埠才會打開，才可以正常使用所提供的服務。

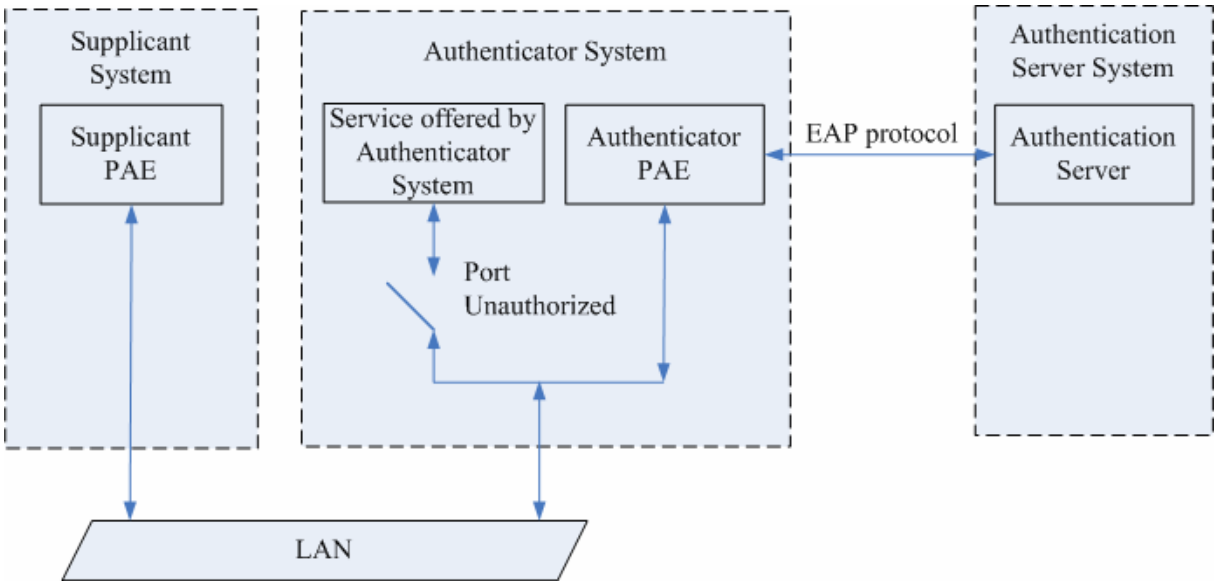


圖 2.3　IEEE 802.1x 示意圖

2.2.1　IEEE 802.1x 系統架構

圖 2.4 是 IEEE 802.1x 的系統架構，主要可以分成三種元件：

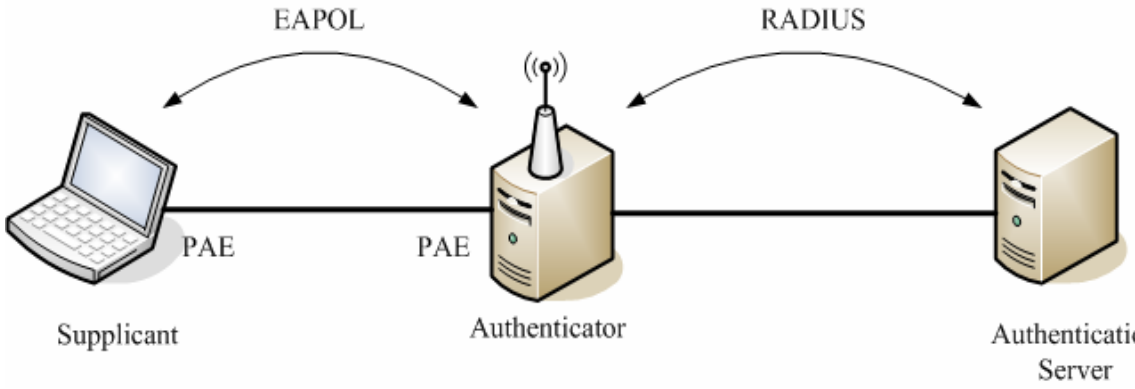


圖 2.4　IEEE 802.1x 系統架構

申請者 (Supplicant)：尋求存取網路資源的使用者機器，在本論文裡通常是指行動裝置或是手持式裝置。

認証者 (Authenticator)：負責控制網路存取，阻擋未經身分認証使用者機器所送出的封包，以及轉送認証封包至認証伺服器，通常由無線存取點擔任。

認証伺服器 (Authentication Server)：所有的認証需求都會被轉送至此，認証中心維護著使用者的資訊，並且決定使用者的認証是否成功以及授權相關事宜。

相關的通訊協定有：

EAPoL (EAP over LAN)：在申請者和認証者之間做訊息的溝通交換，用來承載上層的可延伸認証通訊協定封包，也就是 IEEE 802.1x 封包。

RADIUS (Remote Access Dial-In User Service)[6]：在認証伺服器和認証者之間做訊息的溝通交換，同樣也是用來承載上層的可延伸認証通訊協定封包。

Diameter[7]：同 RAIDUS 功能，但 Diameter 通訊協定在制定時考慮了更多的層面，像是移動管理 (mobility management) 等等，是目前新一代的認証通訊協定。

相關的名詞有：

PAE (Port Access Entity)：具有連接埠認証實體的行動節點，通常是具有認証者、申請者或兩者的功能。

2.2.2 可延伸認証通訊協定 (Extensible Authentication Protocol，EAP)

IEEE 802.1x 定義了申請者、認証者和認証中心三種元件的運作，但真正帶有認証資訊的是 IEEE 802.1x 上層所承載的可延伸認証通訊協定[2]，下圖 2.5 說明了可延伸認証通訊協定的架構。

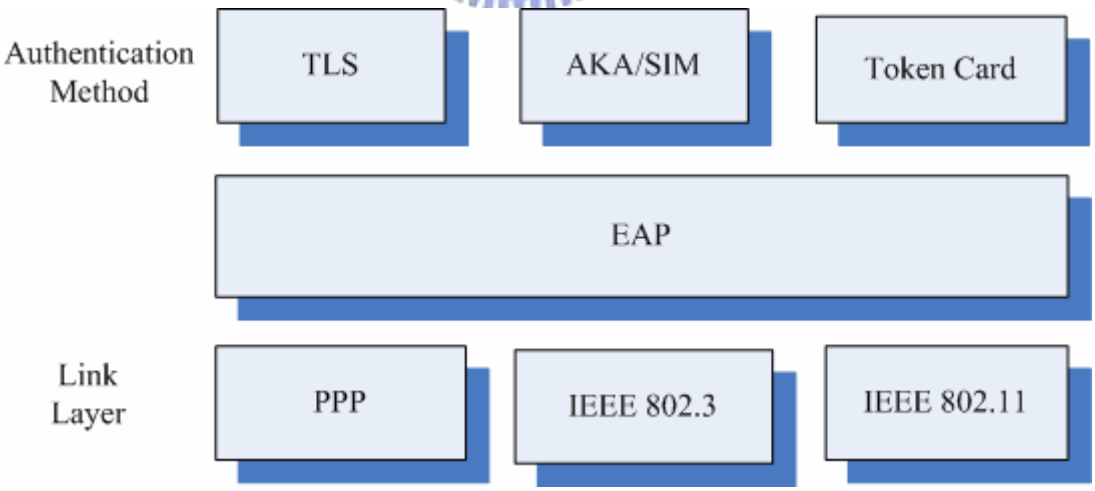


圖 2.5 可延伸認証通訊協定系統架構

由圖 2.5 可知，可延伸認証通訊協定依照不同環境和使用者資訊，可以搭配上層的多種認証方式，像是圖中的一般標記卡 (Generic Token Card，GTC) 是以隨機的方式提供單次密碼的身份認証；SIM/AKA 則是利用手機裡的 SIM 卡來計

算認証所需要的資料；傳輸層安全性 (Transport Layer Security，TLS)[11] 則是用簽發憑証 (Certification Authority) 的方式達成，比較特殊的是傳輸層安全性可以讓雙方互相認証對方的身份，這項特性可以避免惡意人士偽造無線存取點來竊取申請者的資料，本論文在實作上也是採用此種認証方式。

一般的可延伸認証通訊協定訊息交換程序如圖 2.6：

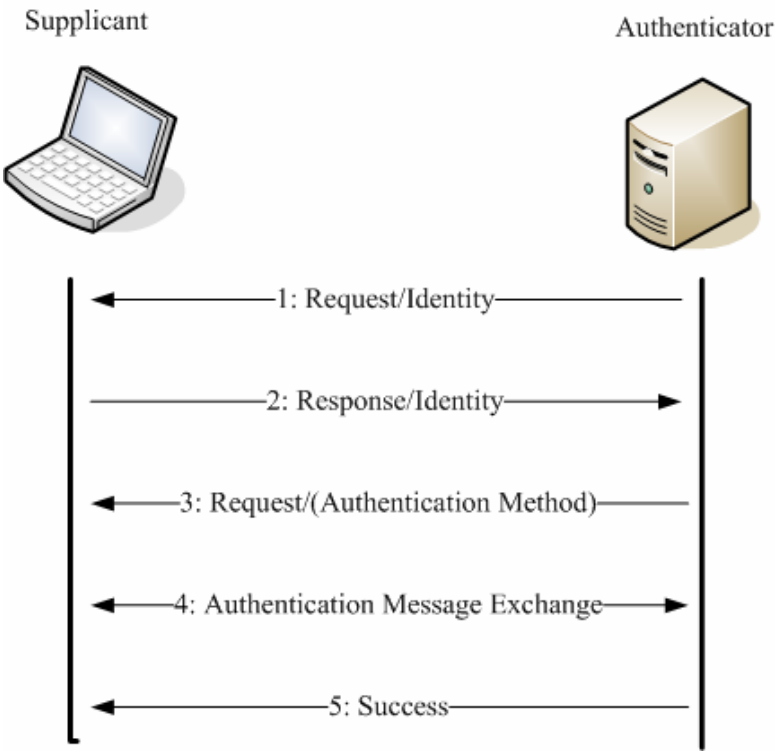


圖 2.6　可延伸認証通訊協定訊息交換程序

1. 認証者首先發出一個 Request/Identity 封包以辨識使用者身份。
2. 申請者將使用者識別碼以 Response/Identity 訊息送出。
3. 一旦辨認出該使用者，認証者隨即以要求 (Request) 封包送出認証盤查，並指明所想要進行的認証方式。
4. 用戶端和認証者進行身份認証訊息交換。
5. 用戶端認証成功，因此認証者發出一個成功的訊息 (Success)。同時也開始提供之前所要求的服務給用戶端。

2.2.3 IEEE 802.1x 運作流程

IEEE 802.1x 和無線網路共同運作的流程如下，其中認証的部分是使用可延伸認証通訊協定，由圖 2.7 可看出原本在可延伸認証通訊協定認証者的角色，在 IEEE 802.1x 中分為認証者和認証伺服器，而申請者可以用 EAPOL-Start 和 EAPOL-Logoff 的訊息來主動要求認証程序或終止目前認証成功的狀態，一般的可延伸認証通訊協定封包則由 EAP-Packet 類別的 IEEE 802.1x 來承載。

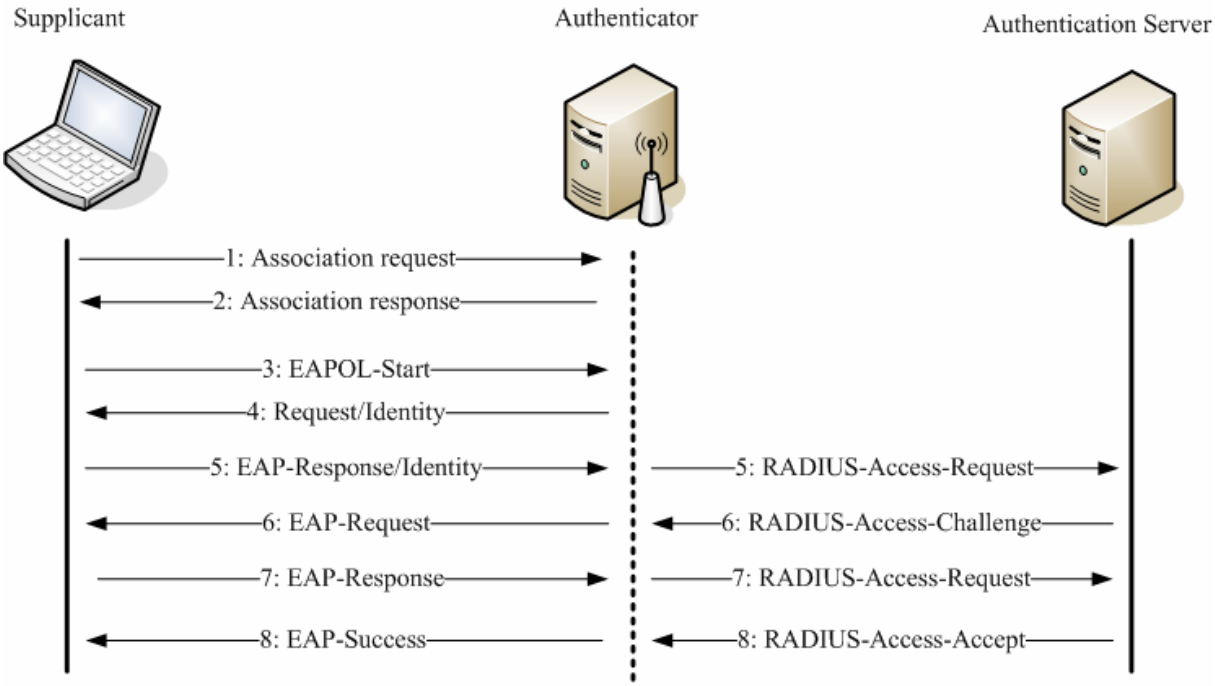


圖 2.7 IEEE 802.1x 交換程序

1. 申請者向無線存取點要求聯結。
2. 無線存取點回應聯結的要求。
3. 申請者以一個 EAPOL-Start 訊息啟始 IEEE 802.1x 交換程序。
4. 開始可延伸認証通訊協定交換程序，認証者會發出一個 EAP-Request/Identity 封包。
5. 申請者回應一個 EAP-Response/Identity 封包，此封包會被轉送到 RADIUS 認証伺服器，作為 Radius-Access-Request 封包。
6. RADIUS 認証伺服器回應一個 Radius-Access-Challenge 封包，此封包會

隨即被當作 EAP-Request 轉送給申請者，其中包含相關的盤查訊息。

7. 申請者計算出盤查的解答包含於 EAP-Response 訊息送回，此訊息由認証者轉換為 Radius-Access-Request 送到認証伺服器上。

8. RADIUS 認証伺服器最後以一個 Radius-Access-Accept 訊息核准對方存取網路，因此認証者會發出一個 EAP-Success 的訊息給申請者，並完成整個 IEEE 802.1x 認証程序。

當完成 IEEE 802.1x 身份認証，認証伺服器和申請者會產生同一把成對主金鑰 (Pairwise Master Key，PMK)，之後認証伺服器會將此成對主金鑰送至認証者，也就是送至無線存取點上，所以 IEEE 802.1x 的目的是申請者向認証伺服器做認証的動作，而認証成功後申請者和無線存取點則會持有同一把成對主金鑰。

2.3 Robust Security Networks

Robust security networks (RSN) 是由 IEEE 802.11i 所定義出的一種網路型態，其考量了當網路從有線到無線所會面臨到的一些挑戰，制定出一套新的安全性網路標準，相較於原先以有線等級隱私為基礎的無線網路環境，RSN 有以下特性：

1. 更難破解的加解密演算法，演算法的金鑰長度也隨之增長。

2. 強制使用 IEEE 802.1x 來負責認証和存取控管的任務。

3. 使用複雜的金鑰管理 (key management) 和階層 (hierarchy)，維護金鑰的新鮮性 (freshness) 和完整性。

RSN 必然是未來無線網路的強制性標準，但由於目前網路卡設備功能的限制，我們無法只藉由韌體的升級達到 RSN 的要求，也就是說全 RSN 網路並不可能在一夜之間完成，但相信不久符合 RSN 規格的產品也會陸續問世，到時無線網路的安全性又邁向前了一大步，讓無線網路更加的普及化。

2.4.1 RSN 系統架構

依據 IEEE 802.11i 的規格，一行動節點要透過無線存取點使用網路的資源，

必須依序執行以下幾個程序。

- IEEE 802.11 三動作：如 2.1 節所所敘述，行動節點必須和無線存取點完成探查、身份認証、聯結等動作。
- IEEE 802.1x 身份認証：如 2.2 節所敘述，行動節點是扮演申請者的角色，透過由無線存取點所扮演的認証者，跟後端的認証伺服器執行 IEEE 802.1x 認証的動作，當此階段身份認証完成，無線存取點和行動節點會持有同一把成對主金鑰。
- 四訊息握手交換：在此階段行動節點和無線存取點會進行一系列訊息的交換，將前一階段所獲得的成對主金鑰經計算而導出成對暫時金鑰(Pairwise Transient Key，PTK)，此成對暫時金鑰會當做加解密演算法的金鑰，用來保護封包的私密性和完整性。詳細的四訊息握手交換流程會在 2.3.3 節說明。
- 安裝並使用成對暫時金鑰：此階段行動節點和無線存取點會將所導出的成對暫時金鑰安裝於加解密演算法中，並建立一個安全的通道，之後所傳遞的封包都會有私密性和完整性的保護。

整個 IEEE 802.11i 網路連線狀態圖如圖 2.8。

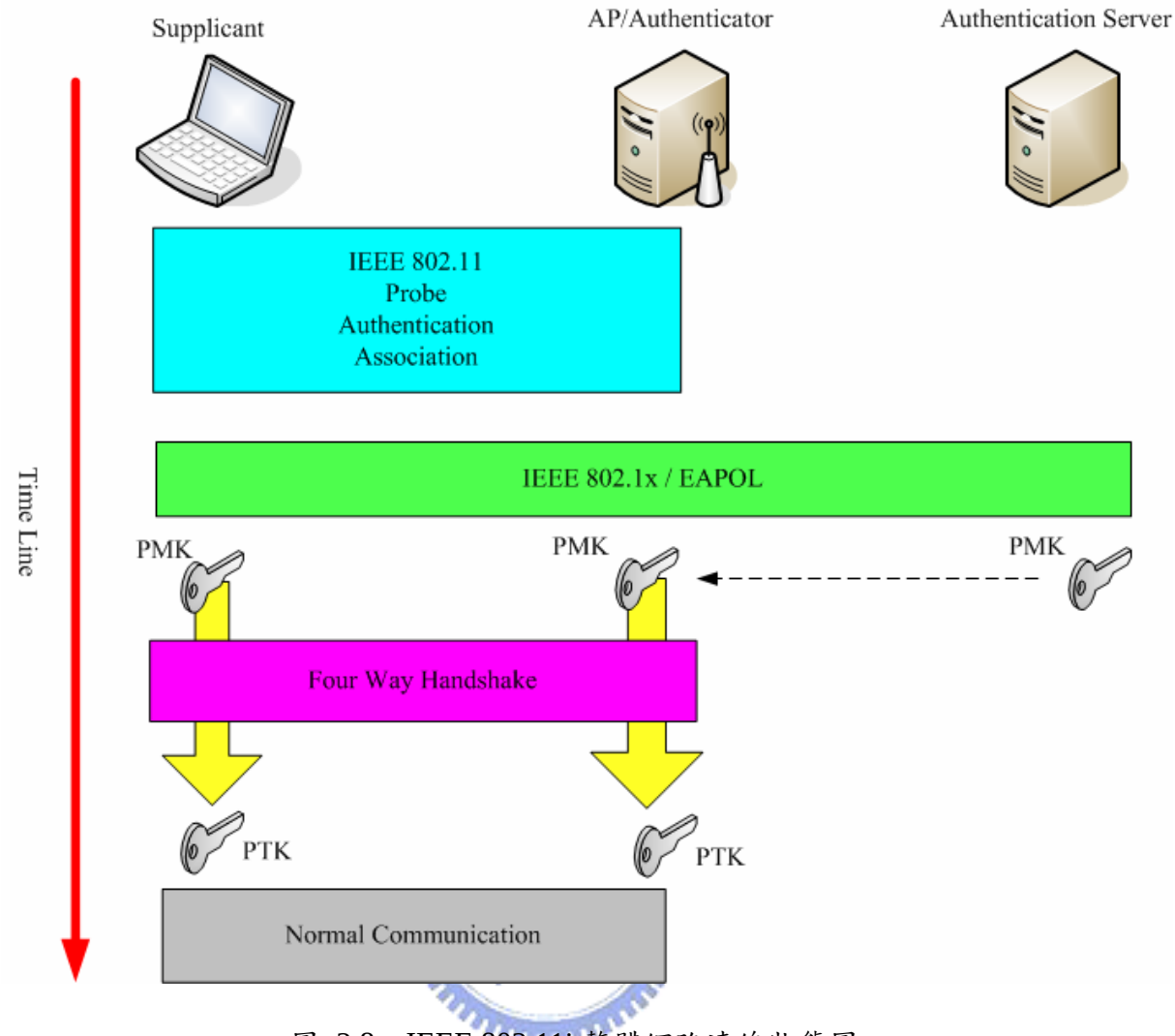


圖 2.8 IEEE 802.11i 整體網路連線狀態圖

由於有線等級私密已被証明有重有的設計瑕疵，IEEE 802.11i 為了補足這個問題，使用了 TKIP (Temporal Key Integrity Protocol) 或是 AES (Advance Encryption Standard) 等演算法來保護資料，茲將有線等級私密的缺點以及 TKIP 針對有線等級私密而改進的地方列於表 2.1 和表 2.2。

1	初始向量 (initial，IV) 長度太短。
2	由初始向量所計算出的金鑰，容易受到脆弱金鑰攻擊 (weak key attacks) 的影響。
3	沒有一個有效方法偵測出訊息被竄改。
4	直接使用主金鑰而沒有一個內定的規範何時要更新金鑰。

5	對於重送訊息攻擊 (reply message attack) 沒有保護的機制。

表 2.1　有線等級私密的缺點

目的	改進的地方	著重的缺點
訊息完整性	新增一個訊息完整性檢查方法來防止訊息被竄改。	3
初始向量選擇	改變初始向量的選擇方法。	1、3
單一封包金鑰混合	對每個封包更改加密金鑰。	1、2、4
初始向量長度	增加初始向量的長度避免用到同一初始向量。	1、4
金鑰管理	增加金鑰散布機制並更改廣播金鑰。	4

表 2.2　TKIP 針對有線等級私密的改進

AES 則是美國 NIST (National Institute for Science and Technology) 公開徵選的新一代對稱式加密演算法，經過幾輪的投票和篩選，最後由 Joan Daeman 和 Vincent Rijmen 兩個所提出的 Rijndael 演算法做為標準。雖然 AES 演算法可以使用 128、192 或是 256 位元做為金鑰及加密區塊大小，但是 IEEE 802.11i 則進一步限制只能使用 128 位元的金鑰及加密區塊大小。

2.4.2　RSN 金鑰管理 (key management)

RSN 把金鑰分成兩大類，一個是成對主金鑰，而另一則是成對暫時金鑰。成對暫時金鑰是由成對主金鑰及其它資料計算而得。

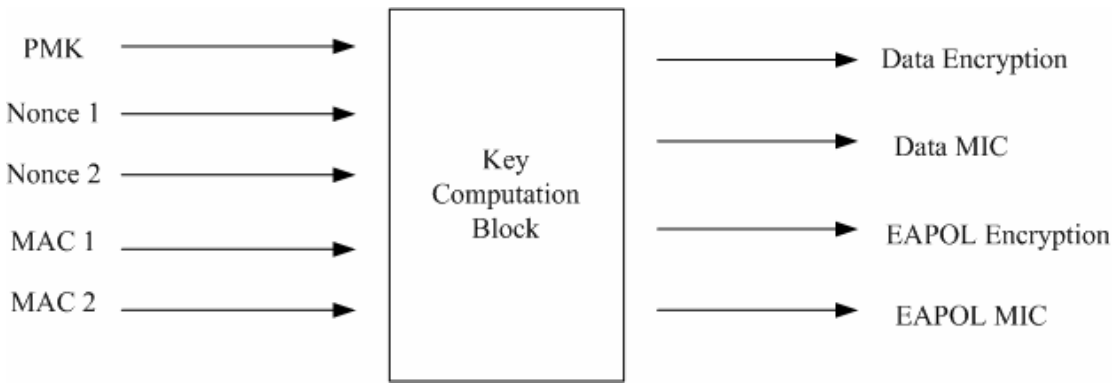


圖 2.9　成對暫時金鑰的計算

如圖 2.9 所示，成對暫時金鑰又可以分為四種，分別當作不同時期訊息完整性檢查碼 (Message Integrity Code，MIC) 所要用的金鑰及訊息私密性金鑰：

- 資料加密金鑰 (Data Encryption key)
- 資料完整性金鑰 (Data Integrity key)
- EAPOL-Key 加密金鑰 (EAPOL-Key Encryption key)
- EAPOL-Key 完整性金鑰 (EAPOL-Key Integrity key)

其中前兩把成對暫時金鑰是用於四訊息握手交換後，傳遞一般封包時用的，而後兩把以 EAPOL-Key 開頭的成對暫時金鑰則是用來保護四訊息握手交換中的封包。圖 2.10 及 2.11 說明了成對暫時金鑰是如何計算以及 RSN 的金鑰階層 (key hierarchy)，其中 PRF-X 是代表一個準亂數函數 (pseudo random function) 會產生 X 位元長度的輸出值。由此可看出若使用 AES 演算法，資料加密金鑰和資料完整性金鑰為同一把 128 bits 長度的金鑰。而若使用 TKIP 演算法，則資料加密金鑰和資料完整性金鑰各為 128 bits 長度的兩把金鑰。

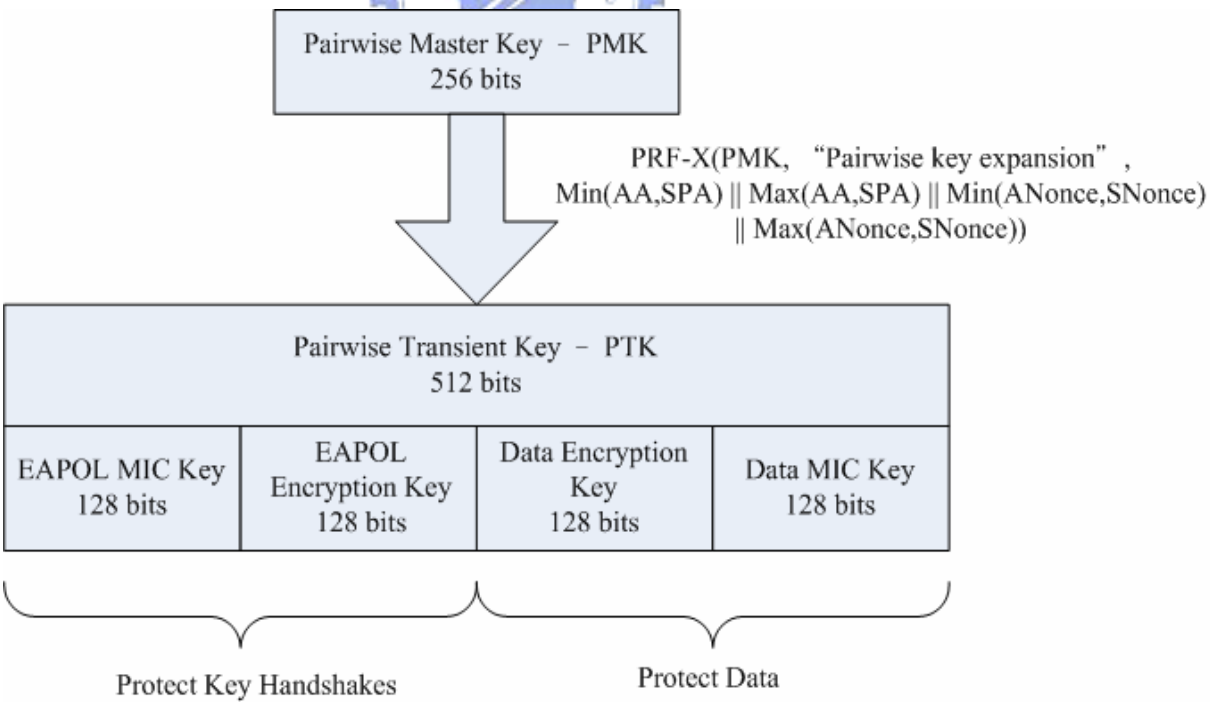


圖 2.10 RSN 金鑰階層(TKIP)

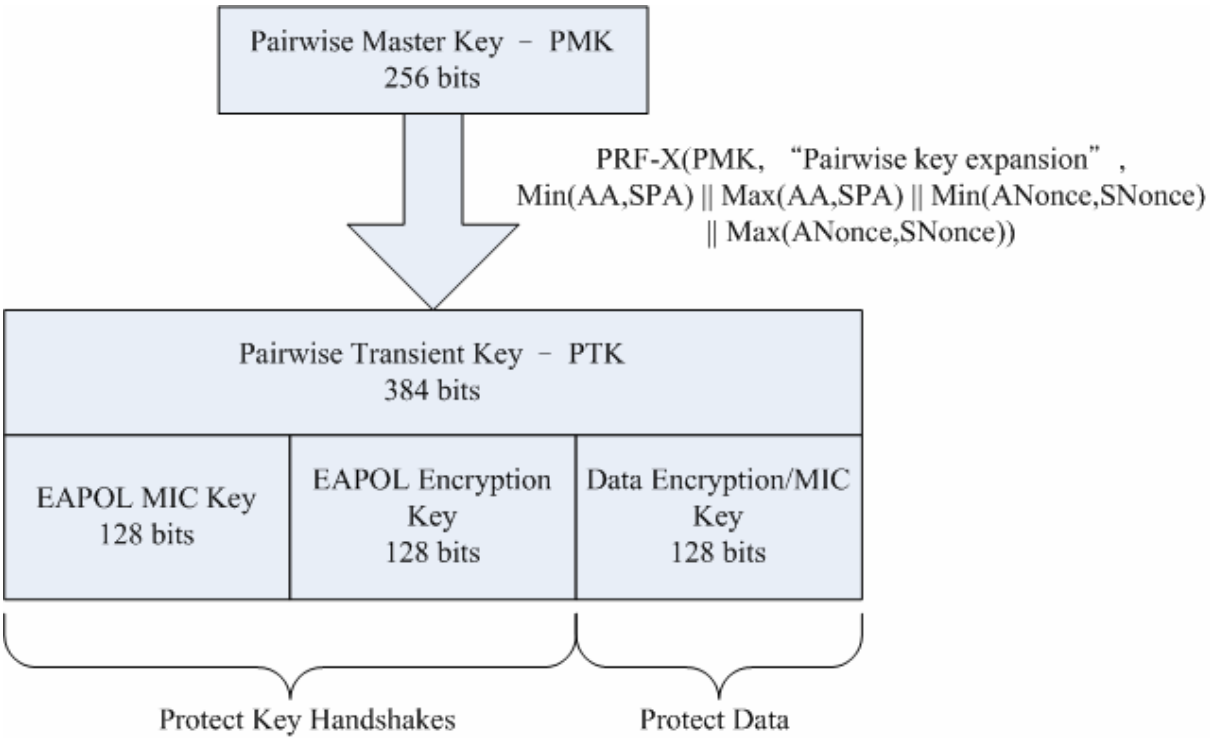


圖 2.11 RSN 金鑰階層(AES)

2.4.3 四訊息握手交換 (four way handshake)

當申請者完成 IEEE 802.1x 身份認証之後，會接著執行四訊息握手交換的程序。四訊息握手交換是由申請者和認証者來完成，其中包含四個訊息的來回，都是以 EAPOL-Key 的封包格式來傳遞，故得此命名。四訊息握手交換的目的如下：

- 確認申請者和認証者雙方持有同樣有效的成對主金鑰。
- 計算出成對暫時金鑰。
- 同步把成對暫時金鑰安裝於網路卡並開始進行加密資料傳遞的時機。

圖 2.12 是四訊息握手交換詳細流程圖，茲將介紹於下。

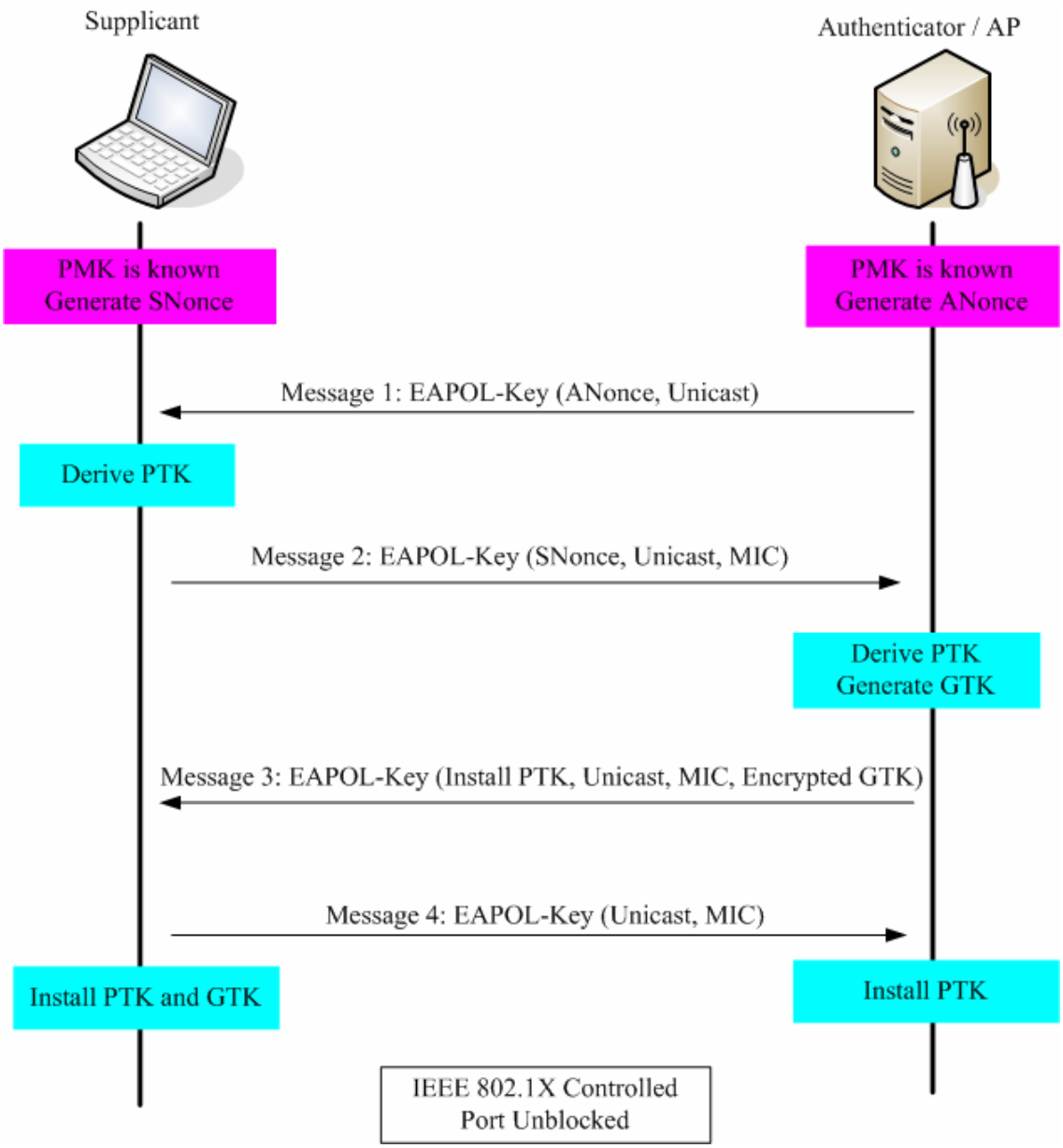


圖 2.12　四訊息握手交換流程圖

1. 由於之前的 IEEE 802.1x 認証完成，所以申請者和認証者會持有同樣的成對主金鑰，此時雙方各自產生一個亂數，將會用於之後的四訊息握手交換裡，此兩亂數稱為 SNonce 和 ANonce，分別為申請者和認証者所產生。

2. 認証者送出訊息一，其中最重要的欄位是由認証者所產生的亂數 ANonce。

3. 當申請者收到訊息二之後，會用本身產生的 SNonce 和接收的 ANonce

依上節所敘述的公式計算出成對暫時金鑰。

4. 申請者送出訊息二，其中最重要的欄位是由申請者所產生的亂數 SNonce，而訊息二的整個封包，會利用成對暫時金鑰裡的 EAPOL-Key 完整性金鑰來計算出訊息完整性檢查碼，用來保護訊息二的內容不被竄改。

5. 當認証者收到訊息二之後，會用本身所產生的 ANonce 和接收的 SNonce 依上節所敘述的公式計算出成對暫時金鑰，接著認証者會用成對暫時金鑰裡的 EAPOL-Key 完整性金鑰來檢查封包裡的訊息完整性檢查碼是否正確，若檢查失敗則代表訊息二的封包有被竄改的可能，認証者將會丟棄此封包。假如有必要的話，認証者也會重新產生群組暫時金鑰 (Group Transient Key，GTK)。

6. 認証者送出訊息三，其中帶有利用成對暫時金鑰裡的 EAPOL-Key 加密金鑰來加密的群組暫時金鑰，也有一個安裝成對暫時金鑰 (install PTK) 的指示，同樣的訊息三也會計算出一訊息完整性檢查碼來保護封包不被竄改。

7. 當申請者收到訊息三，會檢查該封包的訊息完整性檢查碼是否正確，倘若正確無誤，認証者會將訊息中的群組暫時金鑰解密並取出。

8. 申請者送出訊息四來指示對方已完成四訊息握手交換的程序。

9. 申請者及認証者安裝成對暫時金鑰及群組暫時金鑰，同時雙方 IEEE 802.1x 連接埠也打開，開始一般封包的傳送。

2.4.4 預先認証 (pre-authentication)

在 IEEE 802.11i 的規格裡也定義了利用預先認証 (pre-authentication) 加快換手速度的方式，當執行預先認証的程序時，則會有下列兩件事情發生：

- 行動節點的換手決定和 IEEE 802.1x 身份認証將是兩個獨立的事件。換句話說，即使行動節點和目前聯結的無線存取點訊號良好，行動節點仍然可以和其它的無線存取點做身份認証，雖然行動節點並沒有換手的打

算。

- 行動節點可以同時和多個無線存取點進行 IEEE 802.1x 身份認証。

一般的 IEEE 802.1x 封包是使用乙太型別 (EtherType) 88-8E 來作為上層協定辨識，無線存取點會針對此型別的封包做特殊的處理，也就是會將此型別的封包交給 EAPOL 的模組來處理，為了要跟 EAPOL 封包做分別，預先認証的封包則會使用乙太型別 88-C7 來做辨識，而當無線存取點收到此型別的封包，將會和其它任意型別的封包一樣的處理，也就是利用分散式系統 (distribution system，DS) 把封包傳遞出去。而在預先認証程序中，IEEE 802.1x 只限於傳送 EAP-Packet 和 EAPOL-Start 這兩種類別的封包。

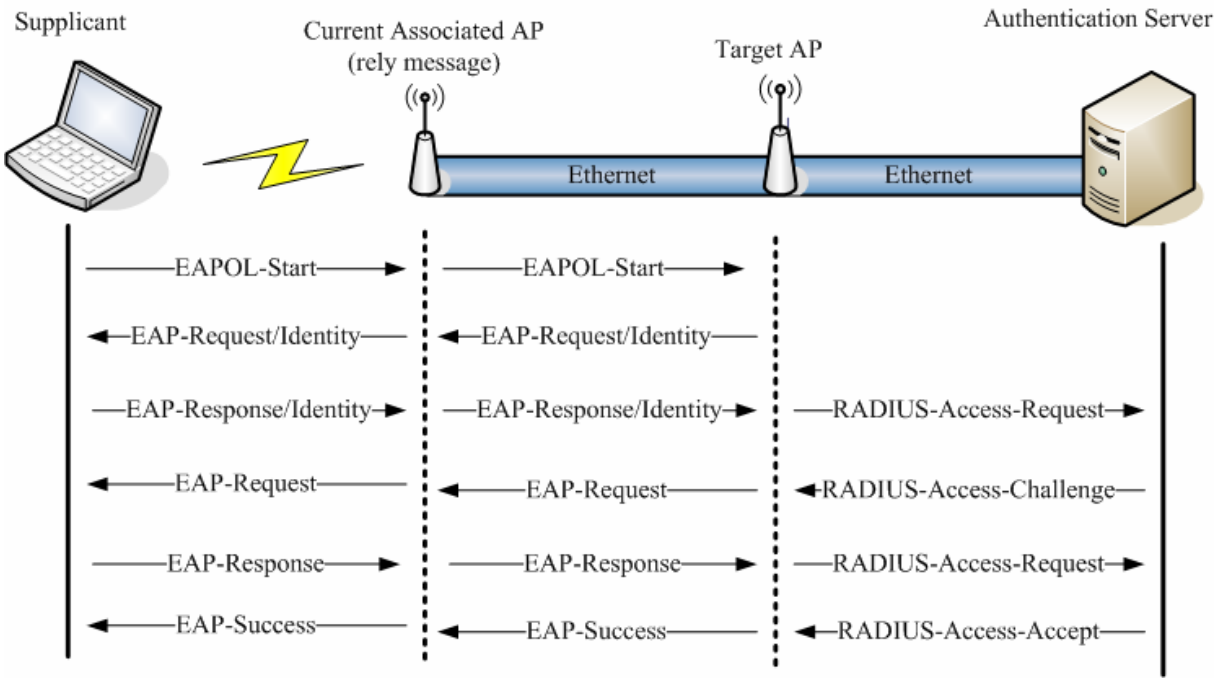


圖 2.13　預先認証流程圖

圖 2.13 說明了預先認証的流程，由圖可看出行動節點欲跟目標無線存取點進行預先認証，則必須透過目前聯結的無線存取點做轉送，此時有一個很重要的先決必要條件：行動節點知道目標無線存取點的媒體存取控制層位址 (MAC address)。當行動節點在目標無線存取點的電波範圍之內，則可以聽到該基地台的信標進而得知媒體存取控制層位址，但若行動節點不在電波範圍內，則必須依靠別的機制才能得知此資訊，本論文利用位置伺服器以及位置資訊交換流程來解決此問題。

當預先認証成功之後，行動節點和目標無線存取點會持有同樣一把成對主金鑰，而雙方會用 PMKSA (PMK Security Association) 的資料結構儲存，之後行動節點換手到該目標無線存取點，就可以利用 PMKSA 而省略 IEEE 802.1x 身份認証，直接進行四訊息握手交換的程序。

2.4 相關論文研究

2.4.1 Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE 802.1x Model[17]

這篇論文是由 Sangheon Pack 和 Yanghee Choi 兩位所提出，它提出了一個利用頻繁換手區域 (Frequent Handoff Region，FHR) 概念達到快速換手的機制，在行動節點聯結到目前的無線存取點後，會由目前無線存取點向外擴展出一個頻繁換手區域，之後行動節點會向在此區域中的無線存取點執行預先認証的動作，而此頻繁換手區域則是利用一些參數計算而得的，圖 2.14 左半是一具權重及方向圖 (weighted directed graph)，而其各邊 (edge) 的權重計算方式如下：

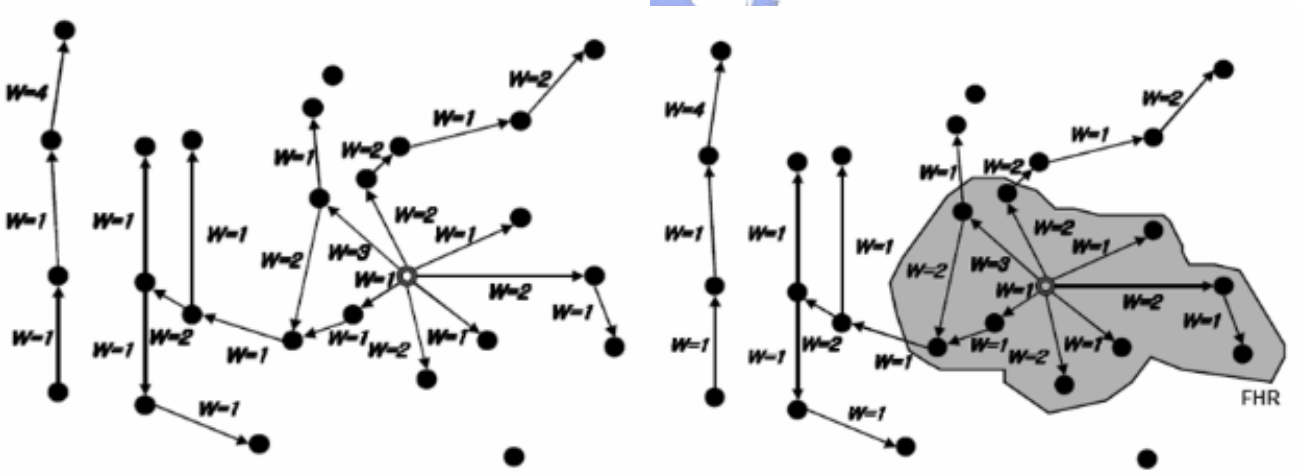


圖 2.14 頻繁換手區域的選擇

$$H(i,j)=\frac{N(i,j)}{R(i,j)} \qquad W(i,j)\propto\frac{1}{H(i,j)}$$

N(i,j)：由無線存取點 i 換手至無線存取點 j 事件發生的次數。

R(i,j)：當由無線存取點 i 換手至無線存取點 j 事件發生時，在無線存取點 i

停留的時間的總和。

H(i,j)：由無線存取點 i 換手至無線存取點 j 的換手比例 (handoff radio)。

W(i,j)：無線存取點 i 及 j 之間邊的權重，會和 H(i,j)成反比關係。

接著會執行頻繁換手區域的選擇，選擇的方式是由目前聯結的無線存取點向外擴展，且會用兩個參數來控制區域的大小，一個是最大 hop 數，另一是權重總合上限，圖 2.14 右半是頻繁換手區域的選擇結果，裡頭最大 hop 數為 2，而權重總合上限則設定為 3。在此區域中的無線存取點是行動節點未來比較有可能會換手到的，所以對這些無線存取點預先認証可以加快換手的時間。

2.4.2 Proactive Key Distribution Using Neighbor Graphs[15]

此篇論文是由 Mishra 等人所提出的，它提出了一個鄰居圖 (Neighbor Graph)的概念，以圖為例，左半部是在建築物中無線存取點布建的位置圖，可以看出其中有 A 到 E 共五個無線存取點，而在無線存取點之間的虛線則是換手發生的事件，像無線存取點 C 在一房間之內，只能由無線存取點 B 換手過來，我們可以將這些事件對應成圖右半的鄰居圖，藉由此建構出的鄰居圖，行動節點會向目前聯結無線存取點的鄰居無線存取點做預先認証的動作。例如若行動節點目前聯結至無線存取點 D，則會向 B、E 預先認証，又若行動節點目前聯結至無線存取點 C，則只會對 B 做預先認証的動作。

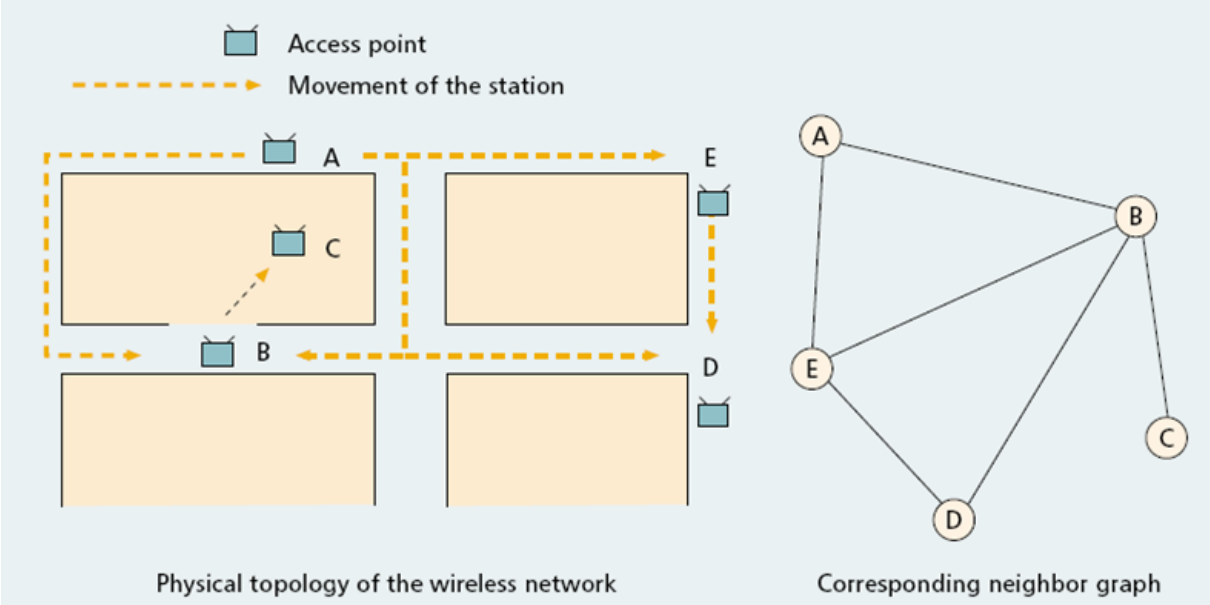


圖 2.15　鄰居圖的建構

2.4.3　Location-based Fast Handoff for 802.11 Networks[14]

這篇是由 Tseng 等人所提出的，其提出利用行動節點的位置資訊來達成快速換手的目的。如圖 2.16 右半部所示，首先我們可利用行動節點在過去時間內的位置，來推算出其移動的方向及路徑，再用移動方向及路徑來計算行動節點在未來時間可能會到達的位置範圍。

圖 2.16 左半部說明了如何去選擇可能會換手到的無線存取點，假設無線存取點目前的位置是 (x_0,y_0)，並且利用其先前的位置資訊計算出移動向量 V，藉由此向量順時針及逆時針旋轉一定角度 θ，可以圈出一段區域，行動節點則會對在此區域的無線存取點執行預先認証的動作。

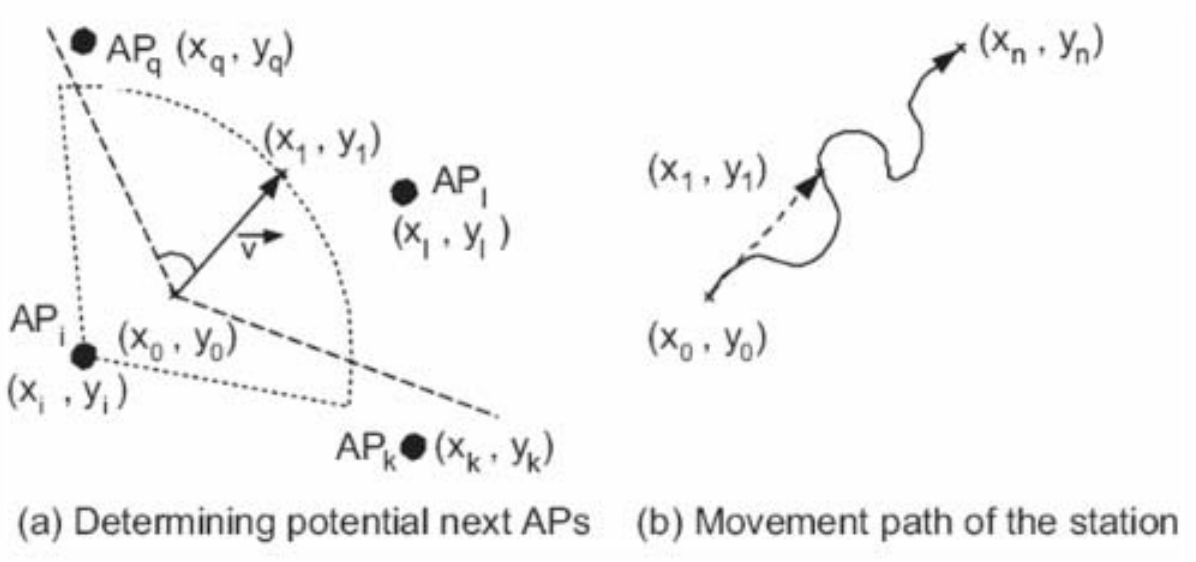


圖 2.16　用位置資訊決定下一無線存取點示意圖

第三章　IEEE 802.11i 無線網路快速換手之設計與架構

3.1　快速換手之設計架構

在支援 RSN 的無線網路環境裡，換手的時間流程和延遲如下圖所示。在此換手延遲時間內上層應用程式的封包是完全無法傳送的，太長的換手延遲時間會導致程應用程式的中斷，對於當紅的即時應用程式來說，其對換手延遲的要求更為嚴格，這也是本論文的研究動機，要達成快速換手的目的。

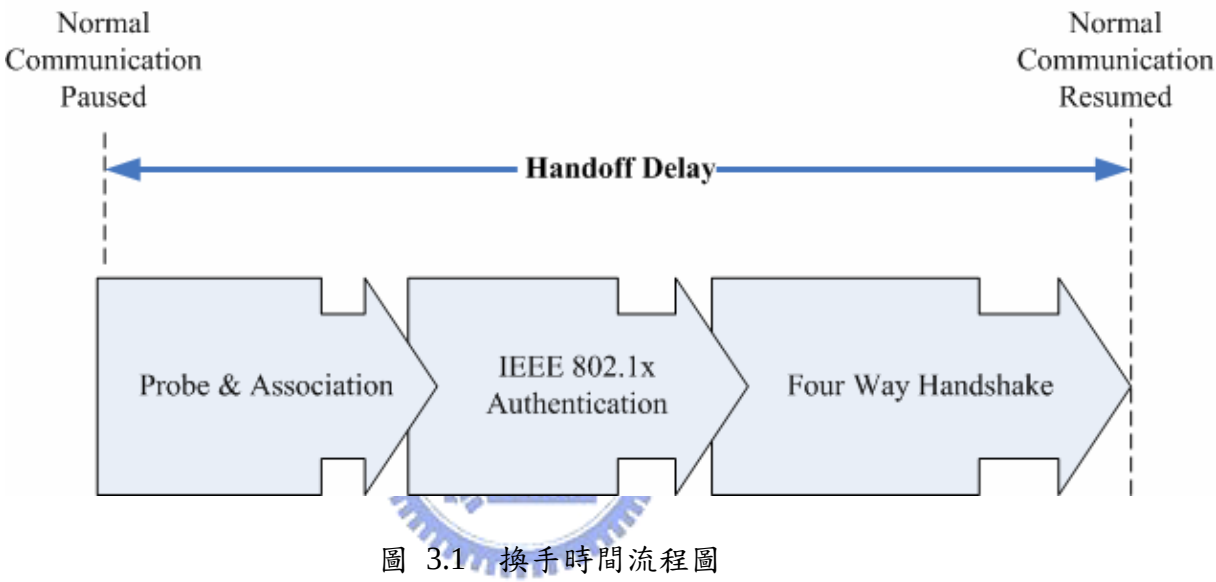


圖 3.1　換手時間流程圖

圖 3.1 中 IEEE 802.1x 身份認証所需的時間，可由前述之預先認証方式來解決。本論文提出了利用預先四訊息握手交換的方式，來縮減換手後四訊息握手交換的程序，根據 2.3.4 節的介紹，預先認証及預先四訊息握手交換程序中，行動節點都必須有目標無線存取點的位址，本論文也會提出一位置資訊訊息交換架構，設置一位置資訊伺服器，行動節點將會提供給伺服器目前網路環境的狀況，而伺服器也會幫助行動節點取得目標無線存取點的位址。

3.2　預先四訊息握手交換 (Pre-Four-Way-Handshake)

當預先身份認証完成之後，會用 PMKSA 來儲存成對主金鑰，此時行動節點和目標無線存取點接著繼續做預先四訊息握手交換之程序，而預先四訊息握手交換的特性如下：

- 因為行動節點尚未跟目標無線存取點聯結，所以整個預先四訊息握手交換必須透過目前聯結的無線存取點來轉送所有訊息，又第一個封包是由目標無線存取點送出。

- 利用 EAPOL 封包來傳遞，為了跟原本的 EAPOL 封包有所區別，所以其乙太型別為 88-C7，無線存取點對此乙太型別的封包不會做任何特殊的處理，目標無線存取點在接收到封包時，也可以用此乙太型別來分辨是由目前未聯結在其下的行動節點發出的預先四訊息握手交換，而預先四訊息握手交換所使用的 EAPOL 封包類別為 EAPOL-Key。

- 由於執行預先四訊息握手交換的行動節點，實際上並未聯結到目標無線存取點，所以對目標無線存取點來說，其下管理的行動節點並沒有更動，所以和聯結行動節點的群組暫時金鑰在此程序不必重新產生和傳遞，當然在第三個封包中，也不會有被加密的群組暫時金鑰存在。

- 同樣由於行動節點尚未聯結至目標無線存取點，第三個封包也不會有安裝成對暫時金鑰的指示，當完成預先四訊息握手交換後，雙方也都不會將成對暫時金鑰安裝至網路卡上。

- 當完成預先四訊息握手交換後，雙方會用 PTKSA (PTK Security Association) 將結果儲存下來，PTKSA 會包含以下物件：

  - PTKID
  - 成對暫時金鑰
  - 成對編碼套件選擇器 (Pairwise cipher suit selector)
  - 有效生命週期 (Life Time)
  - 行動節點的媒體存取控制層位址
  - 目標無線存取點的媒體存取控制層位址

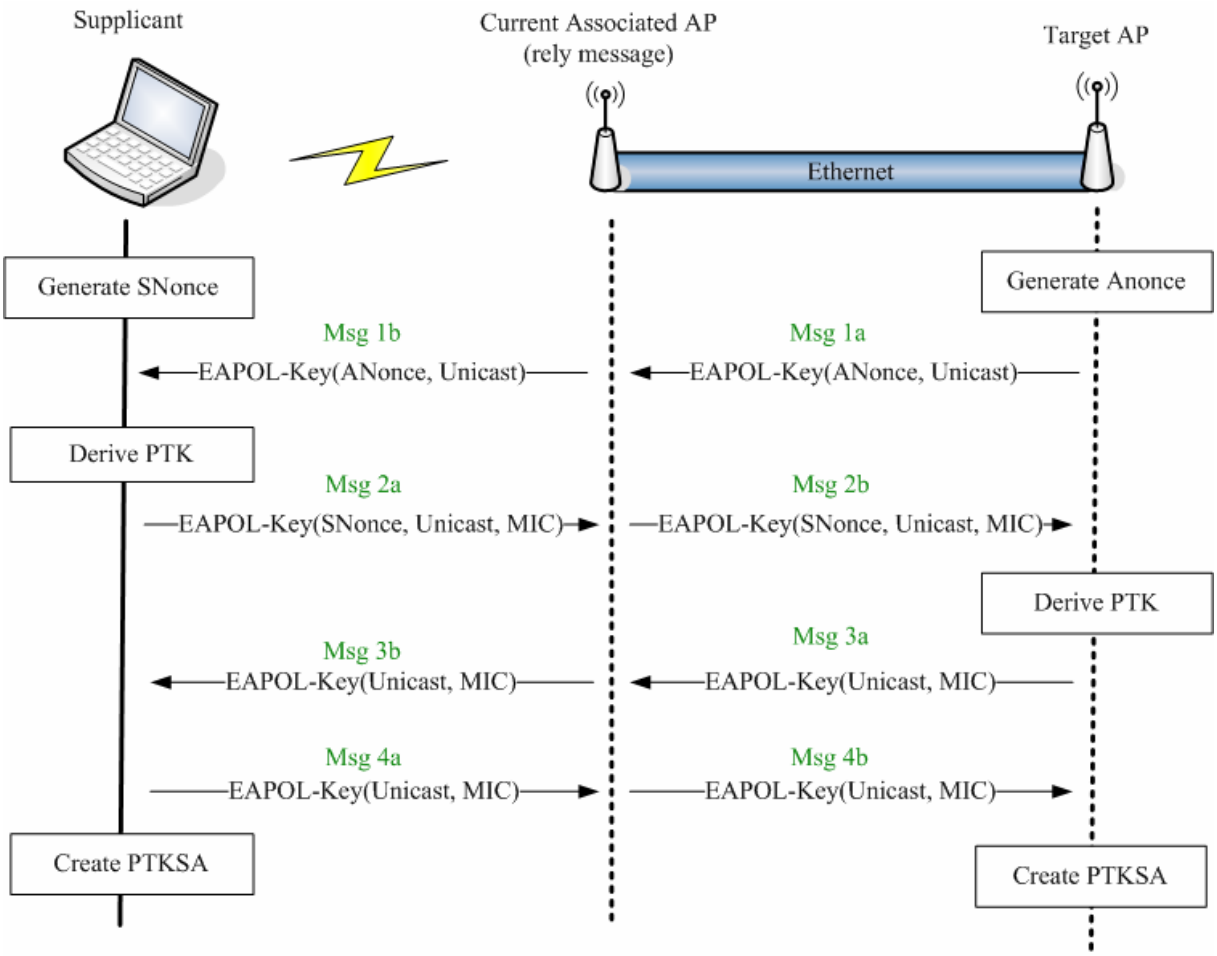


圖 3.2 預先四訊息握手交換流程

圖 3.2 表示預先四訊息握手交換的流程，詳細的訊息傳遞為：

1. 由於之前的預先認証完成，所以申請者和目標無線存取點會持有同樣的成對主金鑰及 PMKSA，此時雙方各自產生一個亂數，將會用於預先四訊息握手交換裡，此兩亂數稱為 SNonce 和 ANonce，分別為申請者和目標無線存取點所產生。

2. 目標無線存取點送出訊息一，其中最重要的欄位是由目標無線存取點所產生的亂數 ANonce。

3. 當目標無線存取點收到訊息二之後，會用本身產生的 SNonce 和接收的 ANonce 依上節所敘述的公式計算出成對暫時金鑰。

4. 申請者送出訊息二，其中最重要的欄位是由申請者所產生的亂數 SNonce，而訊息二的整個封包，會利用 PMKSA 中成對暫時金鑰裡的

EAPOL-Key 完整性金鑰來計算出訊息完整性檢查碼，用來保護訊息二的內容不被竄改。

5. 當目標無線存取點收到訊息二之後，會用本身所產生的 ANonce 和接收的 SNonce 依上節所敘述的公式計算出成對暫時金鑰，接著目標無線存取點會用 PMKSA 中成對暫時金鑰裡的 EAPOL-Key 完整性金鑰來檢查封包裡的訊息完整性檢查碼是否正確，若檢查失敗則代表訊息二的封包有被竄改的可能，目標無線存取點將會丟棄此封包。

6. 目標無線存取點送出訊息三，同樣的訊息三也會計算出一訊息完整性檢查碼來保護封包不被竄改。

7. 當申請者收到訊息三，會檢查該封包的訊息完整性檢查碼是否正確，此訊息可確認目標無線存取點也計算出同樣的成對暫時金鑰，若檢查失敗則代表訊息二的封包有被竄改的可能，申請者將會丟棄此封包。

8. 申請者送出訊息四來指示對方已完成預先四訊息握手交換的程序。

9. 申請者及目標無線存取點將計算出的成對暫時金鑰用 PTKSA 的資料結構儲存下來，待之後重新聯結上目標無線存取點時再將 PTKSA 裡的成對暫時金鑰安裝於網路卡上。

各封包的相關詳細資料整理如表 3.1。

Message	Source MAC	Transmitter / Receiver MAC	Destination MAC	Media	MIC
1a	Target AP	X	MN	wired	
1b	Target AP	Current Associated AP	MN	wireless	
2a	MN	Current Associated AP	Target AP	wireless	V
2b	MN	X	Target AP	wired	V
3a	Target AP	X	MN	wired	V

3b	Target AP	Current Associated AP	MN	wireless	V
4a	MN	Current Associated AP	Target AP	wireless	V
4b	MN	X	Target AP	wired	V

表 3.1　預先四訊息握手交換封包資料表

3.3　位置資訊管理 (Location Information Management) 設計方法

3.3.1　方法及相關元件

在之前的章節中，我們利用預先認証及預先四訊息握手交換來加快換手的速度，而其中一項必要的條件，就是申請者要得知目標無線存取點的位址，若申請者在目標無線存取點的電波範圍，可以藉著被動或主動掃描來得知此資訊，但在大部分的情況下，為了避免干擾，在布建無線網路環境時，各無線存取點的訊息重疊區域並不會太大，所以在本論文中我們設計一位置資訊管理架構，用來輔助整個快速換手機制的運作。

在此位置資訊管理架構中，存在兩個元件，分別為位置伺服器及行動節點上的客戶端 (client) 。藉由這兩個角色的訊息交換，位置資訊管理架構可以達到以下的目的：

- 位置伺服器可以獲得並記錄行動節點的位置資訊。
- 位置伺服器可以追蹤行動節點的位置，配合當地網路的拓撲狀況，或是網路提供者的政策，計算出行動節點之後可能會連結到的無線存取點。
- 行動節點會搜集自己本身的網路環境資料，提供給位置伺服器。
- 行動節點在必要時可以向位置伺服器發出要求，得知用於快速換手的相關資訊。

整個位置資訊管理的架構拓撲如圖 3.3。由圖中可看出一個位置伺服器管理一個區域的位置資訊，其下可以連接多個無線存取點，甚至連接多個網域，由此可知位置伺服器在整個系統中擔任一個舉足輕重的角色。

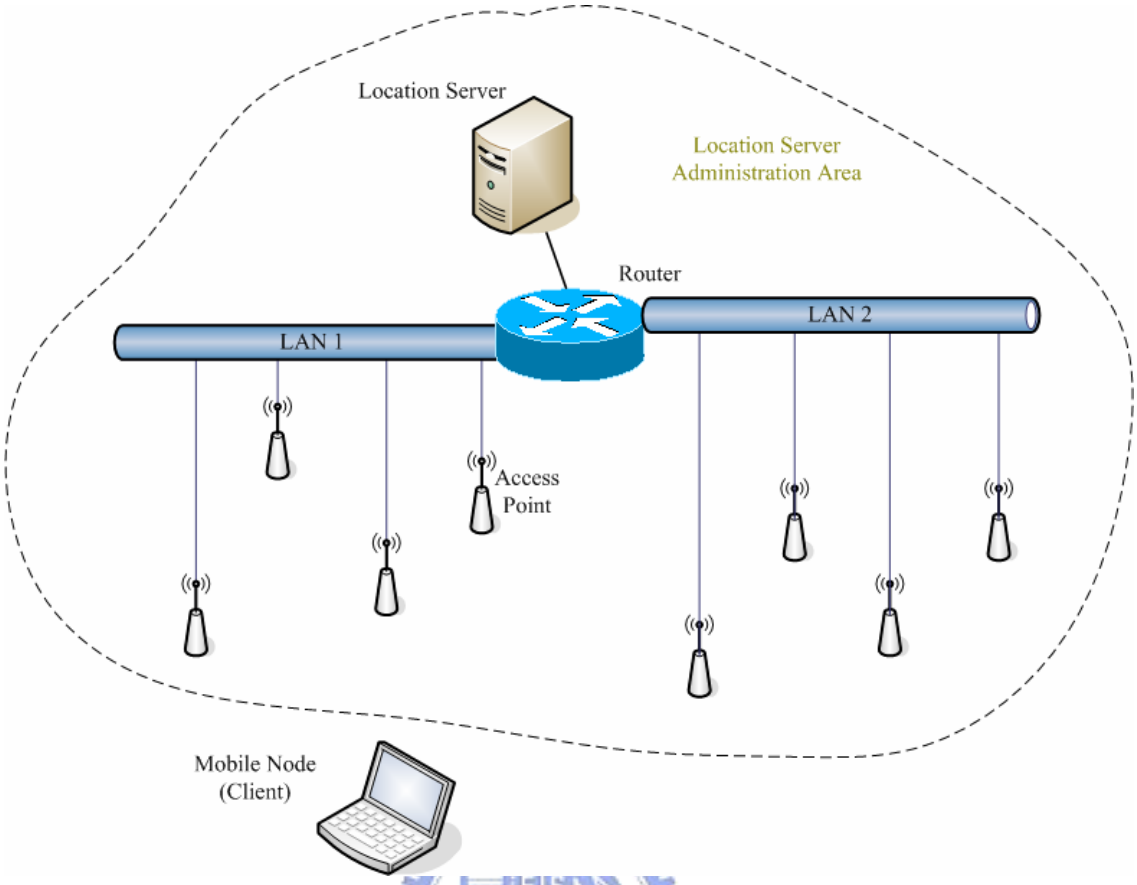


圖 3.3 位置資訊管理架構圖

3.3.2 位置伺服器之設計

位置伺服器會搜集從行動節點送回來網路狀態和位置資訊，並且將各行動節點的位置資訊做追蹤記錄，當收到行動節點要求目標無線存取點列表的訊息時，位置伺服器會利用先前所記錄的位置資訊，來推算出該行動節點可能會換手到的目標無線存取點，將此列表用本論文所訂的封包協定格式送回給該行動節點。

為達成以上目標，位置伺服器要有其下所管理區域的無線網路拓撲相關的知識，像是各無線存取點在地理上的位置，像是座標或樓層等等，相對或是絕對座標皆可，若有各無線存取點的電波傳遞範圍及週遭電子設備的干擾量測，位置伺服器可以更精確的計算出可能會換手到的目標無線存取點，而計算的演算法則可使用 2.4 節所討論的三種方法來實作。

除了用地理位置上的資訊來計算，位置伺服器可以依照使用者日常生活的習慣，像是在上學或上班時我們通常每天都會經過同樣的路線，來進一步過濾無線

存取點列表，或是讓使用者自訂一個人檔案 (profile) 主動告知位置伺服器該使用者的使用偏好或網路優先權，進而提升位置資訊管理系統的運作效能。而位置伺服器若是依附在無線網路服務提供者之下，無線網路服務提供者也可以將其希望使用者選擇無線網路存取點的策略加在位置伺服器上，最後位置伺服器可以多方參考不同的考量來計算出一適合的無線存取點列表。

位置伺服器所要具備的功能甚多，所以其運算能力、記憶儲存空間都要有較高階的設備，由於位置伺服器通常不會移動，所以可以使用固接穩定的電源供應，而其所需要的地理位置資訊，則需要事先建構和量測。本論文將可能會換手的無線存取點決定交由位置伺服器來處理，也是這個原因，行動節點因為其移動性，所以通常使用電池來當作電源，又行動節點的機器體積不大，也多少限制了行動節點的運算能力。又另一個原因是，位置伺服器通常由無線網路系統來提供的，相較於行動節點來說更容易取得當地網路的地理位置資訊。

位置伺服器的運作流程如圖 3.4。

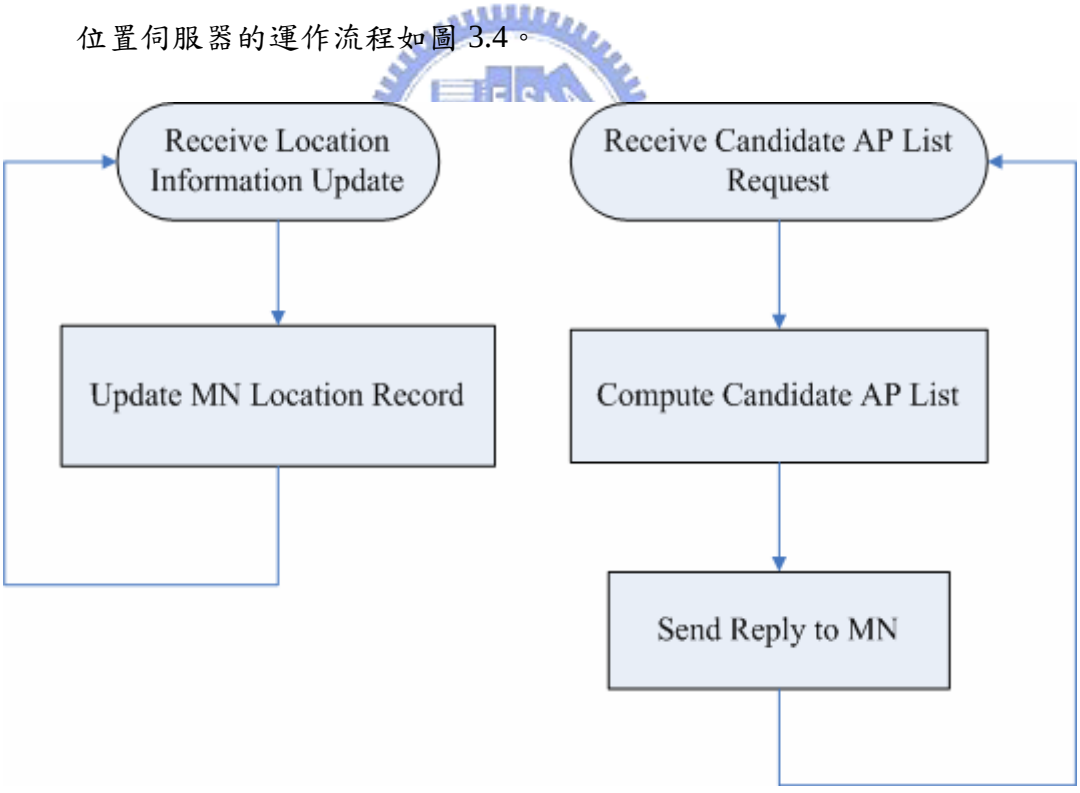


圖 3.4　位置伺服器運作流程圖

3.3.3　行動節點上客戶端之設計

行動節點上會有負責和位置伺服器作訊息溝通的客戶端，此客戶端會週期性

的主動掃描目前無線網路的狀況，並將所掃描得的結果回報給位置伺服器，例如週遭無線存取點的資訊及其訊號強度等等。而行動節點也會週期性的檢查和目前聯結的無線存取點之訊號強度，當訊號強度低於某一個門檻 (threshold) 時時，則此客戶端會送訊息至位置伺服器，要求位置伺服器提供可能會換手到的無線存取點列表，行動節點再依此列表向其它無線存取點進行預先認証及預先四訊息握手交換的程序。

行動節點向位置伺服器送出要求的時機，決定於訊號強度的門檻。若此門檻愈低，則送出要求的時間愈早，行動節點有更充裕的時間完成預先認証及預先四訊息握手交換的動作，但相對的也會造成網路系統更大的負擔，會有更多不必要的動作被啟動。而若此門檻愈高，將有較少的預先認証及預先四訊息握手交換被觸發，但若太晚才觸發這些動作，行動節點可能還沒完成這些動作就已經脫離目前無線存取點電波範圍或是換手了。所以門檻值的設定是很重要的。

行動節點上客戶端的運作流程如圖 3.5。

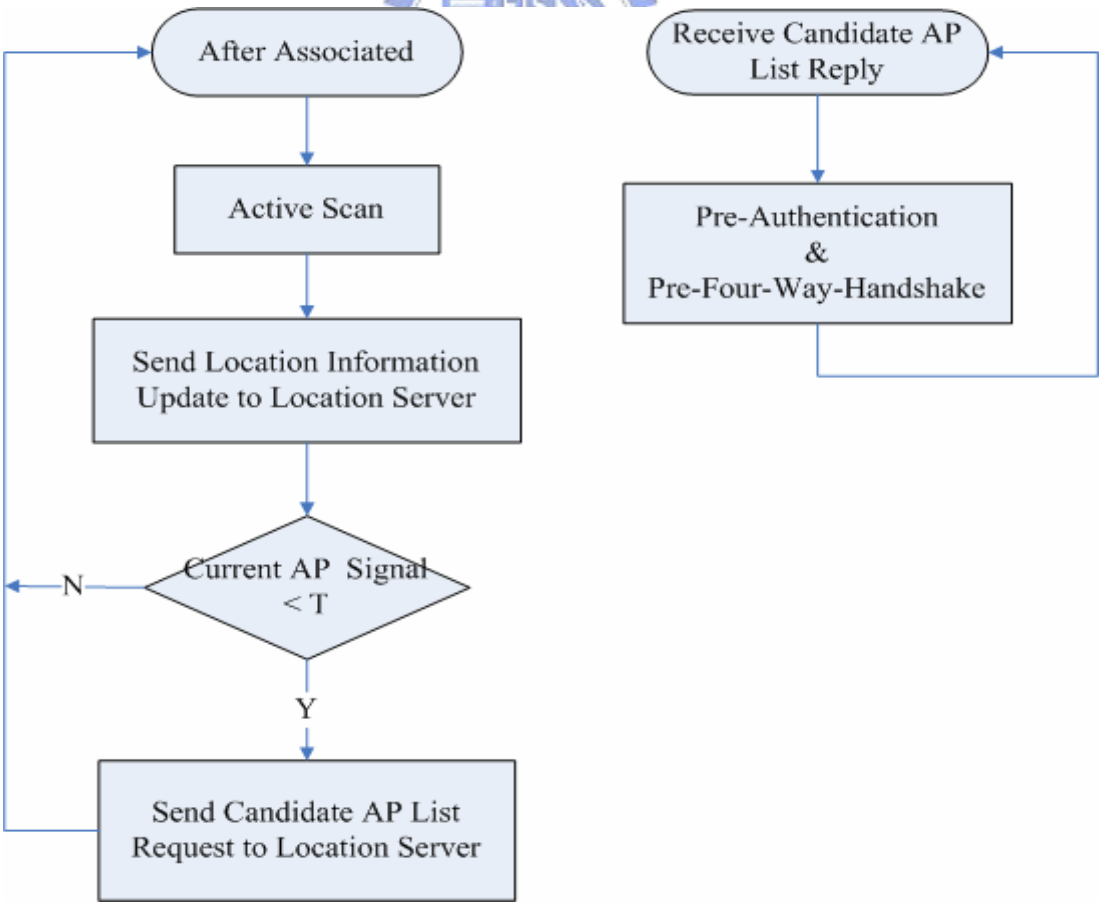


圖 3.5　行動節點上客戶端運作流程圖

3.3.4 位置資訊訊息交換

本論文的位置資訊管理架構，行動節點與位置伺服器之間會有多個訊息交換，來達成行動節點位置資訊的追蹤記錄及可能會換手無線存取點的預測。整個訊息交換的程序如圖 3.6 所示。

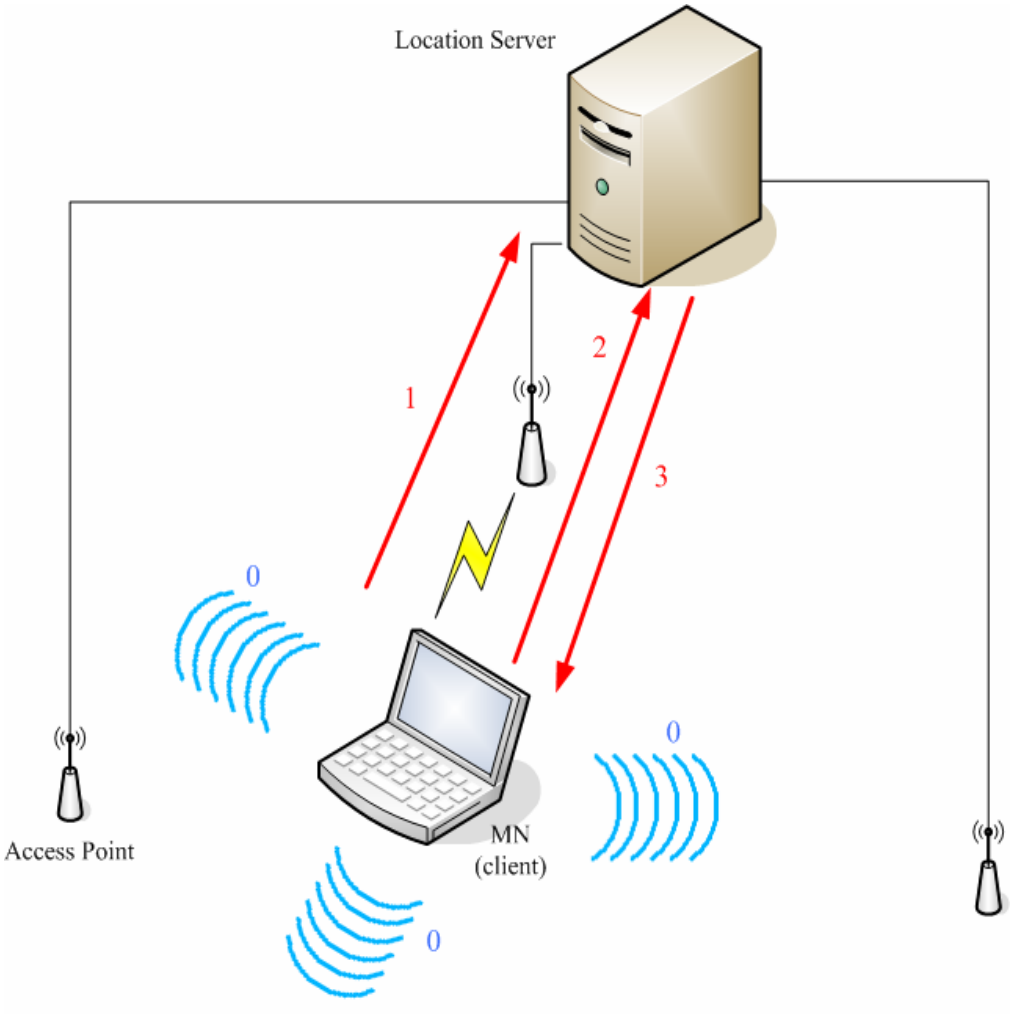


圖 3.6 位置資訊訊息交換示意圖

0. 行動節點利用主動掃描取得所在之處網路及無線網路存點的資訊，並檢查和目前聯結的無線存取點訊號強度。

1. 行動節點將主動掃描所得到的網路及無線存取點資訊送至位置伺服器，位置伺服器會追蹤並記錄行動節點的位置資訊。

2. 若在步驟 0 檢查的訊號低於某個門檻，則行動節點會向位置伺服器送出要求可能會換手的候選無線存取點列表。

3. 當位置伺服器收到行動節點的要求，則會依行動節點的位置追蹤記錄和其它資料推算出可能會換手的候選無線存取點列表，最後將此列表傳送至行動節點上。

位置資訊交換的訊息有以下三種，詳細封包的格式和定義將在第四章說明。

- 位置資訊更新訊息 (Location Information Update Message)
- 候選無線存取點列表要求 (Candidate AP List Request)
- 候選無線存取點列表回覆 (Candidate AP List Reply)

3.4 換手及重新聯結 (Re-association)

3.4.1 換手及重新聯結程序

在一般的換手流程當中，當行動節點跟新無線存取點重新聯結之後，行動節點會主動送出 EAPOL-Start 訊息，或是由無線存取點送出 EAP-Request/Identity 的訊息來啟始 IEEE 802.1x 身份認証，接著行動節點會透過新無線存取點和認証伺服器執行可延伸認証通訊協定的訊息交換，完成之後依 IEEE 802.11i 的規範，行動節點要和新無線網路存取點進行四訊息握手交換，取得成對暫時金鑰再開始正常封包的傳遞。

而根據本論文提出的方法，行動節點在換手之前會先和位置伺服器交換位置訊息，並在訊號低於某一程度時向位置伺服器取得可能會換手到的候選無線存取點列表，並依照此列表進行預先認証及預先四訊息握手交換，最後行動節點和目標無線存取點會將結果儲存在 PTKSA 的資料結構裡，並用 PTKID 作為 PTKSA 的索引。當行動節點實際換手時，會重新聯結至目標無線存取點，此時我們將 PTKID 加在此重新聯結的封包訊息裡。當無線存取點收到此重新聯結封包後，會比對本身暫存的 PTKSA 是否存在相同的 PTKID，若沒有找到則依照一般的換手程序進行，若有暫存的 PTKSA 存在，則將對應的成對暫時金鑰安裝於網路卡上，直接傳送正常的封包。

詳細的換手及重新聯結流程如圖 3.7 所示，其中可分成三個不同情形，若是 PTKSA 存在，則行動節點和無線存取點會將成對暫時金鑰安裝並開始一般封包的

傳遞；若 PTKSA 不存在而 PMKSA 存在，則雙方只需進行四訊息握手交換來產生成對暫時金鑰即可；若 PTKSA 和 PMKSA 都不存在則會進行 IEEE 802.1x 的認証和四訊息握手交換來產生成對暫時金鑰。

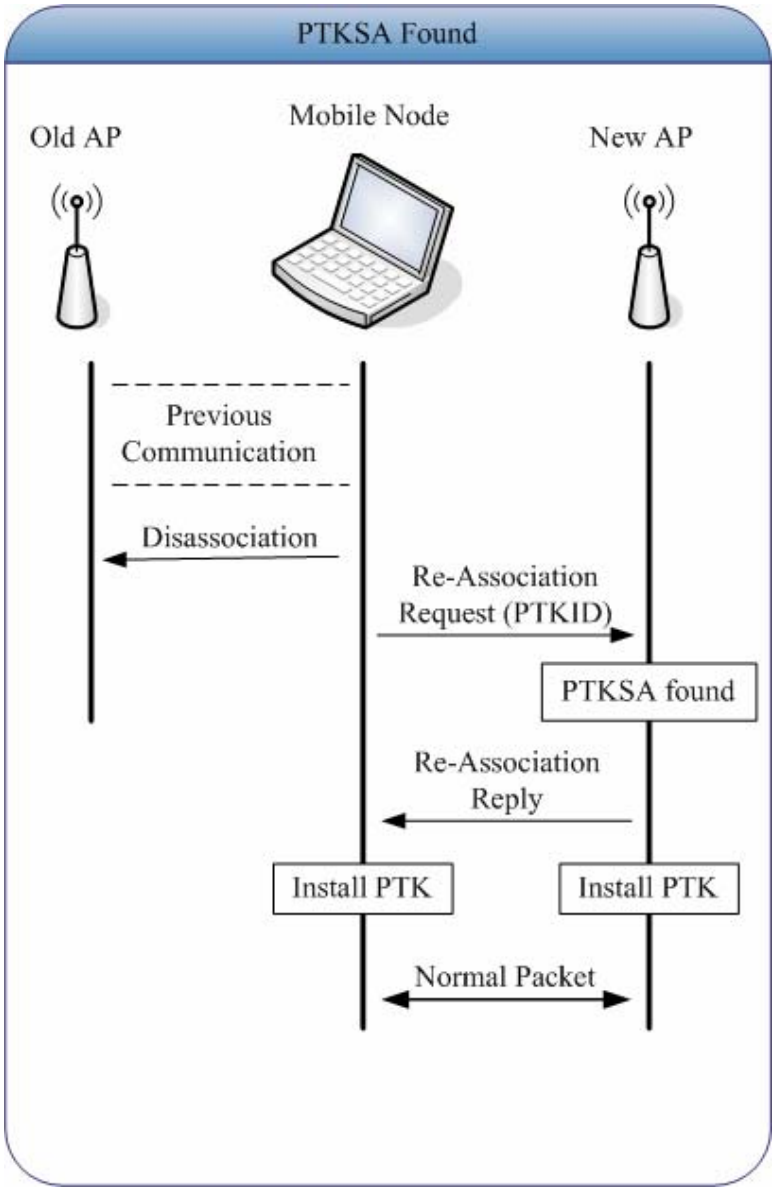


圖 3.7　換手及重新聯結流程

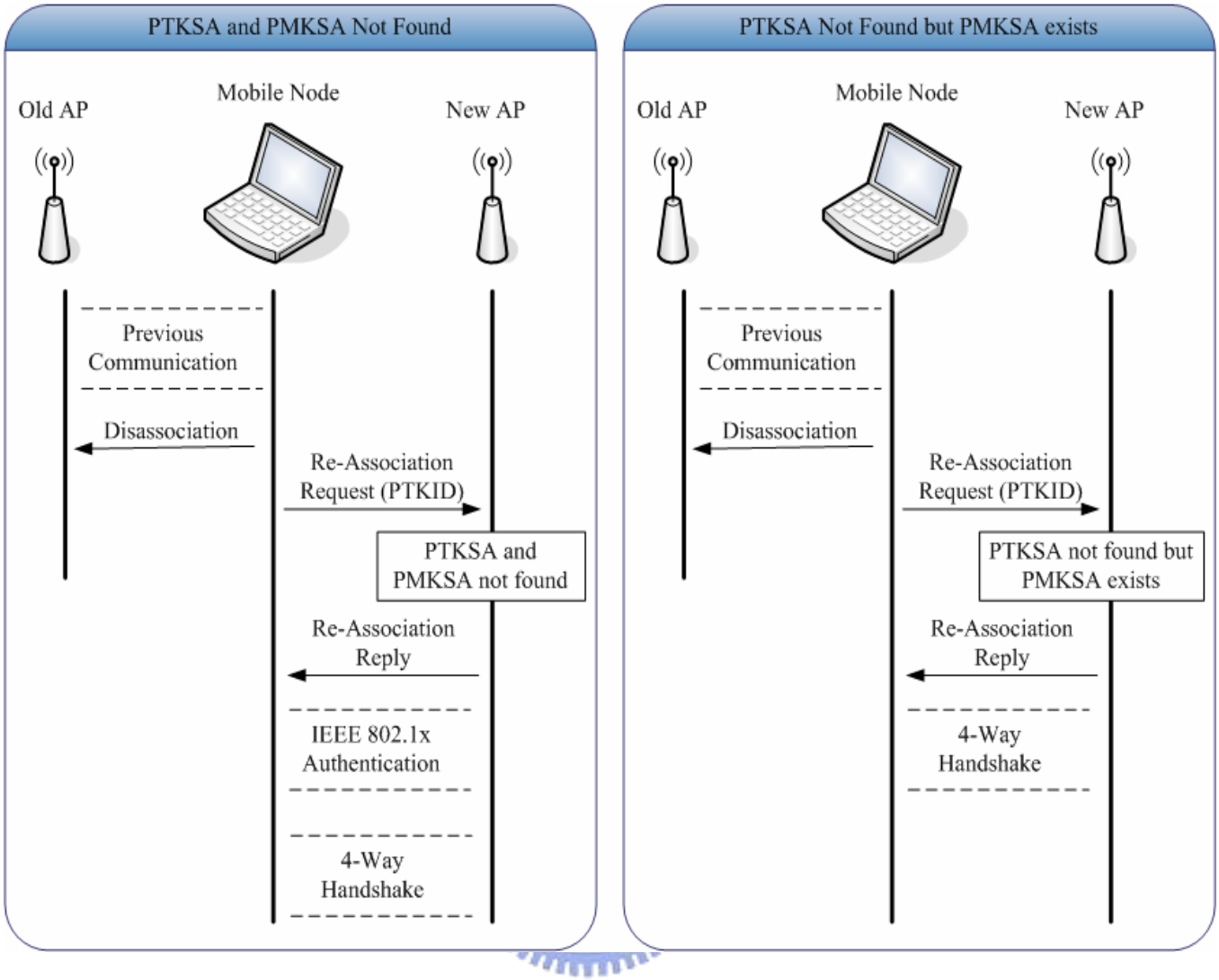


圖 3.7 續　換手及重新聯結流程

3.5　IEEE 802.11i 無線網路快速換手

根據上述幾節的說明，本論文提出的 IEEE 802.11i 無線網路快速換手詳細的操作過程如下圖 3.9。依序的步驟為：

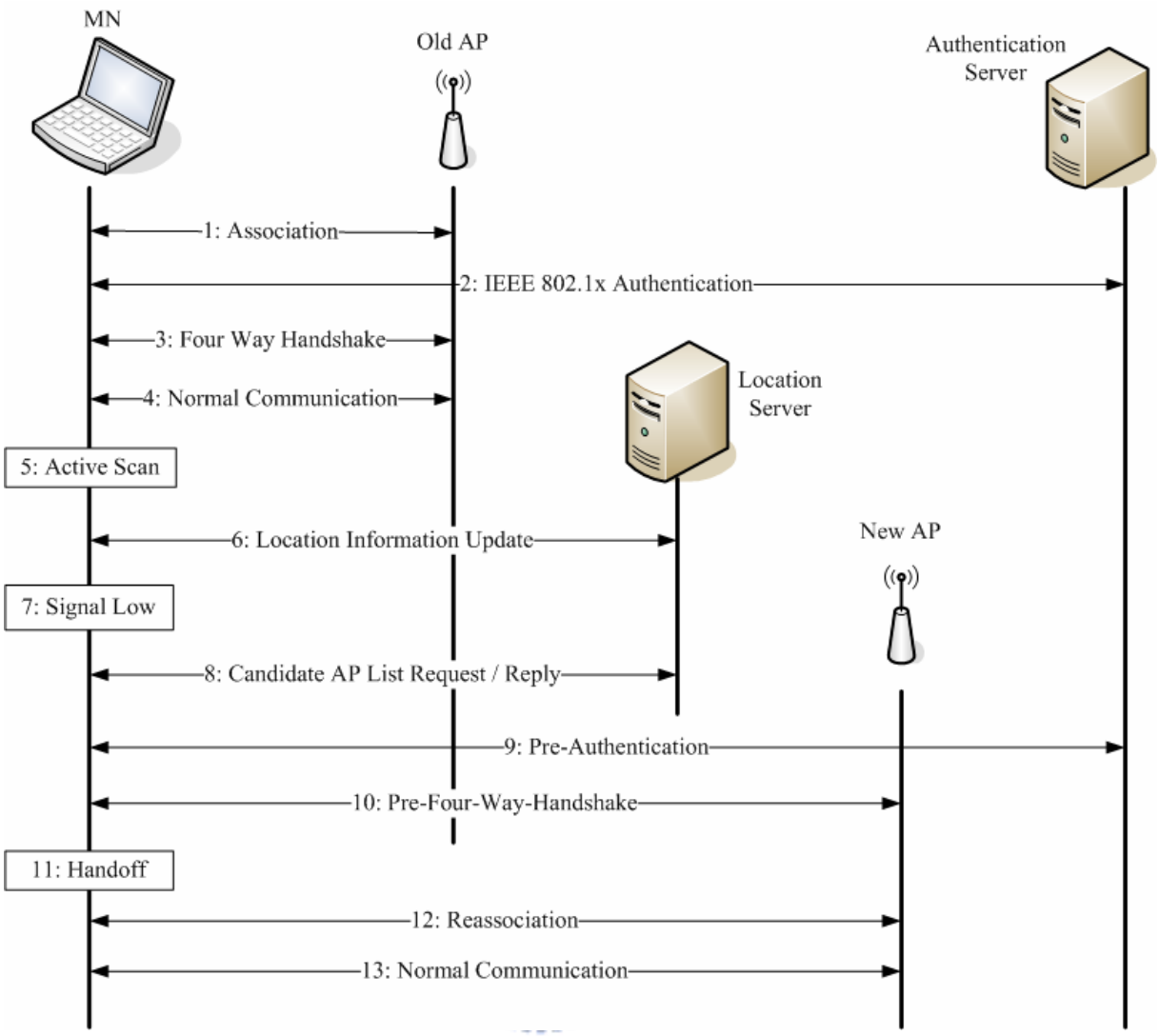


圖 3.8　IEEE 802.11i 無線網路快速換手流程圖

1. 行動節點經由探查、身份認証之後聯結上一無線存取點。
2. 行動節點和後端的認証伺服器執行 IEEE 802.1x 身份認証，認証完後行動節點和無線存取點會持有相同的成對主金鑰。
3. 行動節點和無線存取點進行四訊息握手交換，完成後會持有成對暫時金鑰。
4. 行動節點和無線存取點將相關金鑰安裝好，開始傳送正常的封包。
5. 行動節點利用主動掃描取得當地無線網路環境及無線存取點資訊。
6. 行動節點將所得的資料送回至位置伺服器，位置伺服器會記錄下來。

7. 行動節點偵測出和目前聯結的無線存取點訊息低於某一個門檻。

8. 行動節點送出候選無線存取點列表要求至位置伺服器，位置伺服器會利用當地的網路拓樸和行動節點的位置資訊計算出可能會換手到的候選無線存取點，最後將此列表送回到行動節點上。

9. 行動節點透過目前的無線存取點和後端的認証伺服器進行預先認証。

10. 行動節點透過目前的無線存取點和目標無線存取點進行預先四訊息握手交換。

11. 行動節點切斷目前的聯結，開始換手程序。

12. 行動節點重新聯結上新無線存取點。

13. 行動節點和新無線存取點安裝成對暫時金鑰並開始正常封包的傳遞。

第四章　IEEE 802.11i 無線網路快速換手之實作

4.1　系統之軟硬體需求

本論文提出的 IEEE 802.11i 無線網路快速換手系統中，包含了四項系統元件，分別為行動節點、無線存取點、認証伺服器及位置伺服器。本論文使用 Host AP[22] 套件作為無線網路卡的驅動程式及 IEEE 802.1x 的功能，加上 FreeRADIUS[23]及 OpenSSL[24]來實作出本系統，因 Intersil 公司生產的 Prism 2/2.5/3 晶片對 Host AP 有較高的支援度，所以本系統的無線網路卡皆使用 Prism 2/2.5/3 晶片。以下分別針對這四項元件的軟硬體需求做詳細的介紹：

- 行動節點：

  硬體需求：Prism 2/2.5/3 晶片無線網路卡

  作業系統：Linux Red Hat 9

  軟體需求：

  1. Host AP driver：驅動無線網路卡，並使無線網路卡運作在受管理 (managed) 的模式，需透過無線存取點和其它人通訊。
  2. WPA supplicant：讓行動節點能有申請者的功能，跟認証伺服器溝通並完成 IEEE 802.1x 認証，之後也會跟無線存取點完成四訊息握手交換，需修改加上位置資訊客戶端的功能，並完成預先四訊息握手交換及換手相關功能。

- 無線存取點：

  硬體需求：乙太網路卡、Prism 2/2.5/3 晶片無線網路卡

  作業系統：Linux Red Hat 9

  軟體需求：

  1. Host AP driver：驅動無線網路卡，並使無線網路卡運作在主要 (master) 的模式，也就是使機器模擬無線存取點的功能。

2. Host AP daemon：讓無線存取點有認証者的功能，轉送 EAPOL 封包至認証伺服器，需修改符合預先四訊息握手交換及換手功能。

■ 認証伺服器：

硬體需求：乙太網路卡

作業系統：Linux Red Hat 9

軟體需求：

1. FreeRadius：認証伺服器的軟體。

2. OpenSSL：配合 FreeRadius 所要安裝的軟體。

■ 位置伺服器：

硬體需求：乙太網路卡

作業系統：Linux Red Hat 9

軟體需求：

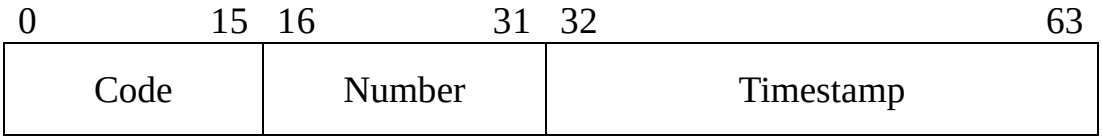
1. Location Server：需實作位置伺服器的功能，管理並追蹤行動節點的位置資訊，利用網路拓樸資訊計算並提供候選無線存取點列表給行動節點。

4.2 位置資訊交換之實作

4.2.1 位置資訊封包基本格式

本論文提出一套使用位置資訊交換來輔助快速換手的機制，此訊息交換程序共包含了三種訊息，分別為位置資訊更新訊息、候選無線存取點列表要求及候選無線存取點列表回覆，而此三種訊息之底層將會由 UDP/IP 來封裝。各訊息都是由一訊息標頭 (header) 之後接著零或一個以上的訊息本體項目 (entry) 所組成。訊息標頭及訊息本體項目的格式將詳列如圖 4.1。

Header Format



Entry Format

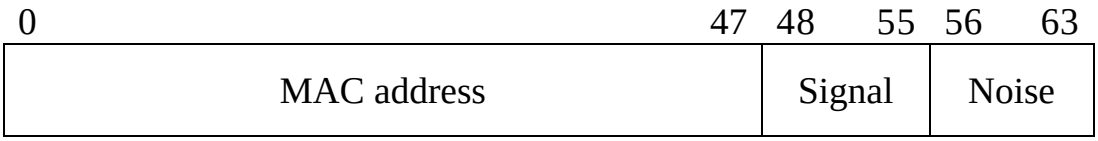


圖 4.1　位置資訊封包基本元件格式

各欄位的定義說明如表 4.1。

欄位名稱	欄位長度	說明
Code	2 bytes	代表此訊息的類型，0 表示位置資訊更新訊息，1 表示候選無線存取點列表要求，2 表示候選無線存取點列表回覆
Number	2 bytes	接在標頭後訊息本體項目的個數
Timestamp	4 bytes	封包送出時的時間標記
MAC address	6 bytes	無線存取點的媒體存取控制層位址
Signal	1 byte	行動節點所掃描到無線存取點的訊號強度
Noise	1 byte	行動節點所掃描到無線存取點的雜訊強度

表 4.1　位置訊息封包欄位定義及說明

4.2.2　位置資訊更新訊息

位置資訊更新訊息是由行動節點傳給位置伺服器的訊息，目的是要將行動節

點主動掃描的結果傳回給位置伺服器，此訊息由一個訊息標頭及一個以上的訊息本體項目所組成，每一個訊息本體項目含有無線存取點的位址和訊號強弱相關資訊，圖 4.2 為一個位置資訊更新訊息的範例，其中包含兩個訊息本體項目。

0x00	2	Timestamp	
00:11:22:33:44:55		Signal	Noise
66:77:88:99:aa:bb		Signal	Noise

圖 4.2　位置資訊更新訊息範例

4.2.3　候選無線存取點列表要求

候選無線存取點列表要求是由行動節點傳給位置伺服器的訊息，目的是要求位置伺服器傳送可能會換手到的無線存取點列表，此訊息由一個訊息標頭組成，沒有任何訊息本體項目，圖 4.3 為一個候選無線存取點列表要求範例。

0x01	0	Timestamp

圖 4.3　候選無線存取點列表要求範例

4.2.4　候選無線存取點列表回覆

候選無線存取點列表回覆是由位置伺服器傳給行動節點的訊息，藉由此訊息位置伺服器將計算出的無線存取點列表傳給行動節點，此訊息由一個訊息標頭及一個以上訊息本體項目組成，圖 4.4 為一個候選無線存取點列表回覆範例，其中包含三個候選無線存取點。

0x02	3	Timestamp	
00:11:22:33:44:55		0	0
66:77:88:99:aa:bb		0	0
cc:dd:ee:ff:00:11		0	0

圖 4.4　候選無線存取點列表回覆範例

4.3　位置伺服器之實作

位置伺服器為一個單一的程式，執行後會先讀入當地無線網路的相關資訊，像是無線存取點的網路拓樸等等，而我們是用鄰居圖的概念將網路環境架構起來，也就是位置伺服器擁有某個無線存取點旁有那些無線存取點的訊息，將此資訊讀入後便開啟一網路連接埠等待客戶端的連線，而所使用的底層協定為 UDP/IP。

當收到客戶端送來的位置資訊更新訊息，位置伺服器會替讓客戶端建立一個資料表，記錄著該客戶端的位置訊息，客戶端也會定時更新這些資訊，藉著三點定位與時間的關係，我們也可以約略推測出客戶端移動的方向和速度。當客戶端送要求過來，則位置伺服器會檢視之前位置追蹤的記錄，配合當地無線存取點的拓樸 (鄰居圖) 和選擇的策略，計算出可能會換手到的無線存取點，有可能不只一個無線存取點被選中，所以會產生一候選無線存取點列表，最後再將此列表送回客戶端。

4.4　客戶端之實作

客戶端的實作比較複雜一點，由於客戶端和申請者的角色是互相運作的，所以我們必須修改 Host AP wpa supplicant 的程式將所要的功能加上。Host AP wpa supplicant 利用許多個事件的資料結構，這裡的事件可能是：

網路事件：封包收送、網路卡的接上與斷接等

訊號 (Signal) 的觸發：系統的訊號，像 SIGHUP、SIGKILL 等

計時器 (Timer) 的倒數結束：任意時間的倒數計時器

在資料結構裡也會記錄各事件的 call back 函式。然後在每一輪迴圈裡主程式都會一一去輪詢 (Polling) 每個事件是否發生，若發生了某事件主程式則會啟動相對應的 call back 函式來動作。

- 首先在行動節點完成四訊息握手交換之後，此時正常封包已可以傳送，客戶端會新增一個(a)主動掃描計時器事件來預定下一次的掃描。
- 當(a)發生時，客戶端會執行主動掃描，並新增兩個事件，分別為下一次(a)主動掃描計時器事件和(b)讀取本次主動掃描結果事件。
- 當(b)發生時，客戶端會讀取主動掃描的結果，並把此結果送回給位置伺服器，同時在此時檢查和目前聯連的無線存取點訊號是否低於一個門檻，若低於此門檻則客戶端會向位置伺服器送出候選無線存取點列表要求，並新增一(c)接收候選無線存取點列表回覆事件。
- 當(c)發生時，客戶端會讀取位置伺服器傳送的回覆，解開封包把其中的無線存取點位址讀出來，之後對該群無線存取點執行預先認証和預先四訊息握手交換。

圖 4.5 為以上各事件的相互關係圖。

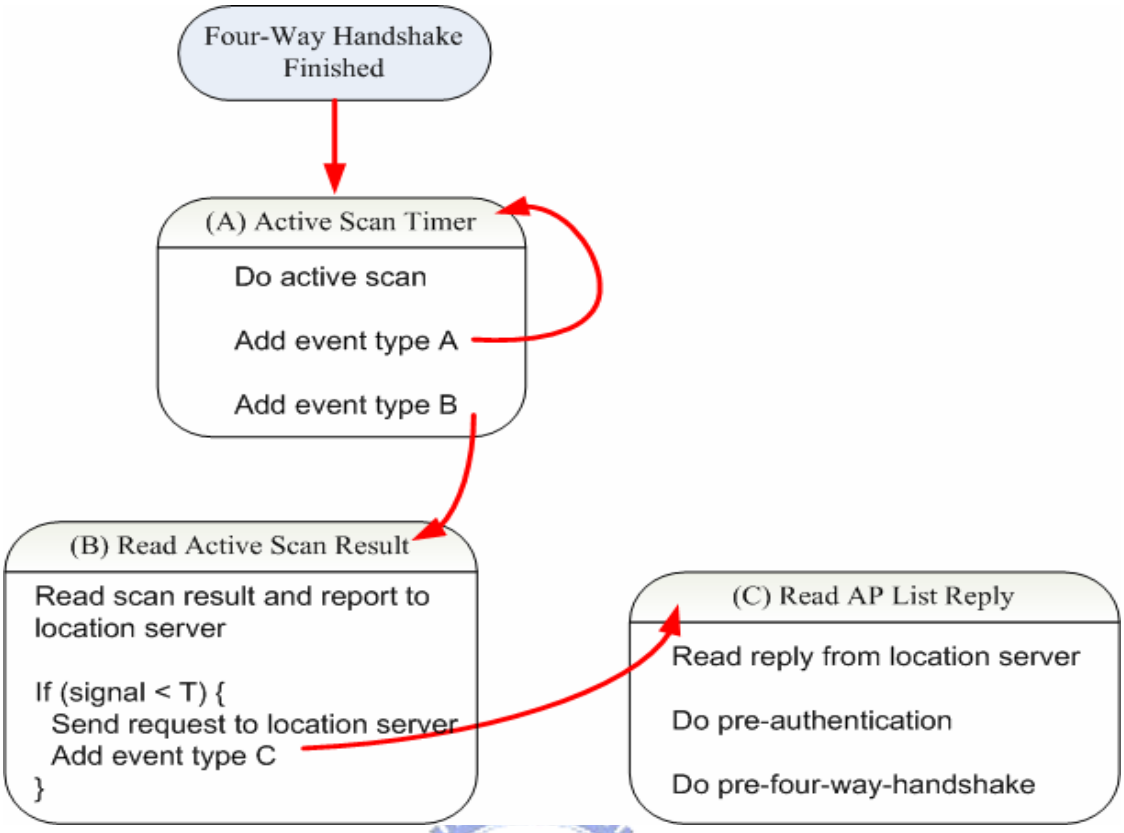


圖 4.5　客戶端事件關係圖

4.5　RSN 資訊元素 (Information Element) 修改

在 IEEE 802.11 無線網路中，管理訊框都會帶有多個資訊元素，像是服務組合識別碼 (Service Set Identity)、所支援的速率 (Supported Rates) 等等，其中和本論文最相關的即是 RSN 資訊元素。圖 4.6 是 RSN 資訊元素的格式，而在行動節點送出的重新連結訊息中會帶有此一資訊元素，根據本論文提出的快速換手機制，行動節點在重新連結時必須提供 PTKID 的資訊給無線存取點，所以本論文在實作上對 RSN 資訊元素做了必要的修改，主要的更動有兩個：

- PTKID 欄位：此欄位為選擇性 (optional) 存在的，若在重新連結訊息中 RSN 資訊元素裡出現此欄位，代表行動節點有經過之前預先四訊息握交換而產生的 PTKSA，其辨識代碼為 PTKID，而行動節點想用此 PTKSA 來達成快速換手的目的，而此欄位之前的 PMKID List 欄位也必定存在於訊息中。

- Pre-Four-Way-Handshake 位元旗標：新增此位元旗標，若無線存取點支

援預先四訊息握手交換，則此位元設成 1，反之則其值為 0。

茲將修改後的 RSN 資訊元素格式也顯示在圖 4.6。

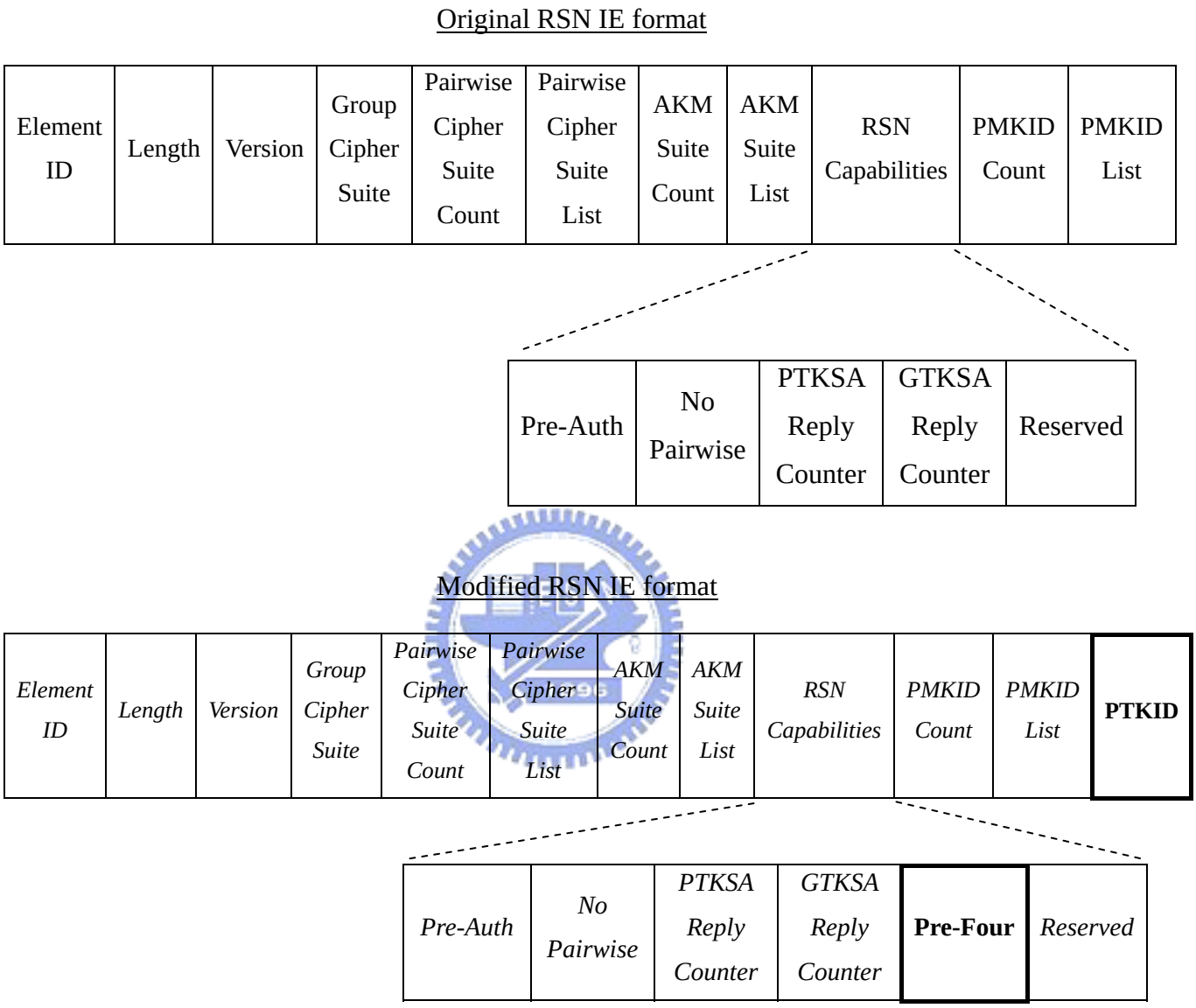


圖 4.6　RSN 資訊元素修改

第五章　效能分析

5.1　換手延遲時間分析

5.1.1　一般換手程序

圖 5-1 是在一般換手程序下延遲時間的分析，圖中的橫軸由左到右代表著時間的演進，而圖中由上到下分別代表著環境中四個不同的元件，依序為舊的無線存取點、行動節點、新的無線存取點及認証伺服器。

圖中可以看到行動節點會先和舊無線存取點聯結，上層應用程式會傳遞所需的封包，之後行動節點會移動到和新無線存取點訊號較佳的位置，行動節點上的網路卡會決定是否要換手到新無線存取點，若決定要換手的話，此時上層應用程式的封包傳送會被中斷，行動節點會和新無線存取點進行 IEEE 802.11 的三個步驟，所需時間是 T1，接著行動節點會和後端的認証伺服器進行 802.1x 認証，所需時間是 T2，最後則是行動節點和新無線存取點的四訊息握手交換，所需時間為 T3，當這些程序完成後應用程式才會繼續之前的封包傳送。

在一般的換手程序下，其所需的換手延遲時間為 T1+T2+T3。

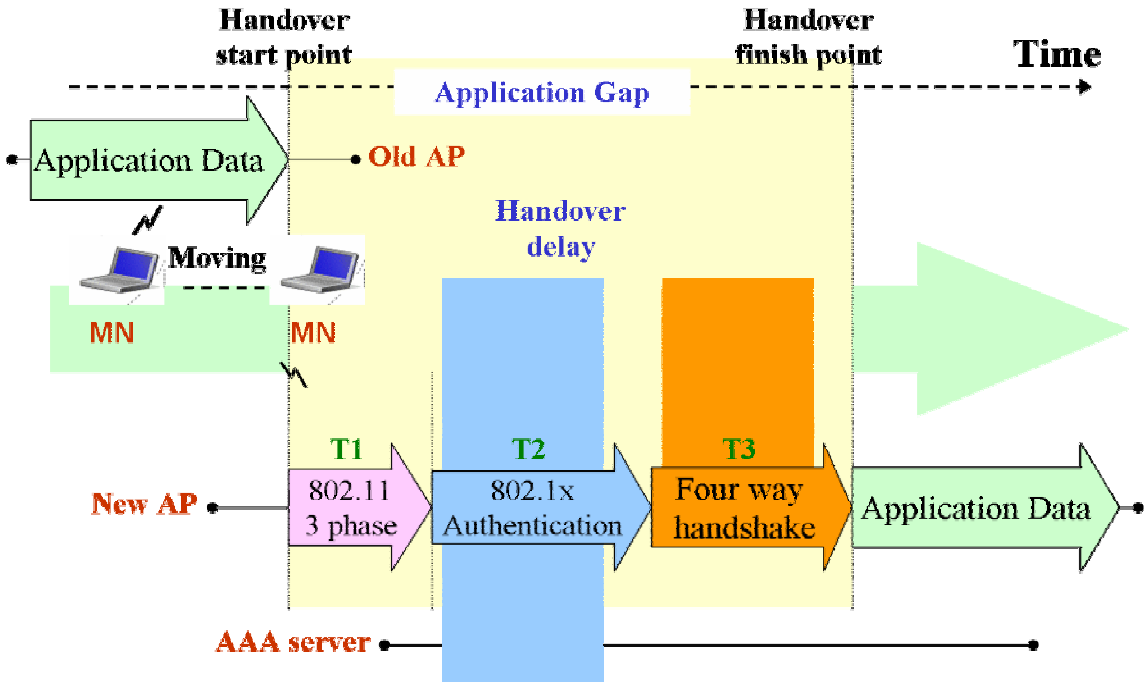


圖 5.1　換手延遲時間示意圖(一般程序)

5.1.2 快速換手程序

圖 5-2 是在快速換手程序下延遲時間的分析，圖中的橫軸由左到右代表著時間的演進，而圖中由上到下依然分別代表著環境中四個不同的元件，依序為舊的無線存取點、行動節點、新的無線存取點及認証伺服器。

如同上一節所述，行動節點會聯結上舊無線存取點並開始傳送應用程式的封包，之後行動節點會移動到和新無線存取點訊號較好的位置，但在移動同時，根據我們所提出的快速換手機制，行動節點會和新無線存取點及認証伺服器進行預先認証及預先四訊息握手交換，之後當無線網路卡決定要換手時，僅需進行 IEEE 802.11 的三個步驟，就可以繼續進行應用程式的封包傳送。

在本論文所提出的快速換手程序下，其所需的換手延遲時間為 T1，証明我們提出的方法確實能減少換手所需的時間。

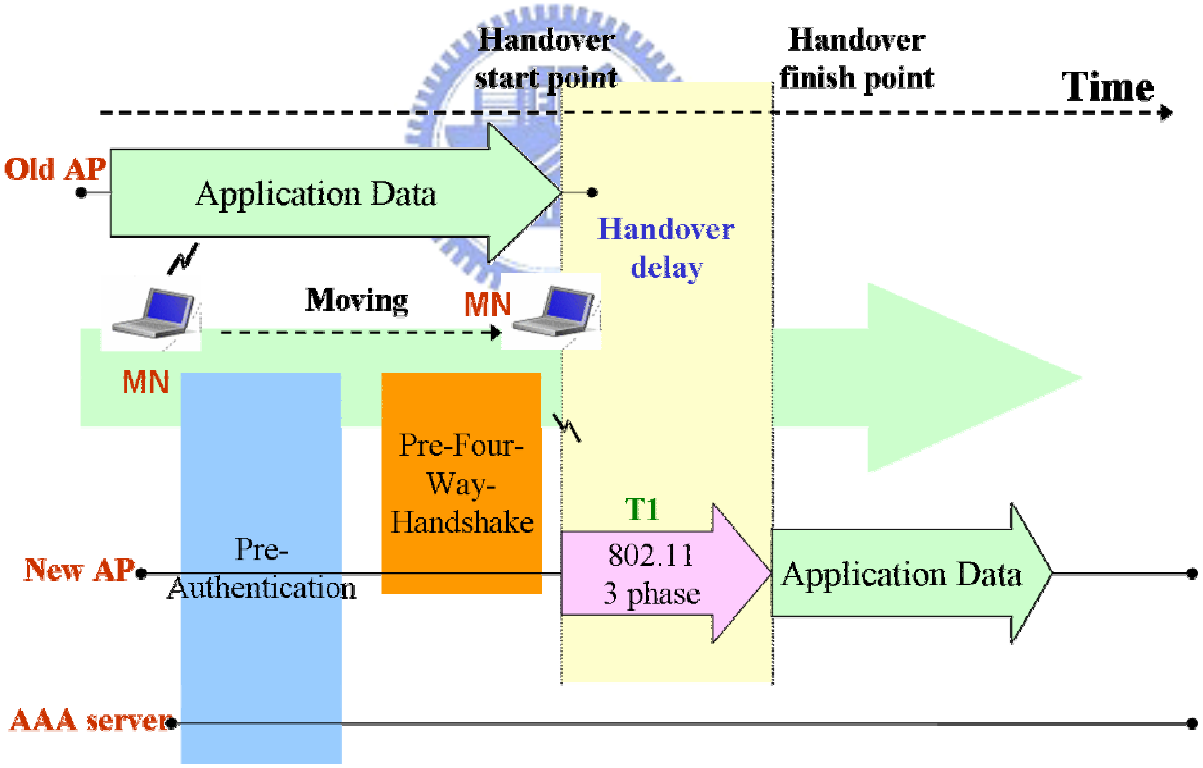


圖 5.2 換手延遲時間示意圖(快速換手程序)

第六章　結論與未來工作

6.1　結論

IEEE 802.11i 是新一代無線網路的安全性標準，由於使用更複雜的訊息交換和金鑰管理階層，行動節點在無線存取點之間進行換手時，將會有較長的換手延遲時間。本論文提出了一在符合 IEEE 802.11i 規格的無線網路環境下快速換手的架構，利用預先認証及預先四訊息握手交換，在行動節點尚未換手之前，即完成認証及導出對應的金鑰用 PTKSA 資料結構儲存下來，待之後真正換手到新的無線存取點後，即可直接安裝成對暫時金鑰且開始一般封包的傳遞。

由於預先認証和預先四訊息握手交換中行動節點都必須知道無線存取點的位址，因此本論文也提出了二種得知位址的方式，分別為由行動節點或是由位置伺服器來決定目標無線存取點，此兩種方式有各自的位置訊息交換封包，本論文也討論了三篇快速換相關論文，我們可以用相關論文中的演算法來決定可能會換手到的目標無線存取點。

最後我們實作出本論文所提出的快速換手架構，並在真實環境下實際做換手的測試，也証明本系統的確是可運行的。

6.2　未來工作

本論文所提的快速換手架構，主要都在解決 OSI 網路七層中的第二層問題，也就是媒體存取控制層的問題，而當行動節點在換手時，其所相關的動作卻不只局限在第二層當中，像是更上層可以用行動式 IP (Mobile IP) 來輔助換手後 IP 位址改變所產生的問題，或者用 SIP (Session Initiation Protocol) 來做移動管理 (mobility management)，將來會一併考慮這些上層協定，將之整合到本論文所提出的架構當中，讓行動節點在換手過程中更加順暢。

另外在本論文所提的架構中，預先認証及預先四訊息握手交換封包是由 EAPOL 的封包所承載，因此這些封包不能夠跨網域的傳遞，若是目標無線存取點位於不同的網域當中，則訊息會無法順利的送達，所以我們會針對此點對本快速換手架構做一補強，讓這些訊息可以跨網域的傳遞，使本快速換手架構能應用於

更多的網路環境當中。

其實我們在日常生活中，可能每天都會經過特定的區域，所會使用到的無線存取點也很固定是某幾個，這些週期性的行為，可以經由統計歸納的方式來推導出一個人的移動樣本 (mobility pattern)，定期的去維護這些移動樣本，我們可以更精準的去計算可能會換手到的無線存取點，將可以大幅減少訊息的傳送數量，則讓本架構所產生的負擔 (overhead) 不會那麼的重。

參考文獻

[1] J. Vollbrecht et al. “AAA Authorization Framework,” IETF RFC 2904, August 2000.

[2] L. Blunk, J. Vollbrecht, Merit Network inc., “PPP Extensible Authentication Protocol (EAP)”, IETF RFC 2284, March 1998.

[3] “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”, IEEE Standard 802.11, 1999.

[4] “Port-Based Network Access Control”, IEEE Standard 802.1x, June 2001.

[5] Arbaugh, W.A.; Shankar, N.; Wan, Y.C.J.; Kan Zhang; **“**Your 80211 wireless network has no clothes**”**, IEEE Wireless Communications, Volume: 9, Issue: 6, Dec. 2002 Pages:44 – 51.

[6] C. Rigney et al., “Remote Authentication Dial In User Service (RADIUS)”, IETF RFC 2865, June 2000.

[7] P. Calhoun et al., “Diameter Base Protocol”, IETF RFC 3588, September 2003.

[8] Arunesh Mishra, Minho Shin, and William Arbaugh, “An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process” (http://www.cs.umd.edu/~waa/pubs/handoff-lat-acm.pdf) .

[9] B. Aboba, Microsoft, P. Calhoun, Airespace, “RADIUS Support For Extensible Authentication Protocol (EAP)”, IETF RFC 3579, September 2003.

[10] “Wireless LAN Medium Access Control Security Enhancements”, IEEE, Standard 802.11i, July 2004.

[11] B. Aboba, D. Simon, Microsoft, “PPP EAP TLS Authentication Protocol”, RFC 2716, October 1999.

[12] Jon Edney, William A. Arbaugh, “Real 802.11 Security”, Addison-Wesley, July 2003.

[13] WiFi Alliance, http://www.wi-fi.org/OpenSection/index.asp.

[14] Chien-Chao Tseng, Kuang-Hui Chi, Min-Deng Hsieh, Hung-Hsing Chang, “Location-based Fast Handoff for 802.11 Networks”, IEEE Communication Letters

[15] Mishra A, Min Ho Shin, Petroni N.L. Jr., Clancy T.C., Arbaugh W.A, “Proactive key distribution using neighbor graphs”, IEEE Wireless Communications, Feb. 2004

[16] Minho Shin, Arunesh Mishra, William A. Arbaugh, “Improving the Latency of 802.11 hand-offs using Neighbor Graphs”, ACM Mobisys 2004

[17] Sangheon Pack, Yanghee Choi, ”Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE 802.1x Model”, Proceedings of the IFIP TC6/WG6.8 Working Conference on Personal Wireless Communication, October 2002.

[18] Hayriye Altunbasak, Henry Owen, “Alternative Pair-wise Key Exchange Protocols for Robust Security Networks (IEEE 802.11i) in Wireless LANs”, IEEE proceedings 2004

[19] H. Jonatban, “RADIUS”, O’REILLY, October 2002.

[20] P. Bruce, F. Bob, “802.11 Security”, O’REILLY, December 2002.

[21] Matthew S. Gast, ”802.11 Wireless Networks: The Definitive Guide”, O’REILLY, April 2002.

[22] Host AP driver, hostapd, and WPA supplicant, http://hostp.epitest.fi

[23] FreeRADIUS, http://www.freeradius.org

[24] OpenSSL, http://www.openssl.org