Wireless Packet Monitoring and Analyzing System

賴源正　　陳彥宏　　林志宗
國立台灣科技大學資訊管理所
laiyc@cs.ntust.edu.tw　M9409105@ntust.edu.tw　samuel7210@yahoo.com.tw

摘要

無線網路若要快速的發展與應用，除協定本身設計的成功與基礎建設架設的完整外，勢必需要適當工具與應用軟硬體的配合。本篇論文描述一個無線網路封包監測與分析系統—Wireless Packet Monitoring and Analyzing System (WPMAS)。WPMAS 能夠擷取、分析、並產生 IEEE 802.11 通訊協定封包。WPMAS 可提供使用者排除及處理網路問題、確認各式的無線網路軟硬體是否運作正常、以及協助使用者瞭解 IEEE 802.11 通訊協定的概念。WPMAS 主要的貢獻包含 (1) 可產生 IEEE 802.11 通訊協定封包；(2) 可針對 IEEE 802.11 通訊協定封包產生統計資料與圖表；(3) 提供使用者中文與英文操作介面。

關鍵詞：IEEE 802.11 Protocol、封包監測與分析系統。

Abstract

To promote the development of wireless network, some tools and software are needed. In this paper, a wireless packet monitoring and analyzing system (WPMAS) is introduced. WPMAS can capture, analyze, and generate IEEE 802.11 protocol packets. WPMAS can also help user to understand the concept of IEEE 802.11 protocol concept, detect the problem of network, and check that the wireless software or hardware works well. The major contributions of WPMAS include (1) generating IEEE 802.11 protocol packets, (2) generating statistic data and chart of IEEE 802.11 protocol packets, (3) providing English/Chinese Interface.

Keywords: IEEE 802.11 Protocol, packet monitoring and analyzing system.

1. 前言

近幾年來人們的行動性(mobility)逐漸增加，但因網路線的物理限制，傳統有線上網方式已無法滿足人們的需求[2]。然而無線網路科技的興起突破有線上網方式的限制，也進一步改變人們在傳統有線網路裡的生活型態。例如公司主管將筆記型電腦從辦公室移動至會議室時，由於網路線的長度限制，該主管無法於會議中利用網路線連上網路讀取會議的相關資訊。若該公司設置無線網路，主管即可於公司內任何位置藉由無線網路卡連上網路以讀取工作時所需資訊。因此，無線網路科技提供人們行動性，讓人們不再拘限於網路線的束縛。

無線網路若要快速的發展與應用，除協定本身設計的成功與基礎建設架設的完整外，勢必需要適當工具與應用軟硬體的配合。例如一個可信賴的無線網路封包監測與分析軟體可以協助使用者排除及處理無線網路問題。使用者可藉由此軟體所擷取的封包資訊來瞭解目前無線網路的運作情況。此軟體也可讓欲發展無線軟硬體的廠商或研究人員針對其研發的軟硬體進行檢測與偵測。另外，此軟體可協助正在學習無線網路的學生瞭解無線網路的概念。學生可經由瞭解所擷取的封包格式及型態來驗證課堂上所學得的知識、進而正確詮釋無線網路的運作方式。

本篇論文在此提出一個無線網路封包監測與分析系統—Wireless Packet Monitoring and Analyzing System (WPMAS)。WPMAS 提供使用者擷取、分析及產生無線網路封包等功能。除此之外，WPMAS 採用友善的圖形化介面，讓使用者能輕易擷取、分析、以及產生無線網路封包，並幫助使用者了解無線網路封包的格式、理解無線網路封包運作流程、進而發掘無線網路問題。WPMAS 也提供使用者中英文介面，讓使用者跨越語言的障礙，輕易地學習無線網路的概念。

本篇論文首先回顧 IEEE 802.11 通訊協定、以及一些相關的封包監測與分析軟體。接下來我們將介紹 WPMAS 系統的設計理念、系統架構以及相關的設計議題。在第四章，我們將介紹 WPMAS 各個子系統的設計方式。然後我們在第五章評估 WPMAS 的執行狀況。最後是本篇論文的結論以及未來展望。

2. 背景知識

本章節將回顧 IEEE 802.11 通訊協定，以及相關的封包監測與分析軟體。

2.1 IEEE 802.11 通訊協定

本論文所述的 802.11 泛指 IEEE 802.11 通訊協定及後續衍生的 802.11a、802.11b、802.11g 等各項標準。以目前常用的 802.11b 為例，其最高傳輸速率為每秒 11 Mbps，有效範圍為 300 英尺(約 90 公

尺)。表 1 為各種不同 802.11 標準的比較 [3]。

表 1　802.11 標準比較

IEEE 標準	速度	頻段
802.11	1Mbps ~ 2Mbps	2.4 GHz
802.11a	最高可達 54Mbps	5 GHz
802.11b	5.5Mbps~11Mbps	2.4 GHz
802.11g	最高可達 54Mbps	2.4 GHz

802.11 MAC 訊框由標頭(Header)、訊框主體(Frame Body)與錯誤檢查碼(FCS)所構成，其基本結構如圖 1 [3]。

Header	Frame Body	Frame Check Sequence
30-byte	0~2312-byte	4-byte

圖 1　802.11 MAC 訊框結構

- 標頭(Header)：標頭包含 MAC 位址、控制碼等 802.11 訊框資訊。
- 訊框主體(Frame Body)：訊框主體亦稱為資料欄位(Data Field)，負責在工作站間傳遞上層資料(Payload)。
- 錯誤檢查碼(Frame Check Sequence)：錯誤檢查碼通常使用循環冗餘檢查碼(Cyclic Redundancy Check)。

802.11 設計三種 MAC 訊框，分別為資料訊框、控制訊框及管理訊框。

- 資料訊框(Data Frame)：資料訊框負責在工作站之間傳送資料。不含任何資料的空訊框也屬於資料訊框。
- 控制訊框(Control Frame)：控制訊框通常與資料訊框搭配使用。該訊框主要負責區域的淨空、頻道的取得以及載波偵測的維護，並於收到資料時予以回應，藉此促進工作站間資料傳輸的可靠性。
- 管理訊框(Management Frame)：管理訊框負責監督無線區域網路的運作。該訊框主要用來加入或退出無線網路，以及處理基地台之間連結的轉移事宜。

因應無線資料鏈的差異，802.11 MAC 標頭採用許多特殊的功能，包括使用四個位址欄位。並非所有訊框會使用所有位址欄位，且位址欄位的用途會由於 MAC 訊框種類的不同而有所差異。802.11 MAC 訊框標頭欄位格式如圖 2 所示[1,2]：

Frame Control	Duration /ID	Address1	Address2	Address3	Sequence Control	Address4	Frame Body	FCS
2-byte	2-byte	6-byte	6-byte	6-byte	2-byte	6-byte	0~2312	4-byte

MAC Header

圖 2　802.11 MAC 訊框標頭格式

- Frame Control：Frame Control 欄位包含以下各種次欄位，如圖 3 所示。

Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order
2-bit	2-bit	4-bit	1-bit	1-bit	1-bit	1-bit	1-bit	1-bit	1-bit	1-bit

圖 3　Frame Control 欄位內容

- Duration/ID：此欄位有三種形式，包含(1)當第 15 個位元設為 0 時，此欄位用來設定 NAV (Nework Allocation Vector)；(2)當第 14 個位元為 0 而第 15 個位元為 1，表示在免競爭其間所傳送的訊框號碼；(3)當第 14 與第 15 個位元同時設為 1，表示為省電模式-輪詢（PS-Poll）訊框號碼。
- Address：一個 802.11 訊框最多包含四個位址欄位。這些位址欄位隨著訊框類型的不同，其作用會有所差異。
- Sequence Control：此欄位用於重組訊框片段以及丟棄重覆訊框。它是由 4 個位元的 Fragment Number 次欄位及 12 個位元的 Sequence Number 次欄位所組成。

在安全性方面，802.11 採用 WEP(Wired Equivalent Privacy)加密技術[2]。WEP 主要提供認證(Authentication)及資料保密(Privacy)兩種功能。

802.11 提供兩種認證的服務：開放系統式(Open System)及共享密鑰式(Shared Key)，前者是 802.11 內定的認證方法。工作站提出認證要求時可指定任一種方法進行雙向認證。

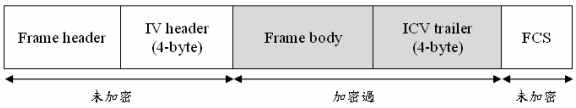

圖 4　WEP 加密訊框

圖 4 為經過 WEP 加密的訊框格式[2]。訊框透過完整性檢驗演算法，產生一個稱為完整性檢驗值(Integrity Check Value，ICV)的雜湊值(hash)。ICV 可確保訊框在傳送過程中未被竄改。

2.2 IEEE 802.11 通訊協定

目前封包監測及分析軟體主要分兩種類別，一種是將軟體架設在一般主機上，另一種是將軟體架設於路由器上。

第一種類別的運作方式為：首先把網路卡設定成 Promiscuous Mode，此時網路卡會擷取網路上的

所有封包(不論 Mac Address 是否為該張網路卡的 MAC Address)。而另一種類別的運作方式是應用其路由器的特性。因為不同網路的封包傳送時皆需經由此路由器的轉送，此路由器不需將網路卡設定成 Promiscuous Mode 便可監測這些轉送的封包。

表 2 封包監測及分析軟體之比較

軟體名稱	作業系統	Open Source	圖形介面	支援 Wireless
Snifffer Wireless [4]	Windows	不是	有	有
NetworkView [5]	Windows	不是	有	無
LanExplorer [6]	Windows	不是	有	無
TCPdump [7]	Linux	是	無	部分
Ethereal [8]	Windows/Linux	是	部分	部分
Sniffit [9]	Window/Linux	是	無	無
Airopeak [10]	Window	不是	有	有
Kismet [11]	Linux	是	無	有

如表 2 所示，在 Windows 環境下具有良好使用者介面的封包監測及分析軟體大多為商用收費軟體。其軟體往往不公開其原始碼，也鮮少支援擷取、分析 802.11 無線網路封包的功能。在 Linux 環境下常用的 TCPdump 雖有釋出原始碼並提供擷取 802.11 無線網路封包的功能，但是沒有圖形介面的設計讓使用者感到非常不便。另外 TCPdump 著重於根據使用者設定的參數擷取所需的封包，幾乎無法分析、統計所擷取的封包。Ethereal 可擷取 802.11 無線網路封包，並可利用圖形介面來設定擷取過濾的功能。但是 Ethereal 為針對有線網路所設計的軟體，尚未針對 802.11 無線網路的特性設計適當的封包監測與分析功能。

3. WPMAS 綜述

WPMAS 是以 Ethereal 為基礎所開發的封包監測與分析系統。此系統的設計滿足使用者以下六個需求：

- WPMAS 能夠擷取並分析 802.11 無線網路封包。
- WPMAS 介面設計必須抱持「對使用者友善」的原則。
- WPMAS 能夠立即提供 802.11 無線網路封包的相關統計資料與圖表。
- WPMAS 提供使用者兩種語言介面，即中文介面與英文介面。
- WPMAS 提供使用者產生 802.11 無線網路封包的功能。
- WPMAS 為開放性原碼軟體。

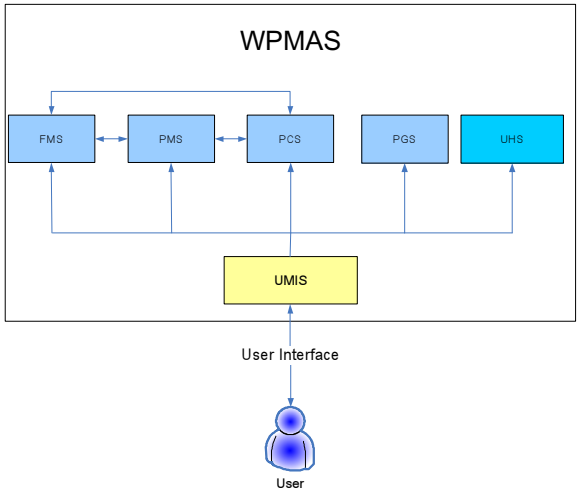

圖 5 WPMAS 系統架構

如圖 5 所示，WPMAS 包含六個子系統，即使用者主畫面子系統(User Main Interface Subsystem, UMIS)、封包擷取子系統(Packet Capture Subsystem, PCS)、檔案管理子系統(File Management Subsystem, FMS)、封包監測子系統(Packet Monitor Subsystem, PMS)、封包產生子系統(Packet Generator Subsystem, PGS)、以及使用者輔助子系統(User Help Subsystem, UHS)。每個子系統的功能描述如下：

- 使用者主畫面子系統負責聯繫其他子系統，並顯示已擷取的封包清單與封包格式列表。
- 封包擷取子系統負責擷取、篩選封包的功能。
- 檔案管理子系統負責儲存、讀取、以及列印封包擷取子系統所擷取的封包。
- 封包監測子系統提供使用者封包擷取子系統所擷取的封包統計資料與圖表。
- 封包產生子系統提供使用者產生封包的功能。
- 使用者輔助子系統提供使用者 WPMAS 操作說明手冊以及中英文介面轉換的功能。

由於無線網路卡的晶片設計與驅動程式的限制，部分網路卡無法解析 802.11 無線網路封包標頭格式。因此 WPMAS 只支援特定的網路卡晶片與驅動程式。目前所知提供支援的網路卡晶片有 Prism 2 系列，如 Dark Marketing Corp. 所製造的 XI-325PCMCIA 網路卡[12]，其網路卡所使用的驅動程式為 The Linux pcmcia-cs Package 所提供[13]。

4. WPMAS 設計方式

WPMAS 包含了六個子系統，其中 PCS、FMS、UMIS 等三個子系統是 Ethereal 原有的功能，而 PMS、PGS、以及 UHS 是修改 Ethereal 的部分功能或新增的子系統。本章節除了 Ethereal 本身已經架構的子系統外，我們將詳細地描述 WPMAS 各個子系統的設計與運作流程，即 PMS、PGS、以及 UHS 子系統。

我們利用 C 與 C++程式語言在 Linux 上開發

WPMAS。開發 WPMAS 時需要三個函式庫的協助，即 Libnet、GDChart Library、以及 GTK+。我們修改並新增 Libnet 的部分函式以協助開發 PGS。GDChart Library 是用來協助開發 PMS。另外 GTK+是用來協助開發圖形化使用者介面。

4.1 PMS

PMS 包含四個元件，分別為封包統計圖表、協定分佈圖、過濾器與選擇協定設定。這些元件中，協定分佈圖、過濾器、選擇協定設定是 Ethereal 原有的功能，封包統計圖表是我們加以修改的元件。

我們主要使用三個函式來開發封包統計圖表，即我們新增的函式庫：Satistic_Graph()，以及 GDChart 所擁有的函式庫：GDC_out_pie() 和 GDC_out_graph()。

這裡用一個例子來說明 PMS 如何產生統計圖表。當使用者點選「Frame Type Statistic Graph」後，PMS 呼叫 Statistic_Graph()。Statistic_Graph()將呼叫 GDC_out_pie()產生所需的圓餅圖。當 PMS 完成所需的統計圖表後，再利用 GTK+所撰寫的視窗介面顯示於螢幕上。

4.2 PGS

我們主要使用 Packet_Lib 函式庫來開發 PGS。Packet_Lib 函式庫使用 Libnet 函式庫以及部分新增或修改過的 Libnet 函式庫來產生封包。使用者設定完各層封包的欄位並按下「Send Packet」按鈕後，Packet_Lib 函式庫將產生使用者所需的封包並經由使用者所選擇的網路卡傳送出去。

這裡用一個例子來說明 PGS 如何產生封包。當使用者填完各層的封包欄位並按下「Send Packet」按鈕後，PGS 從使用者圖形化介面擷取使用者的輸入值，並將其輸入值儲存至 WPMAS 所定義的變數，例如 wifi_packet、ipv6_packet、udp_packet，以及其他相關變數。PGS 隨後將這些變數傳遞至 Packet_Lib 中的 packet_create() 函式。最後 packet_create()根據所傳入的變數產生無線 IPv6 UDP 封包。

4.3 UHS

UHS 包含兩個元件，即中英文介面轉換以及 WPMAS 使用手冊。中英文介面轉換的功能讓使用者可選擇其熟悉的語言介面。另外，使用者可查閱 WPMAS 提供的使用手冊來操作 WPMAS。

這裡用一個例子說明 UHS 如何從英文介面選轉換至中文介面。當使用者選擇中文介面的選項後，WPMAS 將在/tmp/PMASv6.lang.conf 設定其環境變數。WPMAS 重新啟動後，WPMAS 檢查其環境變數，然後利用 menu.c 中的 switch_language()將英文介面轉換至中文介面。

5. WPMAS 系統評估

WPMAS 可於無線網路環境中完整執行擷取無線封包、產生封包、產生封包統計圖表、以及中英文介面轉換等功能。本章節分成三個小節分別介紹並評估這些功能的執行狀況，即產生封包、封包統計圖表、以及中英文介面轉換。擷取無線封包的功能為 Ethereal 原有的功能，本章節不加以描述。

本章節的測試環境為 CPU 是 Intel Centrino 1.4GHz、記憶體大小為 1GB，Linux 的版本是 Redhat 9.0，Kernal 版本是 2.5.13-8，無線網路卡為 Dark Marketing Corp.所製造的 XI-325 PCMCIA 無線網路卡。

5.1 產生封包

WPMAS 提供使用者產生封包的功能。如圖 6 所示，使用者可編輯 IEEE 802.11 無線封包標頭的各個欄位，例如訊框控制欄位(Frame Control)中的 Subtype、ToDS、以及 FromDS 等等欄位。除此之外，使用者也可編輯其他類型的封包標頭，例如資料連結層的 Ethernet 標頭、網路層的 IPv4 與 IPv6 標頭、以及傳輸層的 TCP 與 UDP 標頭。

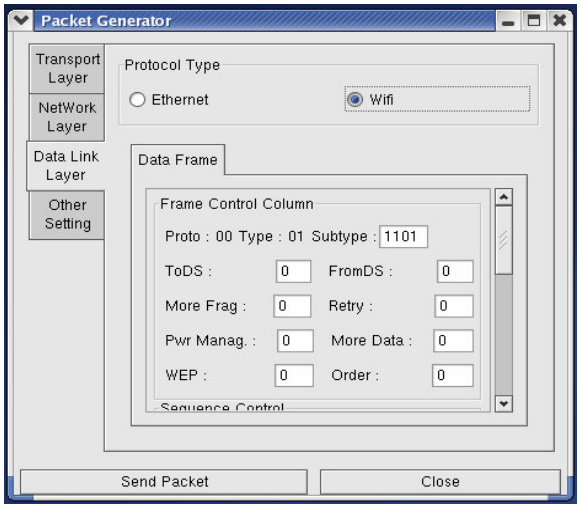

圖 6 封包產生器的 802.11 表頭設定介面

使用者可以設定封包傳送相關參數。如圖 7 所示，使用者可以設定單次封包傳送數量(Packet Amount Per Time)、封包傳送的間格(Packet Burst Interval)、以及封包傳送次數(Packet Burst Amount)。使用者也可指定網路卡傳送封包。

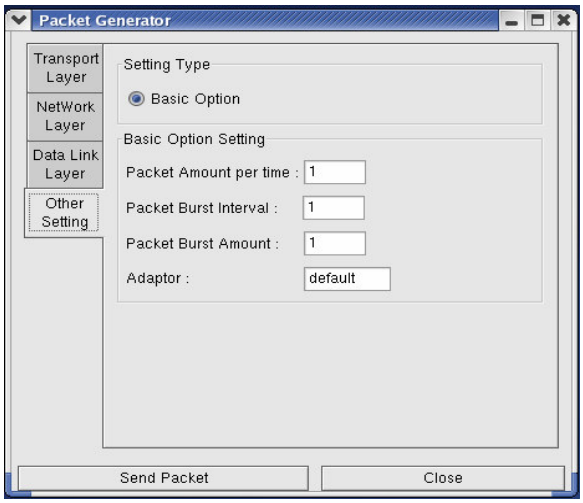

圖 7　封包產生器的其他參數設定介面

PGS 產生封包的速度約為每秒 30 個封包。比起坊間製造的硬體封包產生器的封包產生速度[14]，軟體所產生的封包速度較為緩慢。因此，提升封包產生速度即為此系統未來的改進工作之一。

5.2 產生封包統計圖表

WPMAS 提供使用者相關無線網路封包統計資料與圖表，包含無線網路訊框統計圖表、資料訊框(Data Frame)統計圖表、控制訊框(Control Frame)統計圖表、以及管理訊框(Management Frame) 統計圖表。

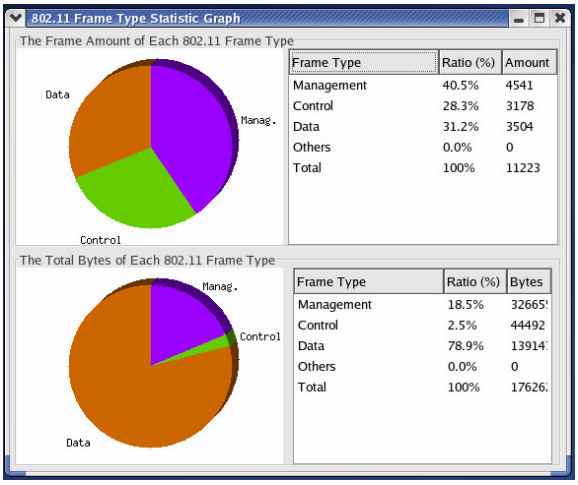

圖 8　無線網路訊框統計圖表

無線網路訊框統計圖表統計所擷取的封包中資料訊框、控制訊框、以及管理訊框等三類訊框所含的封包數量以及大小比例。如圖 8 所示，此統計圖表由兩個圓餅圖以及兩個表格所組成。上方圓餅圖與表格顯示三種無線網路訊框的封包數量與其比例。下方圓餅圖與表格顯示三種無線網路訊框的封包大小總量與其比例。

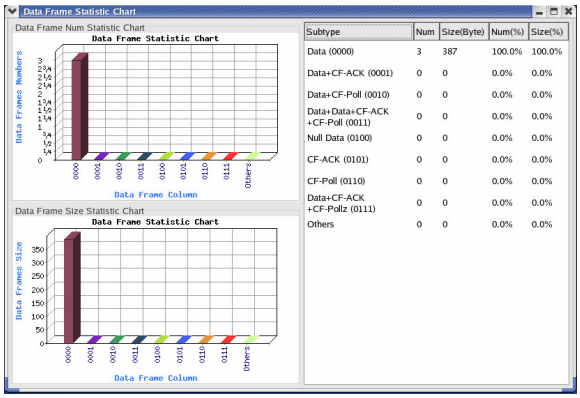

圖 9　無線網路資料訊框統計圖表

資料訊框統計圖表、控制訊框統計圖表、以及管理訊框統計圖表皆為統計其 Subtype 的封包數量以及大小比例。以圖 9 資料訊框統計圖表為例，此統計圖表由兩個長條圖以及一個表格所組成。左邊兩個長條圖分別顯示資料訊框中各個 Subtype 的封包數量以及大小總量。右邊表格則顯示各個 Subtype 的封包大小總量詳細數據與比例。

WPMAS 產生一種統計圖表的效能為一萬個封包的分析時間加上繪製圖表的時間共約需三秒。針對統計資料的效能，此系統的未來目標是縮減 20% 的資料處理時間。

5.3 中英文介面轉換

如圖 10 與圖 11 所示，WPMAS 提供使用者兩種語言介面，即中文介面與英文介面。使用者可藉由此功能選擇其熟悉的語言介面。

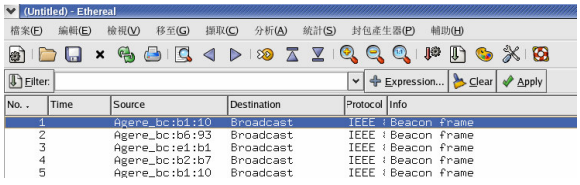

圖 10　WPMAS 中文介面

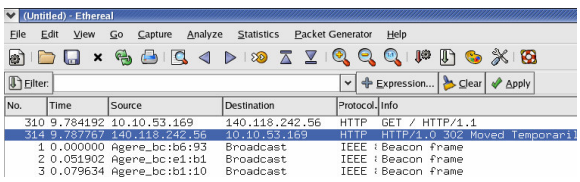

圖 11　WPMAS 英文介面

使用者切換介面語言後，必須重新啟動 WPMAS 才能生效。即時轉換介面語言是此系統未來要改進的目標之一。

6. 結論與未來展望

本篇論文描述一個無線網路封包監測與分析系統—WPMAS。此系統能擷取、分析、並產生802.11 無線網路封包。WPMAS 可協助使用者排除及處理網路問題。使用者也可藉由 WPMAS 學習無線網路封包的格式與運作方式。此外，WPMAS 也可讓欲發展無線軟硬體的廠商或研究人員針對其研發的軟硬體進行檢測與偵測。

WPMAS 主要的貢獻包含：

- 可產生 IEEE 802.11 通訊協定封包。
- 可針對 IEEE 802.11 通訊協定封包產生統計資料與圖表。
- 提供使用者中文與英文操作介面。

WPMAS 仍處於開發階段，許多方面的設計需持續地加強與改進。在封包產生子系統方面，產生封包的速度需要加快，另外也需添增更多封包表頭格式的支援。在使用者輔助子系統方面，轉換介面語言需立即的轉換而不必重新啟動系統。另外也希望未來能在 WPMAS 系統中新增破解無線封包 WEP 加密的功能，讓學習無線網路的學習者徹底瞭解無線網路的安全威脅。

致謝

本論文為行政院國家科學委員會之 NSC 94-2218-E-011-009、NSC 94-3114-P-001-001-Y、NSC 94-3114-P-011-001 研究計畫的部分研究成果。本論文承蒙行政院國家科學委員會補助，特此致謝。

參考文獻

[1] ANSI/IEEE Std 802.11, 1999 Edition.

[2] M. S. Gast, “802.11 Wireless Networks: The Definitive Guide”, O’REILLY Publisher April 2005.

[3] Wei-Ming Shi Lab, “Implementing Practice of Wireless”, Flag Publisher, July 2002.

[4] http://www.sniffer.com/

[5] http://www.networkview.com/

[6] http://www.sunrisetelecom.com/lansoftware/lanxplorer.shtml

[7] http://www.slackware.org.tw/

[8] http://www.ethereal.com/

[9] http://reptile.rug.ac.be/~coder/index.html

[10] http://www.wildpackets.com/

[11] http://www.kismetwireless.net/

[12] http://www.tw-wireless.com/

[13] http://pcmcia-cs.sourceforge.net/

[14] http://www.infinet.com.tw/product-1/Xtramus/