行政院國家科學委員會補助專題研究計畫 ■ 成 果 報 告 □期中進度報告

無線家庭網路安全認證與存取控制機制

計畫類別：■ 個別型計畫　　□ 整合型計畫
計畫編號：NSC 97－2410－H009 －041
執行期間：　97　年　08　月　01 日至　98　年　07　月　31　日
計畫主持人：羅濟群 教授
共同主持人：
計畫參與人員：　張栩嘉、何冠儒、黃世豪、呂志健、高湘婷

成果報告類型(依經費核定清單規定繳交)：■精簡報告　□完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：

中　華　民　國　98　年　07　月　31　日

目錄

無線家庭網路安全認證與存取控制機制研究

摘要

無線網路可能遭遇的攻擊和安全威脅已有許多技術報告的揭露和探討，所以無線網路是有賴加密技術與驗證機制來達成其安全性。目前無線網路在家庭的應用上越來越普及，但是許多無線家庭網路使用者仍認為安裝、設定與配置無線網路是非常繁複的，或是採用加密方式的金鑰數值太複雜、太長也增加了設定的困難。目前對於家庭網路的安全性，礙於安全設定之技術操作與密碼組合讓家庭使用者忽略家庭網路安全之重要，無形中讓家庭網路傳輸之資訊可能被有心人監聽或竄改。此外，控制家庭使用者對於網路存取的權限，亦是家庭網路管理的重要議題。由 Wi-Fi 聯盟提出的 Wi-Fi 保護設定(Wi-Fi Protected Setup)可以提供簡單設定，利用輸入 PIN 碼即可建立具備安全的無線家庭網路連線，達成無線網路安全的認證。家用使用者的存取權限將定義家用成員的身分進行連線存取控制。

故本研究將設計以無線家庭網路使用者自訂的預先共享金鑰，結合橢圓曲線金鑰交換演算法與 WPS 交握，其產生出一組安全的 WPS PIN Code 可進行具有認證與存取權限控制與無線家庭網路安全機制。

關鍵字:無線家庭網路、Wi-Fi 保護設定、橢圓曲線金鑰交換、存取權限控制

A study on authentication and access control security mechanisms of home wireless network

Abstract

Wireless network may meet the attack and with threatened had already reveal and discussion of a lot of technological reports, so the wireless network depends on the encryption to reach its security with verify the mechanism. Wireless networks are becoming increasingly popular at homes, but many home wireless network users find that installation, setup, and configuration are still very complicated. Perhaps selected the encryption method the key value is too complex、too long, also increased the setup difficulty. At present regarding the home network security, obstruct of technical operations and the password combinations to the security setup let home users neglect the home network security to be important. Imperceptibly, lets information of the home network transmission possibly monitor or modify by other person. In addition, manages the access rights of home users is also the important subject of home network management. The Solution to simple authentication of wireless network security is Wi-Fi Protected Setup (WPS).WPS makes setting up a security-enabled Wi-Fi network in the home as simple as entering a PIN or pushing a button.

Therefore this research will design an authentication and access control of home wireless network security mechanism that use Elliptic curve Diffie-Hellman (ECDH) and WPS PIN code, which will derive from to subscribe by the each home wireless network user's pre-shared key and WPS.

Keywords: Home Wireless Network、Wi-Fi Protected Setup(WPS)、ECDH、Access Control

第一章 緒論

1.1 研究背景

家庭網路安全隨著數位家庭網路服務的興起而備受重視，家庭網路可以聯繫各種不同的數位家電、娛樂裝置、PC 設備、以及電信裝置等。隨著無線網路的普及應用，提供快速且無接縫的網路架構，對家庭網路使用上而言，無線網路是簡易、不需佈線、低成本的連線選擇，達成共享網路資源與週邊設備資源。但是在部署無線家庭網路時，如何建立安全管理的無線家庭網路，當下存在著技術面與管理面的兩難。目前無線家庭網路環境的安全設定對於一般使用者來說，過於複雜或缺乏技術能力，往往令使用者無所適從，而忽略家庭網路安全的重要性。管理面而言，在加密方式上，為了確保傳輸的高安全性，會利用特殊的數值建立加密金鑰，也建議金鑰的組成越隨機越不容易被解，如果加密金鑰的數值太複雜或太長，隨機性的金鑰不易記憶，很可能使用者連線容易輸入錯誤；相對地，金鑰設定太簡單又容易破解。

然而無線家庭網路環境之設計是以無線電技術為基礎，利用空氣作為介質，與無線電波具有穿透性，這使得有心人士得以在無線電波涵蓋的範圍內進行通訊內容的竊聽。家庭網路的傳輸內容可能包含家庭成員的個人帳號與密碼等，若使用者傳送的資訊並未經加密處理，則入侵者很容易便可以擷取所有的通訊內容，並進行監控或網路監聽，再者分析網路通訊流量和內容，例如密碼分析，將造成資訊安全上一大威脅。

Windows 作業系統內建了無線網路連線精靈，已經簡化連線方式，自從家庭用戶在幾年前開始使用無線區域網路以來，當我們連線無線家庭網路時，通常必須設定/選擇無線基地台的 SSID，並且建立 WEP 或 WPA 加密方式，以避免連線時遭駭客入侵竊取機密資料等常見無線網路攻擊。以開放式系統驗證及 WEP 加密為例，無線 AP 之設定步驟:

- 無線網路名稱 (SSID)
- 啟用開放式系統驗證
- 啟用 WEP
- 選擇 WEP 金鑰格式:使用鍵盤 (ASCII) 字元鍵入 WEP 金鑰，必須為 40 位元 WEP 金鑰鍵入 5 個字元，為 104 位元 WEP 金鑰鍵入 13 個字元。如果使用十六進位數碼鍵入 WEP 金鑰，必須為 40 位元金鑰鍵入 10 個十六進位數碼，為 104 位元金鑰鍵入 26 個十六進位數碼。如果能夠選擇 WEP 金鑰的格式，請選取十六進位。
- 選取 WEP 加密金鑰數字

以採用 WPA 加密方式為例，對於 WPA 預先共用金鑰驗證及 TKIP 加密，使用者必須為無線 AP 進行下列設定:

- 無線網路名稱 (SSID)
- 啟用 WPA 與 TKIP 加密
- 啟用 WPA 預先共用金鑰驗證
- 鍵入 WPA 預先共用金鑰:WPA 預先共用金鑰必須是長度至少 20 個字元的鍵盤字

元 (大小寫字母、數字及標點) 或長度至少 24 個十六進位數碼的十六進位數碼 (數字 0-9 及字母 A-F) 組成的隨機序列。

由上述兩個操作連線AP的設定步驟可知，加密方式的安全性與金鑰的長度、隨機程度、編碼方式有很大的關連，就WEP而言，已經被證實是不安全的，有多項安全性弱點；WPA加密也在擷取到具有交握（Handshake）封包，並配合字典檔可被破解，破解的可能取決於字典檔的豐富性。因此在無線網路的設定技術中，關於One Touch的概念開始發酵，廠商企圖透過很容易的操作方式，就能協助用戶端電腦完成安全的無線網路連線。這些產品剛推出時，大多是廠商的獨家技術，因此只能透過單一品牌的無線基地台及無線網卡，才能建立這類型的安全連線。Wi-Fi聯盟也於2004年開始建立Simple Config Task Group，討論是否能建立具備安全且容易使用的無線網路連線標準，這是Wi-Fi Protected Setup標準的起源。

2007年，WPS已被發佈認證，使用WPS的接入點就可以自動產生一個網路名稱。使用者既可以透過輸入四位或八位的PIN（個人識別號碼）也可以透過按下接入點和用戶端上內建的特殊按鈕來將用戶端添加到安全網路中，此認證方法可以改善Wi-Fi認證產品用戶的產品使用能力。利用WPS達成使用者身份認證確保家用無線網路的安全，而存取控制之實現使得具有合法身份之使用者，在適當的權限控管下只能做該限制範圍下的連線與資訊存取。

因此，希望藉由本研究從無線網路之認證機制與存取控制，探討無線家庭網路的連線存取安全，以WPS使連線操作簡單化，再透過家用成員的身份建立存取控制，建立提供一個符合Wi-Fi認證與具備使用者存取權限的安全無線家庭網路。

1.2 研究目標

當前無線家庭網路環境不但多半缺乏完善的安全意識及防護措施，且有相當數量的家庭網路可能並無安全設定。Wi-Fi 聯盟希望可以透過簡化操作來保證無線區域網路的安全，發佈了 Wi-Fi 保護設定（Wi-Fi Protected Setup, WPS）規範，它可以精簡設定安全網路所需的操作步驟。

隨著家庭用戶對網路安全與資訊安全的重視，雖然有多數用戶已懂得透過設定密碼來為無線家庭網路把關，但礙於無線網路傳輸介質的特性與弱點，無線家庭網路的安全解決辦法並無法單靠簡易的金鑰就能防堵安全威脅。

本研究為設計能符合無線家庭網路環境所需認證與存取權限的安全機制，並進行相關性之研究，包括:

(1) 適用於無線家庭網路認證機制之探討

(2) 適用於無線家庭網路存取權限控制之設計

(3) Wi-Fi Protected Setup技術與加密演算法之研析

(4) 使用者預先共享金鑰與WPS進行交握推導WPA PIN Code演算法之研析與設計

(5) 無線家庭網路認證與存取權限管理安全機制分析

1.3 重要性

IEEE 802.11 無線網路可能遭遇的攻擊和安全威脅已有許多技術報告的揭露和探討，囿於無線網路傳輸介質與安全弱點，以及預設的方法已被攻擊等，突顯出無線網路廣泛使用下的便利性隱藏的安全危機，所以目前無線網路的安全性是有賴加密技術與驗證機制來達成。

故根據 IEEE 所制定的標準，一個無線網路必須提供的三項基本網路安全服務為:

(1) 使用者的身分認證 (Authentication)

(2) 資料內容的保密(Confidentiality)

(3) 資料完整性確認 (Integrity)

家庭無線區域網路市場的主要考慮因素是成本、易於使用和易於安裝，以資料為主的家庭應用絕大多數都是網際網路連線的分享，家庭網路已普遍從有線延伸至無線家庭網路，安全問題亦是在無線區網範疇內，確保無線家庭網路安全的重要性與無線區網的安全性等同視之。尤其工作者可能會將電腦帶回家用網路上網，或存取家用網路的資料帶至公司，這過程中，如果無線家庭網路沒有完善的安全設定，其 AP 可能被他人存取上網，外加資料沒有加密傳輸，可能被竊聽或攔截甚至竄改，尤其家庭網路傳輸的內容與個人的隱私相關性較高，包含身份證字號、密碼、銀行帳號等，也有可能遭受病毒或後門程式的攻擊...

這些安全威脅不僅影響家庭內部網路，更可能成為企業內部網路的隱憂，如此突顯了無線家庭網路傳輸安全認證與加密設定的重要性。

第二章 文獻探討

2.1 家庭網路

家庭網路(Home Network)的概念，IBM 等國際電腦大廠自 1998 年起已提出，最初概念是使用者可以透過伺服器管理家庭中兩台以上的個人電腦，藉由網路互相連接。微軟在 1999 年延伸推動萬用隨插即用(UPnP) 介面標準，連接的硬體平台包括所有數位化電子產品，不再囿限於個人電腦。故家庭網路透過網路的連結，平台間的互動可以用無線傳輸方式進行，不需要藉由伺服器管理。

家庭網路的組成元件，可從硬體與軟體兩方面來看，家庭網路一開始是從自動化與保全為著眼點，其後演變成為傳輸影音、視訊以及數據的媒介。家庭網路聯繫各種不同的家電、娛樂裝置、PC 設備、以及電信裝置等。總括來說，家庭網路就是語音、視訊和資料、以及相對應裝置的整合。

家庭網路與企業網路都可視為一個 LAN，但是與企業網路不同之處在於家庭網路設備成本較低、使用裝置可以連結資訊家電與電腦和周邊設備，以及簡單佈建為特點。消費者對家庭網路的需求以及家庭網路的使用者對網路的要求，與傳統的企業網路環境有相當的不同，這些要求包括:

- 易於使用，低複雜度:在家中自然沒有網路系統管理者或MIS進行網路管理，因此家庭網路必須容易安裝和連線，最好能夠不需要重佈建，讓使用者不須花時間去照料。
- 可靠度:家庭網路必須要可靠，這點和企業網路相近，網路必須能夠隔絕。
- 擴充性:當家中可連網的裝置越來越多，擴充性就成為一大考量，最好在一開始安裝時就考慮到這個問題，省得以後的投資。網路裝置不是買進來就算了，事實上，它是整個家庭網路的基礎，因此，消費者也要避免買到即將過時的科技產品。家庭網路必須兼具互通性（Interoperability），與未來的應用相容，以保障消費者的投資。
- 標準相容性:要獲得主流市場的認同，家庭網路標準是不可或缺的要素。
- 對寬頻多媒體的支援：在企業網路中所傳輸的檔案與資料型態，大多不需要很高的頻寬。反觀家庭網路，必須支援各種寬頻的多媒體內容，像是電視、DVD 播放機、數位錄影機、數位音響／MP3 播放機、DBS（俗稱的小耳朵）、平面顯示器、機頂盒等等，而PC 更是創造家庭多媒體需求的來源。支援多媒體成為家庭網路如雨後春筍般發展的關鍵。
- 成本:網路資源（如印表機、掃瞄器）分享有助於降低成本。

所以對家庭用戶而言，家用網路最主要的功能在於分享網際網路資源、週邊設備資源，以及數位影音服務等，因此在佈線、價格及安裝上，則以方便、便宜、簡單為要。目前家庭網路的介質分別朝向家庭既有之電話線、電源線及無線網路等三個方向發展，但也有廠商為求得更佳之效能而發展必須全新佈線的家庭網路系統。

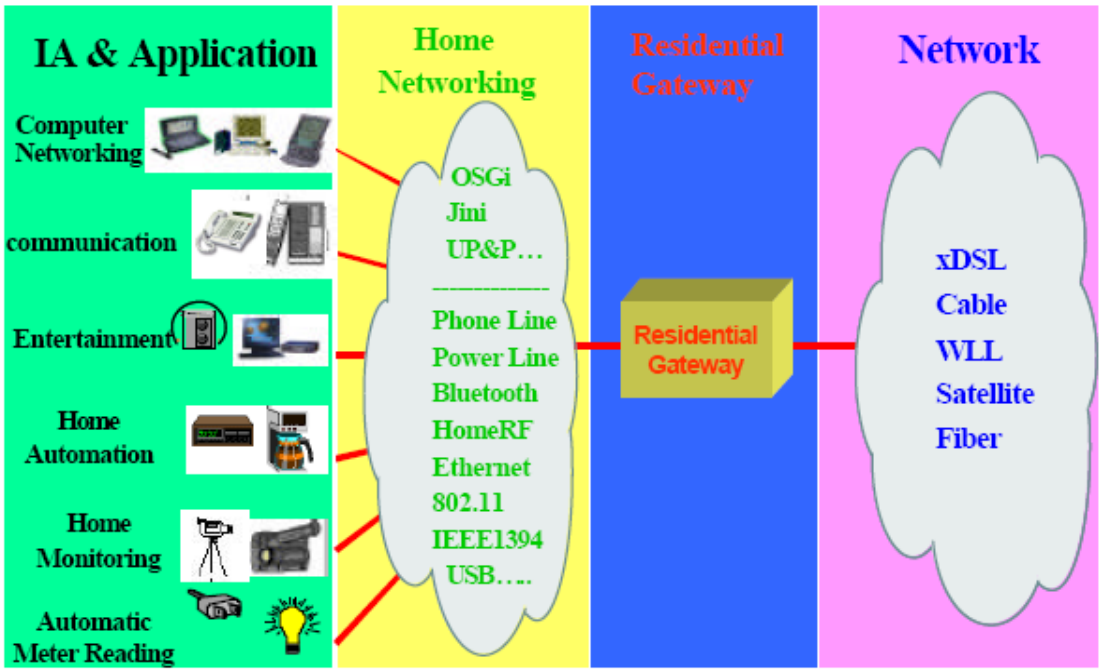

圖 1:家庭網路相關技術

家庭閘道器(Residential Gateway, RG)負責將家庭網路中不同的傳輸技術達到資訊家電產品間的溝通與分享，並全部統一集中從家庭閘道器設備對外透過各種寬頻媒介連上網際網路。如圖1，家庭網路(Home Networking)技術標準包括:網路實體層之上的OSGi(Open Service Gateway Initial)、UPnP(Universal Plug and Play)等連結家電設備標準，與Bluetooth、HomeRF、Wi-Fi等，曾一度是Wi-Fi規格最大競爭對手之一的HomeRF，在1998年成立，成員一度包括Proxim、西門子、摩托羅拉與康柏。由於Wi-Fi形勢比人強，近乎全面取代HomeRF，HomeRF無線家庭網路規格已經於2003年解散。英特爾最後宣布退出並轉向Wi-Fi也對HomeRF帶來致命一擊。

所以本研究討論的無線家庭網路技術以 Wi-Fi 之無線網路為標準，探討 IEEE 與 Wi-Fi 聯盟提出的無線安全解決方案。

2.2 無線網路安全問題

無線網路面臨的攻擊手法和有線網路其實大同小異，隨著無線網路設施的普及化，無線網路中的攻擊行動與種類隨著時間而不斷翻新，也有各種監聽探嗅工具能用來進行攻擊。這些攻擊雖然方式不同，其實掌握的仍是無線網路的幾個主要弱點。以下介紹無線網路的幾個主要弱點與可能遭受攻擊類型:

(1) 網路分析

這是無線網路攻擊的必要先行項目之一，在此階段，攻擊者很難被察覺。攻擊者為了得到此網路的相關資訊，特別是由 802.11 MAC Header 中提供的資訊，會將其節點的 Wireless NIC 設定成雜聽(Promiscuous)模式，收集網路上來往的資料封包。一般來說只需要一台移動性佳的網路節點如 Notebook 或 PDA，搭配上具備聆聽功能的無線網路介面，再加上一具簡單的指向性天線，就能夠進行網路分析。網路分析的重點在於找尋到無線網路的存在並利用 MAC Header 中紀錄的資訊進行整個網路的分析，為接下來的攻擊行動做準備。例如:從標頭中可得知此網路

是否受到 WEP 加密保護，或是此無線網路的 AP 實體位址。

(2) 被動式竊聽

與網路分析不同的是，攻擊者在此階段積極的收集網路上的 Session 資訊與其資料酬載。假使封包在沒有加密的狀況下，重要的資訊在此時就能被攻擊者完整的接收下來；若資料有進行加密，則可以讓攻擊者耗費一些時間在解密的進行上。同樣的，此類攻擊也很可以很難被察覺或掌握，利用指向性天線，攻擊者可以在無線網路有效理論距離外進行資料的竊取。被動式竊聽也可以收集到相當數量的封包資訊，這對於破解 WEP 加密有相當程度的幫助。由於 WEP 加密採用的是人工管理金鑰以及固定數量的起始向量值(IV)，在一定數量的封包中有機會能夠重複，因此給了攻擊者相當大的機會能夠破解。一但破解後將會揭露其下保護的上層 Layer 標頭資訊，如 Source IP address、Destination IP Address 等等，攻擊者將握有更多資訊來發動更進一波攻勢。

(3) 主動式竊聽

被動式竊聽因為完全不對網路發送任何資訊，所以可以幾乎不被任何人察覺。主動式竊聽則將會對網路進行一些設計過的訊息發送或是發送被修改過的封包，例如 IP Spoofing 就是主動式竊聽的利用。所謂的 IP Spoofing 主要是更改封包的標頭，讓整個攻擊封包看起來像是來自可信任的網域，而被允許進入 Router 或 防火牆(Firewall)，直接攻擊網路主機。

(4) Man-in-the-Middle(MITM)攻擊

藉由分析攻擊目標與 AP 之間的封包往來，攻擊者可以得到完整的 Session 資訊。當 Session 再度開始時，攻擊者發送干擾封包將目標與 AP 之間的 Session 中斷並阻斷其與 AP 之間的連線路徑，並將其導引到攻擊者自己的網路節點中。在此同時攻擊者開始假冒目標的身分和 AP 進行身分認證，並重新啟動 Session。此時目標將以為 Session 將繼續進行，但其實資料的交換完全透過攻擊者的機器進行處理，而攻擊者可完整得到攻擊目標與 AP 之間傳送的所有 Session 資料。為了達成目標，攻擊者必須先使用 ARP Spoofing 將原有的 IP/MAC 對映資料破壞，以故意發送 ARP Reply 的手法更新 AP 的 ARP Cache，就可能將封包和 Session 重新導向至攻擊者希望的節點當中。

(5) 綁架 Session

假設攻擊者由之前的準備工作取得了足夠的身分認證資料，可以假冒攻擊目標對 AP 進行身分確認時，攻擊者可以在目標進行 Session 時將其 Session 中斷，目標雖知 Session 已經中斷但無法察覺 Session 的控制權已遭到搶奪。此攻擊方式需要預先取得大量關於使用者的資訊，因此需要完美的竊聽、封包分析和解密工作；一但取得所有需要的資訊，攻擊者將可以利用攻擊目標的 Session 進行任何工作，損失將難以估計。攻擊者也可以採用 Replay 的攻擊方式，不中斷目標 Session 但在其 Session 結束後再進行開啟 Session 的工作，將更難以被使用者察覺有異。

(6) MAC / AP Spoofing

在IEEE 802.11b中，使用者認證較明確的是透過AP記錄每個授權用戶端的MAC address 於資料庫，只有加入Access Control List (ACL)中的MAC address才可被允許對此AP作存取及認證動作。或以SSID表示某一群無線區域網路子系統設備所共用的網域名稱，提供最基本的存取控制。攻擊者可以透過資訊監聽來簡單取得該網域的一些資訊，如SSID 或是MAC address等，利用改變自己的實體位址來加入一個無線網路，或將自己的非法AP偽裝為合法的AP，進而對此無線區

網進行一些不可預期的破壞或是竊取敏感與機密的資料。當合法的Station在不知情的情況下與非法AP 連線時，可能會導致資訊被其竊取。而非法的Station可能會對合法AP進行攻擊行為，導致其他合法使用者的連線受到影響；偽裝合法的Stations可能對合法的AP發動攻擊來破壞AP的正常運作。

(7) 破解加密金鑰

WEP 和WPA 是無線網路常用的加密機制，目前已有許多網路上的工具便透過各自加密方法的弱點來破解兩者的加密金鑰。破解原理如下:

1. WEP破解

- 暴力攻擊法(Brute Force):所謂的暴力攻擊法，指的是靠電腦的運算能力，在有限的密鑰空間內，找出使用者所選用的密鑰。
- 已知IV攻擊法(Known IV Attack):藉由特定IV 型式的封包，來反推出使用者設定的密鑰，當封包收集量愈多，找出原來使用者密鑰的可能性就愈高。此法發現RC4 用來產生密鑰的演算法有缺陷，在選用某些IV 的情況下，使用者密鑰的某部份仍會出現在最後產生的位元串流組裡，這類密鑰在密碼常上稱為弱密鑰(Weak Key)，只要收集這些並研究這些弱密鑰加密後的資訊，便可以反推出使用者密碼。這本來不是件容易的工作，但拜WEP 並未將IV 加密之賜，而是以明文傳遞的方式，使得這方法的可行性大為增加。目前網路上已有公開可取得對破解工具，例如WEPCrack、AirSnort 等。近來發生的公開攻擊事件更進一步證明了WEP 這項協定比原本各界所以為的更為脆弱且易於破解。

2. WPA破解

由於目前利用WPA-PSK還原金鑰沒有有效的統計攻擊法，所以退而求其次使用字典攻擊，也就是暴力法的一種。

- 字典攻擊法:所謂的字典攻擊法，使用字典中常見的單字、片語、數字、名字和引語去解出密碼。由於一般的使用者常會選擇短的、有意義的英文字、常用的號碼等，做為其密碼，而這些密碼，數量是有限的，因此攻擊者可以快速地反覆猜測與比對，在短時間內就有可能。破解的可能取決於字典檔的豐富性。

上攻擊手法通常是針對具有 AP 的 Infrastructure 無線網路,若無線網路不具備任何加密手法或保護使用者的身分認證機制，對於攻擊者而言將輕而易舉能進入網路取得其所需而徹底不被察覺。而即使具有完好的加密手法，也難以保證完全不可能被攻擊者所破解。因此主動式的防護與多層的資料保護手法仍是不可或缺的安全要素，能夠提早杜絕未經過授權的使用者或在其下手前使其現形，成為無線網路安全的主要目標。基本上攻擊者的攻擊模式除了完全靜默的竊聽之外，如果要實際進行具有威脅性的攻擊必定需要親自進入網路發送某些資訊，此類資訊必定不是網路的正常行為，因此網路監察者藉由對該網路一定程度的觀察還有行為的統計分析後建立網路行為模式參照表，必定可以比對出資料流中這些異常的資訊內容。

2.3 無線網路安全機制

由於無線電波的廣播特性，無線網路可能遭遇的弱點攻擊都可在欲竊聽者將其竊聽設備的接收頻率調至傳送頻率即可順利展開。而大多數的 WLAN 設備都是以 IEEE 802.11 協定為基礎的，該標準為解決 WLAN 的安全問題，提出了一系列的安全機制， IEEE 802.11 的安全相關機制分述如下:

(1) WEP(Wired Equivalent Privacy)

最初的無線安全標準是在 1997 年由 IEEE 公佈， WEP 是為了保護在無線區域網路的資料傳輸安全所設計的加解密系統，透過加密網路流量，防止未經授權的使用者讀取用戶端和基地台之間的無線資料封包。WEP 本身是屬於一種對稱式(Symmetric)的密碼系統(Crypto system)，意即用來加密及解密的密鑰是相同的。明文(Plaintext)經過密鑰加密(Encryption)之後得到密文(Ciphertext)，而密文亦使用相同密鑰來解密(Decryption)以還原得到明文。

WEP 加密的步驟如下:

1. 首先將明文經過 CRC-32(cyclic redundancy check)演算法的處理產生長 4 Bytes 的完整性檢查值(Integrity Check Value，ICV)。
2. 將明文與 ICV 合併起來。
3. 隨機選取一長度為 24 bits 的初始向量值(Initialization Vector，IV)，然後將 AP 及工作站(Station)之間共享之 40 或 104 位元的 WEP Key 合併。
4. 將 IV+WEP Key 合併起來的 64 或 128 位元資料，輸入密碼器以產生加密用的位元組串流(byte stream)。
5. 將合併過 ICV 的明文與 RC4（Rivest Cipher 4）產生的位元串流做 XOR 運算求出密文。
6. 最後將 IV 置於密文前面即為最終傳送的資料訊框(data frame)。

WEP 解密的步驟如下:

1. 將 IV 及 WEP Key 合併。
2. 將 IV+WEP Key 導入 RC4 密碼器以產生位元組串流。
3. 將位元組串流與密文做 XOR 的動作，可以得到明文 ICV。
4. 將解出的明文 CRC-32 演算法處理求得新的 ICV’。
5. 若 ICV=ICV’，則接收的資料正確；否則，即丟棄此資料訊框，並送出錯誤訊息給原來的工作站。

WEP 已被證實是不安全的，有多項安全性弱點，包括 IV 值過短、RC4(Rivest Cipher 4)演算本身的缺點、欠缺金鑰管理機制，無法提供雙向認證等。

(2) 802.1x

為解決 IEEE802.11 安全性不足的問題，因而產生了一個新的標準– IEEE 802.1x-「以連接埠為基準的網路存取控制」(Port-Based Network Access Control)，此機制是目前無線區網最常見的身分認證與密鑰管理規約。透過 802.1x 能將無法通過認證的使用者隔絕於網路之外，使其無法利用任何網路資源。802.1x 則藉由使用者輸入帳號／密碼或提供 X.509 認證，來達到『認人』的進階安全。如果有某個無線網路使用者經由 802.1x 驗證進行網路存取，在存取點上就會開啟

一個允許通訊的虛擬連接埠。如果授權不成功，就不會提供虛擬連接埠，而通訊就會受到阻擋。所以 802.1x 標準利用下列兩個特點來達到每一個連接埠的存取控制:

1. 建立邏輯連接埠:在EAPOL協定的交換過程中使用了客戶端及AP的MAC address以達到對邏輯層位址的控制。
2. 金鑰管理:客戶端在認證完成後，AP才會送出或收到包含金鑰資訊的EAPOL-Key訊息。其中不包含WEP或其他的加密演算法，它透過EAPOL-Key訊息即可讓AP 發佈加密金鑰的資訊到客戶端。這個訊息是每個session使用一次，如果有心人士想要擷取WEP金鑰，下個session後這個金鑰就沒有用了。

802.1x 驗證有三項基本要件，每一個角色須支援一致的認證方法(LEAP、MD5、TTLS、TLS 或 PEAP)，才能完成 802.1x 認證。

1. 申請者(Supplicant):請求無線網路存取權，並且需接受 Authenticator 的認證稽核，例如無線工作站。
2. 驗證者(Authenticator):要求並且接受未受信任端網路節點的認證請求的實體，例如無線存取點(AP)。
3. 驗證伺服器(Authentication Server):驗證資料庫，通常是一個 Radius 伺服器。

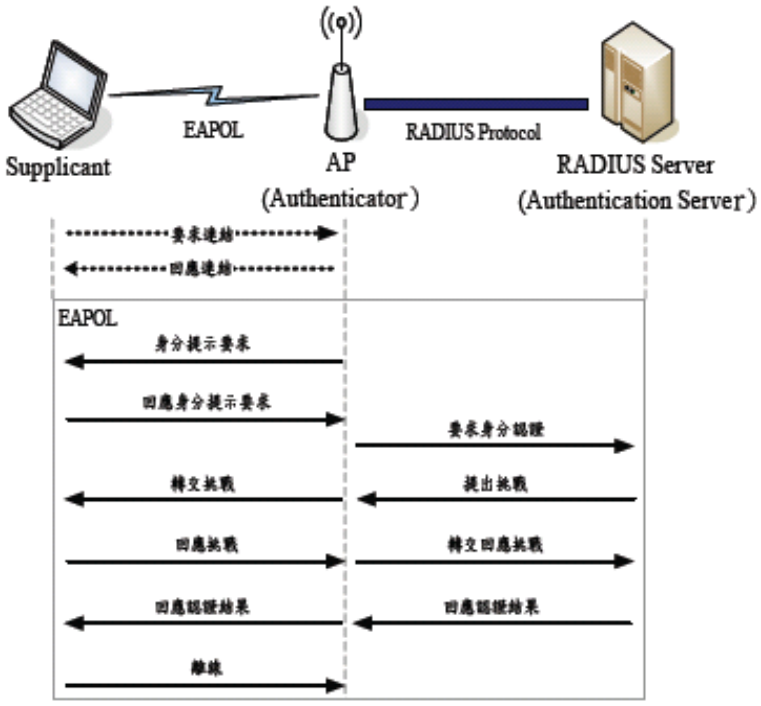

圖 2 : 802.1x 認證機制

在 IEEE 802.1x 標準所控管的網路下，如圖 2 所示，使用者必須透過 EAPOL(Extensible Authentication Protocol Over LAN)，藉由無線擷取器或無線頻寬路由器來提供使用者帳號與密碼或數位憑證(Digital Certificate)至後端 Radius Server。Radius Server 即根據這些資訊對使用者進行認證，認證通過的合法使用者方可被授權使用該無線區域網路，此外 Radius Server 亦會記錄每個使用者的登入與登出之時間資訊，作為日後計費或網路資源使用情形的監控之用。因此透過 IEEE 802.1x 協定的施行以及 Radius Server 與使用者帳號資料庫的配合使用，一般企業、ISP 乃至各無線區域網路服務提供者均可以有效管理行動使用者在該網路的存取行為。

(3) EAP(Extensible Authentication Protocol)

EAP提供一個可彈性選擇認證機制的架構。申請者 (無線工作站) 與驗證伺服器之間會使用 EAP 來傳遞驗證資訊。EAP 類型會定義及處理實際的驗證，是PPP(Point-to-Point Protocol)的延伸，主要用來在PPP 中提供額外的遠端登入可彈性選擇認證機制的架構。EAP 支援多種認證方式，常被討論的有較早的EAP-MD5 與後期的EAP-TLS、EAP-TTLS、EAP-SIM、EAP-AK。以下將介紹兩種最常見的無線區域網路的認證方式，分別是EAP-MD5及EAP-TLS兩種認證方式:

1. EAP-MD5無線網路認證機制

EAP-MD5無線安全協定其特點在於結構非常簡單，不需用到其他額外的資訊（如憑證），很容易實現，但是只有單向認證機制，僅由認證伺服器認證無線網路使用者，使用者無法認證對方，缺乏雙向互相認證（Mutual Authentication）的機制，很容易遭受中間人攻擊（Man-in-middle Attack）或是連線劫奪（Session Hijacking）的攻擊，且在認證伺服器端的共享資訊以明文儲存時，很容易成為攻擊的重點。但是一般而言，因具有容易實作的優點，而且使用者只需記住密碼就可以，不需申請憑證這種繁雜的程序，目前大部分的無線區域網路系統都會提供此一認證機制。

2. EAP-TLS無線網路認證機制

EAP-TLS為目前802.1x中以憑證為基礎的認證機制，主要在802.1x中利用目前嵌入最廣被接受的TLS（Transport Layer Security）安全協定，此標準定義在RFC 2716。因為使用憑證就結構上而言比較複雜，相對的安全度相對比較高。EAP-TLS要求認證伺服器與使用者都要有憑證，所以能夠提供雙向認證機制，讓認證伺服器與無線網路使用者再登入無線網路的認證過程中互相認證。就實務上而言，無線網路認證機制跟現有憑證，如自然人、金融等領域之憑證亦可進行整合，實現網際網路/行動網路單一簽入及交易認證之整合應用。

表 1 整理無線網路安全等級分類使用的加密與認證技術，依安全分級建議分成四級:

EAP-MD5與EAP-TLS認證機制可以分別應用至第二級與第三、第四級的安全等級。

- 第一級:無安全保護(No Security)
- 第二級:使用者認證(User authentication only)
- 第三級:雙向認證(Mutual Authentication)(between SS/MS and BS)
- 第四級:使用硬體保護的雙向認證(Mutual Authentication using hardware protection)

表 1: Wi-Fi 安全等級分類

Wi-Fi 安全等級	第一級 (Open System)	第二級 (單向認證)	第三級 (雙向認證)	第四級 (雙向認證+硬體保護)
加密技術	無	WEP	WPA/WPA2	WPA/WPA2
認證技術	無	EAP-MD5 EAP-SIM EAP-AKA	EAP-TLS EAP-TTLS EAP-PEAP	EAP-TLS EAP-TTLS EAP-PEAP

(4) 802.11i

過去企業採用無線網路時，由於 WEP Key 的內容都是固定的，為了避免惡意的入侵，網管人員必須每隔一段時間通知使用者更換加密的 WEP Key，進而降低被入侵的風險。有鑑於此，IEEE 802.11i 針對無線網路原本所具備的弱點加以補強，目前 802.11i 主要定義的加密機制可以分為 TKIP (Temporal Key Integrity Protocol，暫時密鑰集成協定) 與 AES(Advanced Encryption Standard，高級加密標準)。

TKIP 定義了加密金鑰的交換方式，並利用雜湊函數(Hashing)以擾亂金鑰的組成，提供 Per-packet Keying。在 TKIP 加密的機制下，會經過兩個階段產生之後要透過 RC4 加密的 Key，也就是說基本上 TKIP 的加密機制與 128-bits WEP Key 是一樣的，只是在於產生 Key 的方式不同，主要的差別就是 WEP Key 是把使用者輸入的 WEP Key 與 IV 值直接作為加密的 RC4 Key 值，可是對於 TKIP 而言使用者所輸入的 TKIP Key 與封包的 IV 值都只是產生最後加密所用 128 bits 的參數，而不是直接把輸入或是夾帶的 IV 值拿來加密，相對的也就提高它的安全性。更可為每一個封包不同加密的 128 bits Key 值，提供最完整的安全性。而原本用來加密的 48 bits IV 值，被分為兩個部分(32 bits 與 16 bits)，分別在階段 1 與 階段 2 的程序中參與加密 Key 的產生。

(5) WPA(Wi-Fi Protected Access)/WPA2

Wi-Fi 聯盟與 IEEE 組織為了補足現有市場上無線網路產品安全性上的不足，合作訂定了 WPA 的安全標準，並於 2002 年 10 月 31 日公佈。它是為了可以立即取代現有市面上 802.11 標準中的 WEP 加密方式，直接透過軟體或韌體昇級即可達到較高的安全等級。它不但提供了較為強化的資料加密功能，也新增了原本在 WEP 中沒有的使用者認證功能。

WPA 是 IEEE 802.11i Draft 為藍圖，基本上仍然以 RADIUS(Remote Authentication Dial-In User Service)為基礎，透過 EAP(Extended Authentication Protocol)來進行使用者的驗證，主要包含了下列機制:

1. TKIP:定義加密金鑰的交換方式，利用雜湊函數以擾亂金鑰的組成，提供 Per-packet Keying。
2. Pre-shared Key:在沒有 RADIUS 的情況下，使用者與 AP 間可透過一組預先指定的金鑰先行溝通驗證，並在之後以這組主要金鑰再行產生各使用者自己的加密金鑰，並利用 TKIP 進行更換。
3. Re-keying: AP 會透過公告(Advertise)的方式將 Global Key 通知使用者，利用 TKIP 來交換唯一的金鑰。
4. Message Integration Check:對於資料完整性的檢查，除了原本 WEP 所使用的 CRC-32 演算法，另外利用 Michael 演算法產生 8bytes 的訊息完整性檢查碼(Message Integrity Code, MIC)，以進行更周延的檢查，一方面避免無線傳輸過程中所產生的封包錯誤，另一方面也藉此避免有心人士透過竊取他人封包以 replay 的方式入侵。

WPA 使用了一個加強型的加密機制，一樣也使用 RC4 串流加密演算法來加密每個傳輸的封包，讓每個封包都提供不同的加密 Key 值，並且在傳輸前加上了 CRC 檢查。結合 802.1x 與 EAP 的認證機制及 MIC 以防止封包被偽造。WPA 有分成家用的 WPA-PSK (Pre-Shared Key)與企業用的 IEEE 802.1x Port-Based Network Access Control 版本。

2004 年 9 月 Wi-Fi 聯盟宣佈支援 WLAN 安全國際標準規格 IEEE802.11i 的安全規定 WPA2（Wi-Fi Protected Access 2）開始進行認證作業，顧名思義就是 WPA 的加強版，能夠加密流量並要求用戶在接入網路之前提交身份驗證。WPA2 要求產品支援加密演算法 AES。AES 於 2002 年 5 月被美國商務部定爲美國政府的標準密碼，它以美國政府的安全標準“FIPS 140-2”爲基準。隨著 WPA2 的亮相，美國政府以及採用 FIPS 140-2 標準的機構、企業就可以使用符合標準規格的 WLAN。WPA2 也支援 RC4，具有對 WPA 的向下相容性，能連接 WPA 支援產品及 WPA 的安全級別。但 WPA2 不相容 WPA 的前身 WEP。

WPA2 PSK（Pre-Shared Key），PSK 會同時以用戶端與存取器的密碼或識別碼（亦稱為通關密語）來確認使用者。假如用戶端的密碼符合存取器的密碼，即可存取網路。PSK 也提供 TKIP 或 AES 為各個封包的傳輸資料產出加密碼的密鑰素材。PSK 比靜態 WEP 更安全，但兩者都儲存於用戶端，一旦用戶端設備失竊，PSK 同樣會被破解。建議使用混合字母、數字與非字元符號的複雜化 PSK 通關密語。

2.4 Wi-Fi Protected Setup (WPS)

WPS (Wi-Fi Protected Setup) 這是一個 2007 年年初由 Wi-Fi 聯盟才發布的認證，目的是讓消費可以透過更簡單的方式來設定無線網路裝置，並且保證有一定的安全性。目前 WPS 允許透過 Pin Input Config (PIN)、 Push Button Config (PBC)、USB Flash Drive Config (UFD) 以及 Near Field Communication Contactless Token Config (NFC) 的方式來設定無線網路裝置。

WPS 提供容易操作的步驟外，在無線安全方面支援 WPA 及 WPA2 等加密方式，它基於 EAP(Extensible Authentication Protocol)的認證協定，SSID 及加密金鑰都是在此協定上傳輸資料，所有的資料都是先經過加密再傳送到無線網路中，參與者收到資料後，再轉換成可接收的內容，安全性較佳。

WPS 建立無線網路的連線步驟:

- WPS 會自動搜尋無線網路中，相互匹配的無線網路資料
- 使用者先在無線基地台上設定 SSID 與加密方式(WPA/WPA2)的金鑰
- 當用戶端電腦連線時，WPS 則透過 PIN 資料或 PBC 按鈕等兩種方式即可快速建立連線
- 無線基地台就會自動將 SSID 及 WPA/WPA2 加密金鑰派送給無線用戶端電腦，同時也會設定完成無線網卡的連線方式

所以 WPS 的操作步驟幾乎在無線基地台設定，用戶端電腦只需要選擇啟動連線，就能完成無線網路連線，以減少使用者在用戶端電腦的操作錯誤(例如:輸入錯誤的加密金鑰)的機率。

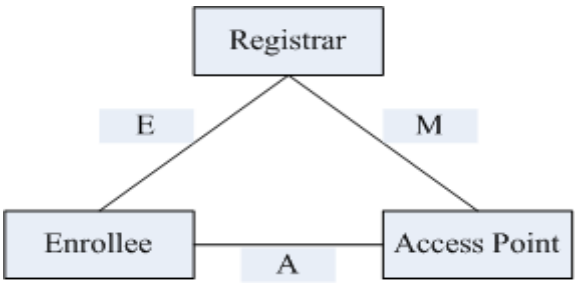

圖 3 :WPS 組成元件

在 WPS 的技術中，圖 3 為 WPS 組成元件，包括登錄者（Registrar）及參與者（Enrollee）與 AP，登錄者建立完成設定後，參與者只需要選擇連線，就會建立完成，目前一般基地台多為登錄者，用戶端則是參與者。

Enrollee → Registrar: $M_1 =$ Version || N1 || Description || PK_E

Enrollee ← Registrar: $M_2 =$ Version || N1 || N2 || Description || PK_R [|| ConfigData] || $HMAC_{AuthKey}(M_1 \| M_2^*)$

Enrollee → Registrar: $M_3 =$ Version || N2 || E-Hash1 || E-Hash2 || $HMAC_{AuthKey}(M_2 \| M_3^*)$

Enrollee ← Registrar: $M_4 =$ Version || N1 || R-Hash1 || R-Hash2 || $ENC_{KeyWrapKey}$(R-S1) || $HMAC_{AuthKey}(M_3 \| M_4^*)$

Enrollee → Registrar: $M_5 =$ Version || N2 || $ENC_{KeyWrapKey}$(E-S1) || $HMAC_{AuthKey}(M_4 \| M_5^*)$

Enrollee ← Registrar: $M_6 =$ Version || N1 || $ENC_{KeyWrapKey}$(R-S2) || $HMAC_{AuthKey}(M_5 \| M_6^*)$

Enrollee → Registrar: $M_7 =$ Version || N2|| $ENC_{KeyWrapKey}$(E-S2 [||ConfigData]) || $HMAC_{AuthKey}(M_6 \| M_7^*)$

Enrollee ← Registrar: $M_8 =$ Version || N1 || [$ENC_{KeyWrapKey}$(ConfigData)] || $HMAC_{AuthKey}(M_7 \| M_8^*)$

圖 4 : WPS registration protocol

圖 4 為 WPS 認證協定的訊息傳遞參數介紹:

- || 代表這個 Message 中還有連續的參數。
- Description 代表一般可讀性的資訊。
- PK_E and PK_R 是 Enrollee 與 Registrar 在 Diffie-Hellman 金鑰交換之公開金鑰。
- N1 為一個由 Enrollee 所產生的 128 bit 隨機數字組(Nonce 臨時亂數)。
- N2 為一個由 Registrar 所產生的 128 bit 隨機數字組(Nonce 臨時亂數)。
- $HMAC_{AuthKey}$ 代表確認器(authenticator)的欄位，其內包含一個經由 HMAC 雜湊出來的值，此金鑰雜湊函數演算法為 HMAC-SHA-256，但考慮到其長度效益，僅使用前 64bits 為確認器(authenticator)的欄位。
- E-S1 為 Enrollee 所使用的第一個秘密臨時參數(Secret Nonce)。
- E-S2 為 Enrollee 所使用的第二個秘密臨時參數(Secret Nonce)。
- R-S1 為 Registrar 所使用的第一個秘密臨時參數(Secret Nonce)。
- R-S2 為 Registrar 所使用的第二個秘密臨時參數(Secret Nonce)。
- E-Hash1 為透過 PIN code 前四 Bytes 做 HMAC，與 E-S1、PK_E 和 PK_R 做 $HMAC_{AuthKey}$ 運算所得出之值。
- E-Hash2 為透過 PIN code 後四 Bytes 做 HMAC，與 E-S2、PK_E 和 PK_R 做 $HMAC_{AuthKey}$ 運

算所得出之值。

- R-Hash1 為透過 PIN code 前四 Bytes 做 HMAC，與 R-S1、PK_E 和 PK_R 做 $HMAC_{AuthKey}$ 運算所得出之值。
- R-Hash2 為透過 PIN code 後四 Bytes 做 HMAC，與 R-S2、PK_E 和 PK_R 做 $HMAC_{AuthKey}$ 運算所得出之值。
- $ENC_{KeyWrapKey}$ 為一種使用 AES-CBC 的對稱式加密法產生一把 KeyWrapKey。

所以 Wi-Fi Protected Setup 所使用的安全演算法共包括: Diffie-Hellman 金鑰交換、1536-bit MODP group 5、SHA-256、AES-CBC 等，根據此複雜的安全程序中提供相當的安全保護。

簡言之，我們用“鎖與鑰匙”來形容 Wi-Fi Protected Setup 認證產品的配置及安全機制。該標準自動使用註冊表為即將加入網路的設備分發證書。用戶將新設備加入 WLAN 的操作可被看作是將鑰匙插入鎖的過程（即啟動配置過程並輸入 PIN 碼或按下 PBC 按鈕）。此時，Wi-Fi Protected Setup 啟動設備與註冊表之間的資訊交換進程，並由註冊表發放授權設備，加入 WLAN 的網路證書（網路名稱及安全密鑰）。隨後，新設備通過網路在不受入侵者干擾的情況下進行安全的資料通信，這就好像是在鎖中轉動鑰匙。資訊及網路證書通過擴展認證協定（EAP）在空中進行安全交換，該協議是 WPA2 使用的認證協定之一。此時系統將啟動信號交換進程，設備完成相互認證，用戶端設備即被連入網路。註冊表則通過傳輸網路名（SSID）及 WPA2 預共用密鑰（PSK）啟動安全機制，由於網路名稱及 PSK 由系統自動分發，證書交換過程幾乎不需用戶干預。 WLAN 安全設置的“鎖”就這樣被輕鬆打開了。

2.5 存取控制(Access Control)

在資訊安全領域中，存取控制包含了認證、授權以及稽核。存取控制管理的目標是要確保授權使用者對資訊的存取與防止未經授權的存取，保護網路服務，偵測未經授權的活動，與確保使用行動式電腦作業與遠距工作設施時之資訊安全。

在存取控制模式中，可以對系統進行操作的實體(人或系統)稱為 Subject，而需要被限制存取的資源稱為物件(Object)。存取控制的方法如下:

(1) 存取控制矩陣(Access Control Matrix): 當主體(Subject)發出要求存取某個檔案時，系統先會檢查主體和該檔案在存取控制矩陣中所對應的存取位置，系統會去找出其對應的權力以決定此次存取的合法性。

(2) 存取控制串列法(Access Control List, ACLs): 此方法類似存取控制矩陣方法，其是將存取控制矩陣以行的形式儲存，整個存取控制的型式如同一個個串列一般。該串列所記錄的是此物件進行存取所有主體及每個主體所擁有資訊存取權限；即每一個檔案皆能對應至一個列向量，該向量記錄著所有能存取該檔案之使用者及其存取權，是屬於資源導向的應用方式。

(3) 能力串接法(Capability Lists, CLs): 能力串列法是將存取控制矩陣以列的形式儲存，即每一個主體或使用者皆能對應至一個權利列，該列記錄著此使用者所能存取的檔案以及對於檔案的存取權，即對應一連串的物件所作的存取控制權限，該串列記錄著此主體所能存取的物件以及對於物件的存取權力

(4) 角色為基礎存取控制(Role Based Access Control):主體與權限是間接存有互動關係，透過角色來達成彼此的關聯性，角色的概念相當於企業組織的職務，代表著具有不同的工作功能。角色被定義為與特定工作有關的責任之集合，能表現特殊的職務分派(Assignment)，物件的存取授權是指定給角色，每個主體被授予可執行的存取控制工作不需要一個一個指定，只要將主體指派到某一特定角色，主體就可依所扮演的角色去執行所有該角色的所被授予權限的存取活動。

下表 2 為存取控制方法的比較:

表 2:存取控制法

	存取控制矩陣	存取控制串列法	能力串接法	RBAC
說明	二維矩陣	資源導向	使用者導向	角色為主
	主體與物件權利對映	以行式儲存	以列式儲存	主體透過角色取權限
優點	簡單	物件權限管理較容易	使用者權限管理較容易	可提供權限細部描述，權限繼承，簡化管理
缺點	控制數量很大時，管理不易	主體異動頻繁造成系統負擔	變更物件的資格權限較耗時	利用兩個資料表來維護主體-角色、角色-權限的關係
主體	人、物件	物件	人	角色
主物更新	高	高	高	低
繼承	無	無	無	有
維護成本	高	高	高	低

2.6 預先分享金鑰(Pre-Shared Key)推導演算法

WPA-PSK 或 WPA2 PSK 是特別為家庭用戶使用的加密保護方法，不需使用認證伺服器。PSK 會同時以用戶端與存取器的密碼或識別碼（亦稱為通關密語）來確認使用者。假如用戶端的密碼符合存取器的密碼，即可存取網路。PSK 也提供 TKIP 或 AES 為各個封包的傳輸資料產出加密碼的密鑰素材。PSK 比靜態 WEP 更安全，但兩者都儲存於用戶端，一旦用戶端設備失竊，PSK 同樣會被破解。建議使用混合字母、數字與非字元符號的複雜化 PSK 通關密語。若使用者選用 Pre-Shared Key 進行認證動作時，特別是 passphrase based PSK，將有可能遭受駭客利用字典攻擊法猜中 PSK。由於 PSK 為一個 256bits 的隨機數字或 8 到 63bytes 的 passphrase(通關密碼)，雖然使用者擁有自己的 PSK，但目前製造商的做法都是整個 ESS 使用同一個 PSK，和 WEP 做法一樣，一旦駭客猜中 PSK，駭客即成為 ESS 的一員，整個 ESS 即被入侵。

然而，本研究所使用之 PSK 並非網路安全性所使用之 PSK，而是由家用使用者個人設定，個人擁有之獨特 PSK，使用個人 PSK 之好處為可以將網路使用之金鑰設定為 256bits，可以強化金鑰之安全性，也不會造成使用者在登入網路時輸入密碼之記憶困難，並且透過依據個人 PSK 亦可達成存取控制機制，本研究所使用 PSK 推導 WPS PIN code 之演算法，將以雜湊與公開金

鑰交換機制為基礎，分析與討論可行之演算法設計。

WPS PIN 為一八位之數字組，前 7 個數字為隨機之數字，最後一個位數必須為符合如下公式:（定義於 WPS Spec）

```
int ComputeChecksum(unsigned long int PIN)
{
unsigned long int accum = 0;
PIN *= 10;
accum += 3 * ((PIN / 10000000) % 10);
accum += 1 * ((PIN / 1000000) % 10);
accum += 3 * ((PIN / 100000) % 10);
accum += 1 * ((PIN / 10000) % 10);
accum += 3 * ((PIN / 1000) % 10);
accum += 1 * ((PIN / 100) % 10);
accum += 3 * ((PIN / 10) % 10);
int digit = (accum % 10);
return (10 - digit) % 10;
}
```

因此，如何根據 PSK 共同推算出一個隨機的 WPS 前 7 位數字，可以透過計算 Checksum 公式來產生相同的值，本研究將採取公開金鑰交換模式、橢圓曲線密碼系統(ECC)、HMAC-SHA 等演算法推導之。

(1) Diffie-Hellman 公開金鑰交換

1976 年美國史丹福大學兩位學者 Diffie 與 Hellman 發明公開金鑰交換演算法，可用來使從未曾通信見面的雙方安全地取得共通金鑰，而這把共通金鑰可做為雙方未來資料加解密或防偽之用，為非對稱式的密碼系統。首先，每個人生成一個隨機的私有值，即 a 和 b。然後，每個人使用公共參數 p 和 g 以及它們特定私有值 a 或 b 透過一般公式 $g^n \bmod p$（其中 n 是相應的 a 或 b）來產生公共值。然後，他們交換這些公共值。最後，一個人計算 $k_{ab} = (g^b)^a \bmod p$，另一個人計算 $k_{ba} = (g^a)^b \bmod p$。當 $k_{ab} = k_{ba} = k$ 時，即是共享的秘鑰。

這一金鑰交換協定容易受到偽裝攻擊，即 A 所謂中間人（middle-person）攻擊。如果 A 和 B 正在尋求交換金鑰，則第三個人 C 可能介入每次交換。A 認為初始的公共值正在傳送到 B，但事實上，它被 C 攔截，然後向 B 傳送了一個別人的公共值，然後 B 給 A 的訊息也遭受同樣的攻擊，而 B 以為它給 A 的訊息直接送到了 A。這導致 A 與 C 就一個共享秘鑰達成協定而 B 與 C 就另一個共享秘鑰達成協定。然後，C 可以在中間攔截從 A 到 B 的訊息，然後使用 A/C 金鑰解密，修改它們，再使用 B/C 金鑰轉信到 B，B 到 A 的過程與此相反，而 A 和 B 都沒有意識到發生了什麼。

為了防止這種情況，1992 年 Diffie 和其它人一起開發了經認證的 Diffie-Hellman 金鑰協定。在這個協定中，必須使用現有的私密金鑰/公開金鑰對以及與公開金鑰元素的相關數位簽章，由數位簽章驗證交換的初始公共值。

(2) 橢圓曲線加密(Elliptic Curve Crypto, ECC)

橢圓曲線密碼系統是由Neil Koblitz和Victor Miller兩位學者分別於1985 年首先提出，大多數的橢圓曲線密碼系統是在模p 或2^n F 下運算。此密碼系統仍是存有RSA或ElGamal常見的弱點(如:同模數攻擊、低指數攻擊)。RSA 與ElGamal 系統中需要使用長度為1024 位元的模數，才能達到足夠的安全等級，而ECC 只需使用長度為160 位元的模數即可，且傳送密文或簽章所需頻寬較少，並已正式列入IEEE 1363 標準。橢圓曲線的加密通訊過程如下:

$K = kG$ (其中 K,G為$E_q(a,b)$上的點，k為小於n（n是點G的階）的整數)，點G稱為基點（base point），k（k<n，n為基點G的階）稱為私有密鑰（private key），K稱為公開密鑰（public key)。

- A選定一條橢圓曲線$E_q(a,b)$，並取橢圓曲線上一點，作為基點G。
- A選擇一個私有密鑰k，並生成公開密鑰$K = kG$ 。
- A將$E_q(a,b)$和點K，G傳給B。
- B接到資訊後，將待傳輸的明文編碼到$E_q(a,b)$上一點M（編碼方法很多），並產生一個隨機整數r（r<n）。
- B計算點$C_1 = M + rK$ ； $C_2 = rG$ 。
- B將C_1、C_2傳給A。
- A接到資訊後，計算$C_1 - kC_2$，結果就是點M。因為
  $C_1 - kC_2 = M + rK - k(rG) = M + rK - r(kG) = M$ ；
  再對點M進行解碼就可以得到明文。

在這個加密通信中，如果有一個偷窺者H，他只能看到$E_q(a,b)$、K、G、C_1、C_2 而通過K、G求k或通過C_2、G求r都是相對困難的。因此，H無法得到A、B間傳送的明文資訊。

橢圓曲線密碼系統的安全性是建立於解橢圓曲線離散對數(discrete logarithm)問題之困難度。離散對數的困難度對於網路中如果有窺視者想竊取資料，則只能取得系統公開的參數P與G以及通信過程中的兩筆資料G^{X_A} mod P與G^{X_B} mod P；如果欲從大質數P與G與 G^X mod P尋找到X是很困難的，這就是所謂的離散對數問題。例如橢圓曲線密碼系統金鑰長度為160 位元，其他著名的系統如RSA用的金鑰長度為1024 位元，二者的安全度是相等的，因此在相同的安全強度下，ECC 系統速度比RSA 系統快上數倍，同時可節約金鑰儲存空間。

(3) 單向雜湊函數(One-way Hash)

在數學上，雜湊函數是多對一的壓縮型(Compression)函數，將多項數值對應到單一的含數值，稱為雜湊值(Hash value)，常見的模餘運算 *f(x)=x mod q* 可視為定義域是正整數集合的湊函數。在密碼學應用上，雜湊函數具有「單向」的特性，表示函數值易於計算，但要從函數值反推回原來代入計算的值就非常困難。

目前常用的單向湊函數有 MD5、SHA-1 等。MD5 訊息摘要(Message Digest)演算法，其輸入是任意長度的訊息，輸出則是一個 128 位元的訊息摘要。輸入的訊息會被分成好幾個 512 位元的區段來處理。SHA1 安全雜湊(Secure Hash Algorithm)演算法以 MD4 為基礎，其輸入的訊息長度不得超過2^{64} 位元，而輸出則是一個 160 位元的訊息摘要。輸入的訊息會被分成好幾個 512 位元的區段來處理。MD5 與 SHA-1 兩者之區段長度相同，雜湊碼與串接變數長度也都是 160 位元。但一般認為 SHA1 比 MD5 更能抗拒窮舉式生日攻擊法之攻擊。

MD5 原理:

1. 填入附加位元(Padding bits):使其位元長度在取 512 的同餘之後會等餘 448，換言之，附加過後的長度會比 512 位元倍數少 64 位元。
2. 附加長度
3. 將輸入分割成 512 位元區塊
4. 初始化鏈結變數
5. 處理區塊
   - 5.1:複製鏈結變數到四個符合的變數中
   - 5.2:將目前的 512 位元分割成 16 個子區塊
   - 5.3:現在有四個回合。在每一個回合中，我們處理屬於每一個區塊的所有 16 個子區塊

SHA-1 原理:

1. 填入
2. 附加長度
3. 將輸入分割成 512 位元區塊
4. 初始化鏈結變數
5. 處理區塊
   - 5.1:複製鏈結變數 A-E 到變數 a-e 中
   - 5.2:目前的 512 位元區塊分割成 16 個子區塊，每一個包含 32 位元
   - 5.3:SHA 有四個回合，每一個回合包含 20 個步驟
   - 5.4:SHA 包含四個回合，每一個回合包含 20 個疊代，總共有 80 個疊代

第三章　無線家庭網路安全認證與存取控制機制

目前無線家庭網路環境的安全設定對於一般使用者來說，過於複雜或缺乏技術能力，往往令使用者無所適從而忽略家庭網路安全的重要性。然無線網路本身安全的弱點與潛在威脅，當前的無線家庭網路環境不但多半缺乏完善的安全意識及防護措施，且有相當數量的家庭網路可能並無安全設定，其家用 AP 甚至可能被鄰居非法存取，更不排除成為駭客攻擊他人的跳板之可能。此外，對於家庭網路的使用成員來說，雖然家庭成員人口數較簡單，但年齡層卻大有不同，如何有效的控管家庭使用者對於網路存取的權限，確保安全性與正當性，亦是家庭網路管理的重要議題。

故本研究將從金鑰管理、安全認證以及存取控制等面向，探討在無線家庭網路環境中，以簡單設定安全的無線家庭網路，結合使用者認證以及使用者存取權限控制，設計建立一個無線家庭網路安全控管之機制。

3.1 無線家庭網路認證機制

無線家庭網路之安全認證機制以經濟性和適用性考量不需建立 RADIUS Server 來進行認證。2007 年 Wi-Fi 聯盟提出的 Wi-Fi Protected Setup(WPS)可以簡化無線網路連線的設定，並支援 WPA 及 WPA2 等加密方式，基於 EAP 的認證協定建立安全的連線。其研究方法先介紹 WPS 金鑰交換的設計流程，如圖 6 為 Enrollee(客戶端)和 Registrar(AP)的認證流程。WPS 是透過 M1 到 M8 的訊息交換，重點在 Enrollee 收到 M8 之後，解密可取得 AP 的安全設定參數(ConfigData) ，建立成目前使用的無線網路設定，成為本網路之使用者。故 WPS 能使傳遞雙方使用者共同得出同一組 PIN Code 進行 WPS 認證過程，如果雙方比對所產生出的 PIN Code 是不相同的，將會在認證過程中失敗。PIN Code 的產生演算法已於文獻 2.6 介紹其安全性。

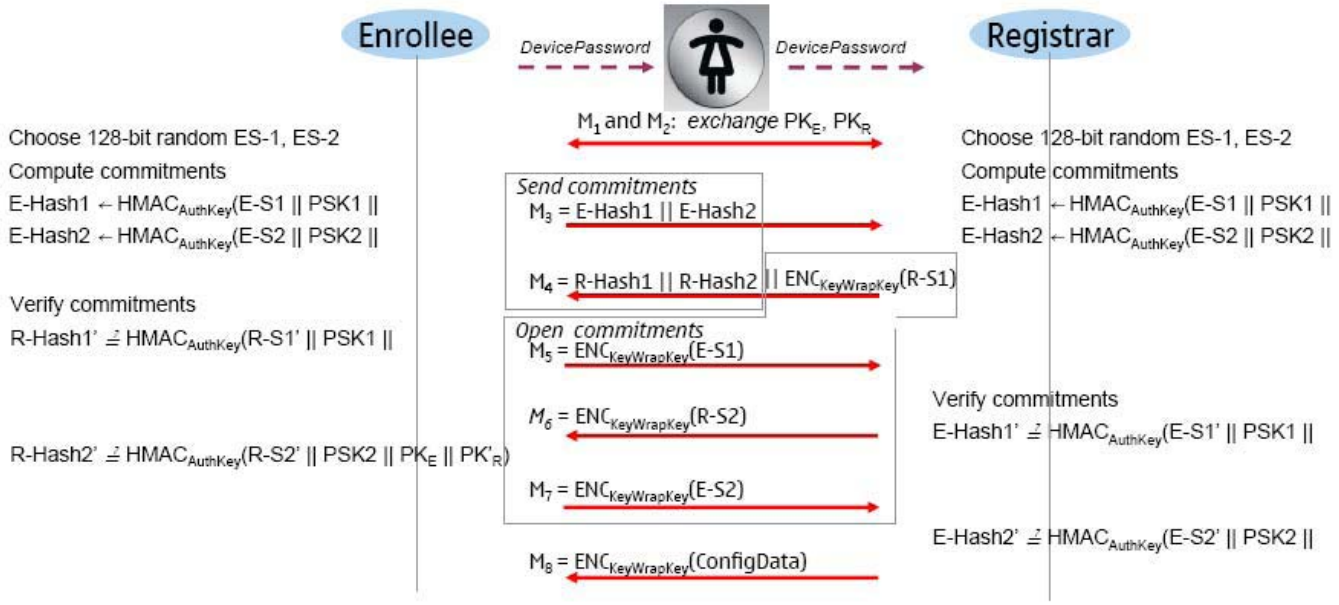

圖 6: WPS 認證協定

3.2 無線家庭網路存取控制

企業對存取控制的設計，通常根據員工所擔任的責任及職務來指派適合存取權限，企業採用角色為基礎的存取控制方式(Role-based Access Control)，可讓員工在職務角色之間易於指派，職

務、角色與權限也容易新增或刪除。存取控制方法以角色的概念與傳統群組(Group)概念不同，主要是在於群組的對象是人的集合，而角色的對象除了人的集合外，還包括了特定的權限許可、角色之間承繼的關係、職務間權責合理配置，以及個體之互動的特定條件。

本研究之家庭網路使用連線的存取控制的設計，採 RBAC 方法設定家用成員的角色，讓家庭使用者個別設定之預共享密鑰(Pre-shared Key, PSK)，建立存取權限之控制。例如:父母、青少年、訪客等；依角色定義出權責，例如:青少年的連線時間不得超過 2 小時、瀏覽的網頁有安全性過濾；而使用者與角色間的關聯則依家庭成員的身分做分派，每個人都必須設定一組自選金鑰，用來作為連線家庭網路存取之用，而訪客的角色可以預先設定一組金鑰提供訪客使用。即使家庭成員多人使用同一台 PC 無線上網，MAC address 就會相同，以個人的 PSK 進行連線也可以識別使用者的角色。因此，透過每個成員自訂的金鑰就可以識別是哪各使用者正在進行連線的服務，使用者的金鑰識別其角色，角色又可對應至設定的權限，故以此角色為基礎和自訂 PSK 可以達成本研究之無線家庭網路的存取控制。

以家庭應用為情境描述，其機制之運作過程如下:

- Super user(父母/成年人): Super user 設定屬於自己使用之 PSK，可以設定多久網路瀏覽時間需合理休息之限制，或最長上網時數等，如此完成屬於自己角色的存取權限設置。
- 青少年: 例如家中有 18 歲 15 歲與 10 歲的小孩，Super User 分別可為其定義之存取權限:10 歲小孩每天所能上網之時間只有在五點至六點，並且沒有辦法存取與暴力、色情相關網頁，甚至只能限制存取設定少數網路內容，15 歲之青少年特別限制其一天所能上網執行網路遊戲之時間為一小時，只有最多兩小時上網時間，但是對於色情與暴力內容依舊完全限制，且在十二點之後完全限制其存取網路之權限，最後 18 歲之青年，故不限制其存取時間僅對色情相關內容作部份之過濾。
- 訪客: 家庭網路如果有客人來家裡預使用網路服務，Super User 可建立一組專門提供給訪客使用的 PSK。

Super User 進行認證與進入網路之流程如下:首先輸入屬於自己的 PSK，經過在與無線基地台之驗證後，在 Association Request 封包的驗證時，無線基地台驗證所收到之 GenPIN NonceE 將可以得知目前所進行之認證角色為 Super User 接著檢查 Super User 目前是否有存取時間限制，接著檢查目前所剩餘的存取時間是否足夠接著才發給 Super User Association Response 成功，如果前面有任何支存取權限受到控制，則對 User 發出 Association Response 失敗，並且將失敗之理由填入其中，在認證成功完成連線時，存取控制機制就開始依據目前所存取之時間進行控管並且如果有設定網路相關內容之限制，存取控制機制將根據所連上線之實體位置(Mac Address)對其所有目的地為此實體位置之封包，進行內容控制，當 Super User 使用網路一小時，存取控制機制將發出斷線並且在十分鐘內不允許 Super User 重新連上網路，下依次 Super User 認證進入網路時，存取控制會先查看目前是否在權限控制情況中，如果不是材提供連線成功之封包給 Super User。

對於 15 歲之使用者進入家庭網路時，其輸入其所擁有之 PSK，在無線網路基地台認證出其

身分時，依據此使用者所能存取之權限檢查其目前所能使用之網路時間是否為結束，並且目前本機之時間是否已過午夜十二點，檢查結束之後會傳連線成功回去，當此使用者開始使用 Super User 所預先設定網路遊戲程式，存取控制機制依據其所連線之網路伺服器開始作存取時間之計算，在存取時間一小時快結束時，無線基地台將告訴本端認證軟體將存取時間將要結束，在存取時間結束後將完全阻擋來至此網路伺服器之封包，當 15 歲使用者想要存取色情相關資訊時，存取控制機制將會根據目前使用之網路實體地址對於其所要存取之封包進行過濾，會阻擋掉目的與來源位址為此實體地址內容關於非允許存取相關之內容。

3.3 PSK 推導 PIN Code 之設計流程

目前 WPS 授權機制主要的動作是由 Enrollee(客戶端)產生八碼的 PIN Code，然後 Registrar(AP) 輸入由 Enrollee 所產生之 PIN Code 進行 WPS 驗證。在家庭網路中，如何讓 Registrar 輸入 PIN Code，是需要進入無線基地台中設定，但如果每次要進入目前無線家庭網路，都需要進入無線網路基地台是很麻煩的。本研究利用橢圓曲線的 Diffie-Hellman (Elliptic Curve Diffie-Hellman, ECDH) 金鑰交換法，透過 ECDH 與 PSK 產生新的一組 PIN Code 直接進入 WPS 進行授權。透過 PSK 在無線基地台的設定，只需要定義一次使用的金鑰，並且因為 PSK 與金鑰交換之密鑰所產生之 PIN Code 為唯一，在 WPS 授權機制如果雙方所計算之 PIN Code 若不相同，將會在 WPS 授權機制過程中失敗。此外，考量 ECDH 的安全性，如果想要破解 ECDH 機制，攻擊者必須在給定 G 以及 kG 的情況下求出 k，基於橢圓曲線離散對術的困難度亦是非常困難破解地。為結合 ECDH 與 WPS 的金鑰交換設計流程的說明，並以傳遞雙方的角色設定為家庭用戶端設備與無線網路基地台 (AP/Registrar)，當無線網路基地台允許新增一個家庭用戶端進行網路連線的流程。首先我們定義了新的 WPS Data Elements 為橢圓曲線參數 Eq(a,b)之 Q、a、b，與橢圓曲線公開金鑰 EDCH Public Key。並在無線基地台所發出的 Beacon 封包增加新的 WPS Data Element，包含:ECDH Q、ECDH a、ECDH b 此三個公開的金鑰交換值，然後在 Enrollee 端(無線網卡)的 Probe Request 中加入新的 WPS IE 的 Data Element EDCH Public Key 以及 Registrar 端(無線基地台端)加入新的 WPS IE 的 Data Element EDCH Public Key，這樣可以不增加任何無線網路的封包與 WPS 行為中完成橢圓曲線金鑰交換的步驟，而且對於 Registrar 端來說可以每隔一段時間就可以簡單的更換目前所使用的任何參數，來降低透過大量的封包監聽與側錄破解雙方所使用的密鑰。此設計建立一個具 ECDH 的加密通道在 Registrar 與 Enrollee 兩端進行 User 帳號/密碼以及時戳(Timestamp)等，產生 PIN Code 的參數資訊。下圖 7 為家庭網路使用者別之 PSK 推導出可結合於 WPS 的 PIN Code 之設計流程:

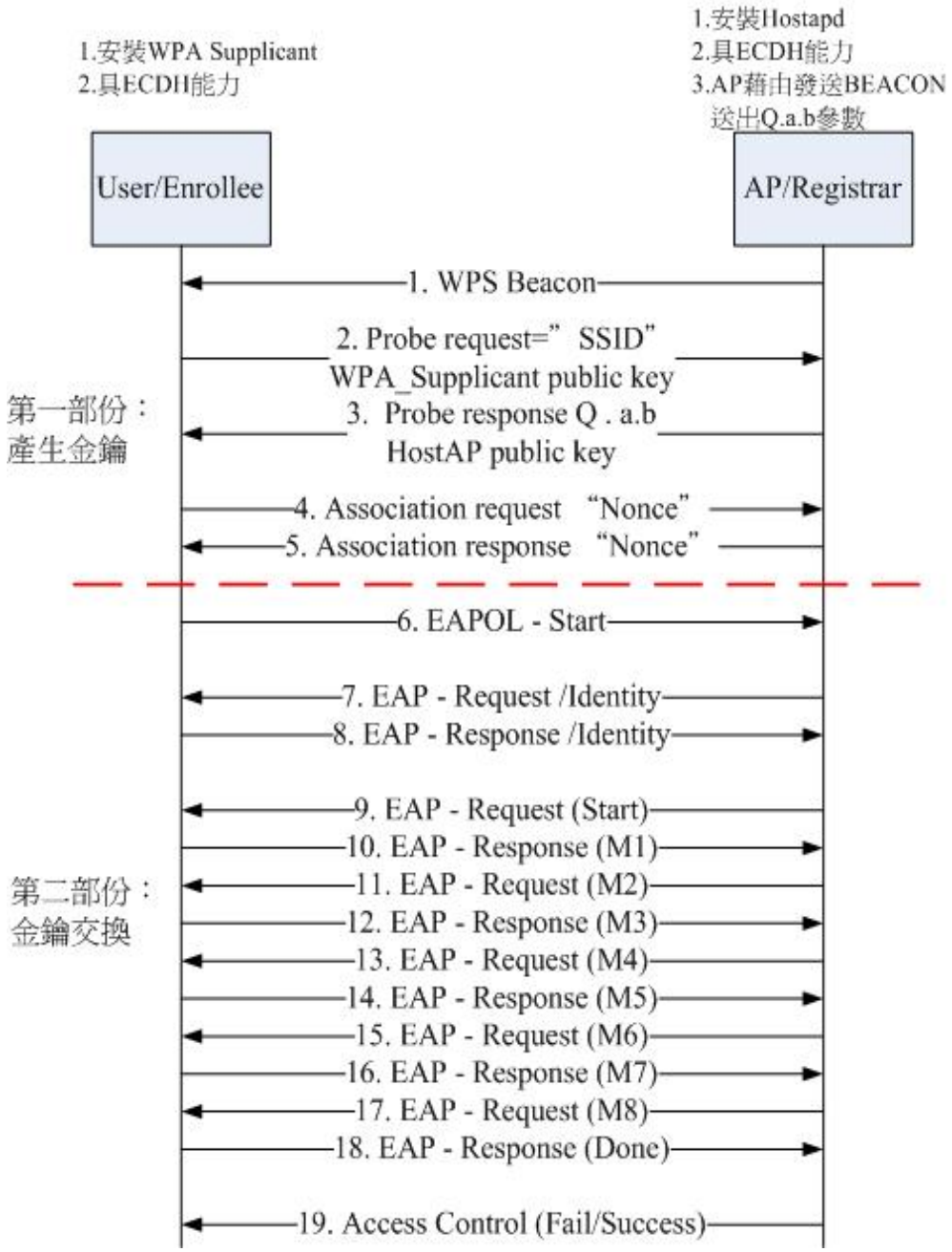

圖 7: PSK 推導 PIN Code 金鑰交換設計流程

使用者別之 PSK 推導出 PIN Code 金鑰交換流程可分為產生共同金鑰(Session Key)，與金鑰交換兩個部分。以下將依序對各連線步驟進行詳細介紹:

STEP1: 欲進 WPS 連線的 User/Enrollee 端會自動搜尋無線網路中，相互匹配的無線網路(AP/Registrar 端)的 Beacon 訊號。

STEP2～3:User/Enrollee與AP/Registrar兩端進行ECDH機制產生一把Session key，ECDH方法如下:

橢圓曲線公式: y2=x3+ax+b，其中a、b係數必須先被指定，且係數a、b 是屬於GF(P)的質數，GF為一有限體，而P是基準點相當於Diffe-Hellman的產生器。

1. 尋找雙方同意之系統橢圓曲線與基點G(橢圓上座標)作為系統公開金鑰，且所有使用者均可用相同且公開的橢圓曲線參數與基點G，G的級數n要夠大(例如大於2^{160}) 。
2. User/Enrollee 端選擇秘密金鑰正整數x，$1 < x < n$，且計算$G^x = x \bullet G$，爾後G^x送給AP。G^x為User/Enrollee秘密金鑰x對應的公開金鑰。

3. AP/Registrar端選擇祕密金鑰正整數y，$1 < y < n$，且計算$G^y = y \bullet G$，爾後將G^y送給User/Enrollee。G^y為AP的祕密金鑰y對應的公開金鑰。
4. User/Enrollee利用自己的祕密金鑰整數x與收到的G^y，計算出公式:

$$K^{AB} = x \bullet G^y = x \bullet (y \bullet G)$$

5. AP利用自己的祕密金鑰整數y與收到的G^x，計算出公式:

$$K^{AB} = y \bullet G^x = y \bullet (x \bullet G)$$

6. 雙方擁有共通的橢圓曲線點$(x \bullet y) \bullet G$。此點的x座標便可當作雙方的共通的Session Key，K^{AB}。

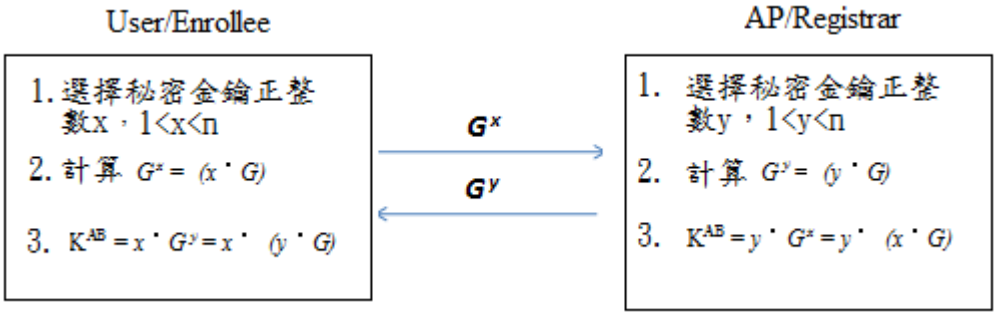

圖8: ECDH金鑰交換

STEP4：User/Enrollee端將家庭使用者之帳號與密碼進行SHA-256計算，並利用共有的Session Key加密，把結果傳給AP/Registrar端。

STEP5：AP/Registrar端將收到的Nonce用同一把Session Key解密，並與原先記錄的PSK比對，可檢視使用者的身分與權限，此步驟的Nonce產生方式如下:

1. 使用者帳號+密碼+Timestamp利用SHA-256產生出的雜湊值，Timestamp可由AP發送並以該Timestamp做為運算基準。Timestamp可用來確保每筆金鑰交換的安全性。
2. 取mod 10的結果成為PIN Code的前7碼，第8碼為檢驗碼，即組成為PIN Code。
3. User/Enrollee與AP/Registrar兩邊皆會進行PIN Code的運算，檢驗是否相同。

執行完此步驟，User/Enrollee與AP/Registrar兩端即可產生兩組相同的PIN Code以進行後續第二部份:金鑰交換的流程。

STEP6～8:此時User/Enrollee端開始準備啟動與AP/Registrar端之間的M1~M8交換過程，並由AP/Registrar端發放加入WLAN 的網路證書(網路名稱(SSID)及安全密鑰(PSK))。在此各種資訊及網路證書將通過擴展認證協定(EAP)上傳輸資料，該協議是WPA2 使用的認證協定之一。所有的資料都是先經過加密再傳送到無線網路中，User/Enrollee與AP/Registrar兩端個別收到資料後，再轉換成可接收的內容，安全性較佳。

STEP9～18:User/Enrollee與AP/Registrar兩端開始進行M1~M8的金鑰交換，兩端將完成相互認證，User/Enrollee端通過此金鑰交換流程即將被連入網路。AP/Register端則通過傳輸網路名稱(SSID)及WPA2預共用密鑰(PSK)啟動安全機制，由於網路名稱及PSK 由系統自動分發，故此M1～M8金鑰交換過程幾乎不需用戶干預，減少錯誤與麻煩。M1~M8的詳細訊息傳遞參數，請參閱文獻探討中2.4。

STEP19:當M1~M8的金鑰交換成功進行後，AP/Registrar端將會進行Access Control機制，將User帳號密碼與自身的資料庫做比對，查驗正在進行連線的使用者是否可以在這個時候使用網路。通過帳密驗證的User/Enrollee端才可以連線上網，反之AP/Registrar端將會拒絕正在要求連線的User/Enrollee端。此外，當User/Enrollee端中斷連線或是重新連線時，將重新進行STEP2~18以取得新的連線安全ECDH Session Key。

本研究所提出之產生推導的PIN Code界接使用者行為與無線網路連線的安全管理。即透過使用者自定的帳號密碼可以達成身分存取權限的控制，並結合ECDH的金鑰交換出可運行於WPS的一組PIN Code，達成無線家庭網路使用者方便、安全的連線管理。其方便性來自於，無線家庭網路使用者只需簡單記憶個人之帳號密碼資料，不必輸入長度過長的金鑰，並在WPS的協定下即擁有WPA2等級的安全性。

第四章 無線家庭網路系統設計

本章節將介紹無線家庭網路認證與存取控制的開發環境和實作步驟。

4.1 WPS 系統安裝與設定

WPS 安裝設定的系統環境需求如表 3。

表 3: WPS 環境需求

Server	Client
筆記型電腦:IBM R40	筆記型電腦:Dell Inspiron 9200
作業系統:Debian squeeze/sid	作業系統:Ubuntu 8.10
無線網卡:D-Link AirPlus DWL-G650	無線網卡:ASUS WL-167g USB WLAN Adapter
無線網卡驅動程式:Madwifi Driver v0.9.4	無線網卡驅動程式:Madwifi Driver v0.9.4
無線 AP 軟體: Hostapd-0.6.9	無線網路 client 軟體:WPA_Supplicant-0.6.9

4.1.1 Madwifi Driver 安裝與設定

進行 Madwifi 驅動程式的安裝之前，必須先準備以下的作業環境，透過 Debian 的 APT 套件管理程式，我們利用下行的指令安裝所需的作業環境。

```
# apt-get install build-essential linux-headers-$(uname -r) libssl-dev
```

接著將介面停止運作(介面不一定會被產生和啟動，所以可能沒有這些介面)。

```
# ifconfig ath0 down
# ifconfig wifi0 down
```

此外，預設的 linux 環境在安裝新的 Madwifi Driver 之前，必須先將舊的 Madwifi 模組移除，以避免版本衝突而產生錯誤,執行以下的指令即可將舊有的 Madwifi 從作業系統和記憶體中移除。

```
# cd madwifi(移動到 Madwifi 的目錄下)
# cd scripts(進入 scripts 這個目錄中)
# ./madwifi-unload(將 Madwifi 從記憶體中移除)
# ./find-madwifi-modules.sh `uname –r`(移除系統中的 Madwifi module)
```

移除舊有的 Madwifi 模組後，進行編譯和安裝的動作。

```
# make(在 madwifi 的目錄中，執行編譯動作)
# make install(執行安裝動作，程式自動會將 module、man pages 和工具複製到相關正確的目錄中)
```

另外，由於 Debian 預設包含 ath5k 這個模組，但此系統環境需要的是 ath_pci 模組，為了避免系統預先載入 ath5k，我們可將 ath5k 模組加入 modprobe 的黑名單中，避免 ath5k 被自動載入。

```
# vim /etc/modprobe.d/blacklist.conf(編輯 modprobe 的黑名單檔案)
加入 blacklist ath5k(在黑名單設定檔中加入)
```

最後，載入 ath_pci 模組即完成最基本 Madwifi driver 的安裝及驅動。

```
# modprobe ath_pci
```

載入 ath_pic 之後，在 server 機器上，系統給予無線網卡 ath0 這個網路介面名稱；在 client

機器上則給予無線網卡 wlan0 這個網路介面名稱。

4.1.2 Hostapd 安裝與設定

透過網址 http://hostap.epitest.fi/releases/ 下載最新的 hostapd 軟體版本，本研究之實作環境以 hostapd-0.6.9.tar.gz 的版本為例。

為了讓 hostapd 支援 WPS 的運作，需要設定以下的參數。

CONFIG_DRIVER_MADWIFI=y(由於網卡驅動使用 Madwifi，所以必須設定支援 Madwifi 模組)

CFLAGS += -I/usr/src/madwifi(設定路徑為 Madwifi 原始碼的目錄位置)

CONFIG_EAP=y(支援 EAP)

CONFIG_WPS=y(支援 WPS)

CONFIG_WPS_UPNP=y(支援 WPS UPNP)

設定好.config 檔的內容之後，進行編譯和安裝的動作。

```
# make
# make install
```

啟動 hostapd，執行 hostapd 時需要讀取 hostapd.conf 設定檔作為執行的組態設定，此 hostapd.conf 設定檔位在 hostapd 的原始碼目錄當中，為了讓 hostapd 符合環境的需求，因此先編輯 hostapd.conf。

```
# vim hostapd.conf
```

在 hostapd.conf 設定檔中可以看到非常多的設定選項，其中必須設定的參數如下。

interface=ath0(將網路介面設為無線網卡的介面)

driver=madwifi(驅動程式使用 madwifi)

ssid=”WPS”(AP 的 SSID)

hw_mode=g(設定作業模式 a、b、g 或 n，此處 g 表示為 IEEE 802.11g)

channel=6(channel 使用 6)

eap_server=1(將 hostapd 內建的 eap_server 啟動，如此便不需要再額外處理 EAP server)

wpa=1

wpa_passphrase=12345678

wpa_psk_file=/etc/hostapd.wpa_psk

wpa_key_mgmt=WPA-PSK

wpa_pairwise=CCMP

wps_state=2

ap_setup_locked=1

完成 hostapd.conf 的設定後，執行 hostapd，將 hostapd.conf 設定檔的位置路徑帶入。

```
# hostapd hostapd.conf
```

4.1.3 WPA_Supplicant 安裝與設定

WPA_Supplicant 為使用者端的套件，透過此網址 http://hostap.epitest.fi/releases/ 下載最新的 wpa_supplicant 軟體版本，以 wpa_supplicant-0.6.9.tar.gz 的版本為例。

複製 defconfig 為 .config 檔案，.config 檔案為 wpa_supplicant 編譯用的組態設定。

```
# cp defconfig .config
# vim .config
```

為了讓 wpa_supplicant 支援 WPS，必須打開某些設定。

CONFIG_DRIVER_MADWIFI=y (讓 wpa_supplicant 支援 madwifi)

CFLAGS += -I/usr/src/madwifi(Madwifi 原始碼的目錄位置)

CONFIG_DRIVER_WEXT=y(支援 generic Linux wireless extensions)

CONFIG_EAP=y(支援 EAP)

CONFIG_WPS=y(支援 WPS)

設定完 .config 檔案後，進行編譯和安裝的動作。

```
# make
# make install
```

完成 wpa_supplicant.conf 的設定之後，便可執行 wpa_supplicant。

```
# wpa_supplicant –i wlan0 –c wpa_supplicant.conf
```
(帶有兩個參數 i 和 c，其中 i 表示使用的網路介面，而 c 指的是 wpa_supplicant.conf 檔案位置)

利用 wpa_supplicant 掃描目前現有的無線網路。當 wpa_supplicant 啟動之後，可以利用下面這個指令掃描區域內的無線網路 AP 訊號，其中可以看到顯示具有[WPS]標誌的無線訊號代表支援 WPS。

```
# wpa_cli scan_results
```

最後將進行 WPS 連線，將 hostapd 和 wpa_supplicant 分別成功啟動後，便可進行 WPS 的連線。首先，在 wpa_supplicant 的機器上，輸入下面指令表示要開啟 WPS 的連線，wpa_supplicant 會回傳一組 pin code，並嘗試執行 WPS 連線。

```
# wpa_cli wps_pin any
```

將 wpa_supplicant 的 WPS 連線啟動並取得 pin code 後，一定時間內將 PIN Code 輸入到具有 hostapd 的機器上，便可開啟 hostapd 的連線且只允許具有相同 PIN Code 的連線請求，其指令如下所示。

```
# hostapd wps_pin any pin_code
```

步驟至此，hostapd 和 wpa_supplicant 會自動將連線完成。以上為本研究無線家庭網路之 WPS 系統環境的安裝與設定。

4.2 WPS 客戶端系統安裝

WPS 客戶端系統是以 Java 開發並使用到密碼學和 OSI Layer 2(Data-Link Layer)封包傳輸的 Open Source Library。表 4 列出實際佈署所需要的檔案。

表 4: WPS 客戶端原件

函式庫名稱	所需檔案
Bouncy Castle Crypto	bcprov-jdk16-143.jar local_policy.jar US_export_policy.jar
Jpcap	jpcap.jar

所需的函式庫安裝:

至 Bouncy Castle Crypto 網站(http://www.bouncycastle.org/latest_releases.html) 依照 JDK 的版本下載其對應的 JAR 檔案。將下載好的 JAR 檔案移動到 {JRE 安裝目錄}\lib\ext\ 中。

至 Java 官方網站下載 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files，將下載好的檔案解壓縮會得到 local_policy.jar 和 US_export_policy.jar。將這兩個 JAR 檔案移動到{JRE 安裝目錄}\lib\security\ 中。

開啟 {JRE 安裝目錄}\lib\security\java.security 檔案，並在檔案中加入 security.provider.n=org.bouncycastle.jce.provider.BouncyCastleProvider (註: n 為整數類型，代表第幾個 security provider，此數值請依自己的檔案為主)

此外，還需要 Jpcap 的安裝，為 Java 中的數據鏈路層控制函式庫。至 Jpcap 項目的網站 (http://netresearch.ics.uci.edu/kfujii/jpcap/doc/download.html)依照自己的作業系統下載檔案安裝。

4.3 WPS 客戶端操作流程

本研究之 WPS 客戶端設計提供簡易的操作介面。其無線網路連線使用的流程主要可分為以下 4 個步驟:

(1) 當使用者開啟界面，將自動掃描所有具有 WPS 協定能力的家用設定 AP。

(2) 家庭網路使用者輸入個人的帳號和密碼。

(3) WPS 客戶端會將帳號、密碼和相關參數與指定 AP 進行交握生成 PIN Code。

(4) 若雙方的 PIN Code 比對無誤，即成功連線至指定的 AP。

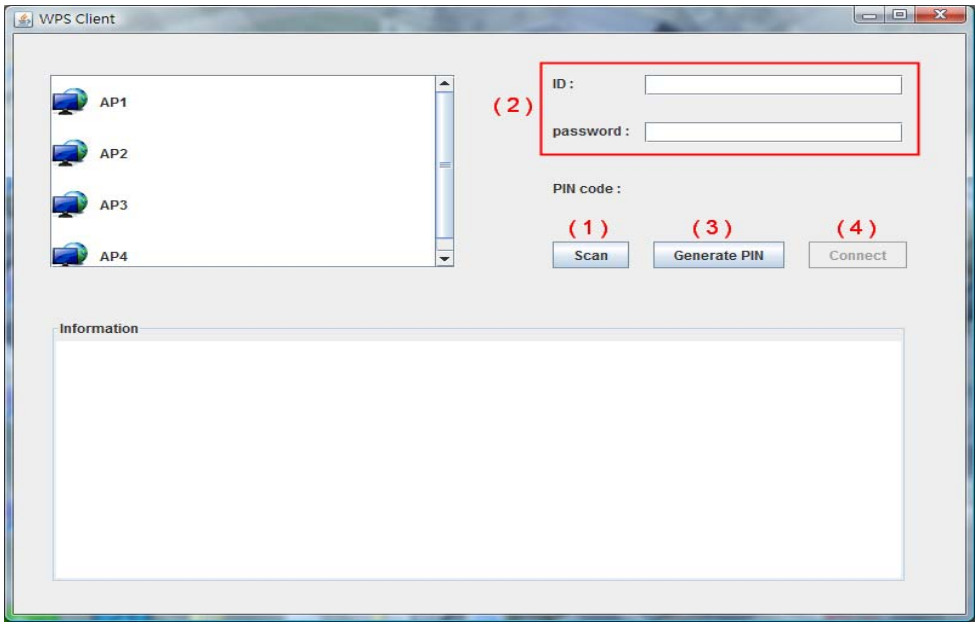

圖 9: WPS 客戶端操作介面

如上圖 9，其界面上(1)~(4)的標示與上述之無線網路連線使用的流程是相同的。

步驟(1): 按下「Scan」按鈕，程式會掃描具有 WPS 協定能力的 AP 列表於介面的左上方，點選具連線能力的一個 AP 來進行步驟(2)。

步驟(2): 於介面右上角的輸入框填寫用戶的帳號和密碼。

步驟(3): 按下「Generate PIN」按鈕，程式會把用戶的帳號和密碼以及產生 PIN Code 所需之相關參數來生成 PIN Code，並且會將新產生的 PIN Code 顯示於畫面處。如圖 10 所示，新產生的 PIN Code:40628400。

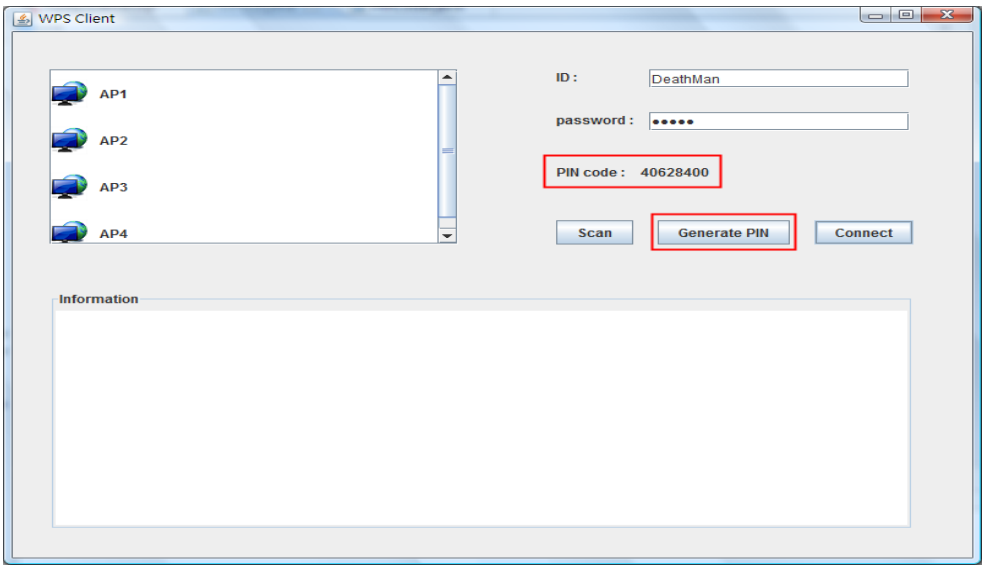

圖 10: PIN Code 產生畫面

步驟(4):按下「Connect」按鈕，連線指定的 AP。

當 PIN Code 比對產生錯誤、中斷連線或是重新連線時，使用者都將重新進行步驟(1)~步驟(4)的操作，以取得新的連線 PIN Code。介面上的 Information 將顯示連線計時或錯誤連線等訊息。

4.4 ECDH 金鑰分析

無線家庭網路認證與存取控制系統之實作，採結合 ECDH 金鑰交換演算法來推導出使用者進行 WPS 連線的 PIN Code。研究重點除了加強無線家庭網路存取的安全性外，亦進行加入 ECDH 金鑰交換演算法於認證流程中的金鑰交換時間統計。ECDH 參數表現方式是以 16 進制法表示，圖 11 為 30 筆 ECDH 金鑰產生時間的記錄，時間單位為毫秒(ms)，金鑰產生時間的最大值為 1411ms，最小值為 1162ms，平均時間為 1236 ms。就家庭無線網路連線的應用上，ECDH 金鑰產生時間的附加，並不會造成等待。因此，選擇橢圓曲線密碼系統實現家庭無線網路安全認證與存取控制之結合 WPS 協定，此安全性是依賴橢圓曲線離散對數問題，降低攻擊威脅; ECDH 的金鑰長度與 RSA、AES 加密演算法相較，也能以最少金鑰長度 512bits 達成相同的安全性等級。

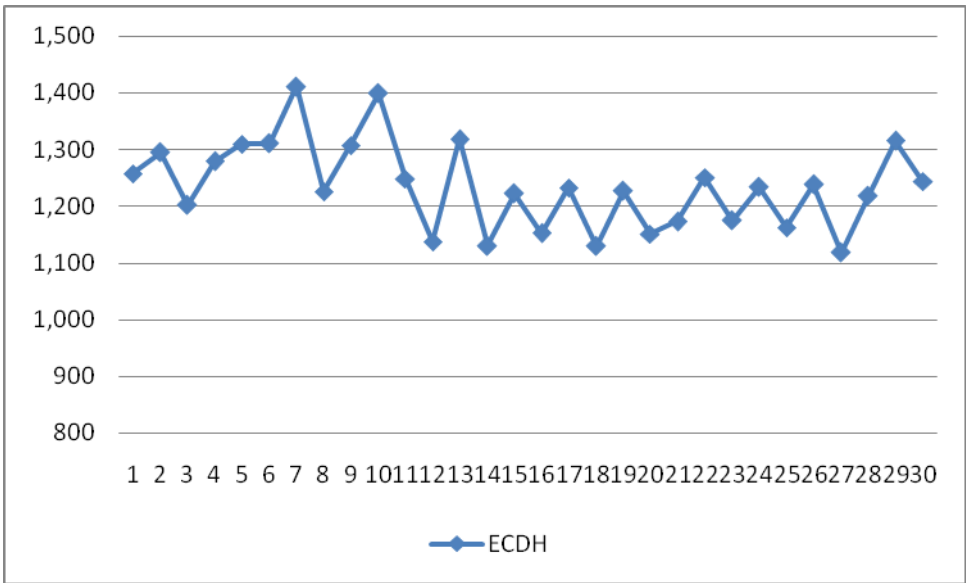

圖 11: ECDH 金鑰產生時間

第五章 結論

目前家庭網路的安全性，往往礙於安全設定之技術操作與密碼組合讓家庭使用者忽略家庭網路安全之重要，無形中讓家庭網路傳輸之資訊也可能被有心人監聽或竄改，同樣面臨無線區網弱點的攻擊。以及目前家庭網路大多不只使用一台電腦上網，還可能使用其他設備，如筆記型電腦、PDA、Xbox 遊戲機或 Voip 等數位應用服務，因此形成無線家庭網絡之連線。故一個家庭網路中的各個成員在存取無線網路時，以安全管理的角度思考是應具備有不同存取權限之限制，例如:未成年之家庭成員，可進行上網時間與網頁安全性過濾等存取限制。這樣的存取權限機制對一個家庭網路是相當有幫助的，因此本研究的貢獻為提供認證與權限管理的安全無線家庭網路之建立，以簡單設定家庭網路連線和個人設定之金鑰達成快速認證，並且根據在家庭網路的角色，獲得相對的存取權限，以一個透過 PSK 預先共享金鑰推導出的 WPS PIN Code 機制，界接使用者權限存取行為與無線網路連線的安全管理。

故本研究實作以 ECDH 金鑰交換演算法結合 PSK 與 WPS 協定，即透過使用者自定的帳號密碼生成一組 PIN Code 可運行於 WPS，達成無線家庭網路使用者方便、安全的連線管理。其方便性與安全性來自於，無線家庭網路使用者自訂之金鑰可方便個人記憶與設定，並確保此金鑰之安全性與保密性，且不必輸入長度過長的金鑰，並在 WPS 的協定下即擁有 WPA2 等級的安全性，降低無線家庭網路安全威脅之風險。

家庭網路的應用和整合議題將隨著資訊家電設備、影音娛樂等生活需求而愈顯重要，未來的研究發展可將此改良的認證 WPS 協定結合智慧型資訊家電設備的存取管理平台。

參考文獻

[1] 無線區域網路認證技術及應用研究報告，工研院電通所，CCL-9201-P104-063，2003

[2] 數位家庭之互通關鍵-UPnP 技術分析，資策會，2004

[3] 802.11 無線網路技術通論 第二版，黃裕彰 譯，O'REILLY，2005

[4] 802.11 完全剖析無線網路技術，鄭同伯 著，博碩，2004

[5] 網路安全理論與實務，葉乃菁、李順仁 著，文魁，2004

[6] 橢圓曲線金鑰加密, Available at http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm

[7] 感測網路 Elliptic Curve Diffie-Hellman 金鑰協議資料安全傳輸模式 Hyper Cube 路由通訊協定，ICIM2009，林華乙、黃俊國、蔡忠和

[8] 結合政策管理與職務角色控制機制之虛擬私有網路系統架構，資訊管理學報，第 11 卷第 2 期，羅濟群、莊秉文、邱士哲

[9] 家庭網路簡易監控機制，中國文化大學資訊管理研究所，謝文恭、黃鈞鴻

[10] Hung Lin Chou, "無線網路 WPA 安全機制剖析", Available at http://lee-1.com/hlchou/WLANWPA.htm

[11] 為居家或小型企業設定 Windows XP IEEE 802.11 無線網路. Available at http://www.microsoft.com/taiwan/technet/prodtechnol/winxppro/maintain/wifisoho.mspx

[12] Bowman Barb, "WPA Wireless Security for Home Networks," Microsoft 18 Feb, 2004. http://www.microsoft.com/windowsxp/using/networking/expert/bowman_03july28.mspx

[13] B. Ross, "Home networks: a standard perspective," IEEE Communications Magazine, Vol. 39(12), Dec. 2001, pp. 78-85.

[14] Bouncy Castle Crypto, Available at http://www.bouncycastle.org/latest_releases.html

[15] C. M. Ellison, "Home Network Security," *Interoperable Home Infrastructure*, vol. 6 (4), Intel Technology Journal, 2002.

[16] Chiu Ngo, "A Service-Oriented Wireless Home Network," Samsung Information Systems, 2004.

[17] Donald Welch, "Wireless Security Threat Taxonomy," Proceedings of the IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June, 2003.

[18] Geon-Woo Kim, Do-Woo Kim, Jun-Ho Lee et al., "Considerations on Security Model of Home

Network," ICACT, 20-22, 2006.

[19] Hostapd, Available at http://hostap.epitest.fi/hostapd/

[20] Jani Suomalainen, "Towards Fine-Grained Authorizations in Small Office and Home Networks," ICSNC, 2007.

[21] Jpcap, Available at http://netresearch.ics.uci.edu/kfujii/jpcap/doc/download.html

[22] K. Kostiainen et al. "Usable Access Control inside Home Networks," Nokia Research Center Technical Report, 2007. Available at http://research.nokia.com/tr/

[23] Laverty. Denis, "WPA vs WEP: Why is WPA better than WEP?" OpenXtra-Network Management Services Training, 2004. http://www.openxtra.co.uk/articles/wpa-vs-wep.php

[24] L. Shen, "The Key Technologies on Short Distance Wireless Network and the Research on Wireless Home Network".

[25] Madwifi driver, Available at http://madwifi-project.org/

[26] Men Long. David Durham, "Human Perceivable Authentication: An Economical Solution for Security Associations in Short-Distance Wireless Networking," 2007.

[27] M. Hottell, D. Carter, and M. Deniszczuk, "Predictors of home-based Wireless Security," *Proc. 5th Worshop on Economics of Information Security*, June 2006.

[28] N. Asokan, "Initializing Security Associations for Personal Devices," ZISC workshop on Wireless Security, September 2007.

[29] OpenSSL, Available at http://www.openssl.org/

[30] Stallings, Cryptography and Network Security-Principles and Practices, 2004.

[31] Shengbao Wang, Zhenfu Cao, Maurizio Adriano and Lihua Wang, "Cryptanalysis and Improvement of an Elliptic Curve Diffie-Hellman Key Agreement Protocol," IEEE Communications Letters, Vol.12, No.2, 2008.

[32] WiFi Protected Setup Specification, Version 1.0h, 2006.

[33] WiFi WPS Test Plan. Wi-Fi Alliance Version 1.0

[34] "Wi-Fi CERTIFIEDTM for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi® Networks," 2007.

[35] WNN Wi-Fi Net News, "Weakness in Passphrase Choice in WPA Interface," 2003.

Available at http://wifinetnews.com/archives/002452.html

[36] WPA_Supplicant, Available at http://hostap.epitest.fi/wpa_supplicant/

[37] Yun-kyung Lee, Jong-wook Han, Kyo-il Chung, “Home Device Authentication Method in Ubiquitous Environment,” IEEE, 2006.