國立交通大學

電機學院與資訊學院 資訊學程

碩 士 論 文

基於 IEEE 802.11i 的快速預先認証

Fast Pre-Authentication based on IEEE 802.11i

研 究 生：黃玉佳

指導教授：簡榮宏　教授

中 華 民 國 九 十 五 年 六 月

基於 IEEE802.11i 的快速預先認証

Fast Pre-Authentication based on IEEE 802.11i

研 究 生：黃玉佳　　Student：Yu-Chia Huang

指導教授：簡榮宏　　Advisor：Rong-Hong Jan

國 立 交 通 大 學

電機學院與資訊學院專班 資訊學程

碩 士 論 文

A Thesis

Submitted to Degree Program of Electrical Engineering and Computer Science

College of Computer Science

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of Master of Science

in

Computer Science

June 2006

Hsinchu, Taiwan, Republic of China

中華民國九十五年六月

基於 IEEE 802.11i 的快速預先認証

學生: 黃玉佳　　指導教授: 簡榮宏

國立交通大學 電機學院與資訊學院 資訊學程（研究所）碩士班

摘　要:

IEEE 802.11i 目的是為了加強無線網路(IEEE 802.11)的安全，但太過複雜的認証程序會增加無線工作站(STA)在漫遊時重新連線所需的時間，影響即時性軟體的傳輸品質。對此 IEEE 802.11i 提出兩個因應的技術，分別為 PMK 快取(PMK Caching)以及預先認証(Pre-Authentication)；藉由無線工作站與下一個 AP 連線前事先完成認証的過程，並把認証的結果 PMK 快取下來，將可大幅減少漫遊過程中重新認証所造成的延遲情況。但缺點是會產生過多的封包流量以及佔用認証伺服器的資源，此外過長的時間亦會增加無線工作站的負荷。本篇論文即在此架構下提出一個新的機制-快速預先認証(Fast Pre-Authentication)，方法為在相同延伸服務區(ESS)的無線基地台(AP)中透過認証伺服器的協助建立一個安全的通道，將無線工站作先前完成認証所產生的金鑰相關資訊，提前交送給下一個連線的無線基地台，以較少的負擔(Overhead)達到快速漫遊的目的。另外以較少的時間完成預先認証，意謂著我們所提出的機制更加適合快速移動的無線設備。透過實作比較的方式，証明此機制是有效的。

Fast Pre-Authentication based on IEEE 802.11i

Student：Yu-Chia Huang　　Advisor：Dr. Rong-Hong Jan

Degree Program of Electrical Engineering and Computer Science
National Chiao Tung University

ABSTRACT

The goal of IEEE 802.11i is for strengthening the wireless local area network (IEEE 802.11) security, but it's complex authentication procedure will increase the STA's re-authentication time while roaming happened, and affect the quality of real-time application. To solve this problems, IEEE 802.11i proposed two methods called the PMK Caching and Pre-Authentication, which complete the authentication in advance between STA and next candidate APs and then caching the PMKSA each others, will reduce the roaming latency caused by re-authentication procedure. However the shortcoming besides will produce too much message flow and engage the resource of authentication server, the long duration will also increase more burden to the STA. This thesis presents a new approach called as Fast Pre-Authentication which achieve the goal of fast secure roaming with less overhead. Adjacent APs in the same ESS will set up secure channels through the assistance of the authentication server, and then transfer the STA key relevant information to the candidate AP in advance. Shortening of pre-authentication time will be more suitable for the faster wireless device. Experimental results are given to show the effectiveness of the proposed approach.

目　　錄

圖　　目　　錄

表　　目　　錄

第一章　前言

網際網路(Internet)的盛行加速有線網路的建構規模，而無線區域網路(IEEE 802.11)的技術則提供給使用者另一個不受拘束的不同体驗，此外無線的移動特性也提供更廣泛的應用，其中包括語音的通訊(VoIP)。當無線網路的佈建日漸普及，具有無線模組的移動工作站(STA)發生漫遊(Roaming)的機率的勢必會隨之增高，但在漫遊過程中所產生的延遲(Roaming Latency)將會造成上層應用軟体中斷及傳輸品質下降的影響，尤其是對時間敏感度較高的應用，例如聲音、多媒体…等等。針對第二層(IEEE 802.11)所造成的延遲因素，可分為 Probe Delay[7]、Authentication Delay(802.11)、Re-association Delay 以及 Re-authentication Delay(802.1x/EAP);而其中又以 Probe Delay 與 Re-Authentication Delay 所造成的影響最大。

因此有些相關的研究文件[1][2][3][4][11]即針對 Re-Authentication Delay 這方面的議題提出改進的策略，分別採用的不同的預測方式(Neighbor Graph、FHR)與溝通機制，預先將認証的相關資訊送至相鄰 AP 上儲存。藉此讓發生漫遊的 STA 可以省略大部份的認証過程，達到快速漫遊的目的。若以結果來看，他們所提的方法皆能有效達到縮減重新認証所需的時間，但共同的缺點是都會耗用不同程度的系統資源。包括額外的封包傳輸流量、存放認証相關資訊所需的空間以及用來維護特殊資料結構(Neighbor Graph、FHR)所需的計算資源。

IEEE 802.11i[8]中亦提出兩個解決方案，分別為 PMK 快取(PMK Caching)與預先認証(Pre-Authentication)。方法為在漫遊前，由 STA 透過目前連線的 AP，經由 DS 對其他 AP(在 STA 目前所在地所能搜尋到的訊號)進行完整的認証程序，並透過 PMK 快取的功能將認証所產生的金鑰快取在 STA 與 AP 中。以結果來看，802.11i 的方式也可以得到預期的效果;且相對上述文件[1][2][3][4][11]所提的預測方式，比較簡單不需採用特殊的資料結構記錄 AP 之間相鄰的關係，且對於存放金鑰空間的利用效率比較好。但預先認証的方式，與一般正常認証的過程幾乎是一樣的(少了四手交握協定，但多了 AP 之間轉送的 EAP 封包)。因此不可避免的，也會佔用網路的資源及增加認証伺服器的負擔，

此外整個過程中 STA 皆全程參與，過長的時間亦會增加 STA 的負擔。

因此本文研究的動機就是如何在浪費最少資源的情況下達到快速漫遊的目的。我們針對 802.11i 的預先認証功能，提出一個改良的方式，稱為快速預先認証(Fast Pre-Authentication)。主要目標為在安全的前提下達到(1)減少額外的封包流量(2)減輕認証伺服器的負擔(3)以較短的時間完成預先認証的過程。並經由實作的方式，與 IEEE802.11i 的預先認証做個比較。

本論文接下來的章節分別簡述如下，在第二章的內容將會簡短介紹 IEEE 802.11i 的主要規範與 Needham-Schroeder 認証協定。在第三、四章說明快速預先認証的內容與架構流程。第五章為實作的軟硬體平台介紹與相關實驗數據分析比較。第六章則為我們的結論與未來的工作方向。

第二章 相關背景資料

IEEE 802.11i 是針對 IEEE802.11 提出一個進階的安全解決方案。目的是加強無線區域網路的安全性，並且改善已知的安全漏洞。其中 IEEE802.11i 定義了一個新的安全模式，稱為 RSN(Robust Security Network)。此外為了讓舊有的無線設備在不需更換硬體的前題下，亦定義了一個 TSN(Transitional Security Network)模式。在本章節 2.1 至 2.6，將針對 RSN 部份的特色，包括 802.1x、EAP、金鑰的管理、四向交握協定、PMK 快取以及預先認証做一個概略的介紹。在 2.7 節中則是針對 Needham-Schroeder 認証協定做個簡介。2.8 節則會說明 STA 漫遊的決策機制。

2.1 IEEE 802.1x 簡介

存取控制在網路安全的領域中是相當重要的一環。802.1x 定義了連接埠控管協定(port-based access control protocol)，可有效阻隔未經認証的使用者使用網路資源或佔用網路頻寬。802.1x 已廣泛的被使用在區域網路上的設備，其中包括最常見到的網路交換器(Switch Hub)。早期 IEEE 802.11 標準中關於認証的功能僅提供簡易的 SSID 識別與共享金鑰認証，若採用 802.1x 的架構，它會在允許存取無線網路之前，對無線工作站(STA)強制進行以使用者為基礎的憑證驗證，並依據所採用的驗證方法，動態的產生無線通訊所需的加密金鑰。無線區域網路的環境中，雖然沒有像網路交換器(Switch Hub)一樣有實體埠的存在，但我們可以將每一個 STA 與 AP 之間的鏈結狀態視為一個虛擬的連接埠(如圖 2.1)。

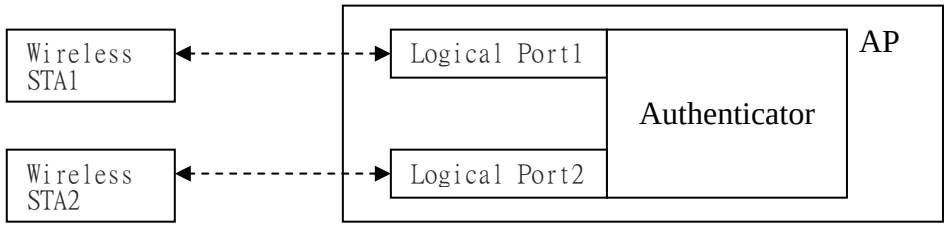


圖 2.1 Logical Port in 802.11

2.1.1 802.1x 的組成

802.1x 的架構主要由三個不同的角色所組成(圖 2.2)，分別說明如下:

驗證者(Authenticator)

主要負責驗證把關的工作，根據認証的結果來決定是否允許透過這個連接埠進行網路存取的服務。對於無線區域網路而言，驗證者就是 AP 上的邏輯連接埠；在這個基礎結構中運作的無線用戶端必須透過它才能存取有線網路。

請求者(Supplicant)

主要負責向驗證者提出存取服務要求。對於無線連線而言，請求者就是在無線網路介面卡上要求存取有線網路的邏輯連接埠。不論是使用於無線連線或有線連線，請求者與驗證者都是由邏輯或實體點對點所連接。

認證伺服器(Authentication Server)

為了驗證請求者的身份，驗證者會向認證伺服器查詢。認證伺服器負責執行認證的功能以檢查請求者的身份，並向驗證者指示該請求者是否獲得認證伺服器的授權。儘管 802.1X 並沒有強制要求使用遠端認證撥入用戶服務(RADIUS)，但 RADIUS Protocol 事實上已經成為驗證者和認證伺服器之間最常用的協議。

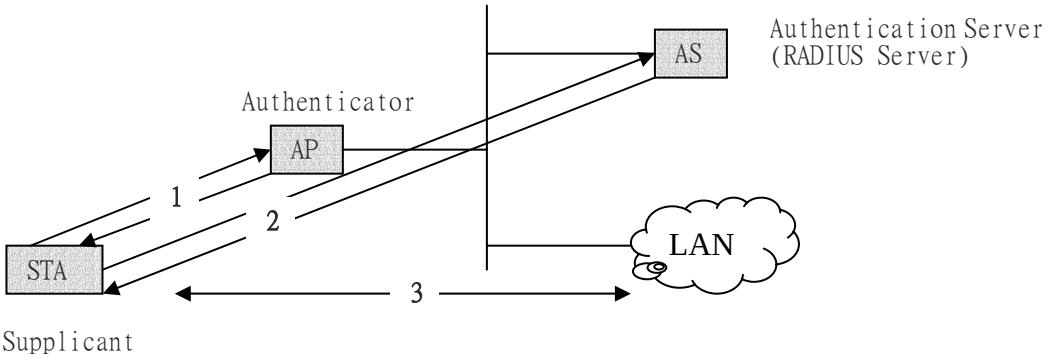


圖 2.2 802.1x 的架構與流程

2.1.2 802.1x 的運作流程

透過(圖 2.2)簡單描述 802.1x 的基本運作流程。

(1). STA 與 AP 建立一個邏輯埠之後，會送出一個使用網路的要求，AP 則要求 STA 傳送身份証明;當 STA 未完成認証程序時，AP 僅允許認証的封包(EAP)通過。

(2). STA 開始與 AS 進行認証程序，此時 AP 會將 EAP 的資訊，轉成 RADIUS 封包格式送給 AS。在整個認証程序的過程中，AP 會持續擔任轉送封包的角色。

(3). 當完成驗成程序時，AS 會傳遞一個成功的訊息給 AP，AP 則將邏輯埠的狀態設為已授權(Authorized)，STA 即可開始傳送與接收其他的封包。

2.2 擴充式認証通訊協定(EAP)

在上節所提到的 802.1x，主要是提供一個基於連接埠的控管平台，本身並沒有規範認証的方法。而 EAP(RFC 2284)源自於點對點通訊協定(PPP)，目的是提供一個認証擴充的基礎。EAP 本身定義了一組訊息封包(圖 2.3)，可將上層認証的資訊依照不同 RFC 所定義的 EAP 型態進行交換(例如 EAP-PEAP、EAP-TLS…)，直到完成整個認証的過程。因此藉由 EAP 的協助，請求者可彈性的選擇不同的認証方式，也可以很快速的發展新的認証演算法套用在 802.1x 環境。此外 802.1x 亦定義了 EAPOL(EAP over LAN)的通訊協定，以便讓 EAP 的訊息可以在區域網路及無線區域網路上傳送。

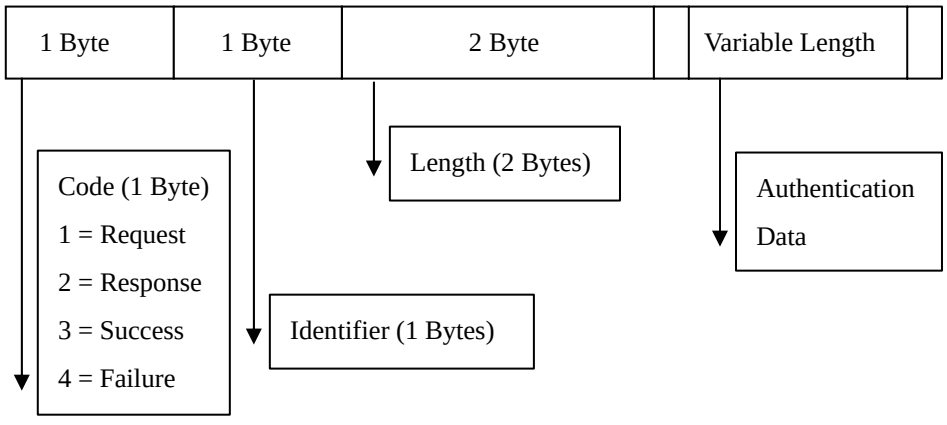


圖 2.3 EAP 封包的格式

2.3 金鑰的管理

無線網路使用兩種不同用途的金鑰，一種是用於點對點(Unicast)通訊，稱為 Pairwise Key。另一種則是用於廣播(Broadcast)通訊，稱為 Group Key。AP 與每台 STA 之間均擁有一把金鑰做為 Unicast 封包加密使用且是唯一的，而 AP 與所有跟自己相連的 STAs 則共享一把相同的金鑰以供廣播封包加密。

2.3.1 動態金鑰與金鑰的衍生

有別於早期 802.11 中 WEP 採用雙方預先輸入固定的金鑰，802.11i 提出一個完善的金鑰管理，可藉由 802.1x/EAP 動態的產生加密所需的金鑰(圖 2.3)。

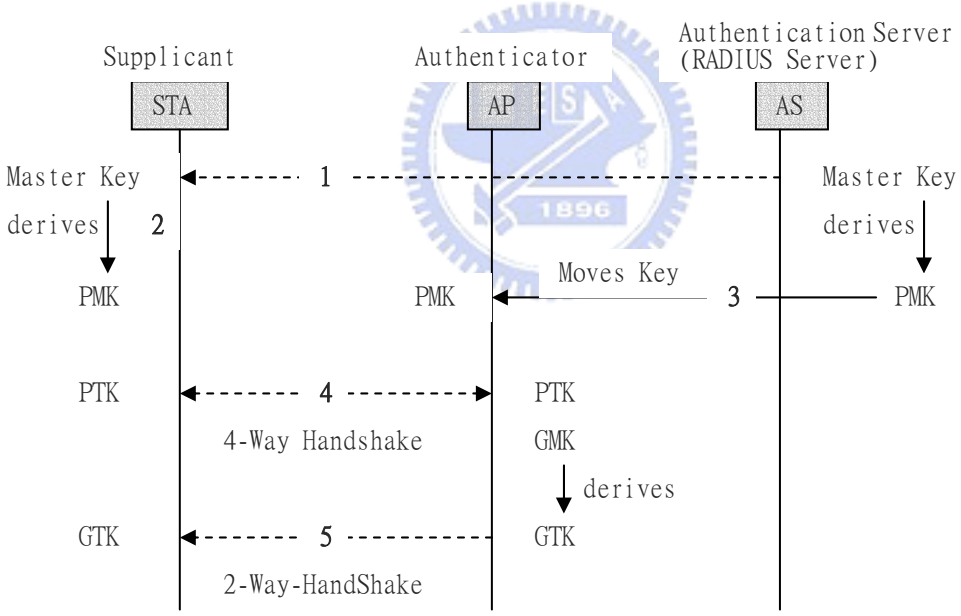


圖 2.4 802.11i 的金鑰衍生過程

(1). STA 與 AS 完成認証程序之後，彼此會產生一把相同的 Master Key。

(2). STA 與 AS 經由相同的運算，衍生出另一把相同的 Pairwise Master Key (PMK); AS 則透過 RADIUS Protocol 將 PMK 傳送給 AP。

(3). STA 與 AP 透過四向交握協定程序，經由 PMK 衍生出 PTK。

(4). AP 隨機產生 GMK，並衍生出 GTK 傳送給所有的 STAs。

2.3.2 金鑰的階層架構

在下列的圖示中(圖 2.5)，分別列出 AES 與 TKIP 在產生其他金鑰時的相對關係，其中包含了金鑰的用途及長度。

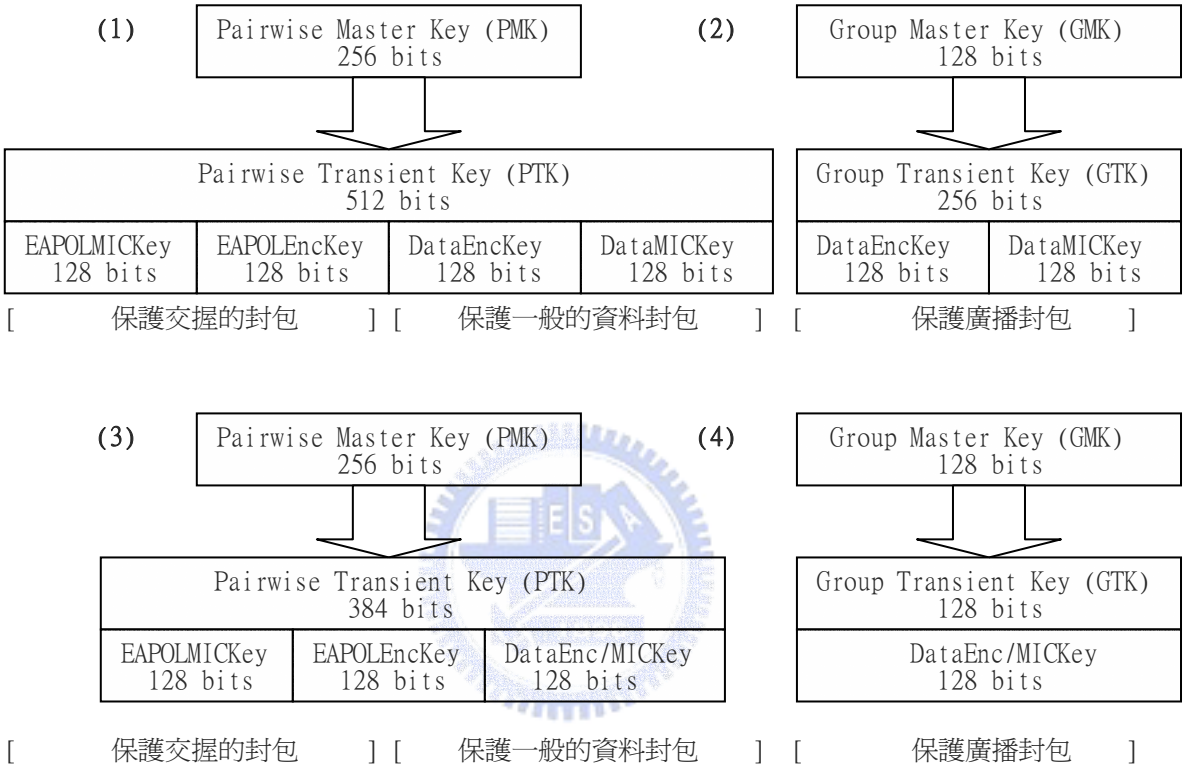


圖 2.5 金鑰的階層架構 (1)TKIP Pairwise Key Hierarchy (2)TKIP Group Key Hierarchy (3)AES Pairwise Key Hierarchy (4)AES Group Key Hierarchy

2.4 四向交握協定(4-Way-HandShake)

在上節所提到的金鑰架構中，我們可以發現，在上層的 PMK 並沒有直接被使用在資料傳輸的加密過程中，反而衍生成一組包含四把金鑰的集合稱為 PTK，以提供請求者與驗證者之間一個安全加密的通道。其中兩把金鑰(KCK、KEK)做為握手交換過程中，加密(Encryption)與一致性(Integrity)的用途，另外兩把金鑰(TK1、TK2)則做為 STA 與 AP 之間傳送一般資料時，加密(Encryption)與一致性(Integrity)的使用，如圖 2.6 所示。而採用四向交握協定主要目的為

(1). 確認 STA 與 AP 彼此的 PMK 是相同的。

(2). 間接確認 AP 是否為合法的身份。

(3). 確認彼此使用的密鑰組合(Cipher suit)是否一致。

(4). 建立具有時效性暫時的金鑰以供安全加密使用。

(5). AP 傳送 GTK 給 STA (RSN 模式)。

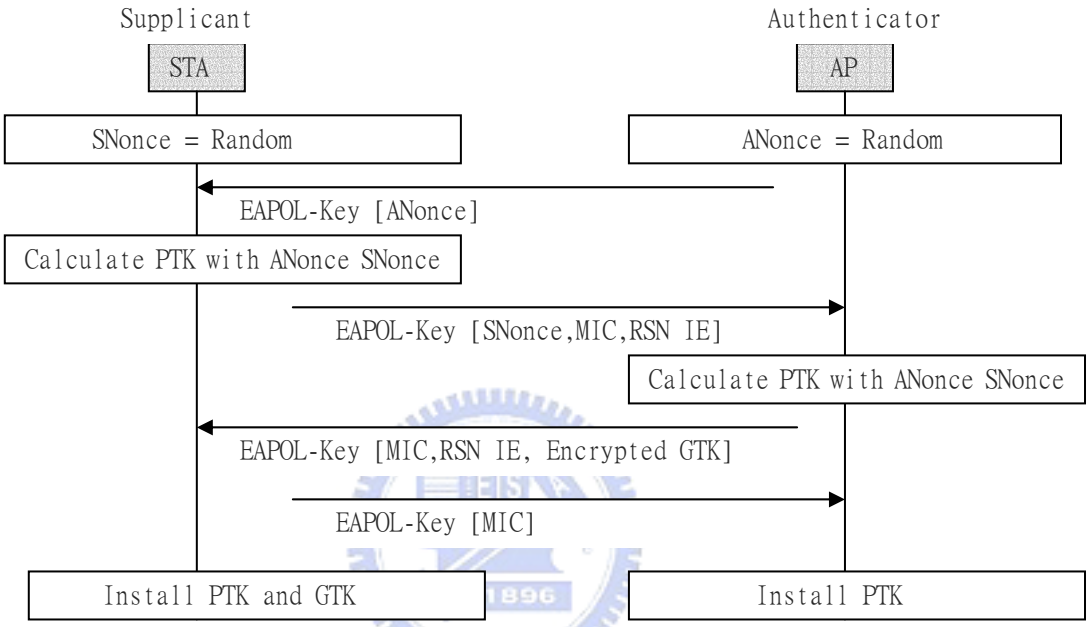


圖 2.6 四向交握的訊息流程

(1). 訊息一: AP 送一個亂數(ANonce)給 STA。

(2). 訊息二: STA 回送一個亂數(SNonce)給 AP，這時 STA 已經可以透過 PMK、ANonce、SNonce、以及雙方的 MAC Address 產生 PTK，並將 Association Request 中所使用到的 RSN IE 放在 Key Data 欄位，最後用 PTK 中的 KCK 對整個封包加密產生一個 MIC 值，隨訊息一起送出。

(3). 訊息三: AP 收到 SNonce 之後，亦可衍生出相同的 PTK，進而確認訊息三的正確性; 比對 STA 送過來的 RSN IE 之後，將 Beacon 中的 RSN IE 放在訊息三的 Key Data 欄位的前面，用 PTK 中的 KEK 對 GTK 加密後放在 Key Data 中，最後用 KCK 對整個封包加密產生一個 MIC 值，隨訊息一起送出。

(4). 訊息四: STA 回應 AP，告知開始使用加密的方式傳送資料。

2.5 PMK 快取

802.1x 認証的目得是為了確認 STA 的身份是否合法，並且在完成認証之後讓 STA 與 AP 之間擁有相同的 PMK。但在這個認証過程中，AP 必須持續擔任轉送認証封包的工作，勢必會增加整個認証的時間。假如 STA 與 AP 兩者可以保留之前認証所產生的 PMK，則當 STA 與 AP 重新連線時，就可直接進入四手交握協定的過程，加速連線的過程。其過程描述如下(圖 2.7):

當 STA 發現目前預連線的對像(AP)，在其暫存區中有相對應的 PMKSA 記錄時，會在(Re)Association Request 的封包內附上此筆記錄相對應的 PMKID。當 AP 收到此封包時，會先依照 PMKID 比對自己暫存區的資料是否存在相同且合法的 PMKID; 若有則在完成 Association 程序後跳過與後端認証伺服器確認的過程直接進行四手交握協定,AP 亦會在四手交握協定過程中，將 PMKID 加入在第一個訊息的金鑰資料欄位，以供 STA 查核。反之則要求連線的 STA 必需進行完整的 802.1x/EAP 認証程序。

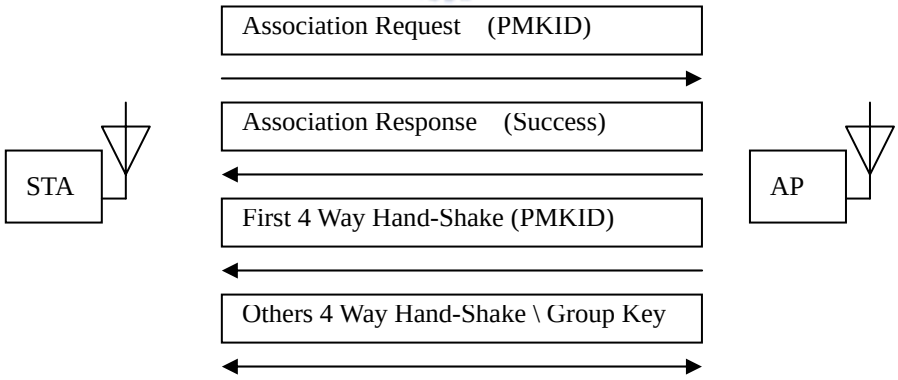


圖 2.7 PMK 快取的訊息流程

2.6 預先認証(Pre-Authentication)

預先認証的功能允許 STA 可以在相同的時間對多個 AP 進行認証的動作，即使在尚未完成 Association 的情況下。其目的是讓 STA 發生漫遊之前，就先對鄰近 AP 進行完整 802.1x/EAP 認証，並利用 PMK 快取的功能將 PMK 及相關資訊快取保存下來;當 STA 與已完成預先認証的 AP 連線時，即可直接進行四手交握協定。

支援預先認証功能的 AP，利用信標(Beacon)和探測回應(Probe Response)封包中的 RSN 資訊對外廣播。當 STA 偵測到附近有支援預先認証的 AP 時,即送出預先認証的封包,透過連線中的 AP(Old AP)經由有線的網路與 AP(New AP)進行 802.1x/EAP 的認証(圖 2.7)。

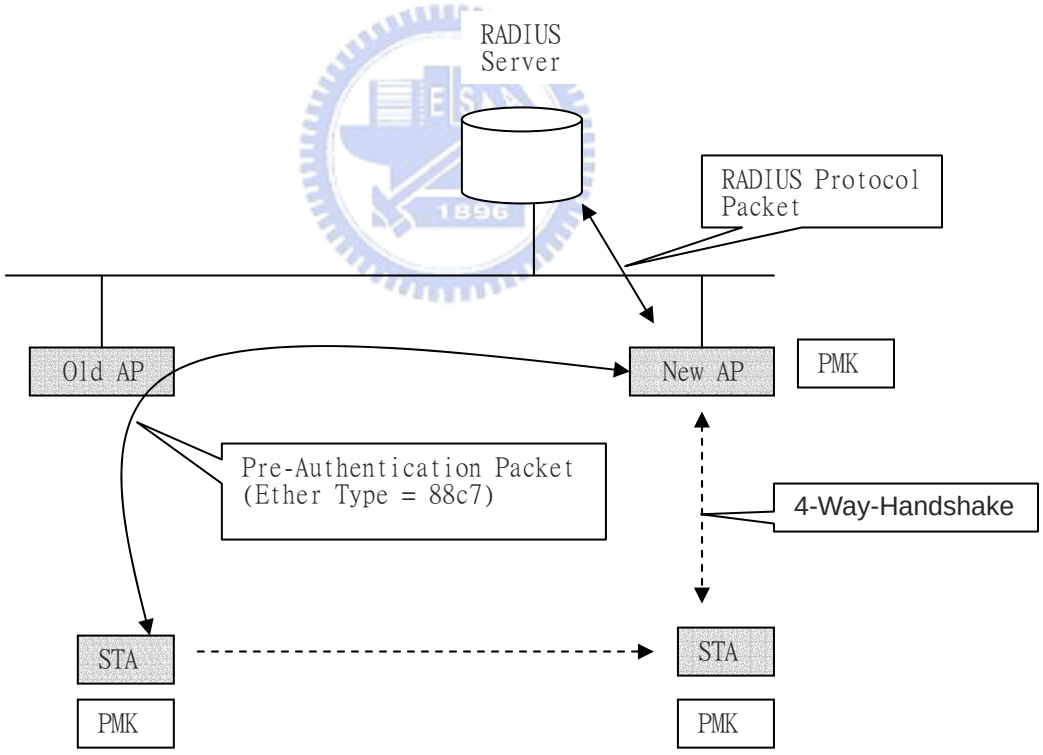


圖 2.7 預先認証流程

2.7 Needham-Schroeder 認証協定

Needham-Schroeder[9]是一種網路認証的協定，是由 Roger Needham 與 Michael Schroeder 兩人於 1978 年所發明的，其方式是透過信任的第三者，例如認証伺服器(Authentication Server)，對合法的用戶端(Client)與伺服器(Server)，提供一個安全的存取環境。

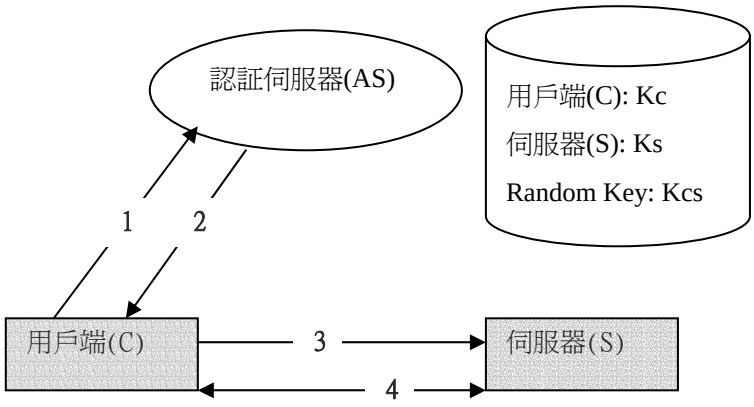
在此架構下，每個用戶端、伺服器與認証伺服器之間皆分別共有一把通訊用的秘密金鑰(Shared Key)，這把金鑰是彼此雙方事先得知。當任何一方(用戶端或伺服器)欲與認証伺服器進行溝通，則會採用這把金鑰加密以此確認彼此的身份。當用戶端向伺服器要求連線服務前，必需先向認証伺服器取得通行証(Token)，而用戶端不需經過伺服器的認証，即可以此通行証(Token)與伺服器進行通訊。

整個認証流程包含了三個主要的訊息如圖 2.8，
(1).首先用戶端先向認証伺服器傳送對伺服器的連線請求，在此訊息中包含了用戶端資訊(C)、伺服器資訊(S)以及一個亂數(IA)，其中的亂數是用以分辨請求訊息，讓用戶端確認收到回傳訊息的正確性。

(2).認証伺服器收到請求之後，會隨機產生一把金鑰(Kcs)以供用戶端與伺服器之間通訊時加解密之用。接下來，認証伺服器會將此把金鑰(Kcs)與用戶端相關資訊(C)用伺服器與認証伺服器之間共享的金鑰(Ks)加密產生通行証(Token = {Kcs + C}Ks)。最後將此通行証與伺服器相關資訊加上在請求訊息中的亂數(IA)以用戶端與認証伺服器之間共享的金鑰(Kc)加密，回傳給用戶端。

(3).用所端收到回傳的訊息，首先用金鑰(Kc)解開訊息，比對亂數 IA 是否與原先送出的 IA 是相同的，若是則可確認此封包中內含金鑰(Kcs)的正確性。用戶端在收到通訊用的金鑰(Kcs)之後，接著根據伺服器的資訊，將通行証送給伺服器。伺服器用金鑰(Ks)解開通行証之後，獲得與用戶端通訊用的金鑰(Kcs)與用戶端資訊之後，用戶端與伺服

器之間即可開始使用金鑰(Kcs)進行安全的通訊。



1. 用戶端->認証伺服器: C || S || IA
2. 認証伺服器->用戶端: { S || IA || Kcs || { C || Kcs}Ks }Kc
3. 用戶端->伺服器: { C || Kcs }Ks
4. 用戶端<-> 伺服器: { Data }Kcs

圖 2.8 Needham-Schroeder 認証流程

第三章 快速預先認証

Fast Pre-Authentication

快速預先認証的目的，在於藉由信任的第三者- 認証伺服器(RADIUS Server)的協助，在相同延伸服務區(ESS)提供一個安全認証與交換金鑰的方式。預先將已完成認証的 STA 的 PMK 傳送至下一個可能相連的 AP。藉此方式，在整個預先認証的過程中，以較少的認証封包取代完整 802.1x/EAP 的認証，以減輕認証伺服器的負荷，並加快整個過程所花的時間(圖 3.1)。如此當 STA 漫遊至相鄰的 AP 時，可透過 PMK 快取的功能，直接進行四向交握協定，進而加快完成重新認証聯線的過程。在此章節將介紹快速預先認証(Fast Pre-Authentication)主要特色，包括 PMK 的重覆使用、安全通道的建立以及可變動的 PMKID。

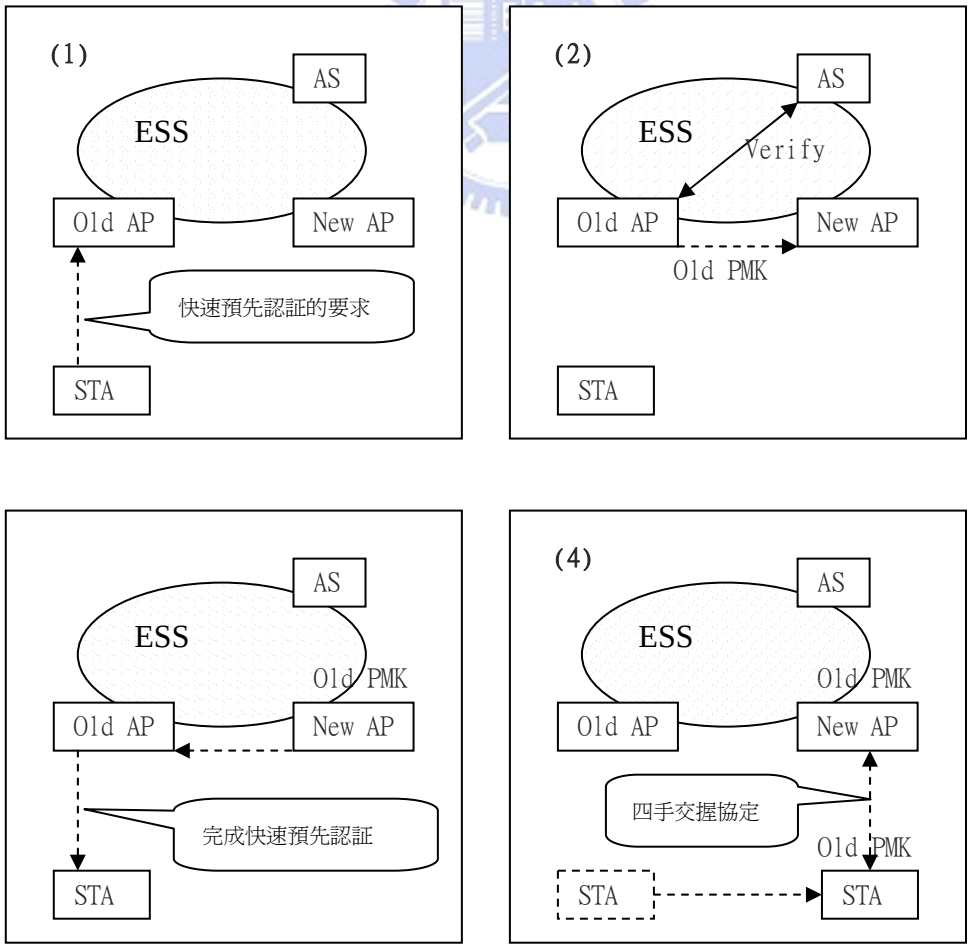


圖 3.1 快速預先認証的流程分解圖

(1)STA 透過 Old AP 對 New AP 發出快速預先認証的要求。

(2)Old AP 在已確認 New AP 身份的情況下，將 PMK 加密傳給 New AP

(3)Old AP 告知 STA 已成功完成快速預認証。

(4)STA 漫遊至 New AP 時，直接進行四手交握協定。

3.1 PMK 的重覆使用

STA 第一次與延伸服務區中的 AP 連線時，必需進行一次完整的 802.1x/EAP 認証，透過後端認証伺服器的授權之後，STA 與 AP 之間將會擁有相同的金鑰(PMK)，並透過四向交握協定產生真正通訊加密的金鑰(PTK);因此金鑰(PMK)可視為 STA 與 AP 之間的通行証(Token)。假設在相同延伸服務區的 AP 之間存在一種彼此信任的關係並可經由安全的管道共用彼此保有的通行証(參閱 3.2)，那麼 STA 對其中一台 AP 所擁有的通行証對其他 AP 而言亦可視為一個有效的通行証。換句話說一旦 STA 透過延伸服務區中任何一台 AP 取得認証伺服器授予的通行証，在通行証有效期限內即可憑此証漫遊於 AP 之間，而不需每次重連時皆要經過認証伺服器的重新認証(圖 3.2)。

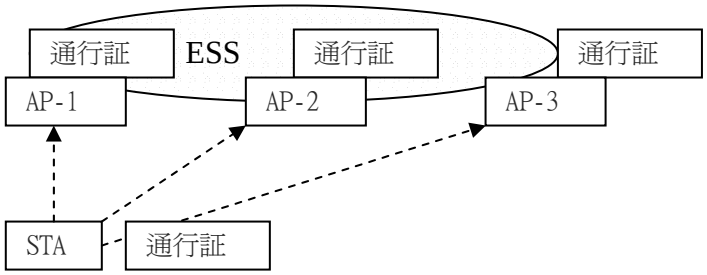


圖 3.2 通行証的使用

3.2 安全通道的建立

為了保障通行証(PMK)能夠在合法的 AP 之間傳遞，以及提供一個安全的傳送管道，可透過信任的第三者-認証伺服器(RADIUS Server)達成此需求。在本文中的 2.7 節中曾介紹過 Needham-Schroeder 認証協定[9]的運作原理，此外 IEEE802.11F[10]中亦提供一種 IPSec 加密通道的方式。在本節的內容中我們將會基於上述的協定提出一些改進的方式，以符合快速預先認証的環境。

1．在延伸服務區中的所有 AP 與認証伺服器之間都存在一組帳號(AP 的 BSSID)和預先輸入的共享金鑰(BSSID Secret)，一方面用以驗証 AP 的合法性，另一方面則可做為彼此之間交換訊息時加密的金鑰。

2．AP 在加入延伸服務區時必需先向認証伺服器進行註冊的程序，目的是讓認証伺服器能清楚掌握現有合法 AP 的狀態。例如 AP1 欲送資料給 AP2 時，可先向認証伺服器查詢 AP2 的身份，此時認証伺服器會在確認兩者(AP1 與 AP2)的合法性之後，再隨機產生 Session Ke 分別用 AP1、AP2 的共享金鑰加密後交予 AP1。

3．AP1 可透過事先得知的共享金鑰解出 Session Key，再將用 AP2 共享金鑰加密過的 Session-Key 傳給 AP2。當 AP2 獲得相同的 Session-Key，AP1 與 AP2 之間即可透過 Session-Key 進行安全的資料傳送。

4．認証伺服器在產生 Session Key 時，亦會付予一個有效期限(Lifetime)。共同保有此把 Session Key 的 AP1 與 AP2 在有效期限內，可以快取這把金鑰，並重覆使用。當欲使用此金鑰，而使用期限已到時，則必需再向認証伺服器查詢以取得新的加密金鑰。

3.2 可變動的 PMKID

根據 IEEE802.11i 的定義，PMK 安全關聯(PaireWise Master Key Security Association)是經由完整 802.1x/EAP 認証之後所產生的一組資訊集合，而 PMK 安全關

聯包含了以下的資料:

1.PMK 識別碼(PMKID)

2.驗証者的位址(Authenticator MAC Address)

3.PMK 金鑰

4.有效期限(Lifetime)

5.認証與金鑰管理協定(AKMP)

其中 PMK 識別碼(PMKID)的作用，在於代表整個 PMKSA 或 PMK 金鑰本身。STA 與 AP 之間可藉由交換比對 PMK 識別碼，即可判斷彼此之間所快取的 PMK 是否相同。

而 PMK 識別碼的運算式如下

PMKID = HMAC-SHA1-128(PMK, “PMK Name”||AA||SPA)

其中”AA”代表 Authenticator Address，亦即 AP 的 BSSID 或 MAC Address，而”SPA”代表 Supplicant Address，亦即 STA 的 MAC Address。

由上面的式子可得知，如果 AP 將手中所快取的 PMK 傳送至其他 AP 時，因每台 AP 的 BSSID 一定不同，即使 PMK 是相同的情況下，單就 PMKID 的定義，每台 AP 所快取的 PMKID 必定不同。因此當 AP 接收其他 AP 傳遞過來的 PMK 時，必需套用自己的 BSSID 重新計算 PMK 識別碼(PMKID)(圖 3.3)。相對的 STA 在發生重新連線時，也必需針對不同的 AP 重新計算 PMK 識別碼(PMKID)，才能在 Association Request 封包中送出正確的 PMK 識別碼。

在上述的情況下，當 STA 在同一個延伸服務區漫遊時，只需保留一個 PMKSA 的空間即可，但缺點是每次重新連線時，都必需重新計算 PMK 識別碼。

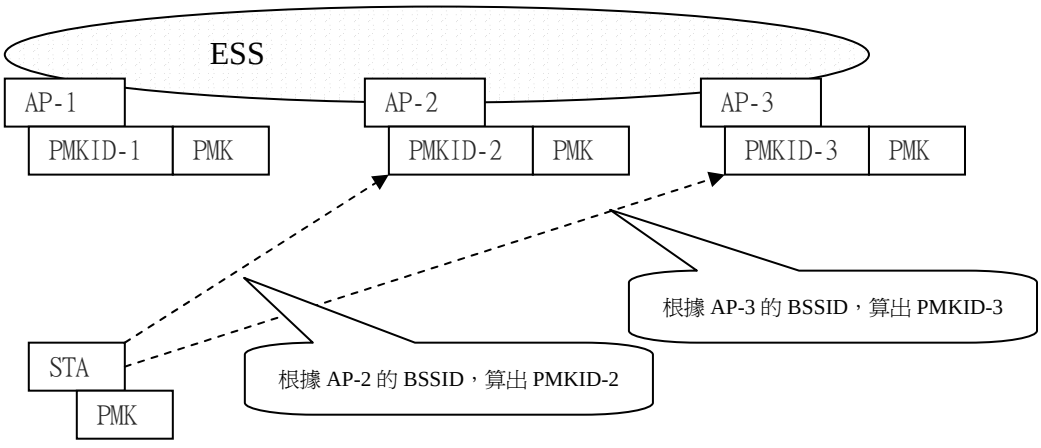


圖 3.3 PMKID 的重新計算

第四章 快速預先認証的流程與架構

快速預先認証的架構可區分為五個基本的流程(如圖 4.1)，分別為

1. 註冊流程
2. 快速預先認証清單的建立
3. 查詢流程
4. Session Key 的傳遞
5. PMK 的傳遞。

註冊流程為 AP 在開機時的首要步驟，必需先向信任的認証伺服器註冊。而當 AP 沒有目標 AP 的快取金鑰(Session Key)時，則需經過查詢流程接著進行 Session Key 的傳遞以及 PMK 的傳遞。若 AP 快取金鑰(Session Key)中，已包含目的 AP 且尚在有效時限內，則直接進行 PMK 的傳遞。STA 可透過背景掃描週遭 AP 的訊號，主動式或被動式的建立快速預先認証清單。在下面的章節將依序介紹五個基本流程的內容。

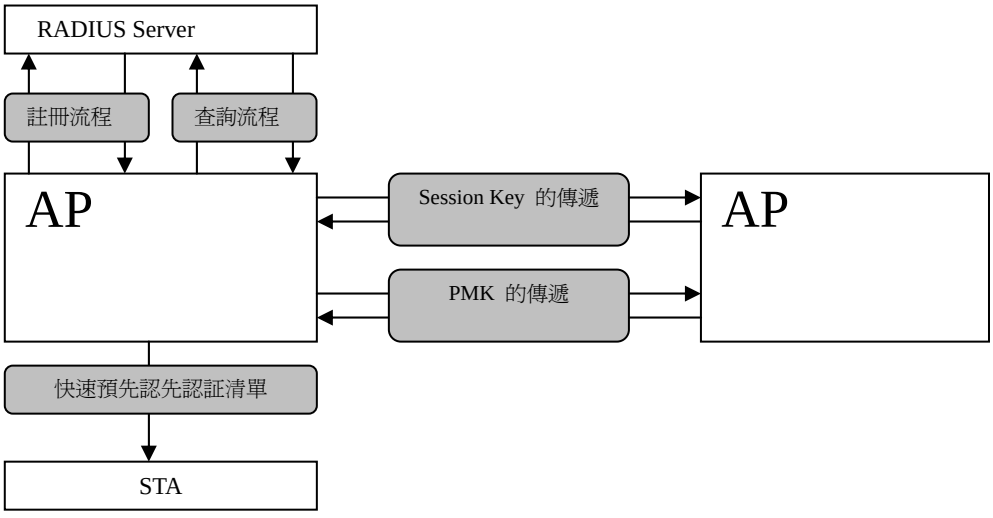


圖 4.1 快速預先認証的基本流程

4.1 註冊流程

屬於相同延伸服務區的 AP，在開機啟動時必需先與信任的認証伺服器進行註冊。認証伺服器中的帳號資料庫除了記錄原先的 NAS Client IP 與 Shared Secret 之外，另外多了一組其他種類的帳號以供 AP 在向認証伺服器註冊時使用。其中以 AP 的 BSSID 做為使用者名稱而 BSSID Secret 則做為彼此認証的密碼。當合法的 AP 完成註冊的程序之後，認証伺服器則會記錄 AP 為此延伸服務器內認可的 AP，亦即表示此 AP 已被認証並允許參與傳遞或接收其他 AP 的 PMK 資料(圖 4.2)。

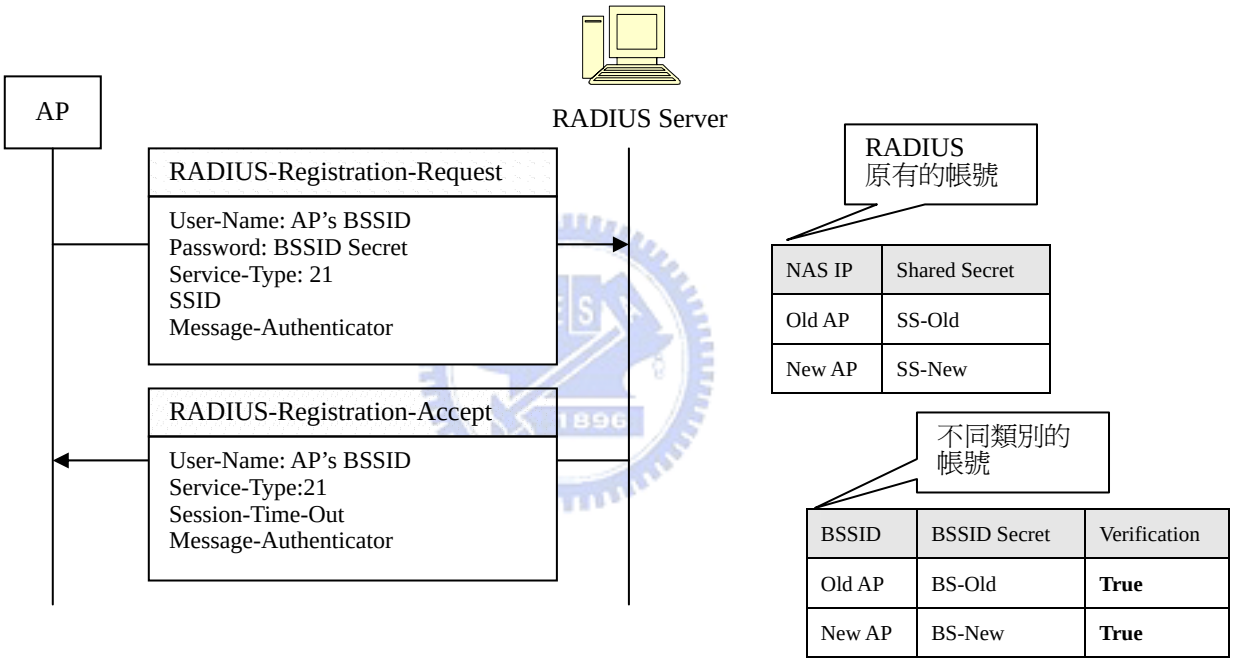


圖 4.2 AP 的註冊流程

在註冊流程中，RADIUS-Registration-Request 的封包格式與 Access-Request 類似，而 RADIUS-Registration-Accept 的封包格式與 Access-Accept 類似。另外我們定義一個新的 Service Type = 21，稱為 FPA registration。

4.2 快速預先認証清單

STA 透過主動與被動的方式收集信標或探測回應封包中含有 RSN Capability (Pre-Authentication bit)的資訊建立預選清單，並根據此清單依序(依據訊號強度)對附近可能發生漫遊的 AP 進行快速預先認証。由於 STA 與目前連線的 AP 已完成認証程序，因而彼此之間的資料交換皆在加密保護的狀態下進行。

首先 STA 會送出一個 EAPOL-Cache-Move(內含目前欲進行預先認証 AP 的 BSSID)的請求給目前正在連上的 AP。AP 如果收到 STA 的請求則會繼續進行後面的程序，如果成功完成傳遞 PMK 的動作，則回傳回 EAPOL-Cache-Success 給 STA;反之則傳回 EAPOL-Cache-Fail 給 STA。STA 根據收到的結果將清單中的該項 AP 標記為成功(Success)或失敗(Fail)，在下次進行快速預先認証時，則跳過這些已標記為成功(Success)的 AP。(圖 4.3 為 EAPOL 封包格式)

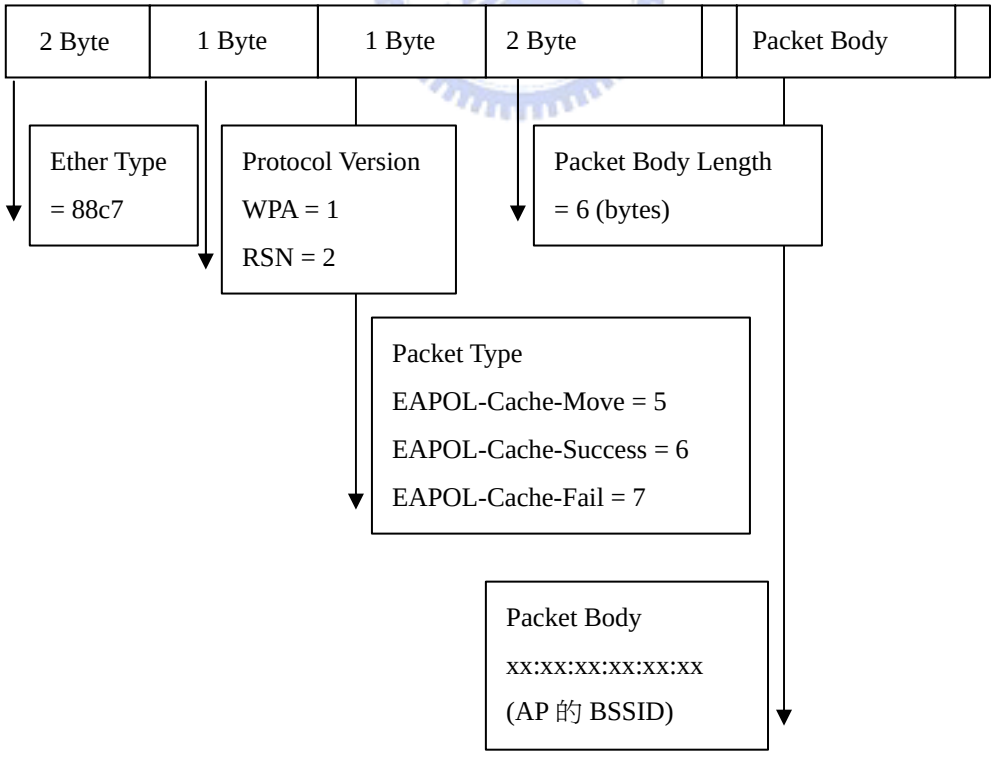


圖 4.3 EAPOL 封包格式

4.3 查詢流程

查詢的目的在於確認 STA 要求快速預先認証的 AP 是否為合法的 AP。而傳遞 PMK 時加密所需的金鑰(Session Key)，則由認証伺服器隨機產生之後，傳送至相對應的 AP。其過程如圖 4.4

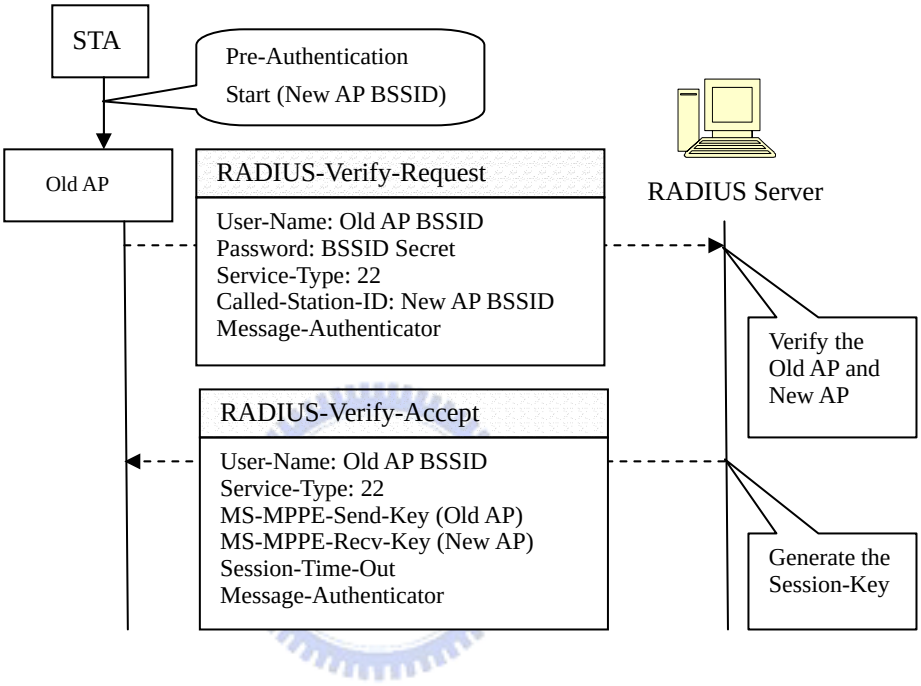


圖 4.4 AP 查詢的流程

1. Old AP 收到 STA 送出的要求(內含 New AP 的 BSSID)，即送出 RADIUS-Verify-Request，以確認 New AP 的合法性。

2.認証伺服器確認雙方 AP 身份的合法性之後，隨機產生一把金鑰(Session Key), 分別以 Old AP 以及 New AP 的 BSSID Secret 加密分別產生 MS-MPPE-Send Key(RFC 2548) 與 MS-MPPE-Recv-Key，回傳給 STA 目前連上的 Old AP。

3.Old AP 將收到的 MS-MPPE-Send Key 用自己的 BSSID Secret 解密即獲得與 New AP 之間的安全金鑰(Session Key)。

在查詢的流程中，RADIUS-Verify-Request 的封包格式與 Access-Request 類似，而 RADIUS-Verify-Accept 的封包格式與 Access-Accept 類似。另外我們定義一個新的 Service Type = 22，稱為 FPA Verify。

此外認証伺服器隨機產生的 Session Key 主要分為兩個部份(如圖 4.5)。KCK 用來產生 MIC 值確保 EAPOL Key 封包的完整性。KEK 則用來加密保護 EAPOL Key 封包中的 Key Data 欄位。

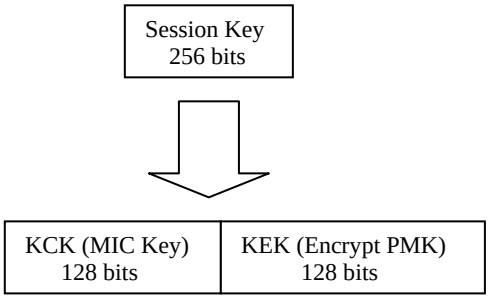


圖 4.5 Session Key 的架構

4.4 Session Key 的傳遞

Session Key 的傳遞主要是確保，欲建立安全通道的 AP 雙方能在安全的狀態下取得所需的金鑰，其過程說明如下(圖 4.6)

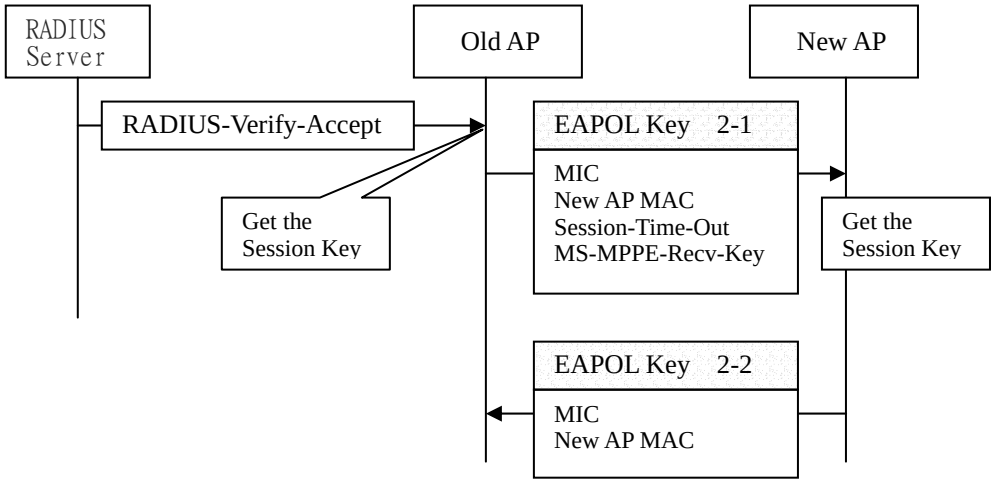


圖 4.6 Session Key 傳遞流程

1、Old AP 將 MS-MPPE-Recv-Key 與其他相關資訊(New AP MAC 與 Session Key 的有效時

間)以 Session Key 中的 KEK 加密之後，放至在 EAPOL Key 中的 Key Data 欄位。最後用 KCK 對整個 EAPOL Key 產生 MIC 值，送給 New AP。

2.New AP 收到 MS-MPPE-Recv-Key，即可用自己的 BSSID Secret 解密獲得 Session Key，並用其中的 KCK 檢查此 EAPOL Key 的 MIC 值。

3.若符合，則將 Session Key 與對應的 Old AP 的 BSSID 以及有效時間，存放在快取區。

4.回傳帶有 MIC 值的 EAPOL Key 給 Old AP。

在傳遞的過程中，封包採用 802.11i 定義的 EAPOL Key 格式(圖 4.7)，其中 Key Descriptor Version= 2 (NIST AES key wrap With HMAC-SHA1-128)，Key Type = 0 (Group Key)。另外定義 Key Information(圖 4.8)的第 13 個位元(802.11i 中的保留位元)等於 1，表示為 Session Key 的傳遞。

Descriptor Type – 1 octet	
Key Information – 2 octets	Key Length – 2 octets
Key Replay Counter – 8 octets	
Key Nonce – 32 octets	
EAPOL-Key IV – 16 octets	
Key RSC – 8 octets	
Reserved - 8 octets	
Key MIC – 16 octets	
Key Data Length – 2 octets	Key Data – n octets

圖 4.7 EAPOL Key 封包格式（資料來源:IEEE 802.11i）

B0	B2 B3	B4 B5	B6	B7	B8	B9	B10	B11	B12	B13 B15
Key Descriptor Version	Key Type	Reserved	Install	Key Ack	Key MIC	Secure	Error	Request	Encrypted Key Data	Reserved

圖 4.8 Key Information 欄位格式（資料來源:IEEE 802.11i）

4.5 PMK 的傳遞

當 AP 雙方擁有建立安全通道所需的金鑰時，即可進行 PMK 的傳遞程序，其過程說明如下(圖 4.9)

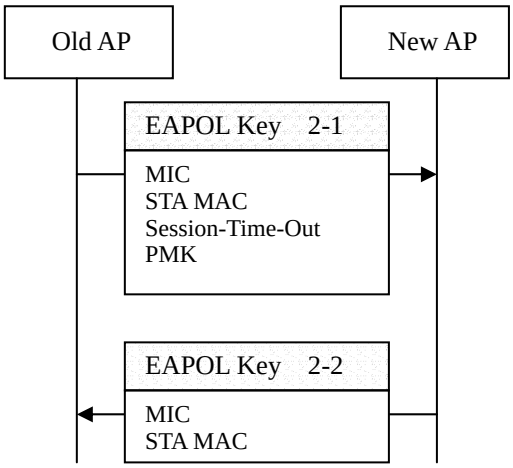


圖 4.9 PMK 傳遞流程

1．Old AP 將 PMK 與其他相關資訊(STA MAC 與 PMK 的有效時間)以 Session Key 中的 KEK 加密之後，放至在 EAPOL Key 中的 Key Data 欄位。最後用 KCK 對整個 EAPOL Key 產生 MIC 值，送給 New AP。

2．New AP 用 Session Key 中的 KCK 檢查此 EAPOL Key 的 MIC 值。

3．若符合，則用 Session Key 中的 KEK 解開 EAPOL Key 中的 Key Data 欄位，將 PMK 及對應的資訊存入快取區。

4．回傳帶有 MIC 值的 EAPOL Key 給 Old AP。

5．Old AP 回傳 EAPOL-Cache-Success (內含 New AP 的 BSSID)給 STA 之後，完成整個預先認証的過程。

在傳遞的過程中，採用 802.11i 定義的 EAPOL Key 格式(圖 4.7)，其中 Key Descriptor = 2 (NIST AES key wrap With HMAC-SHA1-128)，Key Type = 0 (Group Key)。另外設定 Key Information(圖 4.8)的第 14 個位元(802.11i 中的保留位元)等於 1，表示為 PMK 的傳遞。

第五章 實驗結果與分析

針對本論文所提出的改良方式，我們採用在 Linux 作業系統上開發的開放軟體(Open Source) Host AP[16]以及 Atheros 所提供的 Madwifi Driver[17]做為我們 AP 的開發平台; 硬體部份則搭配 Atheros 晶片的無線網卡(DWL-G650)，而 STA 部份則使用 WPA_Supplican[16]。在本章節中，我們將利用實作的方式比較快速預先認証(Fast Pre-Authentication)與 802.11i 預先認証(Pre-Authentication)所需的時間與封包傳輸的數量。

5.1 實驗說明與架構

實驗的目的在於比較完成預先認証所需的時間，因此不包含 AP 註冊的過程。此外關於查詢流程，我們利用 MeetingHouse 的 Aegis Server 作為我們實驗中的 RADIUS Server，分別以 AP1 與 AP2 的 BSSID 建立兩個使用者帳號。並設定收到來自 AP1 與 AP2 的 Access Request 時，回應 Access Response 中所需包含的屬性值(Attribute)。

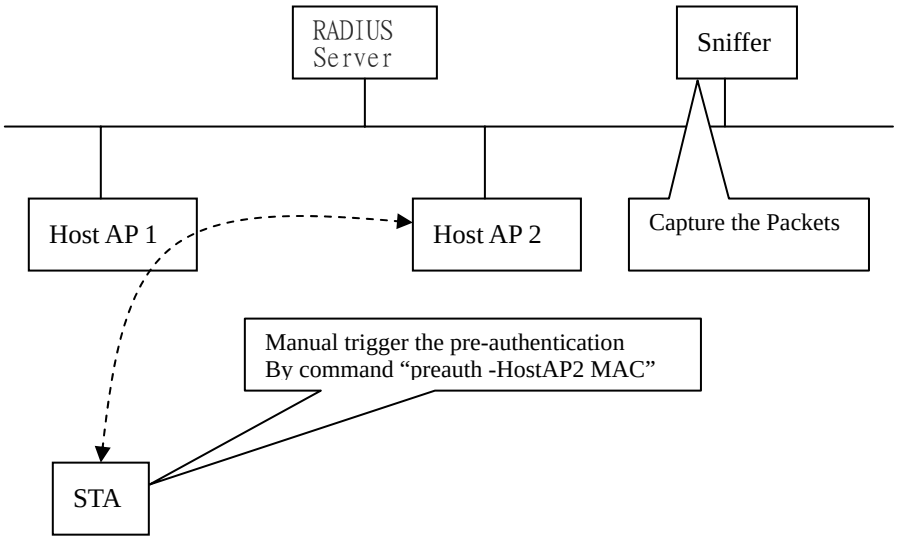


圖 5.1 實驗架構

我們利用 WPA_Supplicant 所提供的 CLI 介面(wpa_cli)，分別以手動的方式啟動對 HostAP2 的預先認証以及快速預先認証程序(preauth “HostAP2-MAC”)。所有的主機以 10M 的集線器聯接，利用 Ethereal 與 Airopeek 抓取過程中所產生的有線與無線的封包。(圖 5.1)

5.2 實驗結果

透過封包擷取軟體，我們可以獲得(表 5.1)的封包數量比較表。其中 FA 代表 IEEE 802.11i 的預先認証，FPA 代表快速預先認証，而 Caching 則表示 Session-Key 在有效的情況下。當認証伺服器收到 Access Request 時會進行相對應的處理，並回傳一個 Access Challenge，我們將這段時期視為認証伺服器所需的處理時間，經由累積整個過程中所有的處理時間得到(圖 5.2)的結果。每個過程中所發出的第一個與最後一個封包的間隔，當作完成過程所需的時間(圖 5.3)。

	有線封包(大小 bytes)	無線封包(大小 bytes)
FPA(Caching)	2 (280)	2 (128)
FPA(No Cache)	6 (944)	2 (128)
FA (PEAP)	38 (9732)	20 (4318)
FA (TLS)	30 (11615)	16 (5358)

表 5.1 快速預先認証與 802.11i 預先認証的平均封包比較表(20 次)

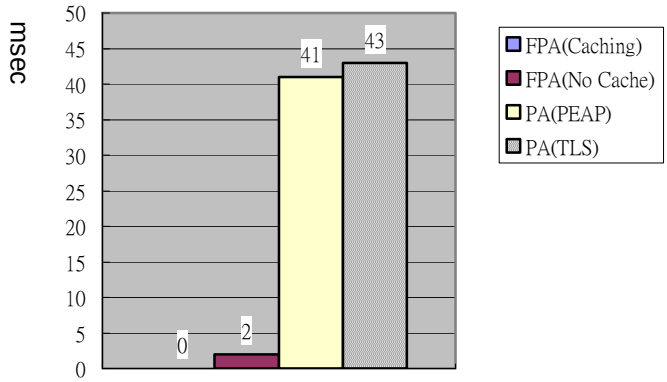


圖 5.2 RADIUS Server 處理時間比較圖(20 次平均值)

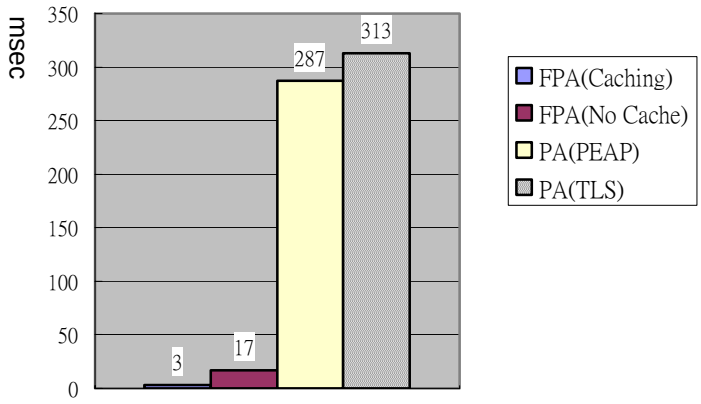


圖 5.3 預先認証完成時間比較圖(20 次平均值)

5.3 實驗分析

802.11i 所提供的使用者層級認証程序之中，STA 必需與後端的認証伺服器進行一系列的 EAP 認証封包的交換，是造成整個認証過程需要較多時間的主因。而 802.11i 的預先認証(Pre-Authentication)，除了完整的 802.1x/EAP 認証之外，更需負擔在兩個 AP 之間轉送封包所需的時間。此外我們也發現過多的無線封包交換，容易產生重傳的情況，亦是增加所需時間的原因之一。

由上面的實驗數據(表 5.1)可得知，採用 802.11i 的預先認証 EAP-PEAP 與 EAP-TLS 的認証方式，所需封包數分別為 58(14k bytes)、46(17k bytes)。而快速預先認証的方式，在 Session Key 快取與沒有快取的情況下分別為 4(0.4k bytes)、8(1.1k bytes)。實驗的結果顯示我們所提的機制，可以有效的減低額外的封包流量。

另外根據(圖 5.2)—RADIUS Server 需花費 41msec(PEAP)、43msec(TLS)來處理一個 802.11i 預先認証的要求。而快速預先認証在 Session Key 沒有快取的情況下只需

2msec，在快取的情況則完全不會使用到 RADIUS Server 任何的資源。因此採用快速預先認証的方式，可有效降低對 RADIUS Server 的依賴。換句話說，RADIUS Server 除了應付一般 802.1x/EAP 的需求外，並不需要耗用太多的資源在處理預先認証的請求。

參考(圖 5.4)，首先 STA 搜尋到 AP1 與 AP2 的訊號並與 AP1 建立連線，以速率 V 向 AP2 前進。到位置(a)時開始透過 AP1 向 AP2 進行預先認証的程序。而在到達位置(b)時開始與 AP2 進行重連的程序。在上述的過程中 STA 從(a)到(b)的時間為 T=D/V，D 為位置(a)與(b)的距離。假如預先認証所需的時間過長(大於 T)，STA 就必須與 AP2 進行完整的 802.1x/EAP 認証程序。因此我們可以發現，較快速的預先認証除了可以減少 STA 的負荷外，也比較適用於移動中的無線設備。或者可以減少 AP 之間訊號重覆的範圍，在相同數量 AP 的情況下，達到較大的覆蓋範圍。

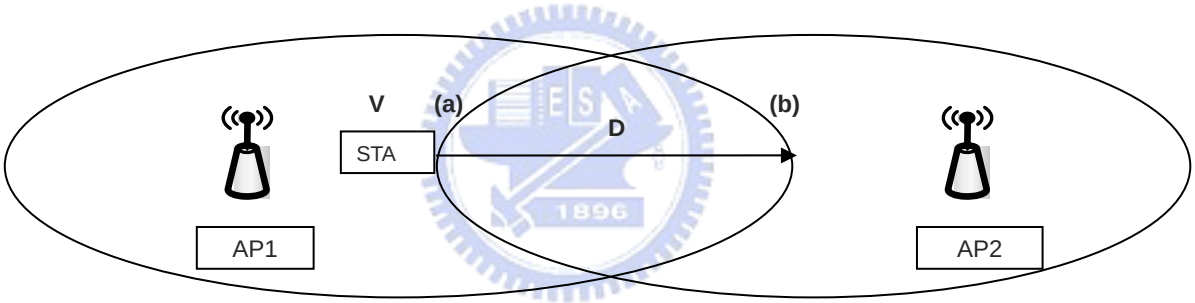


圖 5.4 STA 在兩台 AP 間的漫遊過程

第六章 結論與未來可能的研究方向

無線區域網路的優點，在於方便與較低廉的架設成本，但絕大部份的應用上還是局限在有線區域網路的延伸。主要的原因除了無線區域網路本身是設計為傳輸大量資料的技術，並不適合拿來傳送即時性要求較高的語音與多媒体之外，耗電量高、傳輸不夠安全、欠缺 QoS 機制…等等的因素，也使其難以進入其他的應用領域。然而，時至今日隨著無線區域網路相關團体與廠商的努力，新的無線標準陸續產生，例如 IEEE802.11i、802.11e，已漸漸的針對上述的議題進行排除與改進。可預期的未來，隨著無線基地台的快速佈建，無線工作站漫遊(Roaming)發生的機會勢必會更加頻繁。

而目前大部份針對重新認証所造成延遲的解決方案[1][2][3][4][11]，均利用有線端的資源以預測的方式減少重新認証所需的時間。但此類的方式對於一個漫遊發生較密集的無線環境中，過多的 overhead 勢必會影響系統的整體效能。對於無線網路服務供應商而言，無形中會額外增加所需的架設成本與管理費用。相對的，IEEE 802.11i 所提的方案則太過倚賴 Wireless STA。對於一個有限電源的移動設備而言，例如 Wi-Fi Phone、PDA，將造成能源上的浪費。

本篇論文即針對 IEEE802.11i 的缺點，提出一個改良的方式。在我們的實驗結果中，很清楚的看出快速預先認証的方式，可以很有效的減少額外的封包流量、減輕認証伺服器的負荷並以較短的時間完成整個過程。

造成 802.11 漫遊過程延遲的原因，除了重新認証過長之外，另外一個主因就是掃描過程(Probe Delay)[7]。因此在未來的研究方向，我們將以快速預先認証的架構為基礎，提出一個更完整的方法，以達到無接縫漫遊的目標。

參考文獻

[1] S. Pack and Y. Choi, “Pre-Authentication Fast Handoff in a Public Wireless LAN base on IEEE 802.1x Model”, Proceeding of IFIP TC6/WG6.8 Working Conf. on Personal Wireless Communication, pp. 175-182, Oct. 2002.

[2] S. Pack and Y. Choi, “Fast Inter-AP Handoff Using Predictive-Authetication Scheme in a Public Wireless LAN Networks”, Network 2002, joint ICN 2002 and ICWLHN 2002, pp. 15-26, Aug.2002.

[3] A. Mishra, M. Shin, and W. Arbaugh, “Context Caching Using Neighbor Graphs for Fast Handoffs in a Wireless Network”, in IEEE Infocom 2004, Mar. 2004.

[4]A. Mishra, Min Ho Shiu, N. L. Petroui, T. C. Clancy and W. A. Arbaugh, “Proactive key distribution using neighbor graphs,” Wireless Communications, IEEE Feb. 2004.

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

[6]J. Edney, W. A. Arbaugh, “Real 802.11 Security”, Addison-Wesley, July 2003.

[7] A. Mishra, M. Shin, and W. Arbaugh, “An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process”, ACM Computer Communications Review, Apr. 2003

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

[9]R. Needham and M. Schroeder. Using encryption for authentication in large networks of computers. Communications of ACM, December 1978.

[10]IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution System Supporting IEEE 802.11f, Jul. 2003.

[11]M. Kassab, A. Belghith, J. Bonnin, S. Sassi “Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks“, ACM Wireless multimedia networking and performance modeling, October 2005

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

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

[14]S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[15]W. Willats, P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

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

[17]Madwifi, Atheros Open Source Driver for Linux, http://www.madwifi.org