無線區域網路安全存取管理之研究

陳彥錚 楊志彬 林志和
國立暨南國際大學 資訊管理學系
ycchen@ncnu.edu.tw

摘要

如何有效管理無線區域網路安全是架設無線區域網路首要面對的安全課題，本篇論文探討目前無線區域網路所採行的各種安全存取控制機制，並考量現有無線區域網路環境的限制，研究如何提供一個較方便又有效的安全存取管理機制。本論文提出一個結合網卡位址過濾與網路管理協定的無線區域網路安全存取管理機制，傳統單獨使用網卡位址過濾機制之無線區域網路安全，需要網管人員的介入，且會系統擴充性問題，管理不易，本論文採用後端的網卡位址認證伺服器，並結合無線基地台所支援的標準網路管理協定，設計一自動化的安全存取控制機制，此外為方便網管人員管理網卡註冊，本論文並開發一套安全存取管理系統，確保有效的網路安全管理，並減輕網管人員負擔。

關鍵字: 無線區域網路、MAC位址過濾、網路安全、網路管理。

Abstract

How to effectively perform access control in wireless local networks (WLANs) is an important issue. In this paper, a WLAN access control system is developed by using MAC address filtering and the SNMP network management protocol. There exists a scalability problem when only the MAC address filtering in WLAN access points is used for user access control. By introducing additional authentication server and using SNMP as the signaling protocol between the server and other APs, the filtering overhead of APs can be significantly reduced. To further reduce the administration burden of network managers, a management system for WLAN access control is also developed.

Keyword: Wireless local area network, MAC address filtering, network security, network management

一、簡介

採用IEEE 802.11標準之無線區域網路 [3] (Wireless LAN，以下簡稱WLAN)是近年來頗受注目的新興技術，它提供了一個寬頻的無線與行動通訊平台，越來越多致力e化的企業與組織，已漸將WLAN納為企業內部網路的一環，然而在考量採用WLAN時，最令企業感到疑慮的便是WLAN的開放性無線電波特性所帶來的安全存取問題，在WLAN的安全機制上，目前已有一些方法被提出，如SSID識別碼認證、WEP加密技術 [7]、無線網卡位址過濾、以及RADIUS [6]伺服器認證，在技術上，這些應可符合大部分企業基本的安全需求，然而從管理角度來看，這些方法在實際運作上能否讓使用者很方便地使用無線網路，而網路管理者也能有效率執行安全管理，這是一個值得探討的課題。

使用者存取WLAN的方式，主要是由筆記型電腦或PDA上的無線網卡連至無線存取基地台(Access Point，以下簡稱AP)，目前大部份WLAN AP所提供的安全機制主要有四：[2]

(A)SSID (Service Set Identifier)服務集識別碼認證：SSID可以視為某一群WLAN子系統設備所共用的網域識別碼。每個AP設有一SSID，使用者必須知道此AP之SSID值，方能以此SSID連上WLAN。

(B)WEP (Wired Equivalent Privacy)加密機制：IEEE 802.11b標準制定一個選用的加密機制，使用對稱式加/解密機制，得知加密金鑰的使用者方能據此與AP進行連結與通訊。

(C)採用後端RADIUS認證伺服器：RADIUS (Remote Authentication Dial-In User Service)為一個身份認證協定機制，原作為撥接使用者身份認證之用，使用者連上AP時，使用者必須輸入帳

號密碼，AP會向後端的 RADIUS伺服器詢問帳號密碼是否正確來決定接受或拒絕使用者存取WLAN。

(D)無線網卡位址過濾：每張使用者的無線網卡都有一個48位元的唯一識別碼，即MAC(Medium Access Control)位址，AP根據使用者的無線網卡之MAC位址決定接受或拒絕使用者存取WLAN。具有MAC位址過濾功能之AP大多提供兩種存放MAC 位址的列表方式，一種是列出允許存取的MAC 位址，另一種則是列出不允許存取的MAC位址，網管人員可視管理需要選擇其中一種方式。

以上四種WLAN安全機制在實際使用上可能遭遇的問題有所不同，本篇論文將從使用的方便性與安全管理的觀點，提出一較為可行的WLAN安全存取管理機制，此WLAN安全存取管理機制是以MAC位址過濾技術為基礎，並利用SNMP (Simple Network Management Protocol) [1]網管通信協定來提供即時安全存取控制及有效的MAC位址的管理。

SNMP是Internet網管通信協定標準，一般而言，具有TCP/IP之網路設備均會支援SNMP，網管人員可利用SNMP藉由網路從遠端存取網管資訊，此外，當網路設備發生重要網管事件，該設備也會主動發出SNMP Trap事件通報訊息至網管工作站。本論文所提之安全存取機制便是利用AP 所發出SNMP Trap，來得知一個使用者的連線資訊，再利用SNMP控制此AP接受或拒絕使用者之存取。

本論文除了提出新的MAC 位址過濾機制，並實際開發此安全存取機制，於暨南大學校園無線網路進行實驗試用。本篇論文其餘架構敘述如下，第二節將針對四種WLAN安全機制進行分析比較，第三節將描述結合MAC位址過濾與網管技術為基礎的WLAN安全存取機制，第四節介紹此WLAN安全存取機制之系統實作，最後第五節為結語。

二、WLAN安全存取機制

基本上，目前許多WLAN設備產品在安全性上均強調利用SSID與WEP這兩項功能達到企業用戶對WLAN使用者身分認證及資料傳輸之安全性的需求。但事實上，SSID充其量僅可視為一組密碼，由於SSID必須事先設定於所有使用者的無線網卡及AP中，且所有使用者均共用此組密碼，因此密碼容易洩漏出去，失去了原本使用密碼的意義，而系統管理者也無法利用不同的密碼作不同網路存取政策之控管，因此單獨以SSID作為網路的主要存取控制機制，基本上是較不安全的作法。

使用WEP的主要目的在於秘密通訊，避免遭受竊聽，其主要的功能是針對在WLAN上傳輸之資料及SSID進行加密，加密所須之金鑰，類似SSID，必須靜態地存放在所有使用者之無線網卡及AP中，所有人均共用此組金鑰，因此同樣地較易因人為因素使金鑰洩漏出去。因此，若以此金鑰作為安全存取之依據，也會有與使用SSID相同的情況，也無法因不同使用者採行不同的網路存取政策。

基本上，以上兩種方法較不適用於使用者較多的企業或組織，最近微軟公司與幾個提供WLAN設備廠商績極提出以RADIUS身份認證方式作為WLAN安全存取機制，IEEE 802.1x標準[4]也是建議採用類似的存取控制方式。使用者連上AP時，必須輸入帳號及密碼，經由AP送至後端的 RADIUS伺服器進行身份認證，RADIUS服務除了可以作為WLAN安全存取依據，也可進行計費的管理，因此對於ISP而言，此作法可促進公眾的WLAN服務之實現，使用RADIUS的作為WLAN安全存取機制，並沒有像使用SSID與WEP的缺點，不過此機制需要使用者端支援RADIUS協定，目前只有Windows XP作業本身提供此協定，因此大部份非Windows XP使用者必須額外安裝相關使用者端軟體，對於具有眾多具異質性的使用者環境，目前此方法尚無法廣泛推行。

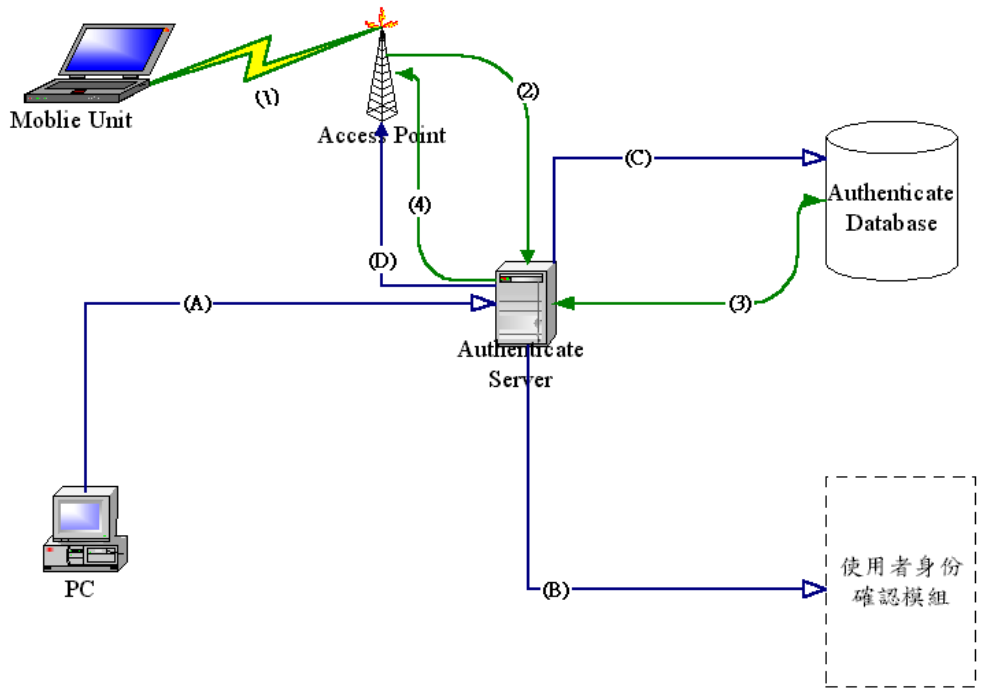
使用MAC位址過濾的WLAN安全存取機制是以使用者端的無線網卡上的MAC位址來判斷可否存取WLAN，AP可以正面表列允許存取的MAC位址，也可負面表列拒絕存取的MAC位址，一般而言，由於網管人員無法預知任一非法的使用者所使用的MAC位址，以負面表列方式似不可行，因此網管人員多會採用正面表列方式，也就是將所有合法使用者的MAC位址儲存於AP

中，此種方式會系統擴充性(scalability)問題，因為每一個AP都必須儲存一份所有使用者的MAC位址資料，由於硬體上之限制，AP針對MAC位址數目均有儲存上限，當使用者數目多時，此種正面表列方式並不可行。

三、應用SNMP網管協定之MAC位址過濾機制

在上節有關各種安全存取機制的比較分析裡，我們認為為了兼顧使用者的方便性及安全存取的要求，採用MAC位址過濾的WLAN安全存取機制是目前較可行的方式，然而如上所述，若無法解決正面表列MAC位址所帶來的系統擴充性問題，此機制的適用範圍將非常有限，若以提供廣大用戶的校園無線網路或無線區網ISP之安全存取機制為目標，單純的正面表列MAC位址過濾機制實際上是不可行。因此，為能使MAC位址過濾機制適用於大量使用者的網路環境，所有合法使用者之MAC位址勢必不能儲存於每個AP之中。

如果我們能在後端的網路選擇一台負責認證的伺服器(Authentication Server)放置這些大量MAC位址，再建立此認證伺服器與各AP的存取控制溝通管道，藉此管道確保AP具有等同的MAC位址過濾功能便可以解決上述系統擴充性問題。基於此構想，我們提出一個利用SNMP網管協定控制的MAC 位址過濾機制，在此機制中AP改採負面表列，只儲存最近拒絕的MAC位址，整個認證系統架構請參考圖一，詳細的運作步驟(對照圖一標示)描述如下：



圖一: MAC位址過濾機制系統架構圖

(1)依據IEEE 802.11標準，使用者行動裝置(Mobile Unit, MU) 欲存取WLAN時，會與AP進行建立連線(Association)步驟。

(2)AP與MU建立連線後，會自動發送SNMP Association Trap至認證伺服器，此Trap中會記錄該使用者所使用無線網卡之MAC位址。

(3)AP使用Trap中所記載之MAC位址至存放所有使用者MAC位址之資料庫進行查詢。如果MAC位址存在資料庫中，不執行任何工作，如果MAC位址不存在，則進行步驟(4)。

(4)認證伺服器立即發送SNMP Set指令至AP，增列此MAC位址至MAC位址過濾負面表列中。

以上四個步驟可以有效提供MAC位址過濾機制而沒有AP MAC位址容量限制的系統延展性問題，雖然本系統也會在非法使用者嘗試連線時使用SNMP至AP新增MAC位址資料，然而非法使用的情況不會經常發生，即使新增MAC位址時已達AP的上限，只要替換列表中任何一筆舊有資料來存放目前此筆新資料即可。剔除替換任何一筆列表中資料並不會造成安全漏洞，因為每當一個非法的MU上線時，上述四個步驟都會執行一次，原先從列表移除的MAC位址，只要再嘗試與AP連線，自然會被再次列於表中。

此種利用認證伺服器與AP的即時溝通達到存取控制的機制，可以避免所有的AP都必須連至統一的防火牆或路由器，並且無須MU端複雜的設定或其他MU端軟硬體的支援，大幅增加WLAN架設的便利性。

四、安全存取控制管理系統

為提供上述的安全存取機制，我們尚須一套有效的安全存取控制管理系統來維護所有使用者的MAC位址資料，對於使用者而言，此系統必須讓使用者很方便地註冊、修改及刪除MAC位址登錄資料，使用者註冊資料之一旦有任何異動，安全存取機制都能即時調整反應；對於網路管理者，此系統則必須能對使用者的註冊進行身分認證，此外對於合法使用者若有不當網路行為也可藉由此管理系統予以暫時斷網之措施，並可針對可疑之MAC位址進行查詢以及找出註冊該卡之使用者。

茲以下四個步驟(對照圖一標示)配合相關系統畫面來說明使用者如何進行網卡位址註冊，以及管理系統如何進行使用者身分認證工作。

(A)使用者可利用任何一台PC之Web瀏覽器連至認證伺服器，輸入帳號與密碼，如圖二所示。

圖二：系統登入畫面

(B)認證伺服器將使用者所輸入之帳號密碼至身分確認模組進行身分確認工作，若通過便可進行MAC位址註冊工作，如圖三所示。

(C)認證伺服器將使用者之網卡註冊資料更新至資料庫中。

(D)若使用者新增或變更網卡資料，認證伺服器會使用SNMP至各AP之MAC位址過濾清單，剔除原被拒絕的MAC位址，使新註冊的網卡立即生效啟用。

為使本系統之設計模組化及能配合企業或校園內部採用不同的身分認證系統，我們將步驟(B)所需之身分確認模組獨立出來，以方便更換。目前我們所採用的身分認證方式，是以使用者

之E-mail帳號來進行認證，為便於管理我們直接使用POP3 [5] 協定至POP3伺服器，不同於讀信動作，我們只執行POP3協定中之授權部分(Authorization State)，此方法可讓本系統省卻使用者

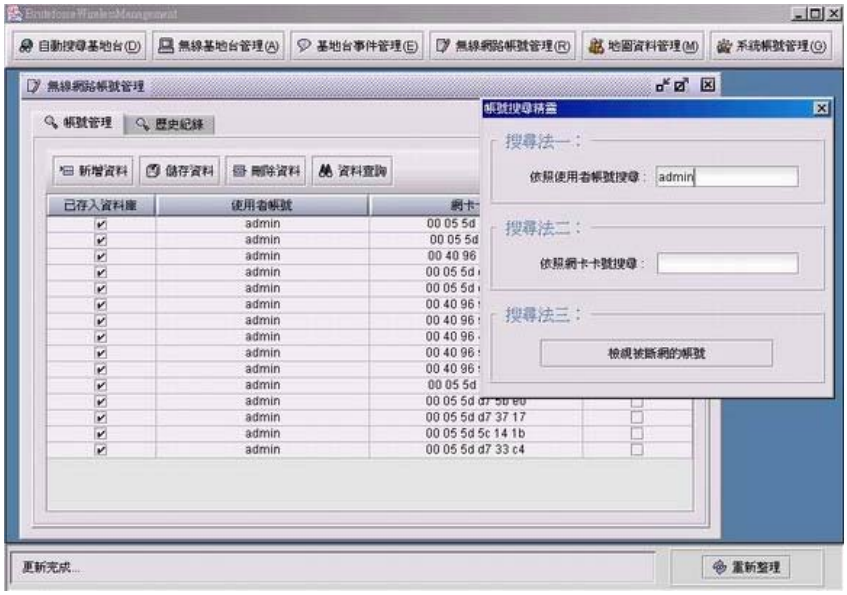
圖三：MAC位址註冊畫面

帳號管理負擔。

此外，網路管理者可利用Java-based管理系統針對不當使用WLAN之使用者進行強制斷網之措施(如圖四所示)，被斷網之網卡如同非法使用者之處理，網卡位址會在使用者再上線時列於AP的位址過濾清單中。

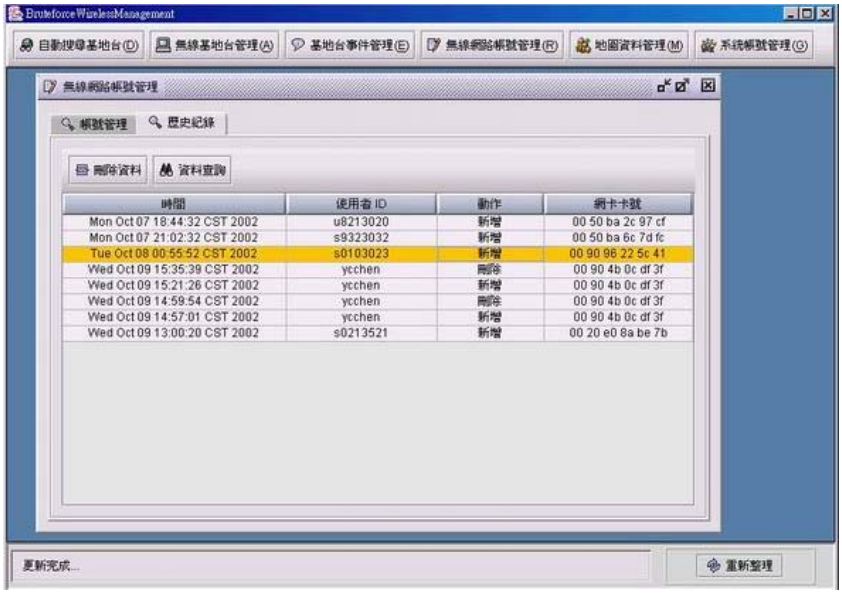
圖四：管理者操作強制斷網畫面

為方便管理者迅速找到可疑或有問題之網卡註冊資料，此管理系統提供管理者依網卡卡號、使用者帳號、及是否斷網來進行查詢(如圖五所示)。



圖五：網卡註冊資料查詢畫面

而為防止惡意的使用者藉由刪除原註冊卡號來躲避管理者追查，此管理系統會記錄使用者的任何註冊動作，並提供管理者查詢註冊歷史記錄(如圖六所示)。



圖六：註冊歷史記錄畫面

五、結語

綜合以上描述，本論文所提結合MAC位址過濾與SNMP網管技術之安全存取控制機制具有以下幾個特點：

- 採用負面表列的MAC位址過濾機制，具系統擴充性，適合大量使用者的大型企業或校園無線網路環境。

- 採用SNMP網管協定，完全自動化管理AP之存取控制設定。
- Web-Based網卡註冊管理機制，網管人員不需離線管理使用者的網卡位址。
- MU端無須任何額外繁雜的設定或其他MU端軟硬體額外支援。
- 所有AP無需架設於單一防火牆後，沒有網路架構限制，可增加網路架設的便利性。
- 提供網管人員完善的網卡管理功能，大幅減輕網管負擔。

目前WLAN的安全仍有許多漏洞，一個了解WLAN網路技術的專家要入侵或破壞WLAN安全並非難事，包括本論文所提的安全存取控制機制，駭客可以經由竊聽合法使用者的MAC位址，再更改其無線網卡卡號，便有可能偽裝成合法使用者存取網路，由於本論文之研究並非以純理論探討的方式進行WLAN安全機制研究，我們的主要考量是如何在目前現有的WLAN環境提供一個較方便又有效的安全存取控制機制。

最近WLAN的安全存取控制問題漸受到重視，IEEE正積極制定802.1x [4]標準，展望未來，使用者端的安全存取控制將藉由EAP(extensible authentication protocol)經過AP至認證伺服器(Authentication Server)，這些認證過程的通訊內容也經過加密，基本上是一個較完善的存取控制方式，在可預見的未來，支援EAP的使用者端行動裝置將越來越普遍，屆時WLAN的安全存取控制問題應可得到妥善的解決。

參考文獻

1. Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol", RFC 1157, SNMP Research, Performance Systems International, Performance Systems International, MIT Laboratory for Computer Science, May 1990.
2. DELL Computer Corporation, IEEE 802.11 Wireless security in Business Networks, DELL Vectors Technology Information Center, (2001), http://www.dell.com/us/en/biz/topics/vectors_2001-wireless_security.htm
3. IEEE Std. 802.11-1999, IEEE Standards for Local and Metropolitan Area Networks:- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
4. IEEE Std. 802.1X-2001, IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control
5. Myers, J. and M. Rose, "Post Office Protocol – Version 3", STD 53, RFC 1939, May 1996.
6. RFC 2865, "Remote Authentication Dial In User Service (RADIUS)", by C. Rigney, S. Willens, A. Rubens, W. Simpson. June 2000.
7. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html