在無線網路中對抗 MAC 位址欺騙威脅之代理人機制設計

黃一軒　　張克塵　　楊正仁
元智大學資訊工程系
{ihhuang, kcchang, czyang}@syslab.cse.yzu.edu.tw

摘要

無線網路提供便利的網路存取服務，但是惡意的使用者可以透過偽造 MAC 位址的方式來非法使用網路。在這種網路威脅中，惡意使用者不但可以自由存取網路、竊取使用者的機密，甚至可以隱藏自己的身份對遠端伺服器發起阻斷式攻擊，或是對使用者正在進行的網路連線進行綁架攻擊。在目前的存取控制協定中雖有方法可以對抗偽造 MAC 位址所產生的威脅，但是其佈建或更新的代價相當高昂。針對於此，本論文中提出了一個代理人機制來對抗 MAC 位址偽造的威脅。此機制的作法主要是利用合法下載之代理人將傳送出去的封包加密，經由存取控管伺服器之驗證與解密，才進行正常傳送流程。由於惡意使用者無法取得合法代理人，傳送出去的封包便會變成無效封包，進而對抗 MAC 位址偽造所產生的威脅。我們將此機制以 JAVA 實作在 Linux 與 Windows 上，並驗證此機制可對抗 MAC 位址偽造的威脅，未來可進一步推廣在無線網路中。

關鍵詞：存取控制，MAC 位址欺騙威脅，代理人機制，無線網路

Abstract

Wireless networks provide convenient Internet services. Unfortunately, malicious users can illegally access the network using MAC address spoofing. They may also initiate other network attacks to violate the rights of legal users. Although many approaches exist to counter MAC address spoofing threats in current access control protocols, their deployment costs are very high. In this paper, we propose an agent-based mechanism to counter MAC address spoofing threats. Because malicious users cannot get the agent, the illegal transmitted packets will be treated as invalid packets and filtered out. We have implemented this mechanism on Linux and Windows in JAVA. We also show that the mechanism can counter MAC address spoofing threats.

Keywords: access control, MAC spoofing, agent, wireless network.

1. 導論

隨著無線網路科技的進步，以及無線網路公共建設的普及，在許多公眾場合中，使用者可以經由筆記型電腦、PDA，或者是手機來連上 Internet。很多公共場合，例如熱門景點，學校以及公司行號等處，相繼提供無線網路存取的服務。然而也隨著無線網路環境的普及，無線網路的安全性成為近年來一項非常重要的議題。

在現行的公眾無線網路系統中，當使用者要使用公眾無線網路時，通常必須先經過一個存取控制協定的認證，才能存取網路服務。首先使用者必須先向提供服務的機構申請一組帳號與密碼，而後使用這些認證的資訊向認證伺服器或是存取點（access point）進行認證。如果通過認證，使用者便可以合法使用公眾無線網路。然而由於無線電波在空氣中是採取廣播的方式進行資訊傳送，電波在傳遞的時候很容易被惡意使用者竊聽及擷取，因此無線網路很容易被入侵。

在這些入侵行為中，以偽造合法無線網路卡位址，也就是 MAC（media access control）位址，的攻擊（MAC address spoofing）最為嚴重。由於 MAC 位址無法在傳輸的封包中隱藏起來，因此入侵者非常容易經由監聽取得 MAC 位址。又因為更改無線網路卡的 MAC 位址十分容易，因此當惡意使用者將本身 MAC 位址改成已經通過認證 MAC 位址時，惡意使用者可以自由地存取無線網路，此時使用者的權益可能受到損害。不僅如此，惡意使用者更可以偽裝成合法使用者，竊取他們的機密資訊。惡意使用者也可以使用偽造 MAC 位址的方式來隱藏自己和達成阻斷式服務（denial of service）攻擊。因此 MAC 位址欺騙是一項嚴重安全威脅。

根據我們的瞭解，目前已經有一些無線網路存取控制機制可以對抗偽造 MAC 位址。例如在 IEEE 802.11 中訂定的 WEP 金鑰加密機制 [1]，或者是結合 IEEE 802.1x 標準及 AES 加密演算法的 IEEE 802.11i [1] 標準都可以對抗 MAC 位址欺騙。然而，這些現行的無線網路存取控制機制若不是不適用於公眾無線網路環境就是因為需要大幅更新網路基礎設施而需要高昂的佈建成本。因此，提出一個可以不大幅更新現有無線網路環境，而又能夠有效對抗 MAC 位址偽造威脅的機制是有立即需要的，而代理人機制正有上述這兩項特點。

在本論文中，我們基於代理人的架構，提出了一個新的存取控制協定來對抗 MAC 偽造的問題。此機制的主要設計概念在於既然 MAC 位址無法在現行無線網路環境中加密以避免被偽造，不如將資料封包透過代理人來完成加密，如此一來惡意使用

者雖然可以偽造 MAC 位址，但所傳送出去的資料成為無效封包，降低安全上的威脅。同時，因為使用代理人的機制，在認證的過程中即被下載，因此無需更動作業系統或是 AP，只需更新認證時所使用之存取閘道器（access gateway，AG），更新的代價可大幅降低。因此我們提出的代理人機制有下列三項優點：1.能夠有效對抗 MAC 位址偽造所產生的威脅。在本論文中，我們將分析此代理人機制的防護性。 2.更新的代價成本較低。此代理人機制不需要更動很多無線網路的基礎設施，只需要更動存取閘道器之功能。所以相較而言，所提出的代理人機制不會花費過高的更新代價成本。 3.不僅適用於私人無線網路，也適用於公眾無線網路。此代理人是在使用者認證成功後自動下載，不需要事前先行散佈，因此沒有 WEP 金鑰在公眾無線網路中容易被惡意使用者知道的問題。此代理人機制可有效運作在公眾無線網路中。

在接下來的章節裡，第二章將進行文獻回顧，討論許多存取控制的相關研究。第三章則是詳細描述所提出的代理人存取控制機制，並且針對不同網路攻擊方式，分析代理人機制的防護性。第四章則分析代理人機制的實作效能表現，透過兩個實驗，可以供作未來實際佈建此機制之依據。最後，第五章是本研究論文的結論。

2. 相關研究

2.1 WEP

在 IEEE 802.11 中提供了一項 WEP 金鑰認證方式 [1] 來對使用者資料進行加密保護。它的全名是 wired equivalent privacy algorithm 或翻譯為「有線等效保密」演算法。在實際運作上，使用者需要先拿到 AP 所認可的金鑰才能存取網路。它的認證方式是先由要求認證者送出 authentication frame，使用者會用 WEP 演算法算出一個盤問全文（challenge text），傳回給 AP，經由 AP 解密後，來辨別該使用者是否可以合法使用無線網路。

在對抗 MAC 位址欺騙上，由於一個無線網路系統只能設定一組 WEP 金鑰，在付費公眾無線網路中，其防護的效果將大打折扣。只要原因是為了讓許多人可以使用此付費公眾無線網路，我們必須大量散佈 WEP 金鑰，導致難以保證 WEP 金鑰不為惡意使用者所獲知。如果惡意使用者獲知 WEP 金鑰，惡意使用者可以根據金鑰來推算傳輸封包的內文。因此，在公眾無線網路中，不常看到使用 WEP 的方式來進行網路使用權的認證。此外，WEP 的加密演算法不夠繁複，容易被破解，這也是 WEP 機制的一大問題 [4]。

2.2 IEEE 802.11i 及 IEEE 802.1x 標準

IEEE 在 2001 年提出的 IEEE 802.1x 標準提供了以埠號為基礎的存取控制機制，並且在 2004 年更進一步制定了 IEEE 802.11i 標準 [1]。在 IEEE 802.11i 標準中結合了 802.1x 標準及 AES 加密演算法（WPA2 模式），提供給網路使用者安全的存取控制機制。

在 IEEE 802.11i 中先利用 IEEE 802.1x 的認證機制，向遠端的認證伺服器執行認證，並交換一組 session key，而後認證伺服器便會轉交剛剛交換的 session key 給 AP，並且設定 AP 開放客戶端的存取網路的權限。當 AP 拿到 session key 之後便會利用 four-way handshaking 與客戶端交換一組暫時的金鑰，之後 AP 與客戶端的溝通便是透過這組暫時金鑰並且利用 AES 加密演算法將封包加密傳輸。

在 IEEE 802.11i 中有 WPA（wireless protected access）及 WPA2 兩種模式供使用者選擇使用。在 WPA 模式中採用了以 WEP 加密演算法為基礎的 TKIP （temporal key integrity protocol）加密演算法，而 WPA2 採用以 AES 加密演算法為基礎的 CCMP（counter-mode/cipher block chaining message authentication code protocol）加密演算法。

在 IEEE 802.11i 的設計中，MAC 位址偽造的問題能夠有效的被防範，同時也能夠防範對遠端的阻斷式攻擊以及綁架攻擊，但是目前在無線網路中大多 AP 的軟體都沒有支援 WPA 及 WPA2 模式。因此如果要使用 IEEE 802.11i 標準，便要更新這些 AP 及相關軟體。所以使用 IEEE 802.11i，所造成的更新代價，例如人力或是金錢，都勢必相當可觀。

2.3 Stanford Protocol

Faria 與 Cheriton 兩人在 2002 年提出 Stanford Protocol [2]來進行存取控制。Stanford Protocol 有兩個重要的協定: SIAP(secure internet access protocol）及 SLAP（secure link Access Protocol）。在 Stanford Protocol 中，SIAP 架構在 UDP 之上的 session 層，SLAP 則是在 link 層以及 IP 層之間。SIAP 主要的功能是提供認證及交換金鑰。當客戶端經由 SIAP 協定取得金鑰後，它會將金鑰傳遞給 SLAP。當客戶端與 AP 之間進行資料傳輸時，SLAP 會將 IP header 以及其 payload 利用金鑰加密。加密後計算封包的驗證碼加入 MAC 框架之中。AP 或客戶端可以利用驗證碼來檢查封包的正確性。由於必須要有相關金鑰才能解開封包，因此 AP 以及客戶端都可以比對封包中彼此的 MAC 位址及 IP 位址，來驗證封包的正確性。

由於 Stanford Protocol 可以驗證 AP 以及客戶端彼此封包的正確性，並且此協定中使用了 AES 加密演算法加密，因此能夠有效的防範 MAC 位址偽造所造成的威脅並且防範對遠端的阻斷式攻擊以及綁架攻擊。但是由於 AP 及客戶端的網路通訊協定必須加入 Stanford Protocol 而加以修改，因此

要佈建 Stanford Protocol 安全網路環境，需要更新相關的網路設備，以及系統軟體，更新的成本也相當可觀。

2.4 Lancaster Protocol

Lancaster Protocol [5] 是運作在Lancaster 城市的公眾無線網路通訊協定。在該計畫中，Lancaster Protocol 修改了系統軟體的protocol stack 來達到存取控制及封包過濾的效果。當使用者向認證伺服器認證通過後，認證伺服器會發送一組隨機產生的access token 給使用者，並且也會發送一份存取控制表（access control list，ACL）及session key 給路由器。該存取控制表中紀錄了使用者的access token 、IP 位址以及MAC 位址以供路由器過濾封包使用。當客戶端傳輸封包的時候，則需要將access token 與封包中的檢查碼一起用session key 加密，當路由器收到封包時，則會解開封包內加密的部份，檢查access token、MAC 位址及IP位址是否符合，若符合則容許通過路由器。

由於Lancaster Protocol在封包內部使用了access token與封包檢查碼一起加密的方式，因此若檢查碼不符合則將封包丟棄，路由器便可以透過此一方式來過濾封包。所以Lancaster Protocol能夠有效的防範MAC位址偽造所帶來的問題，以及防範阻斷式攻擊和綁架攻擊。但是由於此協定對於封包本身的payload並沒有加密，因此封包的資料仍有可能會被竊取。

2.5 Radio Frequency Fingerprinting

在對抗 MAC 位址欺騙的研究中，除了建造能夠阻擋惡意使用者封包的平台外，透過辨識封包究竟來自合法使用者或非法使用者也是可行的方法。Hall 等人 [3] 便發現每一個無線設備都有其獨特的無線電頻率指紋（radio frequency fingerprinting，RFF），透過辨識封包的 RFF 可確認發送者的身分。透過這種方式，當使用者認證通過後，AP 即會紀錄使用者的 MAC 位址以及其 RFF，每次當使用者發送訊息時，就可搜尋資料庫中的資料，來決定該封包是否為合法封包，進行傳送工作。

透過這種方法，MAC 位址偽造的問題能夠有效的被防範，並且可以防範阻斷式攻擊以及綁架攻擊。但在使用者這種方法的時候，AP 端與伺服器端必須要先建立 RFF 與 MAC 位址對應的資料庫，這使得 RFF 機制在實際運用上並不容易普及。同時，要對這些資料庫進行維護，在公眾無線網路環境中，更有其實際運作上的困難。另外由於封包本身的 payload 沒有被加密，因此資料的內容仍然容易被竊取。這些問題使得 RFF 機制的實用性大為降低。

3. 代理人存取控制機制

3.1 存取控制執行流程

在公眾無線網路環境中，當使用者希望連上無線網路時，需要先通過認證。在公眾無線網路的認證程序中，通常由兩個網路設備來負責認證工作。一個是認證伺服器（authentication server，AS），它主要的工作是認證使用者的帳號與密碼。另一個則是存取閘道器（AG），負責 DHCP（dynamic host configuration protocol）協定中的動態 IP 指派，以及傳送代理人給客戶端（mobile host，MH），並與代理人一起協力完成加解密的工作。整個認證的程序，可以分成三個階段：

1. 取得 IP 並通過認證。客戶端透過 DHCP 協定取得一組動態 IP 後，便會經由存取閘道器而被導入到一個認證網頁跟認證伺服器認證。其中使用 HTTPS 傳輸協定來保護使用者的帳號密碼，使認證過程不易被破解。如果認證伺服器通過認證，便會透過認證伺服器進行代理人下載的工作。

2. 下載代理人。通過認證後使用者便可以下載代理人，透過 HTTPS 傳輸協定下載代理人可以確保代理人不被惡意使用者竄改。

3. 合法使用網路。當代理人下載之後，透過自動啟動的方式，合法使用者便可以進行無線網路存取工作。在存取無線網路時，為考慮不同的安全性要求以及效能表現，一共有四種加密存取模式可以選擇。我們依其安全性的等級及上行/下行串流的方式加以區別為：Level 0，Level 1U，Level 1D，及 Level 2。這四種模式將在下節中介紹。

3.2 代理人機制及管理方式

當代理人安裝在客戶端後，所有客戶端向外傳送或由外接收的封包，都將被代理人監控。代理人在監控的過程中，會依照不同安全模式的需求，分別對上行串流（up stream），或下行串流（down stream）的封包加密，藉以達成對抗 MAC 藉以達成對抗 MAC 位址偽造所造成的威脅。

3.2.1 加密模式

客戶端上的代理人會對上行串流或下行串流進行加密。因此它的加密模式分為下列四種:

1. Level 0

在此等級中，代理人完全不加密，無線網路的操作如同一般沒有加密機制的無線網路操作模式。因此在這個等級中，無法對抗 MAC 位址偽造的威脅。

2. Level 1U

在這個等級中，代理人會對上行串流中的封包做單方向的加密，對下行串流的封包則不做任何處理。這些加密過後的封包，在經由存取閘道器時，便會由存取閘道器解密向外傳送，如圖 3.1(a)所示。

由於在此模式下，惡意使用者無法藉由竊聽截取到代理人（由 HTTPS 保護），即使它可以偽造 MAC 位址，但存取閘道器在解密過程中，就會因為 checksum 的不合而發現非法的封包，由此就可以將這些非法封包丟棄，解決 MAC 位址偽造所產生的威脅問題。

3. Level 1D

與 Level 1U 相反，是由存取閘道器加密下行串流，代理人則對此下行串流解密。至於上行串流則不做任何處理，如圖 3.1(b)所示。在這個模式中，惡意使用者依舊可以向外傳送需求，但因為無法取得代理人，所以無法解密所接收到的封包，這些封包對惡意使用者將失去意義，進而阻絕惡意使用者的企圖。不過惡意使用者在此模式中，依然可以展開阻斷式攻擊。

4. Level 2

這個模式乃是結合 Level 1U 及 Level 1D，在上下行串流上都做加密，如圖 3.1(c)所示。如此形成一個加密的無線通訊通道，具有最高的安全防護性。

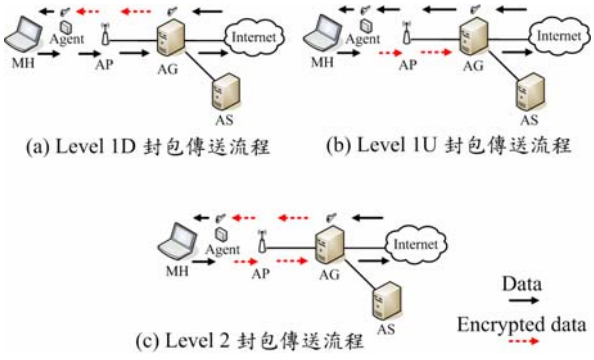

圖 3.1 代理人的封包傳送流程

在代理人的金鑰及加密演算法處理方面。當使用者要從認證伺服器中下載代理人前，認證伺服器會向存取閘道器請求屬於使用者的加密演算法以及金鑰，存取閘道器會隨機的取出加密演算法列表中的其中一個作為存取閘道器以及代理人之間的加解密演算法，並且會產生一組隨機的金鑰，回傳給認證伺服器，認證伺服器便可以依照取得的加密演算法及金鑰產生代理人供使用者下載。而後存取閘道器可以對使用者代理人中的金鑰以及演算法做週期性的更新，如此一來也提高加密的資訊無法成功被惡意使用者破解的機率。

3.2.2 代理人的管理方式

在代理人機制中，認證伺服器將預先決定整個無線網域存取控制的模式。該模式之預設值為 Level 1D，主要是因為封包傳輸效能的考量，從我們的實驗中發現，Level 1D 的傳輸效能要比 Level 1U 或 Level 2 為佳。但當存取閘道器的流量超過一個門檻值後，便會通知認證伺服器，決定是否要切換至 Level 1U 或 Level 2。此時主要是考量是否有惡意使用者大量送出資訊。因此合法使用者可以調者他所使用的安全模式。

我們也可設定整個網域為 Level 1U 或 Level 2，在這種情況下，使用者也可選擇是否要升級成 Level 2。但無論使用者的設定為何，都不可以低於整個網域之安全模式設定，以免造成網路安全之危害。

3.3 安全威脅分析

3.3.1 盜用無線網路

當 MAC 位址被偽造之後，如果未經過任何防護措施的防範，將可欺騙網路設備，進而讓惡意使用者盜用合法 MAC 位址。在所提出之代理人機制中，透過不同的安全模式，進行不同形式的對抗。在 Level 1U 的模式中，惡意使用者所送出的偽造封包，由於沒有經過代理人的加密，當存取閘道器對其進行解碼時，即會因為 checksum 不合而被發覺，此時存取閘道器便會將之視為無效封包而丟棄，讓惡意使用者即使可以偽造 MAC 位址，但卻無法使用無線網路。在 Level 1D 的模式中，代理人對上行串流的封包並不做任何處理，只針對經過存取閘道器加密的下行串流封包進行解密，因此，雖然惡意使用者可以向外發出 MAC 位址被偽造的封包，但是由於送回來的封包會經由存取閘道器加密，此時惡意使用者沒有代理人來將封包解密，拿到的封包在意義上也成為無效封包。而在 Level 2 中，代理人對上行串流及下行串流的封包同時進行加密與解密，存取閘道器會分別進行解密的檢查以及加密的傳送，因此安全防護等級最高。雖然因為上行串流加密的保護，惡意使用者已無法傳送出封包，但下行串流加密的保護可以進一步保護合法使用者的資料不易被竊取。

3.3.2 竊聽防護

如果沒有任何安全機制的防護，在無線網路環境中，惡意使用者可以很容易的竊聽到合法使用者的封包內容。在所提出的代理人機制中，上行串流封包與下行串流封包皆可被加密保護，因此如果使用 Level 2 的安全模式，代理人與存取閘道器之間將可以建立一個類似 VPN（virtual private network）

的安全通道，防止惡意使用者的竊聽。如果使用 Level 1U 或 Level 1D 的模式來傳送資料，由於代理人機制只對上行串流或下行串流其中之來加密保護，因此仍留有被竊取資料的可能性，但此時資料傳輸可以得到較快的傳輸表現。使用者可以視自己的需求，來選擇最適合的安全模式來傳輸資料。

3.3.3 DoS 攻擊

透過封包 MAC 位址的偽造，惡意使用者的攻擊程式可以偽裝成合法使用者，向遠端的伺服器進行阻斷式服務攻擊（DoS attacks），意圖癱瘓這些伺服器。在所提出的代理人機制中，可以透過 Level 1U 及 Level 2 的安全模式來加以防範。此時這些偽造 MAC 位址的攻擊封包會被存取閘道器經由解密的程序而加以攔截，不會對遠端伺服器造成威脅。由於存取閘道器的解密計算通常不需花費大量的計算時間，因此存取閘道器也可以承受大量 MAC 位址偽造封包的驗證工作。

為了傳輸效能的考量，整個環境不在一開始就設定在 Level 1U 或 Level 2。只有當存取閘道器發覺上行串流的封包數量超過某一個門檻值時，才需要動態地起動 Level 1U 或 Level 2 的防護機制，加以阻隔可能的 DoS 攻擊。但如果經過一段時間的監控，發覺其實上行串流封包被丟棄的數量小於某一個預設值，表示實際上並未發生嚴重的 DoS 攻擊，此時無線網路的安全模式便可回到使用者原先設定的模式來進行傳輸。

3.3.4 綁架攻擊

綁架(session hijack) 的網路攻擊方式，乃是惡意使用者透過屏蔽的方式切斷合法使用者的 session 並且偽裝成該使用者繼續進行後續的 session 動作，形成對該 session 的綁架。如果此時該合法使用者啟動代理人機制，在 Level 1U 模式中，由於惡意使用者送出的封包都將被視為無效封包，因此他無法偽裝成合法使用者繼續盜用該 session。在 Level 1D 模式中，由於惡意使用者沒有代理人，無法竊取使用者在網路上的機密資訊，所以也無法繼續使用該 session。Level 2 的安全模式具備 Level 1U 及 Level 1D 的特色，同樣也可以阻止此類的攻擊。如此，合法使用者的權益將可受到代理人機制的保護。

4. 實驗結果

為了實際驗證代理人機制，並了解它的效能影響，我們實作一個雛形系統，使用 ping 及 FTP 兩種方式來測量代理人機制所提供的四種模式，並且詳細討論它的效能表現。

在實驗中我們使用了三台機器來架設一個簡單的環境。一台是 mobile host，使用的是 Windows XP 的作業系統，其他兩台使用 Linux 的作業系統，並且在上面架設了 Apache 網頁伺服器，作為存取閘道器及認證伺服器以及普通的網頁伺服器。無線網路則使用 802.11b。為了測試代理人機制的運作，在代理人中使用了 XOR 做為加密演算法，做為架構功能性驗證。以下是 ping 及 FTP 這兩個實驗的過程及結果。

4.1 封包傳輸實驗

在我們的代理人機制中提供四種模式，這四個模式的加解密以及代理人的處理方式不盡相同，因此我們選擇上行及下行封包大小及數量都一樣的 ping 封包來作為實驗量測的方式，如此便可以了解各個模式下對於網路傳輸效能的影響。所以我們將 ping 封包的大小從 100 bytes 開始，每 100 bytes 測量十次，測量至封包大小為 1400 bytes。在每次測量中傳送 1000 個封包，計算從 mobile host 經由存取閘道器到網頁伺服器的來回時間。圖 4.1 即是測量後的結果。

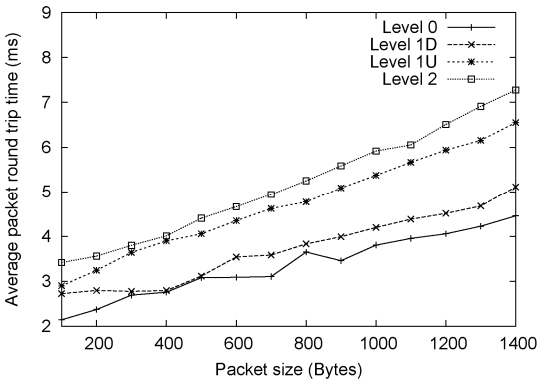

圖 4.1 平均封包來回傳輸時間

在圖 4.1 中可以看在封包大小為 1400 bytes 時，Level 0 的平均封包的來回傳輸時間最短，為 4.45 ms。Level 2 的傳輸時間較長，為 7.27 ms。Level 1U 及 Level 1D 由於只加解密一次，因此它們的傳輸時間會在 Level 0 及 Level 2 的來回傳輸時間範圍內，Level 1U 的傳輸時間為 6.55 ms 而 Level 1D 的傳輸時間則是 5.11 ms。代理人在 Level 1U 模式運作的情況中，當應用程式送出網路封包後，經由作業系統送到網路卡，而此時代理人透過監聽機制截取封包並且加密後傳送出去，此模式與 Level 1D 模式下運作的情形不同。在 Level 1D 中，當客戶端收到加密的下行串流資料，這些資料會先送至代理人，經由代理人解密後再轉送給作業系統，而作業系統收到後送回至應用程式。在這兩種運作的情況下 Level 1U 會比 Level 1D 多一次的記憶體存取，如圖 4.2(a)中所呈現，所以 Level 1U 的平均封包的來回傳輸時間會比 Level 1D 來的高。

另外我們將平均封包的來回時間所換算成傳輸

表現。Level 0的平均封包的來回傳輸時間最短所以傳輸的表現也是最好，在封包大小為1400 bytes時為615 Kbytes/sec，而Level 1D及Level 1U則分別有535 Kbytes/sec及418 Kbytes/sec的表現，安全性最高的Level 2其傳輸表現也有376Kbytes/sec。

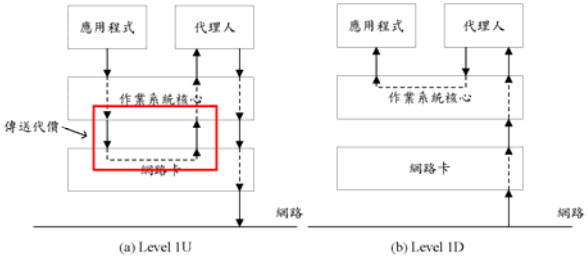

圖4.2 延遲說明

4.2 檔案傳輸實驗

在平常的網路環境中上行與下行封包的數量比，不是如同 ping 封包一般呈現上行與下行封包比為 1:1 的情形，而是呈現下行封包量會比上行封包量來的多的結果。所以我們使用 FTP 這種網路常見的傳輸方式來量測代理人機制的傳輸效能。我們設定一個檔案大小為 100 Mbytes 的檔案作為傳輸代表。分別測試代理人機制所提供的四種模式，並且每種模式分別測試五次。傳輸的封包總量在其中一次的測量中共傳輸 118,935 個封包，上行的封包有 46,474 個封包，而下行的封包有 72,461 個封包。測試的數據如表 4.1 所示。

表 4.1 FTP 檔案傳輸時間

模式	傳輸時間(sec)	標準差	增加比例
Level 0	251.9	20.91	—
Level 1U	358.06	32.79	42.14%
Level 1D	293.04	23.52	16.33%
Level 2	441.79	31.05	75.38%

由數據我們可以知道 Level 0 的平均傳輸時間最短為 251.9 秒， Level 2 為雙向加密所以傳輸時間是最長為 441.79 秒。Level 1U 及 Level 1D 分別平均傳輸時間為 358.06 秒及 293.04 秒。由於 Level 1U 的記憶體存取次數較多。而這些增加的記憶體存取次數是根據封包量的比例增多，FTP 傳輸的情況中上傳以及下載的封包比例為 1:1.55 的情形下 Level 1U 的傳輸時間會比 Level 1D 長。我們另外測量了此額外記憶體存取時間，大約為 1 ms，與實驗數據大致上符合。由標準差來看，可以發現 Level 0 及 Level 1D 的數據變化幅度較小，是由於傳輸時間比較短，受外界其他使用無線網路的電腦影響較小，而 Level 1U 及 Level 2 則影響較大。

5. 結論

在目前的存取控制協定中，雖然有方法可以對抗偽造 MAC 位址所產生的威脅，但是其佈建或更新的代價相當高昂。針對於此,本論文中提出了一個代理人機制來對抗 MAC 位址偽造的威脅。此機制的作法主要是利用合法下載之代理人將傳送出去的封包加密，經由存取控管伺服器之驗證與解密，才進行正常傳送流程。由於惡意使用者無法取得合法代理人，傳送出去的封包便會變成無效封包，進而對抗 MAC 位址偽造所產生的威脅。因此代理人機制有下列三點好處：1.能夠有效對抗 MAC 位址偽造所產生的威脅。2.更新的代價成本較低。3.不僅適用於私人無線網路，也適用於公眾無線網路。

同時，我們利用封包傳輸實驗以及檔案傳輸實驗測試代理人存取控制機制的效能。在實驗結果中，代理人存取控制機制的 Level 1D 模式效能最好，有 535 Kbytes/sec 的傳輸表現。Level 1U 次之，有 418 Kbytes/sec 的傳輸表現。由於 Level 2 的安全防護效果最完善，網路傳輸效能受到的影響也最多，傳輸效能為 376 Kbytes/sec。對於如何改進他們的效能，未來值得進一步研究。

此外，不同加密演算法對代理人機制效能的影響，也值得進一步討論。為了驗證代理人機制實際佈建的可能性，未來也需要在大規模的公眾無線網路中來量測實際的效能。雖然目前只有雛形系統的初步實驗，但相信此代理人機制可以有效地運作在公眾無線網路中，對抗 MAC 位址偽造所帶來的威脅。

參考文獻

[1] *Information technology—Telecommunications and Information Systems — Local and metropolitan area networks —Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer specifications*, Amendment to ISO/IEC 8802-11/1999(I) ANSI/IEEE Std 802.11, 1999 edition, 2004.

[2] D.B. Faria and D.R. Cheriton, DoS and Authentication in Wireless Public Access Networks, in *Proceedings of ACM Workshop on Wireless Security*, 2002, pp. 47 – 56.

[3] J. Hall, M. Barbeau, and E. Kranakis, Detecting Rogue Devices in Bluetooth Networks Using Radio Frequency Fingerprinting, in *Proceedings of International Conference on Computer Communications and Networks*, Oct. 2006. 29

[4] S. Fluhrer, I. Mantin, and A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, in *Proceedings of Annual Workshop on Selected Areas of Cryptography*, Aug. 2001, pp. 1 – 24.

[5] S. Schmid, J. Finney, M. Wu, A. Friday, A. Scott, and D. Shepherd, An Access Control Architecture for Metropolitan Area Wireless Networks, in *Proceedings of Interactive Distributed Multimedia Systems and Telecommunication Services*, Nov. 2001, pp. 29 – 37.