無線區域網路監測管理系統實作

DESIGN AND IMPLEMENTATION OF WINDOWS-BASED WLAN MONITORING SYSTEM

林筠穎（J. Y. Lin）[1]、楊中皇[2]（Chung-Huang Yang）

國立高雄師範大學 資訊教育研究所
Institute of Information and Computer Education, NKNU

摘要

無線技術的發展日新月異，因此無線產品能大量的開發，而隨著產品的量產，價格也隨之降低，這也是無線技術應用愈來愈普遍的原因。同樣的，網際網路亦因同樣的理由蓬勃發展，當網路與無線技術結合時，帶給我們的方便性更勝以往。其好處是環境可以保持清爽的空間，因為不需要鋪設太多管線；可以自由的行動上網，不需局限地點；可以即時達到溝通的目的。然而當大家沉醉無線網路的迷人之處時，卻很容易忽視掉潛藏的重大危機—資訊安全。有線網路在有型的設備下，可以有目標的防範外來的破壞，即使如此，有線網路仍然遭到許多安全的威脅，更遑論無線網路的訊號是發佈於空中，其封包資料輕而易舉的就能被捉取，安全的問題更需受到重視。

無線網路的安全威脅有竊聽、AP spoof、中間人攻擊、DOS 攻擊等，如何瞭解及維護無線網路安全，是管理者頭痛的問題。為協助管理者有便利的管理界面來瞭解無線網路安全狀況，本研究針對在 802.11 下的無線區域網路設計出一套以 Windows 為基礎的中文界面軟體，簡稱 WDMS(Wireless Detect Manage System)，本軟體功能在於針對無線區域網路封包資料掃瞄，藉此分析出封包訊號屬性為何？是否加密?安全性如何等資訊，提供管理者採取因應步驟之依據。

關鍵字：無線網路、網路安全、802.11、WEP

Abstract

The wireless network has recently become more and more popular due to its convenience and falling prices of the hardware. People have the freedom to roam around anywhere within the range of the wireless network. The ubiquity and convenience of wireless LANs (WLAN) is enticing for the users. But there is one important thing to respect about security.

In the traditional Wired LAN, access is via the connection to an Ethernet port, thus access control to the LAN is governed by the physical access to the LAN ports. In a WLAN environment, the data is transmitted by another medium using Radio Frequency (RF). Since RF has the ability to penetrate walls and ceilings, any WLAN client can receive it intentionally or unintentionally if it is within range. So how to manage WLAN is the network manager's main work. In this research, we design and implement a Windows-based WLAN monitoring system － WDMS(Wireless Detect Manage System),which can scan WLAN signals and gather what functions access points

(APs) provided.

Keywords ： WLAN 、 wireless security 、 802.11、WEP

1. 緒論

科技的進步幫助了人們生活，舉凡食、衣、住、行、育、樂。電腦和無線設備即是科技進步的產物之一，如記帳、文書編輯、遙控器、甚至家庭用家電用品，皆因此而更簡便。當兩者結合時，更讓未來的網路生活邁向一大步。著眼於此商機，無線網路相關產品如雨後春筍般冒出，手機、PDA、筆記型電腦等皆屬於無線設備，可移動性與輕便是其最大的好處，不受時間、空間限制，隨時可直接傳遞訊息，讓人們的溝通更快速，且安裝方便，不需花費太多金額[8]。

然而，在大家享受這樣的便利時，安全卻是大家容易忽視或是不瞭解的重點。無線網路的訊號不像有線網路有一層保護且在固定地方，安全的管理較容易；無線的訊號就散佈在我們四周，有心人隨時可以截取這些訊號，只要準備一片網路卡及筆記型電腦就可移動至任何地方進行其截取行為，令網路管理人員無法設防。不管如何，無線網路是未來的趨勢之一；而人們在面對便利與安全時，通常捨安全而取便利，因此無線網路的應用將會愈來愈廣泛。雖然我們無法完全解決安全問題，但可盡力拖延與防範重大的錯誤狀況發生，因此本研究實作一無線網路偵測系統 WDMS 以期能幫助無線網路管理者做到更好的監測效果。

目前大部份的無線區域網路皆採用 802.11 協定之設備及防護措施。因此本研究將對在 802.11 下的無線區域網路及安全作相關的文獻探討;接著說明實作軟體 WDMS 之系統設計及實作。

2. 文獻探討

本研究主要是以 WDMS 這套軟體監測收集無線網路訊號，並由所得資料解析無線網路的安全性；因此本章就無線網路的相關環境背景、802.11 技術標準、使用的安全技術及無線網路安全曾有的相關研究予以說明。

2.1 無線網路

自十九世紀末電磁波發現以來，無線通訊技術便不斷發展； 1971 年，夏威夷大學的研究員創造出第一個以封包式技術的無線電通訊網路，稱為 ALOHNET 網路，當時的科技只能允許七台電腦上無線上網；1979 年，AT&T 於美國芝加哥佈建第一套無線電話系統－ AMPS 系統（Advanced Mobile Phone Service），業界將 AMPS 系統稱為第一代無線網路；1995 年，Unwired Planet 發展了可以讓無線裝置互動地存取 Internet 的技術，並於年底取得美國技術專利[12]；電機電子工程師協會（IEEE）於 1990 年開始進行 WLAN 標準 802.11，1997 年正式完成；1999 年，IEEE 制訂了 802.11a 與 802.11b 的標準，讓無線網路傳輸的速度分別達到 54 Mbps 與 11 Mbps，其中 802.11b 是目前應用最廣泛的無線網路通訊標準，之後陸續因應不同需求而發展了多項標準，802.11g 即是加強了 802.11b 速度的一項標準。

無線網路最大的特點是具行動性，無論在何時，只要有提供無線上網的地方便可連線，安裝方便又簡單，其架構模式有兩種：一、簡易模式（Ad-Hoc Mode）：利用無線網路卡以端點對端點（Peer to Peer）的連接模式。二、基礎建設模式（Infrastructure Mode）：有線與無線區域網路的應用整合模式，由 Access Point(AP) 當橋樑，有線的部分是 AP 與有線網域之間，無線的部分是 AP 與 Station 之間。

無線區域網路（WLAN，Wireless Local

Area Network）傳輸範圍在 1 百公尺左右，傳輸技術約有三種：微波（Microwave）、展頻（Spread Spectrum）、紅外線（Infrared ray），使用的標準是 802.11[4]。

2.2 ISM 頻段

ISM(industrial，scientific，medical band)，FCC 所規範免申請使用執照(Free License)的無線電頻段，目前全世界大部分國家也依循此規範來開放頻段。ISM 頻段包含三個頻帶：902～928MHz、2.4～2.4835GHz（使用最多，3 個頻道）、5.725～5.850GHz(11 個頻道)[2]。

2.3 IEEE 802.11 通訊協定

802.11 是由電子電機工程師協會 IEEE Computer Society 裡的 802 區域型及都會型網路標準委員會(802 LMSC)所制定與 LAN 相關的規格；其規格分成兩部份，第一部份是製定出適用於所有無線網路系統的媒體層(MAC)規格，設計和實體層(PHY)無關的 MAC 協定。第二部份則是製定出和傳輸媒介相關的實體層(PHY)規格[5]。其使用技術有：

DSSS(direct sequence spread spectrum)：透過二進位編碼程序送出資料，此技術將資料與一 multibit pattern 或虛擬亂碼(pseudo-noise code)組合產生欲傳送之內容。

FHSS(Frequency hopping spread spectrum)：利用窄頻載波在不同的頻道間以協定的頻道跳躍順序來傳送訊號。

OFDM(Orthogonal Frequency Division Multiplexing)：一種多載波調變的技術，將一個通訊頻道切成相同大小的頻道，每一頻道都是獨立傳送資料[12]。

802.11 的服務項目包含了分散系統服務（Distribution System Services）的連結服務、重新連結服務、取消連結服務、分送服務、資料訊框的傳遞、整合服務等與工作站服務(Station Services)的身分認證/取消認證服務(Authentication/Deauthentication）、保密性服務（Privacy）[1]。

2.4 無線網路安全服務

依據 IEEE 所定標準，無線網路協定提供的三項基本網路安全服務為：使用者認證、資料完整性確認及資料保密以確保資料的「機密性」、「資料完整性」、「確實性」、「不可否認性」。相關安全措施敘述如下：

使用者認證(Authentication)

開放系統認證(Open System Authentication)

以 SSID (Service Set ID)為認證方式，若 Access Point(AP)接收到空白 SSID (Service Set ID)的 request 時會回應其 SSID (Service Set ID)，Station 便以此 SSID 認證連接此 Access Point(AP)。因此只要訊號正常便可認證連線，等於沒有認證。

封閉系統認證 (Closed System Authentication)

Station 必須設定 SSID，Access Point（AP）才會對其回應進行認證。雖然有此限制，攻擊者只要利用 sniffer 工具竊聽封包取得 SSID，很容易就避開此限制與 Access Point（AP）進行認證連接。

加密認證

以共享金鑰(Shared-key Authentication)的方式進行身分認證，金鑰是以 WEP 機制加密，加密演算法為 RC4。其認證過程如圖 1：

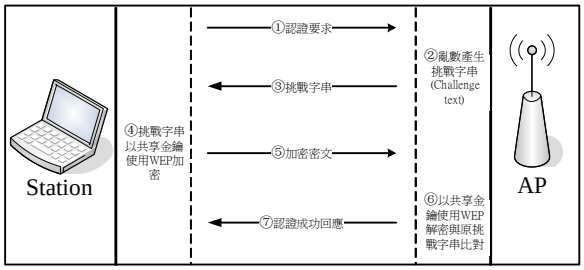

圖 1　加密認證過程

完整性確認

802 系列通常以 CRC checksum 來進行封包內容的完整性確認，而使用 WEP

（Wired Equivalent Privacy）加密機制時，則仍搭配 CRC 對資料進行保護[1]。

2.5 WEP 演算法

WEP（Wired Equivalent Privacy）是由 IEEE 為 802.11 設計的對等式線性加解密的機制，使用相同金鑰加密與解密，WEP 所採取的金鑰為 40 Bits，WEP2 之金鑰可採 40Bits 或 104Bits。其加解密過程說明如下：

WEP 加密運作方式（參考圖 2）

運用演算法產生 24bits 的 IV(Initial Vector)。

IV 與 WEP KEY 以 RC4 運算產生一加密金鑰。

將 Message 以 CRC 運算產生檢查碼 ICV，並將 ICV 與 Message 結合成 PlainText。

將加密金鑰與步驟　之 PlainText 做 XOR 運算，產生 CipherText。

將 IV 附加於密文。

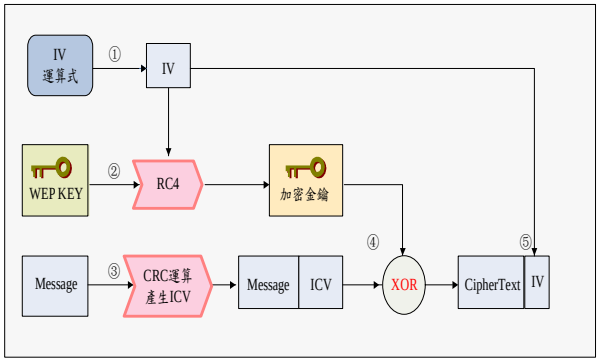

圖 2　WEP 加密運作方式

WEP 解密運作方式（參考圖 3）

取出附加於 CipherText 之 IV(Initial Vector)。

將 IV 與 WEP KEY 以 RC4 運算取得加密金鑰。

將加密金鑰與密文做 XOR 運算，結果就是明文。

明文做 CRC 運算確認完整性。

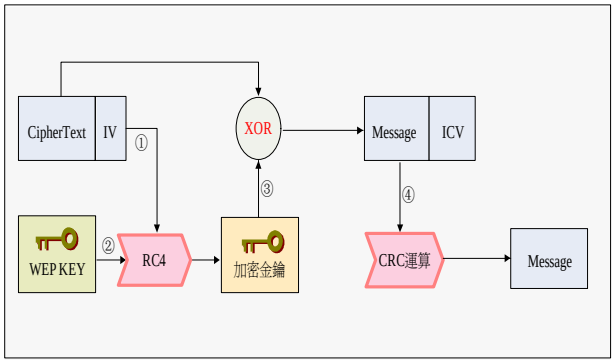

圖 3　WEP 解密運作方式

演算法

參數表示說明：

C　：CipherText

P　：PlainText

M　：Message

IV　：Initial Vector

K　：WEP KEY

⊗　：執行 XOR 運算

RC4　：執行 RC4 運算

CRC　：執行 CRC 運算

‖　：將欲處理的訊息接續

WEP 加密演算式

$$\mathbf{C} = \boldsymbol{RC4}(\mathbf{K}, \mathbf{IV}) \otimes (\mathbf{M} \| \boldsymbol{CRC}(\mathbf{M}))$$

WEP 解密演算式

$$\mathbf{P} = \boldsymbol{RC4}(\mathbf{K}, \mathbf{IV}) \otimes \mathbf{C}$$

2.6 IEEE 802.1x

IEEE 於 2001 年正式核可 802.1x (Port-Based Network Access Control)，是為補強 WEP 安全性不足的認證與動態之金鑰管理機制。透過這樣的機制，過濾沒有經過後端認證伺服器(Radius Server)許可的使用者封包。(參考圖 4)

EAP

EAP(Extensible Authentication Protocol)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的認證機制[9]，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。這五種認證方式中，EAP-MD5 只需要輸入帳號與密碼即可做好身分認

證，EAP-TLS、EAP-TTLS 則需要再於個人電腦上加裝電子憑證，EAP-SIM、EAP-AK 則是以 SIM 卡作為認證方式[3]。

EAPOL

EAPOL(EAP Over Lan)屬於無線網路協定裡 IP Layer 以下的通訊協定,主要定義在 IEEE 802.1x 的 7.6 節中, 可以讓使用者在未經過 EAP 認證登入以前的封包,透過 EAPOL 的傳送,經由 Access Point 與後端 AAA (Authentication, Authorization, and Accounting) Server 進行認證[9]。

Radius Protocol

RADIUS(Remote Access Dial In User Service) Protocol 提供 Authentication 的機制來辨認使用者的身份與密碼，確認通過之後才授權使用者登入網域使用相關資源：並提供 Accounting 機制，保存使用者的網路使用記錄，以提供系統服務業者完整認證收費機制的一個基礎[9]。

802.1x 組合與架構

Authentication Server：提供身分認證服務的實體，如：Radius server。

Supplicant：請求認證的實體,指 Client 端。

Authenticator：要求及接受未受信任端網路節點的認證請求的實體，如 Access Point(AP)。

802.1x 認證方式：Supplicant 使用 EAPOL 向 Authenticator 發出認證請求，Authenticator 接受請求並向 Authentication Server 提出身份確認動作，接著 Authenticator 依據 Authentication Server 確認結果回應 Supplicant 認證是否通過(參考圖 4)。[1]

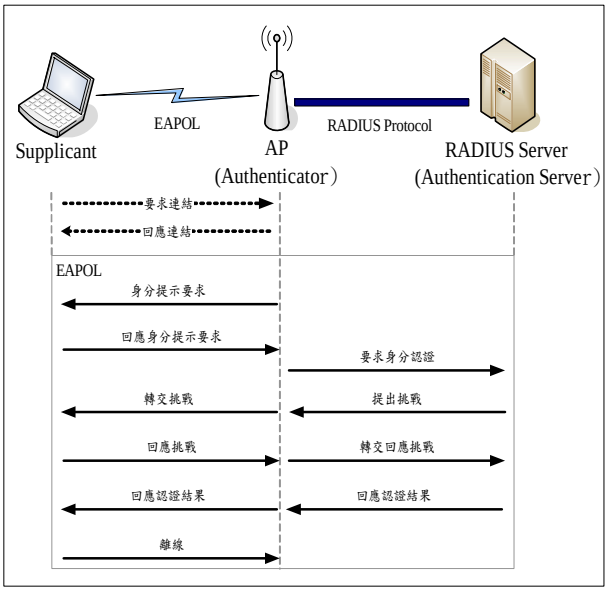

圖 4　802.1x 機制表示圖

2.7 WPA

WPA(Wi-Fi Protected Access)由 WiFi 聯盟針對 802.11 安全漏洞所提出的一種無線安全過渡解決方案，並非 IEEE 的標準協定。其組成包括 802.1x、EAP(Extensible Authentication Protocol)、TKIP(Temporal Key Integrity Protocol)、MIC(Message Integrity Code)，包含三項功能說明如下。

認證：以 802.1x、EAP 作為 WPA 身分驗證的基礎。

加密：使用 TKIP 加密機制，此機制以動態方式產生及交換金鑰，不同於傳統的單一靜態金鑰；基本上 TKIP 的加密機制與 128-bits WEP Key 是一樣的，差別在於 WEP 的金鑰是將 WEP Key 與 IV 值直接做 RC4 運算而得；而 TKIP 中的 TKIP Key 與封包的 IV 值都只是產生最後加密所用 128 bits 的參數[9]。

資料完整性確認：採用 MIC 資料完整性確認機制，發送端送出封包前，把未加密過的資料內容透過 Michael 演算法，求得 64 bits 的 MIC 值；而接收端把收到的封包解密後，對資料內容也以 Michael 演算法計算出 MIC 值，如果一致就表示封包正確無誤，如果不一致，就表示封包在傳輸過程中發生錯誤。

2.8 802.11i

IEEE 為了解決安全漏洞所提出的802.11i標準，終於在2004年6月中批准了。有三個部份是 802.11i 所著重加強的：認證機制、金鑰管理、資料傳遞[[7]，說明如下：

認證機制：802.11i 加強了認證系統，原來的 WEP KEY 認證方式是單向的認證(從主機到 AP)，802.11i 增加了 Authentication Server，以雙向認證方式來防止中間人攻擊；其認證方式源自於802.1x。同時 802.11i 增加兩個 key 來進行雙向認證，第一個 master key (MK)是 Supplicant 對 Authentication Server 間認證的私密對稱金鑰；另一個 pairwise master key (PMK)是 Supplicant 與 AP 間的私密對稱金鑰。

金鑰管理：為了改善 WEP 金鑰管理缺失，802.11i 增加了金鑰管理機制。除了 MK 與 PMK 外，還新增了多個金鑰：pairwise transient key(PTK)、key confirmation key (KCK)、key encryption key (KEK)、group transient key(GTK) and the temporal key (TK)。金鑰管理主分三個步驟：第一步是從 Authentication Server 傳送 PMK 到 AP，第二步利用 PMK 和 PRF(Pseudo-random function)導出和驗證 PTK，最後定出 GMK 利用 PRF 導出 GTK 從 AP 送至 Supplicant[10]。

資料傳遞：有三種資料傳送方法：CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol)、TKIP (Temporal Key Integrity Protocol)、WRAP (Wireless Robust Authenticated Protocol)。CCMP 與 TKIP 這兩個加密機制採用的演算法為 AES。

2.9 無線網路安全

無線區域網路的安全問題一直是大家所關注的問題，尤其是在漏洞和密碼破解上，在此分別對攻擊與弱點及安全維護的方法，說明如下：

無線網路的問題：

無線媒介散佈於空氣中無法控制別人接收。

無線訊號可以穿透建築物，不受空間的限制，很容易被接收。

已有許多捉取無線封包的工具軟體。

私接的 AP。

常見攻擊方式：

竊聽(Eavesdropping)：偵測得通訊資料(如：AP、SSID、Station…等)，並監控網路活動或竊取資訊，甚或進行破壞動作，如：Wardrive。

偽裝(Masquerade)：偽裝成 AP 或 Station，取得登入系統資訊，非法進入系統使用資源，如：中間人攻擊(Man-in-the-Middle)。

重播(Replay)：指攻擊者將從網路上截取的某些通訊內容(如認證資訊) 重新發送，以欺騙伺服器認證機制。

服務阻絕(Denial of Service)：藉著發送不正確的控制訊號或大量的封包資料以癱瘓主機或網路，達到阻撓網路服務功能。

WEP 的弱點：

WEP 設計的錯誤：為了讓 KEY 變化，設計了只有 24bits 的 IV(Initial Vector)，攻擊者只要收集一定量封包就可分析出 IV；進而破解出金鑰。

金鑰管理問題：WEP KEY 為共享 KEY，為了方便，KEY 值通常維持不變，而且記錄在機器中，讓人很容易就取得。

RC4 演算法的漏洞：Scott Fluhrer、Itsik Mantin 以及 Adi Shamir 共同發現 RC4 用來產生密鑰的演算法有數學上的漏洞，演算法產生密鑰時所作的運算有部分會仍然出現在最後所產生的密鑰裡，這類的密鑰在密碼學上稱為”弱密鑰”(Weak Key)。因此，只要攻擊者能收集到越多符合特定特徵的資訊，找出原來使用者指定的密鑰的可能性就越高[1]。

安全維護的方法：網路安全問題並無法完全解決，但可儘量拖延攻擊者的可攻

擊時間使其無法達成目的，讓破壞減至最小或無任何破壞就成了，以下為可注意的方式：

保護硬體設備，將無線相關設備放在適當位置，可避免受到天然或人為破壞及偷竊硬體或軟體(密碼、資料)。

定期掃瞄 AP，除了注意是否有非系統下之偽裝 AP 外；亦控制 AP 訊號的強弱，若訊號太強，別人很容易就接受到，這時應降低功率；若訊號不足，就應提高功率。

使用設備的加密功能，就算其加密方式是簡單易破解的，使用較長的 key，仍能增加網路被破解的時間而採取因應措施。

更改預設 SSID，且儘量關閉廣播 SSID 功能，讓人不容易獲得或猜出 SSID。

驗證使用者，要求他們做身份確認及登入，可防止他們連上惡意之 AP。

設定存取權限，只有授權的無線網卡硬體位址(MAC address)，可以被允許存取無線網路；安裝 RADIUS 伺服器，可以提供另一層的認證。

設定存取權限安裝 RADIUS 伺服器，只有授權的無線網卡硬體位址(MAC address)，可以被允許存取無線網路。

2.10 探測工具

目前有許多探測工具可用在無線區域網路的訊號偵測上，茲將其部份列於表一：

表 1 探測工具

軟體	平台	語言	操作界面	功能
AirSnort	Linux Windows	英文	Window	是屬於被動式的網路監測軟體；若收集足夠的封包，可找出 encryption keys。
Snort-Wireless	Linux Windows	英文	文字	屬於 802.11 的 IDS，功能和 Snort 2.0.x 相符。以
				WiFi 規則為其偵測協定。
Kismet	Linux Windows	英文	終端機視窗	主要在 Linux 作業系統上執行。是網路嗅探工具也是網路解析工具。
NetStumbler	Windows	英文	Window	偵測基地台信號強度與相關資料，支援全球定位系統。
WIDZ	Linux	英文	文字	包含兩部份：一項功能是搜尋基地台，偵測出非法基地台；另一項功能為偵測封包內容及流量。
Prismstumbler	Linux	英文	Window	掃瞄無線區網基地台的信號訊框。支援全球定位系統。
WifiScanner	Linux	英文	終端機視窗	搜尋無線網路節點的工具。小型的 IDS 軟體。
Weplab	Linux Windows MacOSX	英文	文字	破解 WEP KEY 之工具軟體。可選擇 Bruteforce、Dictionary 或 Statistical attacks 三種方式之一破解。屬於文字操作模式。
Snort	Linux Windows	英文	文字	小型入侵偵測系統(IDS)，用來偵測網路上的異常封包。
Nessus	Linux Windows	英文	Window	是一個主從架構式的網路安全檢測工具，屬於 Plug-in 模式，可隨時增加程式。Server 端一定安裝於 Unix-like 平台下。

3. WDMS 系統實作

無線網路的安全維護的一項重點，就是瞭解無線設備及訊號是否在安全的狀況中；因此隨時的監控並偵測是否有入侵者是

必要的工作。WDMS 是在 Windows 系統下實作的中文化界面的偵測軟體，希望能讓網路管理者有最方便的操作界面，並可有效的分析網路現況。接著將分項介紹系統實作。

3.1 實作模式

將 WDMS 建置於筆記型電腦上，選用 Orinoco 無線網卡，平台為 WindowsXP，採用中文視窗界面操作，系統發展語言採 Borland C++Builder 6，實作模式請參考圖 5。

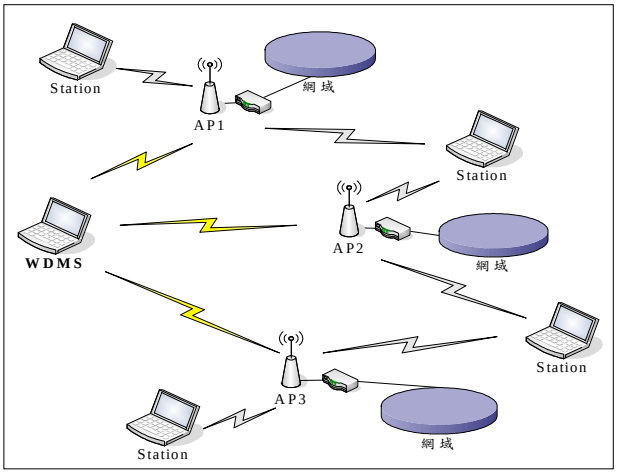

圖 5　WDMS 實作示意圖

3.2 系統功能

WDMS 功能主分檔案、行動、設定、報表(參考圖 6)，說明如下(參考圖 7)：

檔案：

開啟檔案：開啟之前掃瞄或其他偵測軟體掃瞄之 PCAP 檔或文書檔。

儲存檔案：將掃瞄結果儲存為 PCAP 檔或文書檔。

行動：

啟動掃瞄：開始偵測無線基地台及封包，並顯示所得端點詳細資料(如：MAC、SSID…等)，及封包流量觀測與統計；同時可顯示位置圖。

結束掃瞄：停止掃瞄動作。當停止掃瞄之後，可以儲除檔案，或進行密碼破解動作。

設定：設定系統 log、dump 檔既定路徑、聲音、地圖比例等相關系統操作設定。

報表：產生流量統計表及端點明細表。

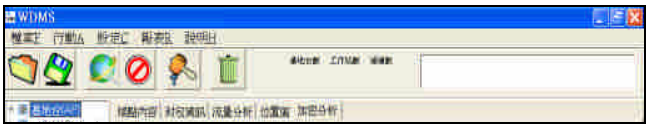

圖 6　WDMS 功能表

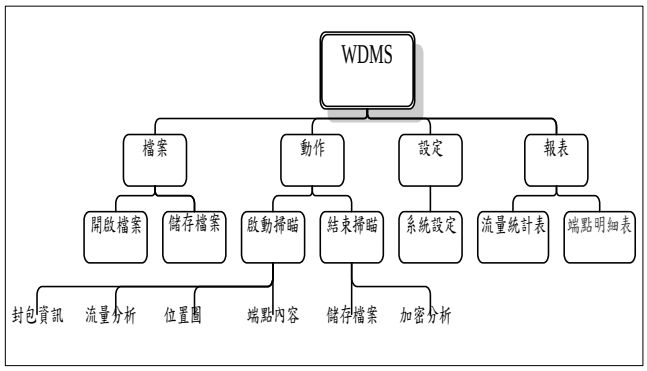

圖 7　WDMS 系統架構圖

3.2 系統操作

啟動系統：WDMS 是 Windows 系統的執行檔，只要直接執行 wdms.exe。程式開始畫面請參考圖 8。

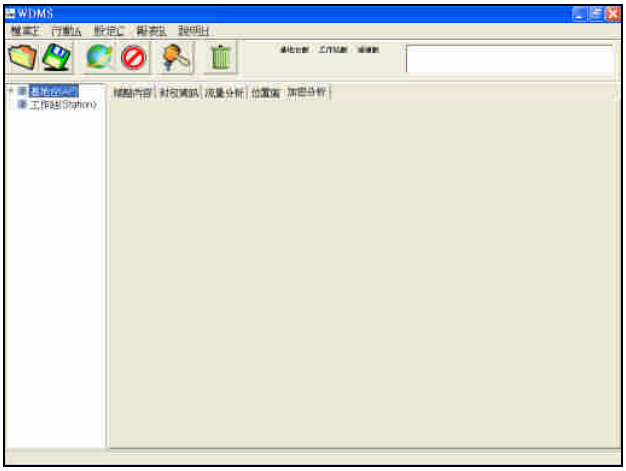

圖 8　WDMS 開始畫面

啟動掃瞄：接上無線網卡，選擇功能中的行動→啟動掃瞄，或點選  鈕啟動。啟動成功，右上角狀態列會顯示"開始掃瞄…."的訊息。若掃瞄到基地台或工作站，左邊樹狀顯示列會顯示搜尋到的基地台或工作站；綠色圖示表示基地台的訊號強度很好；黃色圖示表示基地台訊號強度

較弱；若為紅色圖示即表示基地台無訊號。此時可根據選擇的基地台或工作站，點選右邊各頁面看封包流量資訊及統計與各端點位置圖。加密分析需停止掃瞄才可進行。

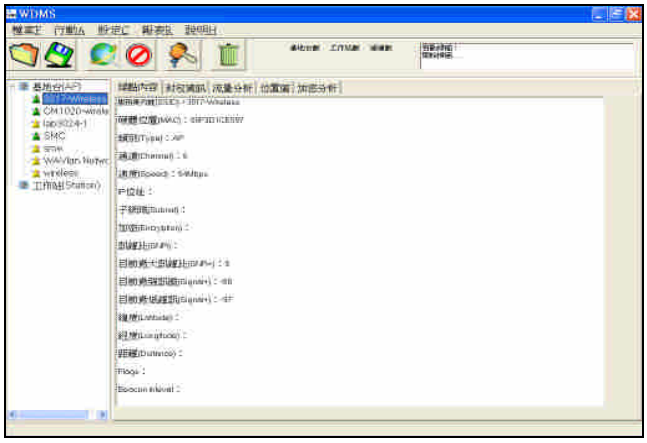

圖 9　WDMS 開始掃瞄畫面

4. 結論

隨著無線網路應用的普及，無線安全的議題也愈來愈為人們所重視；尤其是科技犯罪日益增加的情況下，不論是人們的隱私或公司機關的機密很容易就被竊取，為了保衛資訊，人們常處在便利與安全中掙扎。從本研究實作掃瞄所得的資訊發覺，大多數的基地台是沒有加密保護的，這代表著多數人對於無線網路的安全警覺，不是無知就是疏忽，這是資訊安全的一項隱憂。網管者應不是屬於無知者，若不是疏忽就是惰於維護工作。惰於維護也許是維護工具的使用不便，所以放棄了這個安全工作。

本研究即針對此目標，希望讓網管者有友善的管理工具，協助其在無線網路方面有更安全的應用。簡單的工具讓網管者只要花心思在維護上，不需要再考慮其它的狀況，這是本研究希望達成的貢獻。

5. 結論

1. 林秉忠、陳彥銘(2003)，802.11無線網路安全白皮書，2003年2月，台灣電腦網路危機處理暨協調中心。
2. 周駿呈(2003)，公眾無線區域網路服務市場發展現況與驅勢，無線通訊，2003年5月，工業技術研究院產業經濟與資訊服務中心。
3. 周駿呈(2003)，WLAN網路安全解決方案，ITIS產業評析，2003年5月，工業技術研究院產業經濟與資訊服務中心。
4. 唐政，802.11無線網路通訊協定與應用，2004年8月初版，台北市，文魁資訊股份有限公司。
5. 陳俊利(2002)，無線區域網路架構中有線等效保密演算法安全性分析，2002年7月，國立中興大學電機工程學系碩士論文。
6. AirSnort。 http://airsnort.shmoo.com/
7. Brandon Brown(2003)，802.11:The security difference between b and i，IEEE。
8. Dean Knuth(2004)，SECURE WIRELESS LAN，RSA Conference 2004。
9. HungLin Chou，無線網路WPA安全機制剖析，工業技術研究院電腦與通訊研究所。http://lee-1.com/hlchou/WLANWPA.htm
10. IEEE Std 802.11i-2004。 http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.
11. Kismet。 http://www.kismetwireless.net/
12. Merritt Maxim、David Pollino(2002)著，唐政譯，無線網路之威脅與安全防護，2002年10月初版，台北市，美商麥格羅.希爾國際股份有限公司 臺灣分公司。
13. Nessus。 http://www.nessus.org/
14. NetStumbler。 http://www.netstumbler.com/downloads/
15. Prismstumbler。 http://prismstumbler.sourceforge.net/
16. Snort。 http://www.snort.org
17. Snort-Wireless。 http://www.snort-wireless.org/

18. WIDZ。
http://www.packetstormsecurity.org/wireless/widzv1.8.zip
19. WifiScanner。
http://wifiscanner.sourceforge.net/
20. Weplab。
http://www.sourceforge.net/projects/weplab/