行政院國家科學委員會專題研究計畫 成果報告

異質無線多網安全檢測平台建置計畫(Ⅱ)
研究成果報告(完整版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 99-2219-E-009-013-
執 行 期 間 ：99 年 01 月 01 日至 99 年 12 月 31 日
執 行 單 位 ：國立交通大學資訊工程學系（所）

計 畫 主 持 人：謝續平
共 同 主 持 人：曾文貴
計畫參與人員：碩士級-專任助理人員：陳柏愷
碩士級-專任助理人員：陳柏廷
學士級-專任助理人員：郭明華
學士級-專任助理人員：林慧雯
學士級-專任助理人員：戴君珮
學士級-專任助理人員：謝政翰
碩士班研究生-兼任助理人員：邱世欣
碩士班研究生-兼任助理人員：黃佑鈞
碩士班研究生-兼任助理人員：黃博彥
碩士班研究生-兼任助理人員：林孟緯
碩士班研究生-兼任助理人員：許基傑
碩士班研究生-兼任助理人員：梁偉明
碩士班研究生-兼任助理人員：黃韋翔
碩士班研究生-兼任助理人員：許鴻生
碩士班研究生-兼任助理人員：葉書宏
碩士班研究生-兼任助理人員：籃日全
碩士班研究生-兼任助理人員：彭日伸
碩士班研究生-兼任助理人員：劉恩榜
碩士班研究生-兼任助理人員：周桂伊
碩士班研究生-兼任助理人員：羅日宏
碩士班研究生-兼任助理人員：巫祈賢
碩士班研究生-兼任助理人員：盧豔銘
碩士班研究生-兼任助理人員：鄭又銓

碩士班研究生-兼任助理人員：賴託登
碩士班研究生-兼任助理人員：廖政博
碩士班研究生-兼任助理人員：張家愷
碩士班研究生-兼任助理人員：梁喬峰
碩士班研究生-兼任助理人員：李忠霖
碩士班研究生-兼任助理人員：黃冠霖
碩士班研究生-兼任助理人員：朱慶峰
碩士班研究生-兼任助理人員：蘇修醇
碩士班研究生-兼任助理人員：石穎
講師級-兼任助理人員：吳育松
講師級-兼任助理人員：黃世昆
講師級-兼任助理人員：趙禧綠
講師級-兼任助理人員：黃育綸
博士班研究生-兼任助理人員：蔡欣宜
博士班研究生-兼任助理人員：沈宣佐
博士班研究生-兼任助理人員：林孝盈
博士班研究生-兼任助理人員：陳毅睿
博士班研究生-兼任助理人員：陳彥宇
博士班研究生-兼任助理人員：姜冠妍
博士班研究生-兼任助理人員：郭子綺
博士班研究生-兼任助理人員：何秉哲
博士班研究生-兼任助理人員：林佳純
博士班研究生-兼任助理人員：卓政逸

報 告 附 件 ：國外研究心得報告
出席國際會議研究心得報告及發表論文

處 理 方 式 ：本計畫可公開查詢

中 華 民 國 100 年 03 月 30 日

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

異質無線多網安全檢測平台建構計畫Ⅱ

計畫類別： □ 個別型計畫 ■整合型計畫
計畫編號：NSC 99-2219-E-009-013
執行期間： 2010 年 1 月 01 日至 2010 年 12 月 31 日
計畫主持人：謝續平
共同主持人：曾文貴
協同主持人：黃世昆、黃育綸、楊武、趙禧綠、吳育松、孫宏民

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
研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：國立交通大學資訊工程學系
資通安全研究與教學中心 TWISC@NCTU

中華民國 100 年 01 月 31 日

摘要

異質多網環境中由多種網路環境(包含有線網路、3.5G 行動通訊網路、Wi-Fi 與 WiMAX 無線區域網路等)以及多種使用者裝置(包括個人電腦、筆記型電腦、智慧型手機、PDA 及平板電腦等)所構成。異質多網通訊以及使用者裝置的技術普及提供了使用者許多的便利性，但同時也帶來許多安全性問題。許多政府機關(例如：國安局、中科院、教育部、經濟部等)、財團法人(例如：資策會、工研院等)、產業界(例如：友訊集團、明泰科技、中華電信、宏碁與微軟等)以及一般大眾都因為系統、網路、軟體的安全性問題以及人員安全意識的缺乏，而遭遇重大的財務以及機密資料的損失。由於目前市面上缺少完善且全面性的安全檢測的工具可供使用，為了檢測異質多網之下眾多的安全風險，本計畫開發了一異質多網安全檢測平台，其中包含四大類、總共 16 項軟體系統與工具。本計畫在 2009 年執行初期便邀請研考會、國家資通安全會報技術服務中心、工研院、資策會、國安局、中科院、中華電信、友訊科技、明泰科技、宏碁科技等單位共同協助規劃合作。在 2010 年，我們持續與中華電信、友訊科技、工研院、資策會、中科院共同合作開發多種安全檢測工具。目前此平台可分成四大檢測類別：網路安全檢測、系統安全檢測、軟體安全檢測以及人員安全意識檢測。在 2009 年至 2010 年計畫執行期間，我們開發並建置總共 16 個檢測工具,1 個異質多網擬真模擬平台,用以檢測異質多網環境下的系統、網路、軟體的安全性以及人員的安全意識。此外，本計畫在 2010 年也有豐碩的論文研究成果，我們發表於國際期刊之論文共有 7 篇，發表於國際研討會之論文數共 5 篇以及國內研討會之論文共 4 篇。在專利方面，我們各別有 3 件國外以及國內專利申請。另外，我們在技術服務與產學合作方面的成果包括技術服務共 3 件，產學合作共 7 件，合計總金額達 702.8 萬，其中虛擬機器惡意程式偵測工具，著重於惡意程式偵搜技術，進而分析其行為，其成果技轉中華電信，經中華電信實際網路線上分析，找到兩大類型無法由防毒公司軟體偵測的新型變形惡意程式，另外本中心也已經接受國安會、經濟部委託承接，交付本中心可疑軟體程式，分析與偵測對特定對象攻擊的惡意程式（防毒軟體無法偵測與分析）。調查局也與本中心簽訂合約，2011 年起將使用本中心開發的工具進行電腦犯罪數位鑑識。叡揚資訊公司也與本中心將從 2011 年起合作，轉移兩項技術：文件檔案夾藏惡意程式分析，敲健行為身份認證。此次技術移轉，叡揚資訊公司擬將用於檢測與提升政府機關、企業網路安全。另外，本中心也協助行政院科顧組與教育部提升 Critical Information Infrastructure Protection（CIIP）相關工作，經由 DNSSEC 未來的建立，CIIP 的安全將可大幅提昇。

本計劃在 2010 年開始提供的線上安全檢測的服務，目前已超越 15 萬使用人次，對象包含各教育機構(例如台灣大學、清華大學、中央大學、成功大學、中山大學、交通大學...等)、政府或研究機構(如行政院研考會、中研院、資策會、國家資通安全會報技服中心、法務部調查局...等)、以及海外連線(如北京清華大學、河南師範大學、中國科學技術大學...等)，隨著本服務規模的擴大，預計未來將有更多人可因而受惠。藉由此平台的建置與檢測工具的開發，我們可提供政府機關、財團法人及高科技廠商在系統安全、網路安全、軟體安全檢測以及人員安全意識檢測的服務，幫助上述單位發現安全漏洞、弱點以及提高內部人員安全意識。

感謝網路通訊國家型計畫辦公室與委員評定本計畫「異質無線多網安全檢測平台建置計畫」2010 年成果傑出，評選為優良研究計畫。

關鍵字: 異質多網安全檢測平台、系統安全檢測、網路安全檢測、軟體安全檢測、人員安全意識檢測

Abstract

Internet is a heterogeneous network consisting of various network environments and computer devices. The heterogenous network may includes wired networks, 3.5G mobile networks, Wi-Fi and WiMAX wireless networks. On ther other hands, computer devices may include personal computers, laptop computers, smartphones, netbooks, tablet PCs. Although mobile computer devices provide convenience and efficiency to both work and social life, it also introduces new information security problems. Many government agencies (for example, National Security Bureau, Chung-Shan Institute of Science & Technology, Ministry of Education, etc), research institutes (for example, Institute for Information Industry, Industrial Technology Research Institute, etc), private sectors (for example, D-Link, Alpha Networks, Chunghwa Telecom, Acer, Microsoft, etc) and general public may have experienced system compromise or privacy breach despite of lack of system, network and software security awareness. Since the current commercial tools failed to provide sufficient security test and analysis, this project is aimed to study and develop a heterogeneous networks penetration testing platform to provide such functionalities. The security test services provided by the developed platform cover four main categories; they are network penetration tests, system penetration tests, software security tests, and user security awareness tests. In the year 2009 to 2010, we have successfully developed 16 security test tools that fall into the four main categories. We have also published numerous publications including 7 international journal papers, 5 international conference papers, and 4 national conference papers. We have also submitted applications for 3 international and 2 national patents that are currently under review. As for industrial cooperation and services, we have successfully provided three information security inspection services and established 7 corporation joint research works. The cooperation and services have generated 7 millions of dollars to the account. In the year 2010, we started an online security test service on TWISC@NCTU website. Up to current date, the service website has over 150 thousands website visit counts. Using the developed platforms and tools, we thrive to provide various information security inspection services to government agencies, corporations, and technology based private corporations.

Keywords: heterogeneous networks penetration testing platform, network penetration tests, system penetration tests, software security tests, user security awareness tests

一、 背景

以下將針對本計畫之背景，分成國內需求現況、異質多網安全議題二大部份來分別介紹。

◆ 國內需求現況

現今通訊設備日新月異，各大廠商紛紛推出各式各樣的行動通訊設備、網路硬體設備以及相關應用軟體，以提供使用者更多的功能及便利性。然而伴隨著這些便利性的是隱藏在其後的安全弱點，許多駭客利用這些弱點以及更有威脅性的攻擊技術來策動攻擊或者竊取使用者的資料。對於政府機關(例如：國安局、中科院、教育部等)而言，需要完善的工具來檢測所處的異質多網環境下的安全性。對於財團法人(例如：資策會、工研院等)而言，需要適合的檢測工具可用以檢測所使用的軟體的安全性。對於產業界(例如：友訊集團、明泰科技、中華電信、宏碁與微軟等)而言，則需要完整的檢測工具可以檢測他們所開發的軟體是否存在安全漏洞。而對於廣大的一般大眾而言，經常因為系統、網路、軟體的安全知識不足以及安全意識的缺乏，導致機密資料的外洩及財務上的損失。然而目前市面上並沒有完整及合適的安全檢測工具可以提供檢測服務給上述單位及人員。為了檢測異質多網之下眾多的安全風險，本計畫開發與建置了一異質多網安全檢測平台。本平台提供全方面的安全檢測服務，包括四大檢測類別：系統安全檢測、網路安全檢測、軟體安全檢測以及人員安全意識檢測。在系統安全檢測方面，包含了遠端系統安全漏洞的檢測及網站伺服器的安全漏洞的檢測。在網路安全檢測方面，包含了應用於 WiMAX 的弱點掃描系統以及 Wi-Fi 無線網路金鑰的強度檢測等。在軟體安全檢測方面，包含了目前行動裝置經常使用的 Android 作業系統及 Java 應用軟體的檢測，以及病毒與惡意程式的檢測。在人員安全意識檢測方面，包含了檢驗一般使用者安全意識的網路釣魚檢測及無線網路安全意識檢測。藉由此檢測平台，我們希望提供全面性安全檢測。

◆ 異質多網安全議題

請就異質多網下系統安全、網路安全、軟體安全以及人員安全意識問題來介紹相關的安全議題。

■ 系統安全議題

在網際網路尚未普及的時候，系統安全上最大的敵人就是電腦病毒，電腦病毒破壞使用者電腦，使其不能正常使用或者毀損使用者的個人資料，當時的系統安全，都還在防毒軟體掃毒的階段。伴隨著網際網路的發展與異質多網的演進，使用者的網路環境越來越多樣化，除了傳統有線網路外，尚有 Wi-Fi、3G/3.5G 與 WiMax 等無線行動網路，上網的配備也從傳統的個人電腦、筆記型電腦，進化到現在的輕薄型小筆電、PDA 與智慧型手機。系統安全上的考量必須全面化，除了以往的電腦病毒惡意程式之外，還必須考量到網路所帶來的影響，透過網際網路跨越距離的限制，也讓惡意攻擊者頓時有了無限多的攻擊對象。驅動程式、作業系統、系統程式與應用軟體上的漏洞也被利用來攻擊使用者的電腦系統。使用者必須隨時注意是否有新的漏洞修正更新釋

出，並且即時地安裝這些更新，以防止這些漏洞被攻擊者利用。所謂的 0-day attack(零時差攻擊)，便是利用漏洞修正更新檔釋出時，使用者尚未更新系統前，從更新檔解析出漏洞所在和攻擊手法，並對使用者進行攻擊的手法。除了系統漏洞外，錯誤的系統設定也會造成安全上的危機，即時有再安全的保護機制，沒有正確地設定執行，依然是事倍功半。另一方面，現在流行的手機軟體下載服務，例如 Windows Mobile 的 MarketPlace、Android 的 Android Market、蘋果的 App Store，提供手機軟體販售交流的平台，但也成為惡意程式傳播的手段之一；前一陣子蘋果 App Store 才緊急下架了一套內含惡意程式的手機軟體。系統安全上常見的攻擊大致可分為以下幾類：

◆ 電腦病毒惡意程式

電腦病毒惡意程式經常透過偽裝的方式進行感染散播的目的。這類型的攻擊手法隱藏自己是電腦病毒或是惡意程式的事實，企圖讓使用者執行他所開啟下載的應用程式或是附加檔案，藉此達到感染使用者電腦的目的。此時被感染電腦本身可能被植入後門程式，供惡意攻擊者利用，成為網路上的殭屍電腦，對他人進行 DDOS(Distributed Denial of Service)等進階攻擊，抑或是單純地被植入病毒，再利用檔案共享、即時通訊、電子郵件等方式伺機傳染下一位受害者。使用者可以利用防毒軟體防止已知的電腦病毒及惡意程式入侵，但是對於未知的電腦病毒惡意程式，只能採取觀察監控的方式判斷是否有可能是電腦病毒惡意程式，在影響到使用者系統正常運作前使用者通常不會發現電腦病毒惡意程式的存在。

◆ 系統漏洞錯誤設定

利用使用者系統本身的弱點進行攻擊。攻擊者針對特定的系統或是軟體漏洞，嘗試潛入使用者電腦，跳過身分驗證，取得操作權限，像是開啟 Remote Shell，甚至進一步地獲得管理者權限。這一類的攻擊，攻擊者通常自行尋找系統漏洞，或是利用官方釋出的漏洞修正更新進行逆向工程來發掘漏洞。零時差攻擊便是利用漏洞修正剛釋出，而使用者尚未及時更新時所進行的攻擊行為。攻擊與防護就像時間上的競賽，而不適當的系統設定，亦是攻擊者可利用的弱點，使用者往往做好了各種的安全保護機制，卻因為錯誤的設定，造成系統的漏洞。使用者可以利用弱點掃描工具來尋找系統上的漏洞以及不恰當的系統組態；但是同樣地，對於未知的系統漏洞，弱點掃描就無法發揮作用了。

■ **網路安全議題**

現今常見的網路安全威脅包括連線劫持(Session Hijacking)、網路掃瞄(Network Scan)與阻斷服務攻擊(DoS)/分散式阻斷服務攻擊(DDoS)等。

◆ 連線劫持(Session Hijacking)

在使用者與遠端連線建立之初，假若攻擊者成功居中偽裝成遠端與使用者雙方，則可成功完成連線劫持的動作。通常這類攻擊又被稱為

Man-in-the-middle-attack。攻擊者藉由竊聽雙方的封包，取得兩者溝通過程中的所有資訊。因為是利用竊聽的技術，所以使用者與其遠端通訊對象並不會出現溝通資訊受到改變的異樣，所以通常使用者很難察覺自己正遭受此種攻擊。

◆ 網路掃瞄(Network Scan)

現行網路上已有許多軟體如: nmap, ipsecscan, SuperScan, Angry IP…等掃描主機程式可對遠端主機進行一系列的系統弱點偵測。利用 ping 或是 telnet 等簡易指令方式也可輕易探查出遠端主機的作業系統類型。透過此類的掃描手法也可以找出目前遠端主機存在的漏洞，並依此對其進行攻擊。

◆ 阻斷服務攻擊/分散式阻斷服務攻擊(DoS/DDoS)

阻斷服務攻擊/分散式阻斷服務攻擊是網路安全裡最常見的安全議題之一。阻斷服務攻擊企圖癱瘓企業的防火牆或是大型網站的網路連線，造成一般使用者無法正常存取其所提供的網路服務。阻斷服務的攻擊手法也不斷地推陳出新，從傳統的 Ping of Death、Syn Flood。現在的駭客更進一步結合殭屍網路(Botnet)來發動大規模的分散式阻斷服務攻擊(DDoS)來攻擊擁有大量硬體資源的伺服器。

另外在 Wi-Fi 無線網路方面，資料傳輸方式有明文(無任何加密機制)傳輸或是利用 WEP 或 WPA 加密認證機制來加密傳遞的資料。針對這一些的傳輸方式目前常見的無線網路威脅包括網路釣魚攻擊(Phishing attack)、中間人攻擊(Man-in-the-middle-attack)、Evil Twin、Key Crack 等等。

◆ 網路釣魚攻擊(Phishing attack)

透過郵件、訊息或是其他方式留下網頁連結，誘導使用者連上惡意網頁。攻擊者可能發出一封來自銀行的信件，因為信件上的特定內容誘使使用者連上該連結，該連結可能含有惡意的語法盜取使用者私密資料或是誘導使用者填上該銀行的帳號密碼，因而導致帳號密碼流出。

◆ 中間人攻擊(Man-in-the-middle-attack)

攻擊者可能偽裝成訊息中繼傳輸者的角色，竊取使用者連上網路之後的任何資訊。一般使用者無法決定或是確定自己訊息的傳輸路由方式，以無線網路方式為例，通常使用者使用該區域的無線網路時只能確定可不可以用，但卻無法辨別無線基地台是否為惡意攻擊者所擁有。攻擊者可藉由偽造基地台或是架設惡意基地台協助使用者連上網路，卻在網路資訊傳遞過程中擔任竊聽者的角色，輕而易舉地得知使用者在網路上一舉一動，屆時涉及隱私相關的個人資料，諸如個人信箱、銀行帳戶密碼皆有可能遭到竊取。

◆ 加密方式存在漏洞

目前無線網路加密方式通常採用 WEP 以及 WPA 方式兩種，但已有研究指出，

WEP 金鑰可以在很短的時間之內被破解；而 WPA 則是有可能被攻擊者使用字典攻擊法破解，這將使得使用者傳輸的資料安全性受到嚴重的威脅。

◆ 無線網路硬體上的缺陷

利用 802.11 直接序列展頻(direct-sequence spread spectrum, DSSS)協定的漏洞，雖然不能截擊或修改封包資料，但是卻可以對資料封包傳送的可靠度(reliability)造成威脅，使得在範圍內的使用者無法正常使用線上資源或是溝通訊息。

■ 軟體安全議題

軟體安全一直是很重要的議題。即使是來自全球各地的無數專業程式設計者所開發出來的 Windows 系列作業系統，仍存在許多安全性漏洞。而近兩年來，智慧型手機逐漸取代傳統手機的市場。Android 與 Apple iOS 是大部分智慧型手機所使用的作業系統，也都是屬於 Unix-like 作業系統。由此可見，Unix-like 作業系統已經開始從 15 億個 PC 使用者市場轉移到 35 億個手機使用者的市場。這雖然造就了一個龐大的行動平台，但也很可能把過去 Unix-like 擁有的弱點帶到 SmartPhone 平台來。所以智慧型手機平台的安全議題也必須關注的，否則將直接影響大量的智慧型手機使用者。

圖 1- 1 顯示 National Vulnerability Database 最近十年(2001 年 1 月 ~ 2010 年 11 月)的 Vulnerability 統計，在 2010 年 1 月至 11 月就有多達 4280 個漏洞被發佈。

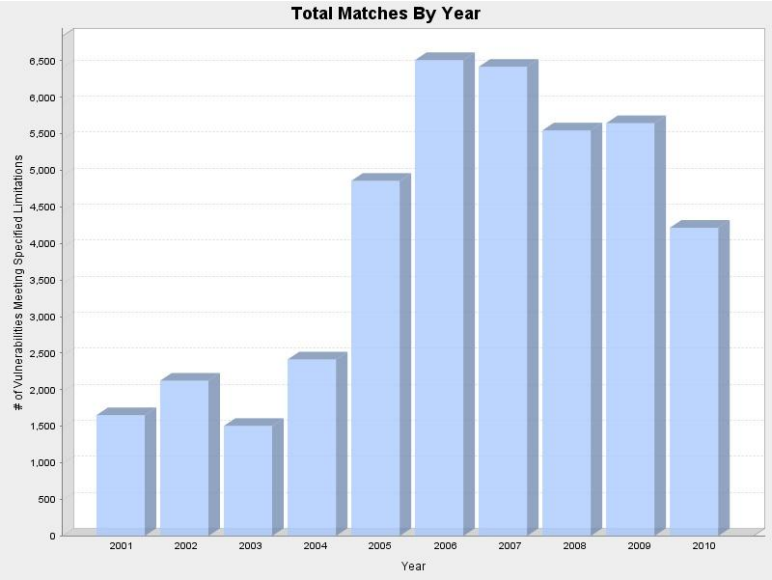


圖 1- 1、Vulnerability statistics (2001 年 1 月至 2010 年 11 月)from National Vulnerability Database

然而，程式漏洞有成千上萬種，在軟體方面的安全性漏洞大致可分為以下類型：

- Memory safety violations
- Input validation errors
- Race conditions
- Privilegeconfusion bugs
- Privilege escalation
- User interface failures

舉例來說,在 Memory safety violations 中,最常見的攻擊方式為 Buffer overflows。駭客可以利用這個漏洞，使得 buffer 的寫入超出原本的長度限制，輕易的控制電腦中的記憶體位置及資料，進而獲得作業系統的 root 權限。Input validation errors 類別中包含了在 Web 應用程式中很常見的 SQL injection 攻擊方式，在輸入的字串中夾帶惡意的 SQL(Structured Query Language)指令，讓資料庫伺服器誤認為是正常的 SQL 指令而執行，造成資料庫資料的外洩。以上各式各樣的漏洞，大部份來自於程式設計者在撰寫程式碼時的不注意、疏忽所產生的，也對整個系統造成了安全性的威脅。

■ 人員安全意識議題

所謂「道高一尺、魔高一丈」，只要有使用電腦或網路的一天，入侵事件便不可能消失殆盡。近年來，伴隨著資訊技術起飛，網路安全、資訊維護等觀念也逐漸崛起。除了透過防毒軟體、防火牆系統等機制的防護之外，操作人員的安全意識更是維護資訊安全的重要一環。因此，如何透過有效地檢測系統操作人員的安全意識便成為資安訓練、系統防護的重要議題之一。檢測人員安全意識的方法有很多種，主要就是透過各種形式的釣魚程式，讓人員在有意識或無意識地下載惡意程式或攻擊碼，並利用由內而外的檢測方式，讓系統管理人員了解機構或單位內部的人員安全意識。以下簡介數種常用於人員安全意識檢測的方法：

◆ 網路釣魚

網路釣魚者（Fisher）傳送含有釣魚網站鏈結的電子郵件給使用者，誘騙使用者連線到該釣魚網站，並輸入個人隱私資料（如身份證號碼、銀行帳號及信用卡號碼等等）。網路釣魚者也可能冒充使用者的朋友在熱門留言板上張貼偽造的服務網頁，誘騙使用者登入該偽造服務網頁。當使用者瀏覽該留言板並登入該偽造服務網頁後，網路釣魚者便讓使用者登出系統，使用者在誤以為被系統偶發性地錯誤登出後，可能會立即輸入帳號密碼，欲重新登入該系統。此時，網路釣魚者便可以透過該偽造網頁程式碼得到某使用者的登入資料，除了在社群網路服務中，對使用者的朋友行使更多詐騙手法外，亦可能利用所盜用的資料，謀取更多不法的利益。

◆ 垃圾郵件

為了避免好友寄送過來的郵件被郵件伺服器的過濾器視為垃圾郵件，使用者通常會將好友的電子郵件地址設為白名單。在此情況下，如果垃圾郵件發送者利用使用者好友的電子郵件做為偽造郵件之發送地址，所送出的垃圾郵件就可能獲得更多的信任，甚至可以騙過垃圾郵件過濾器。有時候，郵件發送者會在郵件的主題或內容中加入使用者好友的姓名或暱稱，即使該郵件已被郵件過濾器判定為垃圾郵件，使用者仍可能會開啟此郵件。如此，這類郵件仍可能對使用者造成困擾，也可能進一步地對整個網路系統造成資源浪費與系統破壞等行為。

◆ 網路攻擊

在偷渡式下載 (Drive-by-Downloads) 越來越風行的趨勢下，網路攻擊者逐漸傾向鎖定一般使用者作為其攻擊目標，企圖誘騙一般使用者下載惡意軟體或誘騙一般使用者洩漏其個資。由於社交服務與電腦上所安裝之作業系統和瀏覽器軟體

並無相關性，此類攻擊所鎖定的目標主要是實際的使用者，而非機器本身的安全漏洞。因此，「人員安全意識」成了這類攻擊的最後把關者；這也是為什麼這幾年「人員安全意識」檢測與訓練逐漸成為各機關單位重視的議題之一。

二、 相關研究

以下將針對各研究範疇，介紹目前國內外相關研究。

■ **系統安全議題**

弱點掃描與滲透測試是常見用來評估系統的安全程度的方式。常見的弱點掃描軟體有 Nessus [1]、Acunetix Web Vulnerability Scanner [2]等。在弱點攻擊方面的工具則有 SAINTexploit [3]、Metasploit [4]、CORE IMPACT[5]等。

Metasploit 是一套已經發展多年的滲透工具，提供攻擊函式庫及攻擊封包，可以滲透系統，取得系統權限，但 Metasploit 並沒有實現滲透測試自動化，測試者需先藉由 Nmap 和 Nessus 等埠掃描和弱點偵測軟體找出連接埠和弱點，再自行由 Metasploit 攻擊函式庫裡找出適用的攻擊程式。CORE IMPACT 是一套商用滲透測試工具，它提供一個具擴充性的滲透測試框架。CORE IMPACT 的主要滲透測試手法是利用受害主機的弱點滲入主機，接著植入一個代理程式，代理程式除了會掃描其他自身的弱點和發動網路攻擊，它也會啟動自動掃描，尋找網路系統中的下一個可能受害主機。另外，國內外學者對於系統安全、弱點掃描、滲透測試也有相關的研究成果 [6,7,8,9,10,11] 。滲透測試的過程由一連串的測試步驟、搭配不同的軟體與滲透路徑、分析方法組合而成，以對大型企業的實體網路進行滲透測試為例，滲透測試者可利用常見的 SQL injection 攻擊或是 DoS 攻擊等手法對企業的對外網路服務，進行攻擊演練，找出潛在漏洞和攻擊路徑。我們以資訊量最少的黑箱測試為例，將滲透測試可分為探測、弱點掃描與弱點攻擊、結果分析等四大步驟[15]。

◆ 探測

探測的目的在於收集以及偵查受測者的環境與背景，例如網路拓撲、受測主機的作業系統(OS)等等。常見的探測軟體為通訊埠掃描軟體 Nmap [16]，檢測者能透過不同的參數設定，得到不同的受測者資訊，諸如受測者的作業系統、開啟的通訊埠、防火牆的通訊埠過濾規則、正在提供的網路服務等。

◆ 弱點掃描

在了解受測者的背景之後，滲透測試者會根據得到的受測者背景資訊，諸如開啟的通訊埠與使用中的網路服務、使用的軟體版本等資訊，進行更進一步的弱點掃描來確認受測者所開啟的服務中是否存在進行攻擊的管道。常見的弱點掃描軟體有 Nessus、SAINTexploit、Acunetix Web Vulnerability Scanner [2]等。Nessus 為一廣泛使用的弱點掃描軟體，它能針對目標主機或網路安全弱點產生評估報告，提供滲透測試者目標主機的安全弱點與安全漏洞等訊息，並提供相關之說明連結等。SAINTexploit 是 SAINT 公司所開發的一套網路系統潛在安全漏洞的搜尋工

具，它可以用於找出攻擊者可能入侵網路的漏洞並且計算網路風險值。

◆ 弱點攻擊

此步驟對掃瞄出來的弱點進行滲透攻擊，嘗試進入目標網路或是取得目標主機的 root 權限。弱點攻擊常用的工具有 Metasploit、CORE IMPACT 等。Metasploit 是一套已經發展多年的滲透工具，提供完整且不斷更新的攻擊函式庫及攻擊封包，滲透測試者可藉由 Nmap 和 Nessus 等埠掃描和弱點偵測軟體找出的連接埠和弱點，從攻擊函式庫中選取適用的攻擊程式進行攻擊。CORE IMPACT 是一套商用滲透測試工具，它提供一個具擴充性的滲透測試框架。CORE IMPACT 通常先針對一台主機的弱點進行滲透攻擊，接著在被破解的主機中植入一個代理程式。代理程式除了會持續掃描被破解的主機中是否存在其他的弱點外，也會啟動自動掃描，嘗試從目標網路的內部尋找網路系統中的下一個可能受害主機，並發動滲透攻擊。

◆ 結果分析

完成上述的步驟後，測試者可依據掃描和攻擊測試結果，完成一份全面性的整合測試報告，說明目標網路或系統中存在的弱點、攻擊者可能的攻擊路徑與手段，以及攻擊成功後，受測主機可能遭受的損害。測試報告也會包含對受測者的補強建議，加強受測機器的安全性和強健度，使有心人士無法針對漏洞有機可乘。

雖然目前的滲透測試多半是針對實體網路主機進行安全檢測，但是隨著行動網路的蓬勃發展，透過 Wi-Fi 或是 3.5G 上網的行動裝置也逐漸成為駭客潛在的攻擊目標。

在系統組態設定檢測方面，微軟的 Baseline Security Analyzer 可以用來偵測 Windows 系統本身的一些組態問題：Incomplete Updates, Password Expiration, File System。以這些例子來說，他們多半針對特定的系統（如防火牆或 Windows），且多半只關注該系統本體。以微軟 Baseline Security Analyzer 來說，其並沒有考量到安裝於 Windows 上面的應用程式相關的組態設定問題。在偵測技巧上，這些現存系統多半可以透過對個別系統所特別打造的偵測法則來檢查系統組態是否有問題。好處是或可很迅速準確地抓出所關心的問題，壞處則是無法應用到不同的系統甚至是同系列系統的新版本。

■ 軟體安全議題

軟體錯誤的產生原因大多來自於程式設計者對於程式流程的失控，且發現錯誤發生時往往不易經由人工方式分析出真正的原因，因此我們需要工具程式來協助分析錯誤點。另外假若軟體錯誤可被利用，這些錯誤就很有可能被轉化為安全弱點。早期的軟體安全測試方式是經由隨機方式產生的測試資料輸入給軟體，並分析軟體的執行狀況。近年來，軟體檢測的方式逐漸有系統化，國內外研究範疇大致上可分為兩大類:

◆ 靜態分析(Static Analysis)

靜態測試是對軟體程式碼作靜態程式碼分析(static code analysis)，檢驗程式碼中是否有錯誤或可能被攻擊的弱點存在，而不需要測試人員的幫助就能作自動化的測試。然而，靜態測試的缺點就是誤判率(false positive, or false alarm)過高。因為靜態分析程式碼沒有實際執行，因此無法保證找到的程式錯誤是真正的錯誤。因此，靜態分析的結果需要靠測試人員進一步檢查才能確定是誤判或是真實的錯誤，但誤判的比例通常不小，使得在測試軟體上的人力花費仍是不少，相關研究工具有 Findbugs、PMD 等等。

◆ 動態測試(Dynamic Analysis)

動態測試與靜態測試最大的不同在於利用實際執行程式來確定是否會引發程式的錯誤。因為實際執行的關係，只要是在執行時期碰到的錯誤很明顯都是真正的錯誤，不會再有誤判的問題。不過要實際執行一個程式會遇到另一個關鍵的問題，即如何提供這程式所需要的輸入，例如函式的參數或標準輸入等。最簡單的方式是亂數產生輸入給程式的測試資料，這樣的工具稱 Fuzzer。因為是亂數產生程式的輸入，Fuzzer 很容易產生一堆輸入資料給受測程式，有一定的機率讓程式行為異常。Fuzzer 把受測程式視為黑盒子，只了解程式的輸入輸出，對其內部結構完全沒有分析，所以測試的範圍無法涵蓋所有程式的路徑，沒辦法測到需要特殊條件的路徑或結構，相關研究有 jCute[4][5]、java path finder[3]等等。

目前已有一種結合靜態測試與動態測試的方法被提出，此方法為 concolic testing[6][7]，此法一方面利用 symbolic execution[8]對所有被程式輸入影響到的變數作符號分析(symbolic analysis)，以解決產生輸入的問題；另一方面用 concrete execution 確定目前輸入所引導的程式執行路徑，來避免誤判率高的缺點。Conclic testing 結合靜態與動態分析以達到優缺點互補的效果，近年來的研究顯示這個方法比起傳統的測試方法有很大的改善，而且已被應用在系統核心的測試以及多線程(multi-thread)的軟體測試上。

另一方面，惡意攻擊者會蓄意利用軟體設計錯誤的漏洞設計出相對應的惡意軟體進行系統攻擊。現行對於惡意軟體檢測的防毒軟體(如:kaspersky[1]，Norton[2])多是利用病毒特徵碼進行惡意軟體判定。惡意軟體為了隱藏自己的存在，不被防毒軟體偵測，因此常透過加殼的方式來打亂程式特徵碼，逃過 bit/byte 特徵碼比對追蹤。只有在程式執行的過程中，惡意軟體才會依序將程式解譯出來並寫入記憶體執行。因此在執行前，是無法透過特徵碼檢驗的方式發現此類惡意程式。目前已有許多研究希望能夠以自動化的方式解譯惡意程序正確執行順序的方法。不過目前為止，除了特定已知的加殼方式之外，無一方法可針對特殊加殼的方式進行解譯。由於執行任何程式之前，必須先將該程式載到記憶體中才能執行，惡意程式當然也不例外。因此在 Renovo[9]的方法中提出，使用模擬環境，讓目標程式在模擬系統上執行，並監控所有進行記憶體寫入與程式執行流程變更的指令。此外，開闢一塊虛擬的記憶體區塊，標記程式執行

過程新寫入記憶體的程式碼，最後將這些程式碼依序複製出來，以取回程式碼執行的正確順序，便能對程式碼進行特徵碼比對。

■ 人員安全意識議題

昂貴的資訊安全設備並未讓資安事件從此在企業網路銷聲匿跡。在技術到位之後，系統的管理與人員安全意識的訓練才是防守企業網路安全最重要的關鍵。當「政策」與「人」無法配合資安設備的情況下 (如缺乏妥善的監控、高警覺性、錯誤的設定、弱密碼的使用等等)，即使採購昂貴的資安設備，仍可能讓企業或組織的網路系統產生很大的安全漏洞。被破解的管理者密碼、維修後忘記關閉已開放的權限、分享的網路資料夾等意識盲點，為駭客及病毒開啟了許多漏洞與後門。在企業的資安議題上，「人員安全意識」與「系統管理問題」已經逐漸取代「技術問題」，成為防護企業資安的最後關卡。唯有妥善的管理，才能降低風險，避免不必要的損失，並能持續企業的營運，積極地掌握每一個商機。以下，本計畫之研究人員將針對人員安全意識之研究範疇，探討國內外相關研究：

◆ 網路釣魚

在網路釣魚攻擊猖獗的今日，教育使用者網路釣魚攻擊相關的知識與觀念是相當重要的。使用者愈了解網路釣魚技術與手法，愈能避開被攻擊的危險。因此，Anti-Phishing Phil [10]透過一個互動式的遊戲設計，教育使用者如何辨別釣魚網址，以避免將來誤入釣魚者陷阱的危險。Kumaraguru et al. [11]設計一系列的教材，藉由各種研究分析，讓使用者學習網路釣魚的知識與觀念，並能識破各種網路釣魚攻擊，以保護其機關單位的網路安全。除了基本的釣魚知識外，研究學者亦投注心力於研究各種網路釣魚攻擊的偵測，例如，藉由分析 URL 來偵測暗藏於釣魚郵件中的以各種形式（如 URL Obfuscation [12]等方法）隱藏的惡意超鏈結，以免使用者誤入釣魚陷阱。另外，Blacklist Generator [13]建議以建立釣魚網站黑名單的方式，讓使用者參考適時更新的釣魚網站黑名單，並有效地避開釣魚陷阱。除此之外，本計劃研究人員亦研究各種不同的釣魚攻擊手法，例如利用 Pharming Attack 的方式，竄改 DNS 紀錄，以達到釣魚攻擊的目的；或利用 Dynamic Pharming Attack [14]等新型攻擊方式，攔截 DNS 資訊，並將惡意的 Javascript 傳到受害者的瀏覽器，再利用 DNS 的弱點，於使用者身分認證完成之後，繼續攔截其通訊內容，如此，不論受害系統使用哪種身分認證機制，這類釣魚攻擊都可以成功。

◆ 垃圾郵件

垃圾郵件的大量寄發常會造成頻寬耗損、儲存資源濫用，並進而導致嚴重的經濟損耗問題。一般來說，垃圾郵件製造者 (Spammer) 常會透過殭屍網路 (Botnet) [15]中因受到入侵攻擊而被外人利用來犯罪的殭屍電腦 (bot) 來發送垃圾郵件。病毒郵件的發送與傳播則又會感染更多的電腦，讓殭屍網路逐步擴大，如此惡性循環，使得完全抑止垃圾郵件來源發信幾乎是不可能的事。為了杜絕這些垃圾郵件所造成的資源耗損，垃圾郵件的防治、分析、分類、過濾與阻擋等已經成了近幾年網路技術快速發展下的重要研究議題之一。垃圾郵件的辨識機制主要分為兩類：身份驗證和內容分析。

- 身分驗證是利用已知的資訊來驗證信件來源，如果信件來源條件不符合使用者設定之規則，則將其視為垃圾郵件，並阻擋之，相關技術如

黑名單[18][19][20]、白名單、灰名單、SPF 等。由於身分驗證機制只是做簡單的資訊比對，處理時間較短，但也因為資訊不足、名單太久未更新名單等因素，造成誤判率過高[16] (如 false positive：正常訊息被誤判為垃圾郵件；false negative：因資訊不足，而無法判斷出垃圾郵件) 。

- 內容分析是透過各種特徵以及規則，分析郵件本文後，再評估其是否為垃圾郵件。一套完善的內容分析機制能夠有效的鑑別垃圾郵件，如 Spamassassin[17]。內容分析對垃圾郵件具有高度辨識率，但由於分析規則繁瑣、處理時間較長，容易影響郵件系統的整體運作效能。為了改善內容分析的效能，許多學者也開始著手研究以郵件日誌為基礎的內容分析技術,希望藉由日誌檔上提供的郵件收送資訊以及系統訊息,達到辨識郵件內容的目的。基於日誌檔的分析技術可減低分析郵件的時間成本，並可避免收信者的隱私外洩。

此外，還有基於機率的「貝氏分類法」[21]，利用「貝氏定理」發明的分類法則，結合事前機率與條件機率，並導出事後機率。此分類法先將信件分割成 n 個斷字 (Token),再統計個別斷字的機率、推算出為該郵件為垃圾郵件的可能性。「貝氏定理」主要仰賴過往累積的數據來判斷未來事件發生的機率，因此如能事先各提供足量的訓練資料（垃圾郵件及正常郵件），將有助於辨識郵件的事前訓練。

◆ 網路攻擊

賽門鐵克(Symantec) 公司 2009 年的調查顯示遭受資訊安全問題的企業平均每家約損失 200 萬美元[22]。確保資料安全與伺服器正常運作是網管人員必須面臨的考驗,如何兼顧高可用性(Availability)、安全性(Security) 與低延遲(Latency)一直以來都是資訊安全最重視的研究議題[23][24]。在網路攻擊方面，由於駭客的攻擊目標大多為使用者的帳號與密碼、信用卡或是提款卡之資訊，透過更新的駭客攻擊手法，近年來，駭客常以網路應用程式作為媒介，透過隱匿強迫下載 (Drive-By Download) 等方式，將惡意程式碼 (如木馬程式、鍵盤側錄、病毒、蠕蟲等) 注入其中，並感染使用者應用程式，利用自動轉址、開啟惡意網站。

在 2004 年，Mihai Christodorescu 與 Somesh Jha Christodorescu and Jha [25]等人針對當年商業防毒軟體，檢測混淆技術的耐受性。其結果顯示，各家的防毒軟體誤判率 (False Negative Rate) 從四成到八成皆有，甚至還有出現完全誤判的情形。惡意程式執行通常是由 Web 應用程式引入來自外部的惡意檔案並執行檔案內容。一般在進行 Web 應用程式的弱點掃瞄時，大部份的工具很難檢測出哪些參數會去讀取檔案[26]。在這類惡意網頁與惡意程式碼的辨識方面，真正的辨識結果是經由訓練有素或資深的資安人員，以人工的方式進行判斷。以上，在在說明自動檢測的迫切性與重要性。

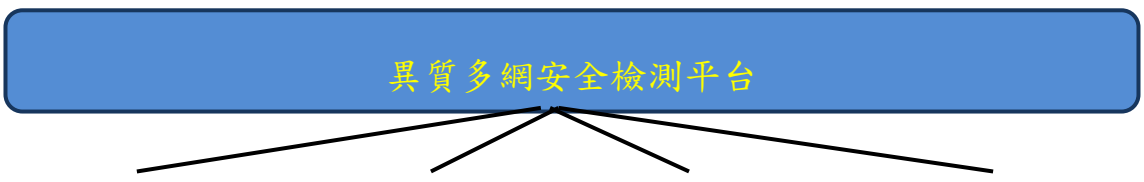
三、 貢獻

本計畫主要目的在於建置一異質多網安全檢測平台，並在此平台下開發完整的安全檢測工具與系統，以提供使用者安全的網路使用環境。異質多網安全檢測平台下開發的工具可分為四大檢測類別：(1)系統安全檢測、(2)網路安全檢測、(3) 軟體安全檢測以及(4)人員安全意識檢測。系統安全檢測提供了遠端系統安全漏洞檢測及網站伺服器的安全漏洞檢測等工具；網路安全檢測提供了應用於 WiMAX 掃描系統及無線網路金鑰的強度檢測等工具；軟體安全檢測提供了目前行動裝置經常使用的 Android 及 Java 應用軟體的檢測以及病毒與惡意程式的工具；人員安全意識檢測則提供了檢驗一般使用者安全意識的網路釣魚檢測及無線網路安全意識檢測工具。藉由本計畫所建置之安全檢測平台，可滿足國內目前對於不同層面的安全檢測需求。在 2009 到 2010 年的計畫執行期間，我們已開發與建置總共 16 個安全檢測工具以及一個異質多網擬真模擬平台。這些工具可檢測異質多網環境下的系統、網路、軟體的安全性以及人員的安全意識，提供使用者安全可靠的網路使用環境，幫助使用者發現系統的漏洞及弱點，並提高內部人員的安全意識。此外，本計劃在 2010 年開始提供的線上安全檢測的服務，任何使用者皆可進行安全檢測。目前已超越 15 萬使用人次。在學術方面，本計畫在 2010 年也有許多論文研究成果，我們發表於國際期刊之論文共有 7 篇，發表於國際研討會之論文數共 5 篇以及國內研討會之論文共 4 篇。在專利方面，我們各別有 3 件國外以及國內專利申請。另外，我們在技術服務與產學合作方面的成果包括技術服務共 3 件，產學合作共 7 件，合計總金額達 702.8 萬。

藉由此平台的建置與檢測工具的開發，我們可提供政府機關、財團法人及高科技廠商在系統安全、網路安全、軟體安全檢測以及人員安全意識檢測的服務，幫助上述單位發現安全漏洞、弱點以及提高內部人員安全意識。

四、 異質多網安全檢測平台介紹

本計畫在 2009 年執行初期便邀請研考會、國家資通安全會報技術服務中心、工研院、資策會、國安局、中科院、中華電信、友訊科技、明泰科技、宏碁科技等單位共同協助規劃合作。在 2010 年，我們持續與中華電信、友訊科技、工研院、資策會、中科院共同合作開發多種安全檢測工具。目前此平台可分成四大檢測類別：網路安全檢測、系統安全檢測、軟體安全檢測以及人員安全意識檢測(請見圖 4-1)。從 2009 年到 2010 年，我們在此平台上共累計建置與開發 16 個工具以及 1 個異質多網擬真模擬平台(請見表 4-1)。藉由這些檢測工具的開發，我們可提供政府機關、財團法人及高科技廠商多樣化的安全檢測的服務，幫助上述單位發現漏洞及弱點。



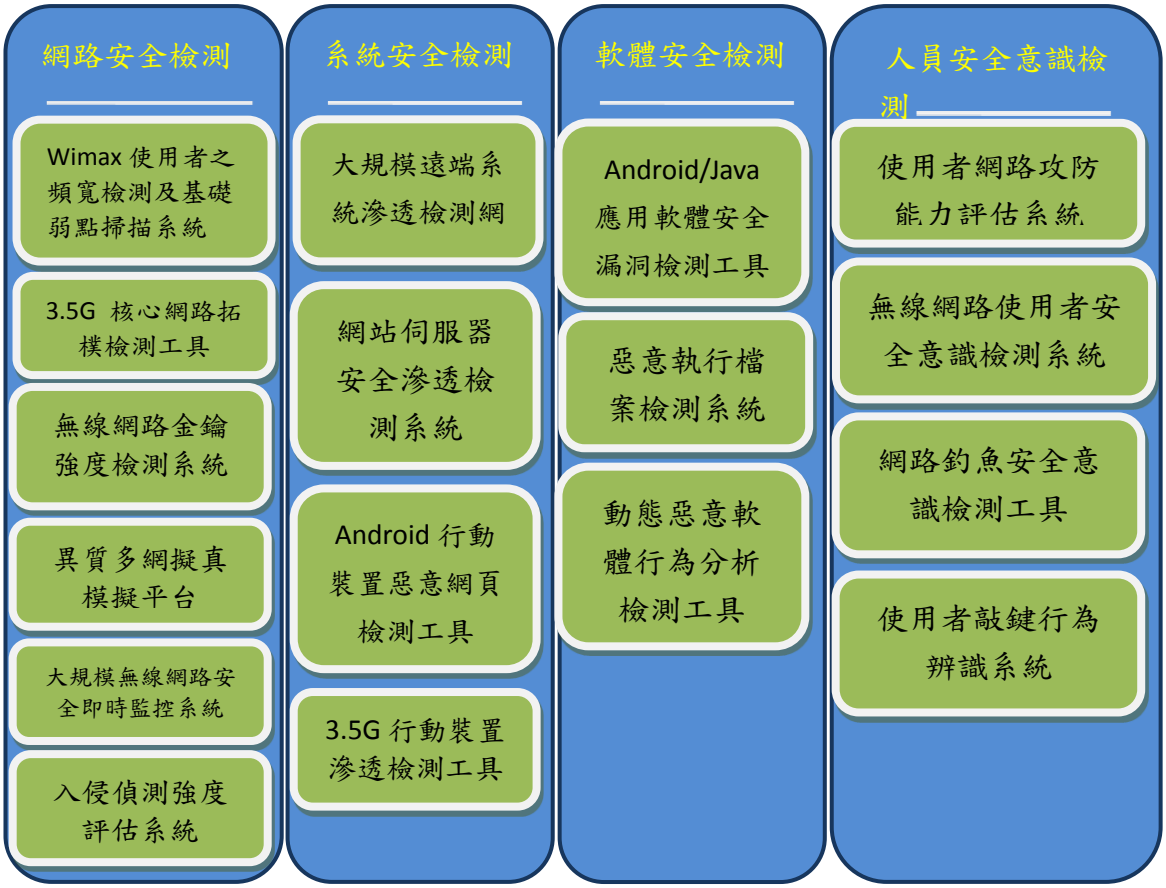


圖 4-1、2010 年異質多網安全檢測平台之架構圖

表 4-1、檢測工具開發清單

2010 年新開發並完成	Wimax 使用者之頻寬檢測及基礎弱點掃描系統
	網站伺服器安全滲透檢測系統
	Android 行動裝置惡意網頁檢測工具
	Android/Java 應用軟體安全漏洞檢測工具(G-exploit)
	網路釣魚安全意識檢測
	使用者網路攻防能力評估系統 (Wargame)
	3.5G 行動裝置滲透檢測工具
2009 年起開發，2010 完成之工具	大規模遠端系統安全滲透檢測網
	異質多網擬真模擬平台
	惡意執行檔案檢測系統
	動態惡意軟體行為分析檢測工具(MBA@TWISC)
	使用者敲鍵行為辨識系統
	3.5G 核心網路拓樸檢測工具 (jtracert)
2009 年開發並完成之具（2010 年主要工作為強功能與維護）	無線網路金鑰強度檢測系統
	無線網路使用者安全意識檢測系統
	大規模無線網路安全即時監控系統
	入侵偵測系統強度評估系統

以下將依分別詳細說明我們所開發的工具。

■ **2010 年新開發並完成之工具**

- Wimax 使用者之頻寬檢測及基礎弱點掃描系統

  WSBW 提供操作容易的網頁介面讓 WiMAX 使用者可輕鬆的得知其使用 WiMAX 網路上行與下載的頻寬，並藉此得知 BS 頻寬控管是否適當以及是否可能會因控管不當而導致阻斷式服務攻擊 (DoS attack)的發生。此外，WSBW 也提供網路狀況資訊讓 WiMAX 使用者容易地了解 WiMAX 網路的目前傳輸狀況。WSBW 系統架構如圖 4-2 所示。

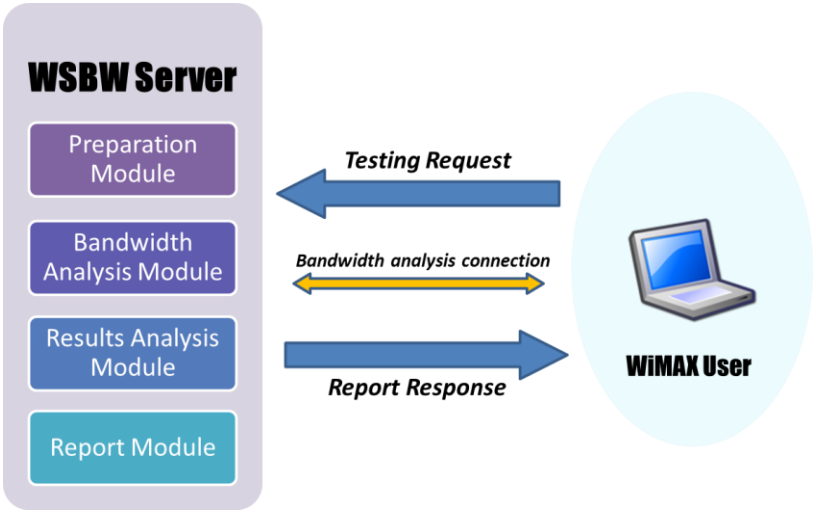


圖 4-2、WSBW 系統架構圖

WiMAX 使用者透過 HTTP Request 與 WSBW Server 建立連線並進行檢測，

連線建立後，WSBW Server 會先後經過四個模組來為使用者進行檢測並且產生報告，以下針對四個 Module 的行為作說明：

1. Preparation Module： 此模組會先檢查使用者裝置的系統資訊，如作業系統版本、Java 版本、防火牆是否開啟、檢測用的連接埠是否開啟、使用者是否位於內部網路等，經過這些檢查來確定後續的測試可正常動作。
2. Bandwidth Analysis Module： 這個部分會與使用者建立上行與下行的連線用以進行 Bandwidth 的測試，上行與下行分別進行數秒的測試並且記錄傳送的資料量以及總計的時間。
3. Results Analysis Module： 從上個模組取得的資訊會在這裡進行分析，計算出測得的上行與下行的速率，除此之外也會根據系統資訊(Buffer size & RRT)計算出理論上的速率上限，最後根據測得的數據與上限值評估是否受到來自網路上的攻擊。
4. Report Module： 這部分會整理上述所有模組回報的資訊，彙整出一份文字報告提供使用者參閱。

圖 4-3 為 WSBW 的首頁畫面，中間的 Java Applet 是本系統的主要程式，使用者可以透過這個 Java Applet 來進行檢測，底下分別有五個按鈕可點選：

- Start： 開始檢測。
- Statistics： 檢測詳細報告 (檢測完畢後可點選)。
- More Details： 提供系統變數 (給開發者檢閱用)。
- Report Problem： 回報問題給系統管理員。
- Options： 可選擇使用 IPv4 或 IPv6。

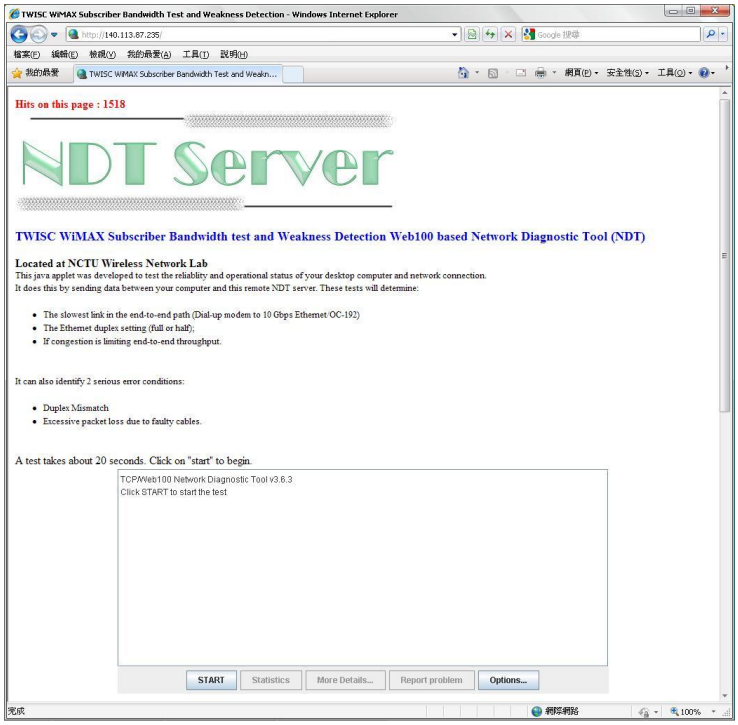


圖 4- 3、WSBW 首頁

在最後的報告部分，我們有提供簡易型的報告給非網路專長的人士閱讀，也

有提供較詳細的報告給網路專長的人士閱讀，以下為測試畫面以及詳細報告的畫面，左方大圖為簡易型報告的畫面；右方的小圖為詳細報告的畫面。

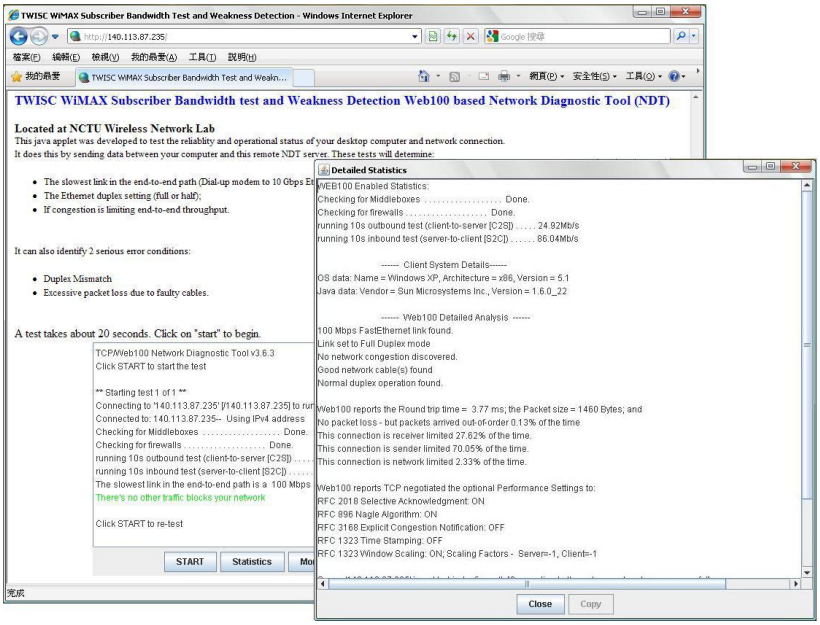


圖 4- 4、測試結果畫面

- 網站伺服器安全滲透檢測系統

網站的安全議題一直是社會大眾關注的焦點，隨著資訊產業的發展，越來越多個人資訊被放置在網際網路中，而網站的安全性就成為了架設網站時必先要考量到的問題。而對一般網站架設者而言，可能並未具備網站安全的相關知識，一般的安全檢測系統也可能過於複雜，對於非相關背景出生的人並不好上手，使用者也為養成定期更新網站安全的習慣。出於此目的，我們在 2010 年開發 WSS (Web Server Vulnerability Scanning System) 用來檢測網站伺服器的安全性，其首頁如圖 4-5 所示。

網站管理者可藉由註冊帳號且經過認證後，透過網頁介面來進行安全滲透檢測服務，對網站管理者而言，所有工作都可以由網頁介面來完成，包含指定掃描之網站以及線上觀看掃描結果報告。網站管理者可省去架設掃描環境的時間與空間，只需透過網頁就能操作安全檢測系統，並且可線上檢閱報告。網站管理者上線進行掃描後，大約三至五分種即可收到掃描報告，也可由線上觀看，並且可檢閱安全報告的歷史紀錄。

WSS 的操作方式如下：網站管理者首先輸入欲進行掃描之網站後，本系統後端就會開始對此網站進行弱點掃描分析，藉由發送檢測封包來和系統中的弱點資料庫來進行比對，再將所得到的結果整合成一份報告，並以網頁的形態提供給網站管理員。為了防止本系統遭到惡意使用者濫用，我們限定掃描服務的時間，半小時之內只能進行一次掃描的動作，而且網站管理者也只能對註冊的網站進行掃描，藉此可防止惡意使用者藉由本系統掃描其欲攻擊之網站伺服器。

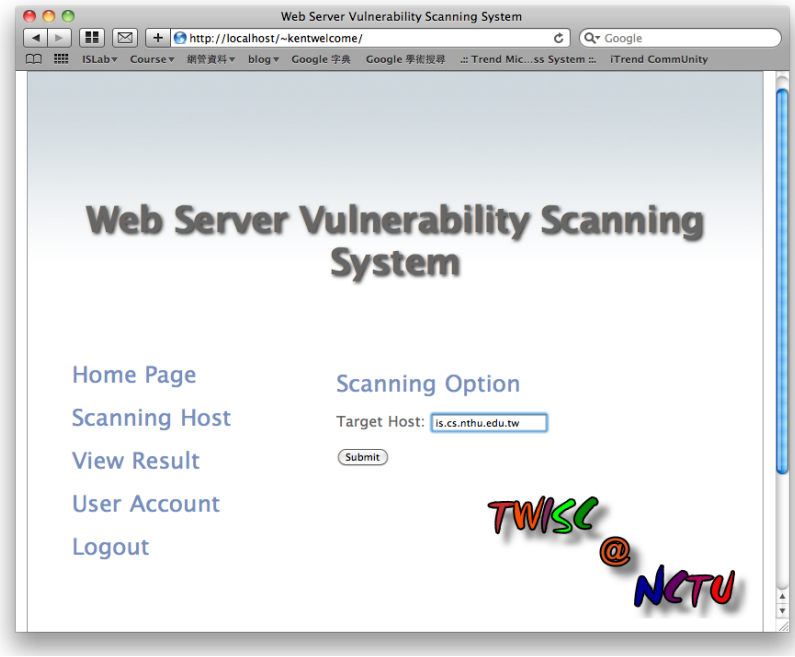


圖 4- 5、WSS 網頁操作畫面

- Android 行動裝置惡意網頁檢測工具

現今網路上存在許多惡意網頁，當使用者瀏覽到這些網頁時將會因為網頁上的惡意程式碼，造成使用者在無意中機密資料外洩。為了檢測惡意網頁，我們在 2010 年針對 Android 手機平台研發 Android 行動裝置惡意網頁檢測工具，藉由在 Android 網頁瀏覽器中建置過濾規則，讓使用者在上網的同時，可即時偵測網頁端所有物件是否具有惡意行為，使得我們可以在不妨礙到使用者正常瀏覽的情況下，進而達到保護的目的。使用者也可以使用 JavaScript 語法及此軟體所提供的函式來達成簡易的修改及增強規則。

由於網頁上多數的惡意語法皆是使用 JavaScript 來撰寫，因此我們透過將瀏覽器中原有的 JavaScript 函式進行包裝，不讓瀏覽器直接去執行原有的 JavaScript 函式，而是透過我們所提供經過包裝後的函式來使用 JavaScript。藉由包裝舊有函式的方式，我們可以在不修改網頁上任何語法的狀況下，藉由在瀏覽器層面的防護，來達到保護的目的。比起單純禁止某些危險性較高的 JavaScript 函式的使用，我們不會禁止任何函式的使用，藉由這樣的方式可以有較高的相容性，並可將為了達成保護的目的所需的花費降低，不需要修改現有的網頁內容。

前面提過我們是透過包裝原有 JavaScript 的方式來進行防護，我們將檢測的機制加入到包裝的函式中，在執行原有的函式前會先進行檢測，並且在檢測的時候加入評分的機制，根據不同的行為給予適當的評分，當檢查完整個網頁後會根據之前的評分加總，並與我們事先設定好的分數區間進行比對，判斷這個網頁處於何種安全等級，決定是否要准許使用者繼續瀏覽這個網頁。對於評分的標準包含了是否有存取私密性檔案(例如: cookie)、是否存取私密性檔案後又進行了寫入的動作等。Android 行動裝置惡意網頁檢測工具之網頁操作畫面如圖 4-6：

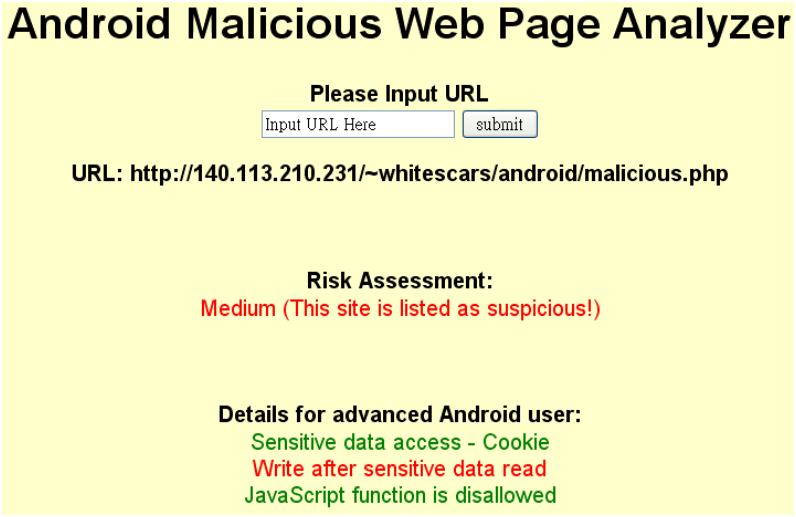


圖 4-6、Android 行動裝置惡意網頁檢測工具之網頁操作畫面

- Android/Java 應用軟體安全漏洞檢測工具(G-exploit)

  我們在 2009 年開發了 G-exploit。它提供自動化的 Java 程式安全檢測，可檢測潛在的程式臭蟲、弱點，並協助程式開發者進行錯誤修正。G-exploit 接受多種檔案格式，包括 java 原始碼、jar 檔、class 檔、android 的 dex 檔等。G-exploit 結合多項檢測功能，可提供受測程式全面性的安全檢測，進而防範某些因開發人員疏忽而潛藏的漏洞。由於行動裝置上的計算資源有限，在 2010 年，我們進而提供 G-exploit 線上檢測服務，使用者可連到 TWISC@NCTU 網站上直接使用 G-exploit 工具，透過 Web 方式上傳受檢測的程式碼，通過簡易的介面選擇多種檢測工具，即可進行詳細的檢測，並即時得到檢測報告。有了完整的檢測報告，可以提供開發者更有效率的解決有問題的程式。此服務不僅降低了安裝與使用專業檢測工具的門檻，也提供全面性的檢測服務。無論是任何行動裝置以及系統平台都可隨時隨地經過網頁瀏覽器使用 G-exploit 所提供的服務。Android/Java 應用軟體安全漏洞檢測工具之網頁操作畫面如圖 4-7 所示。

圖 4-7、Android/Java 應用軟體安全漏洞檢測工具之網頁操作畫面

- 網路釣魚安全意識檢測

網路釣魚安全意識檢測工具 (Phishing Awareness Testing, 以下簡稱 PAT) 是一套個人化之人員安全意識檢測工具。PAT 藉由模擬真實的網路釣魚信件，來評鑑使用者對防範網路釣魚信件的安全意識等級以及相關的網路安全知識，以幫助使用者快速了解自身安全觀念之弱點、降低使用者遭受釣魚攻擊之可能性。

PAT 的系統架構可分為四項主要元件：網頁介面 (Web Interface)、釣魚信件產生器 (Phishing Mail Generator)、檢測報告產生器 (Report Sender) 和儲存使用者和郵件資料的後端資料庫，其架構如圖 4- 8 所示。使用者可透過網頁介面和 PAT 系統互動、申請測試帳號、要求系統寄發釣魚信件，以進行人員安全意識檢測。以下分別介紹 PAT 中各元件之功能：

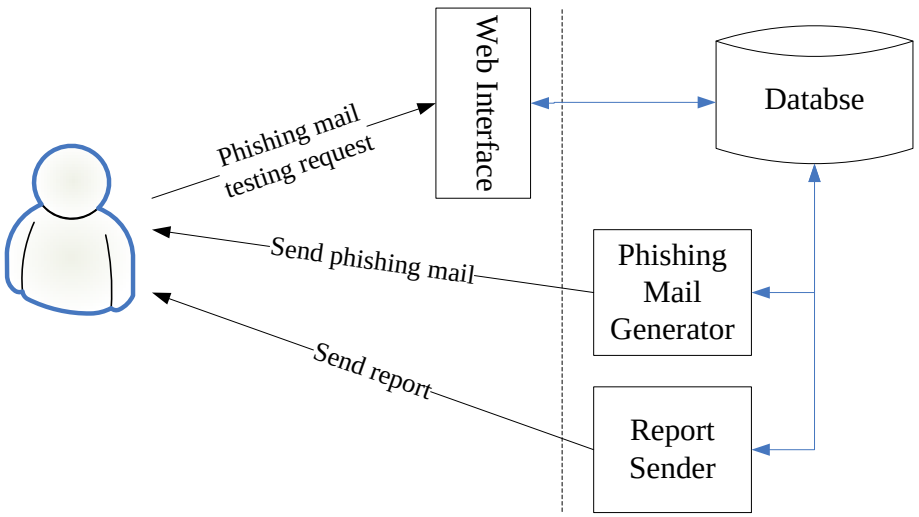


圖 4- 8、網路釣魚安全意識檢測工具（PAT）之系統架構設計

(1) 網頁介面 (Web Interface)

PAT 的網頁介面 (如圖 4-9 所示) 提供使用者申請測試帳號之服務。欲申請檢測的使用者必須先向 PAT 系統註冊自己的 E-mail 信箱，PAT 系統會發送一封認證信至使用者註冊之 E-mail 信箱，以確認申請安全意識檢測服務的使用者為該信箱之擁有人。通過認證之使用者可登入系統選擇欲測試的網路釣魚信件類型，並通知系統開始寄發釣魚信件進行檢測。

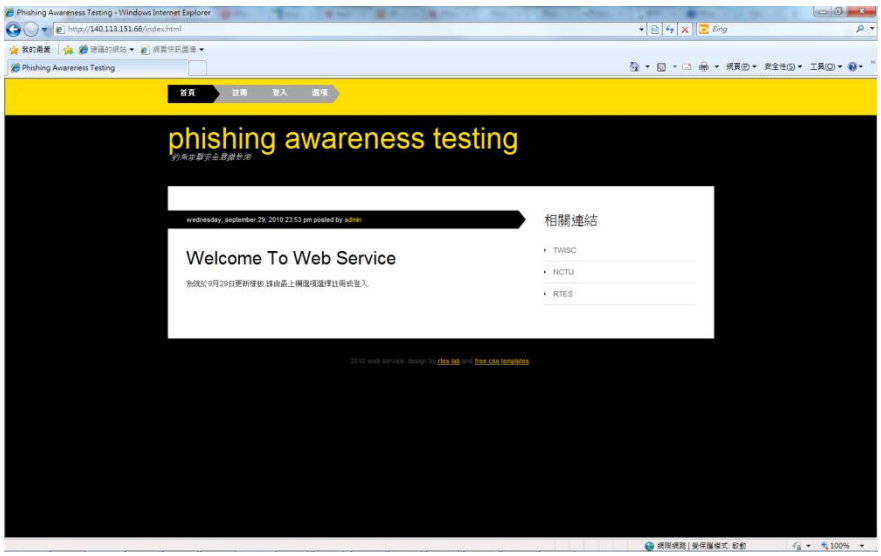


圖 4-9、網路釣魚安全意識檢測工具的網頁介面

(2) 釣魚信件產生器 (Phishing Mail Generator)

釣魚郵件產生器會根據使用者選取之釣魚信件類型，在開始測試後的某隨機時間內，發送釣魚信件給使用者，如圖 4-10 所示。該釣魚郵件內會夾帶若干個偽造之惡意鏈結，當使用者點擊這些鏈結後，就會開啟連線連至 PAT 系統架設的惡意網頁。每封釣魚郵件的惡意鏈結中會夾帶不同的 php 網址參數列，用來記錄釣魚郵件中的惡意鏈結被使用者所開啟的次數。PAT 系統會將惡意鏈結的點擊次數紀錄至後端資料庫中，以作為發送給使用者的測試報告之參考資料。

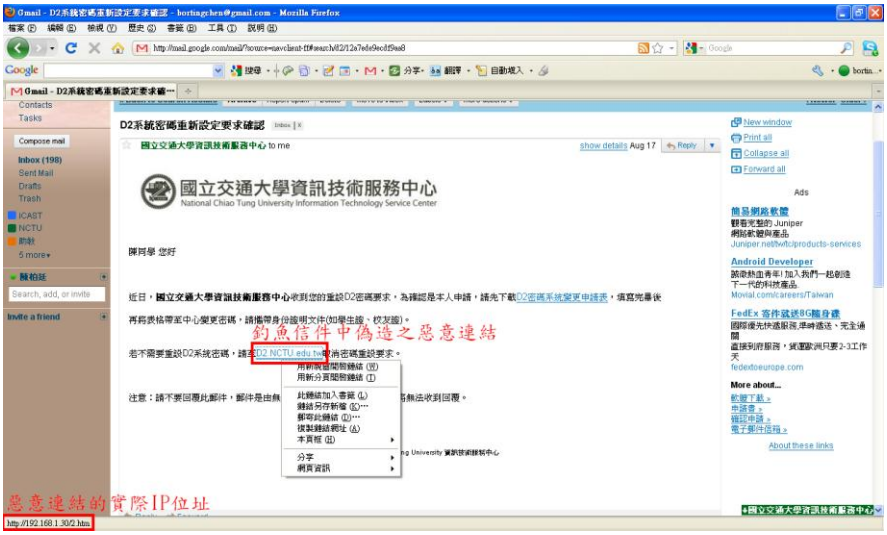


圖 4-10、釣魚郵件產生器偽造之信件（含有連線至 PAT 系統的惡意鏈結）

(3) 檢測報告產生器 (Report Sender)

檢測報告產生器會在寄出釣魚郵件後，根據後端資料庫內存放的使用者點擊惡意網頁的紀錄，評斷使用者對於防範網路釣魚郵件的安全意識等級。檢測報告產生器會將評斷之結果和使用者開啟網頁鏈結之紀錄寄給管理者（或使用者），以協助管理者（或使用者）了解企業內部操作人員（或自身）對防範不同類型釣魚郵件之弱點所在。

(4) 後端資料庫 (Database)

後端資料庫負責存放申請釣魚安全意識檢測使用者的個人資料，包含姓名、電子郵件信箱、所申請之釣魚郵件類型等等。資料庫也會紀錄 PAT 系統所發出的每封釣魚郵件的狀態，包含寄信時間、惡意鏈結被點擊的次數等等，以作為檢測報告產生器寄送檢測結果給使用者時的參考資料。

- 使用者網路攻防能力評估系統 (Wargame)

Wargame 提供各種不同類型具有安全性漏洞的題目，讓使用者能夠在一個安全的平台上，透過實際的攻擊行為來精進程式安全相關的知識與能力。不同於其他 Wargame 平台 (全部使用者分享同一個作業系統)，本 Wargame 平台採用虛擬機器的概念，讓每位使用者都有一部虛擬機器。藉由此種方法，本 Wargame 平台突破以往只能夠提供單一程式等級題目的限制，能夠提供作業系統等級的題目；此外，即使使用者成功取得整個作業系統的 root 權限，亦或造成系統 Crash，也不會影響其他使用者的進行以及整個 Wargame 平台的運作。透過虛擬機器的 snapshot 功能，我們能夠快速復原受損或是被操作過的作業系統，提供下個使用者一個乾淨的操作環境，也能夠快速針對每個使用者複製一模一樣的環境，維持 Wargame 平台的穩定性與公正性。本 Wargame 平台提供了一個全新的架構，讓使用者能夠在一個更安全、穩定的環境下測驗自己的程式安全能力，並且提供了更多元的題目，吸引更多對資安方面有興趣的人員了解程式安全的重要性。使用者網路攻防能力評估系統之網頁操作畫面如圖 4-11 所示。

圖 4-11、使用者網路攻防能力評估系統之網頁操作畫面

- 3.5G 行動裝置滲透檢測工具

3.5G 行動裝置滲透檢測工具是一套建立滲透檢測管道之技術，該工具可在受測者不知情的狀況下，協助檢測者建立和受測者所持有的 3.5G 行動裝置之間的連線，以利更進一步地檢測系統之安全性。目前本計畫之研究人員已針對使用 Windows XP 和 Windows 7 為作業系統之 3.5G 行動裝置，開發了一套基於 VNC 遠端連線技術之滲透檢測工具。以 VNC 遠端連線技術為基礎，此工具兼具自動安裝與背景執行的功能，以方便檢測者對 3.5G 行動裝置進行系統安全之滲透測試。

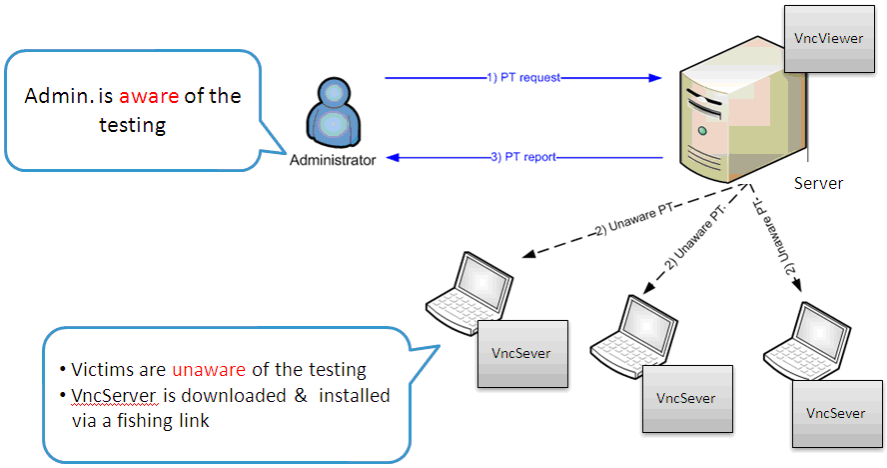


圖 4- 12、以 VNC 遠端連線技術為基礎的 3.5G 行動裝置滲透檢測工具

圖 4- 12 顯示以 VNC 遠端連線技術為基礎的滲透檢測工具的架構。此架構中主要包含了兩大部分：安裝在受測者端的 VNC 後門程式 (VNC backdoor)，以及安裝在伺服器端的 VNC 檢視器 (VNC viewer)。

(1) VNC backdoor

VNC backdoor 以遠端連線時所使用的 VNC server 為基礎，利用 Bat To Exe Convertor 打包工具，將包含安裝 VNC server 指令之批次檔 (batch file)，包裝成一可執行檔，如圖 4-13 所示。該批次檔包含了安裝 VNC server 時所需設定之 Windows 登入檔、以及在 Windows 防火牆上開啟連線至 VNC viewer 時所需之

通訊埠 (port) 等指令與資訊，使 VNC backdoor 可用背景執行的方式在受測者的行動裝置上安裝並執行而不被受測者所察覺。當 VNC server 被植入到受測者之行動裝置後，VNC server 會透過自動反向連接 (auto reconnect) 連線至 VNC viewer，建立滲透檢測之管道。本計畫之團隊所使用的 VNC server 版本為 UltraVNC 1.0.8.2 版，該版本之 VNC server 支援在以 Windows XP 和 Windows 7 為作業系統之行動裝置上進行操作，協助此工具的使用者對使用 Windows 為作業系統之行動裝置進行滲透測試。

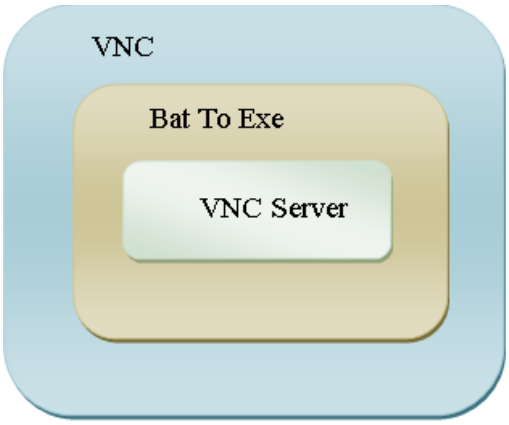


圖 4-13、VNC Backdoor 之架構圖

(2) VNC viewer

VNC viewer 為此工具的使用者檢測受測者的行動裝置時的操作介面。當 VNC server 透過自動反向連接 (auto reconnect) 連線至 VNC viewer 時，使用者的操作介面會出現受測者之遠端連線顯示畫面 (如圖 4-14 所示)，使用者可透過遠端連線檢測受測者行動裝置的作業系統登入檔，以及系統安全設定等資訊。

圖 4-14、VNC server 透過自動反向連接連線至 VNC viewer

■ **2009 年起開發，2010 完成之工具**

● 大規模遠端系統安全滲透檢測網

大規模遠端系統安全滲透檢測網（圖 4-15）是基於 Metasploit 軟體所開發的檢測網站，Metasploit 是一款開放的安全漏洞測試工具，此工具提供了 Shellcode 撰寫、滲透測試及漏洞研究一個整合式的開發環境，讓安全研究人員更容易在此平台上擴充延展檢測的工具。當使用者連上遠端系統滲透測試網後，伺服器將對自動與使用者電腦進行惡意封包的發送測試。如圖 4-16，首先系統將針對使用者的電腦進行全面的連接阜掃描，蒐集所有開啟的服務連接阜的資訊，接著系統將針對已開啟的連接阜發動滲透測試，以並記錄使用者端的系統回應，進以分析使用者電腦端的連接阜安全程度。待分析結果出爐後，使用者將可從檢測結果了解自身的電腦狀況，包含對外連結阜的使用情形、可能遭受的攻擊風險以及可抵禦的滲透攻擊。此外，系統並提供使用者滲透攻擊的資料記錄，使用者可進一步了解攻擊的資訊和對系統加以補強的方法及對應的補丁程式。

圖 4-15、RSPTN 網站首頁

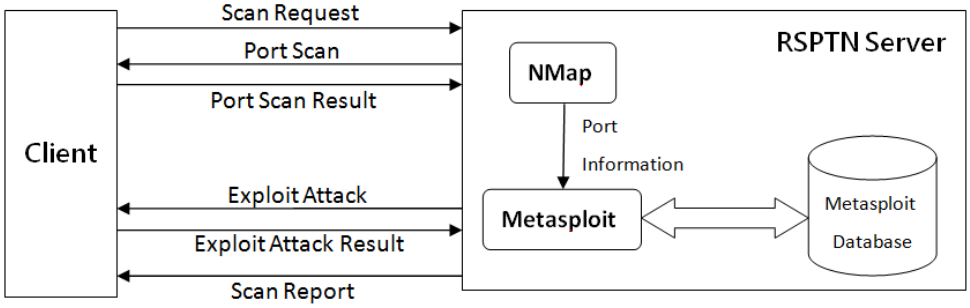


圖 4-16、RSPTN 架構圖

因應無線網路及可攜式移動裝置的興起，我們所要檢測對象的網路組態也比以往複雜。當使用 Wi-Fi 無線網路或是 3G/3.5G 行動網路上網時，行動裝置利用分配到的 privateIP 共用網路資源，無線 AP 或是 3G/G 基地台則透過 Network Address Translation (NAT)的方式將外部連線的 port 與內部 private IP 做一對應，使其能夠正常作用；如圖 4-17，AP 將自身的 port 3 對應內部 private IP 192.168.1.3，當外部的 http 回應給 port 3 時，就將此回應 forward 給內部的 192.168.1.3。

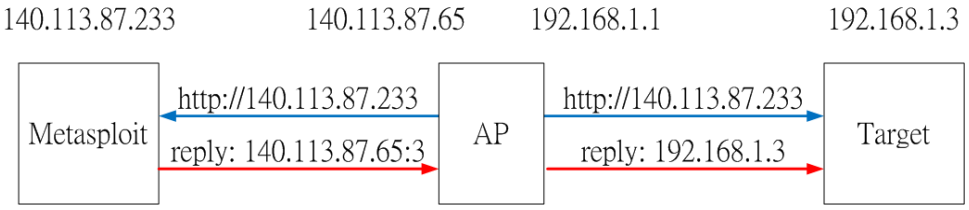


圖 4- 17、NAT 示意圖

然而在使用 NAT 共享網路資源上，卻有諸多限制。當一內部網路的使用者[private IP:port]向外連線時，會在 NAT 表格中加入一項對應：[external IP:port']←→[private IP:port]，此時外部的連線只能連通此內部使用者的該 port，而無法連通其他 port，這將使得我們只能掃描使用者幾個 port 而已，而非是掃描全部的 port；如表 4- 2，內部使用者(192.168.1.3)利用其 80 port 向外連線，此時 AP 將自己的 port 3 對應此連線，所以外部的封包可以透過 140.113.87.65:3 連向 192.168.1.3:80。但是外部的連線也受限於 NAT 表格的對應，只能連向 192.168.1.3 的 80 port 及 8080 port，而無法連通其他的 port。這對於弱點檢測是個問題：只能夠檢測少數幾個特定的 port，其無法全面地進行檢測。

表 4- 2、NAT 表格

外部對應	內部對應
140.113.87.65 : 3	192.168.1.3 : 80
140.113.87.65 : 10	192.168.1.3 : 8080
140.113.87.65 : 201	192.168.1.5 : 21

如何克服私人 IP 的網域掃描成了遠端系統弱點偵測新的挑戰課題。我們已初步研究了跨網域的檢測方法，如圖 4-18，讓使用者能在私人網路的使用上，仍舊可以進行系統滲透測試。我們採用了虛擬私人網路(VPN)技術來跨越不同的網域，同時避免入侵偵測系統(IDS)將滲透攻擊的網路封包誤認為是真實的攻擊行為。我們利用 OpenVPN 於滲透測試網上架設了虛擬私人網路伺服器，跨網域的使用者可建立虛擬私人網路連線，接下來透過虛擬網卡介面連接到滲透測試網進行檢測，此時使用者跟滲透測試網位於同一虛擬私人網域下。

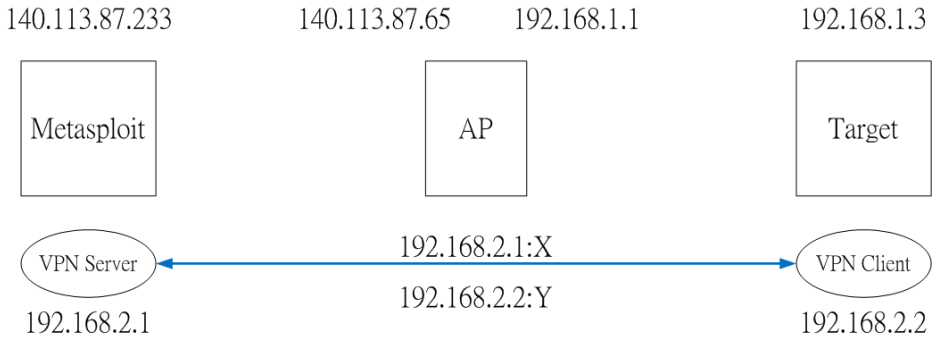


圖 4-18、VPN 示意圖

此外，為了方便使用者下載憑證、設定 VPN 連線、自動定期進行檢測，我們之後將開發一代理程式，未來能提供使用者簡易的下載程式，使用者在安裝完代理程式後，系統將能自動定期地做系統弱點偵測，讓使用者能輕鬆地掌握系統的情報和弱點發現的提醒，達到更即時更完善的測試防護。

- 異質多網擬真模擬平台

  此平台是由交通大學等國內多所大學與美國加州大學柏克萊分校多位專家共同研究開發的異質多網擬真模擬平台，經由本研究團隊進一步研究改良後，目前由 TWISC@NCTU 維護中。此平台可用於進行異質多網的安全測試。此平台支援異質網路之特性，可協助測試新的安全機制和產品在異質無線網路下之效能和表現。使用者可以於此平台上進行 Wired、Wi-Fi、WiMAX 異質網路實驗，毋需重新建置實體實驗環境。異質多網擬真模擬平台操作畫面如圖 4-19。

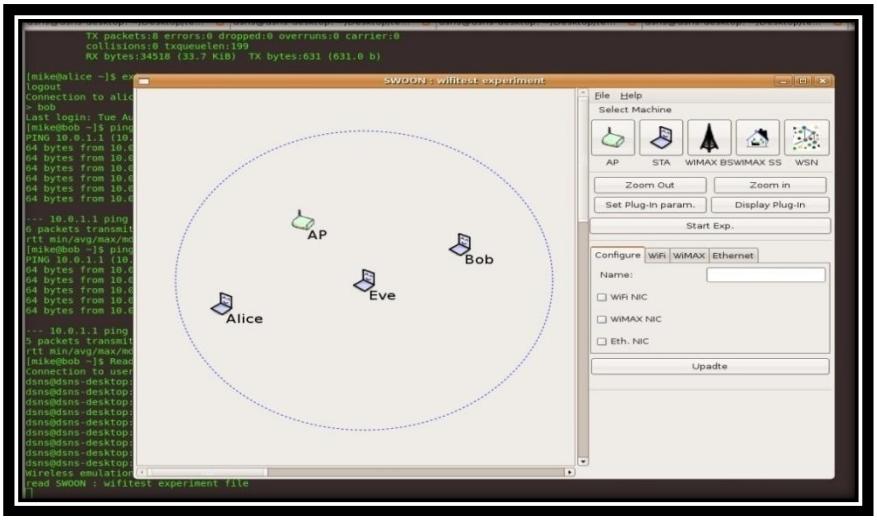


圖 4-19、異質多網擬真模擬平台操作畫面

- 惡意執行檔案檢測系統

  惡意執行檔案檢測系統是用來檢測惡意執行檔的鑑識工具，結合多項分析技術來達成完整且精確的檢測報告。其技術大致可包含如下：載入函式庫檢測和資訊熵分析以檢測加殼加密惡意程式。惡意執行檔大多依賴外部函式來讓自身程式碼精簡，故檢測載入函式庫用來檢查出該執行檔是否引用敏感核心函式，例如：

創建程序、創建檔案和寫入記憶體等。為了避免被分析，惡意執行檔可採用不同的加殼技術以混淆分析人員的判斷。因此，傳統特徵值比對的方式並不能適用在新穎的惡意執行檔之上。資訊熵利用了統計學的原理來判斷該執行檔是否有混淆內容的企圖，國外學者也有發表相關的研究論文指出該方式的可用性。經過以上的技術分析，該系統將會產出一個詳盡的分析結果，並且提醒使用者該檔案是否為可疑，以避免開啟惡意執行檔。在 2010 年，我們提供即時性的線上檢測服務，受惠者除了資安人員、產業界，更包括一般社會大眾。惡意執行檔案檢測系統之網頁操作畫面如圖 4- 20。

圖 4- 20、惡意執行檔案檢測系統之網頁操作畫面

- 動態惡意軟體行為分析檢測工具(MBA@TWISC)

MBA@TWISC 透過收集並分析各種惡意程式(malware)執行檔的行為來預測惡意程式的攻擊路徑。MBA@TWISC 的設計原理是利用 QEMU 模擬機器(emulator)模擬 CPU 執行指令的過程，並在模擬機器上運行的惡意程式。藉由實際程式運作可了解惡意軟體的實際運作過程，模擬機器上的檔案新增、刪減，資料庫的變更或是惡意程式企圖隱藏自身運作的行為等動作。我們將整理並回報程式運行之後可疑行為的詳細報表，供使用本檢測工具的專業人員做更進一步的檔案判定。圖 4-21 是本系統初始執行畫面，系統一開始會要求輸入一個檔案，按下”Chose a file”的按鈕之後，將會顯示挑選檔案視窗，如圖 4-22 所示，要求使用者選擇惡意程式進行行為分析。

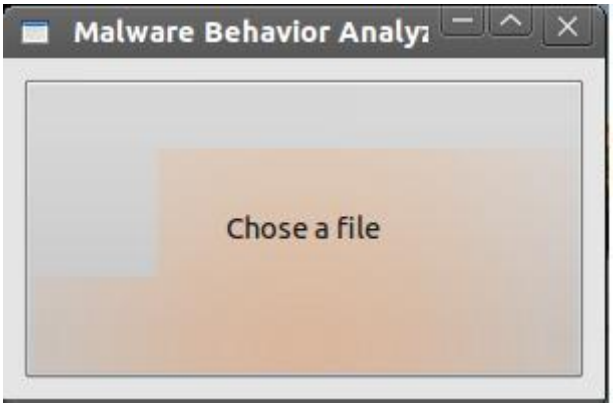


圖 4-21、MBA 初始畫面

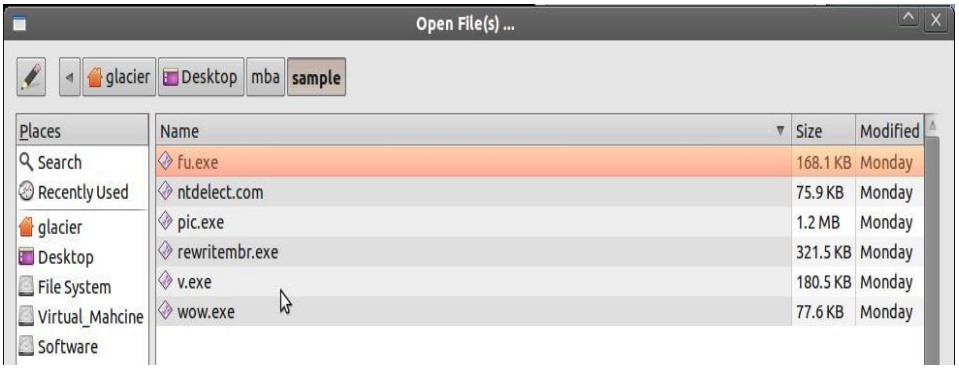


圖 4-22、挑選檔案視窗

- 使用者敲鍵行為辨識系統

  此系統藉由偵測使用者敲鍵行為進行辨識使用者身份。若使用者輸入的密碼正確但其敲鍵行為模式卻不相符，而該使用者將無法通過本系統的驗證。利用本系統可有效地增強系統登入的安全性。此系統亦會隨著使用者行為的些微改變而產生新的預測模型，是一套具有自我學習機制的系統。在 2010 年，我們將此工具更改成為線上版本，目前已可提供即時性的線上服務。使用者敲鍵行為辨識系統操作畫面如圖 4-23。

圖 4-23、使用者敲鍵行為辨識系統操作畫面

- 3.5G 核心網路拓樸檢測工具 (jtracert)

jtracert 為一網路拓樸探索工具，用以探索 3.5G 核心網路之架構，並找出 3.5G 核心網路中潛在的安全弱點，作為滲透測試之前期探索工具。jtracert 以 jpcap、winpcap 等函式庫為基礎，利用 ICMP 封包的回應值取得本機端與目標主機之間的路徑與節點資訊。使用者可進一步將多節點之間的路徑資訊整合，並搭配拓樸分析演算法，歸納出行動網路拓樸，推測出可能遭遇到攻擊的網路節點。

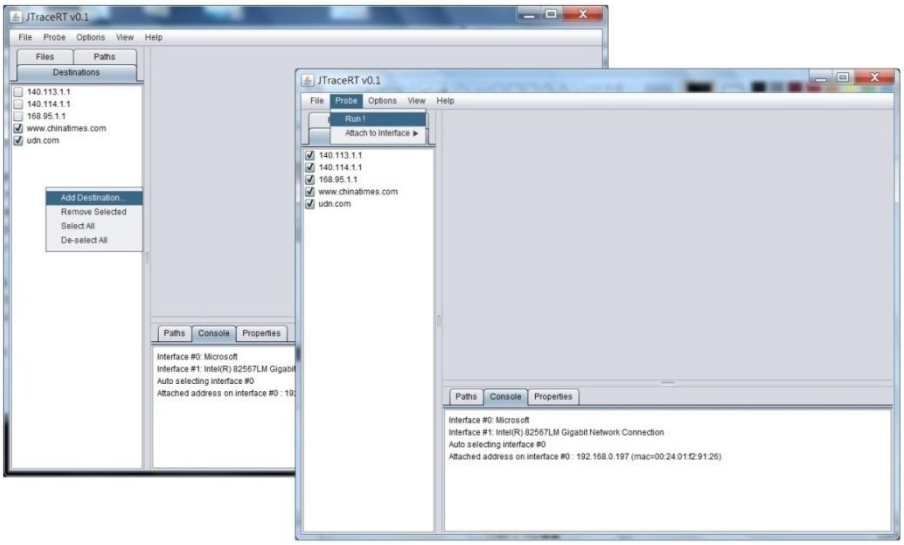


圖 4-24、jtracert 的操作介面

圖 4-24 為 jtracert 的操作介面。當 jtracert 啟動之後，使用者可以利用右鍵開啟選單新增或移除欲探索之目的節點 (destination)，亦可勾選所想要的目的節點，來收集目的節點與來源節點 (source，亦即本機端) 之間的路由路徑 (traces)。當所欲探索之目的節點設定完成後，即可要求 jtracert 開始探索來源節點和目的節點之間的路由路徑，並記錄路由時所經過之中間節點的相關資訊。jtracert 支援多種網路協定，包括 ICMP、TCP 等，使用者可以依據當時的網路設定與狀況選擇

適用的網路協定來收集路由資訊。例如，jtracert 可利用 ICMP 的 echo/reply 封包，找出來源節點 (source)與目的節點之間的路由路徑，以及路由所經過之中間節點的 IP 位址，並可藉由節點回傳之 TTL 值推測節點使用之作業系統版本等資訊。

使用者可以將 jtracert 路徑探索之結果存成路由路徑檔案，並將多個路由路徑檔案匯入到系統中，將各路徑串接成一個網路區域拓樸圖 (graph)。jtracert 建立之網路區域拓樸圖如圖 4-25 所示。

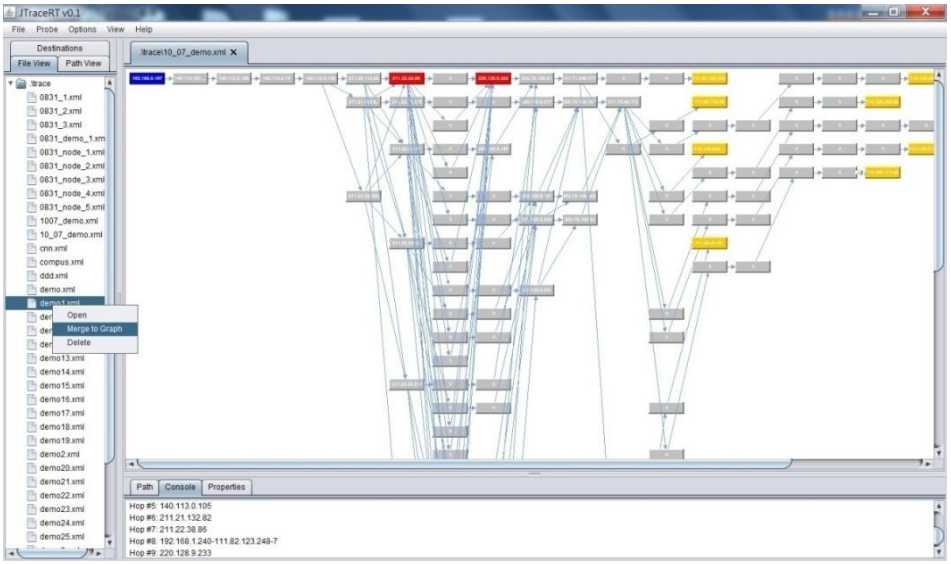


圖 4-25、利用多個路由路徑檔案串接成網路區域拓樸圖

jtracert 在合併多條路由路徑時，會分析上述網路區域拓樸圖中各節點的內分支度 (in-degree)與外分支度 (out-degree)，以決定各節點之類型。jtracert 定義了數種節點類型，包括來源節點 (s-node)、目的節點 (d-node)、中間節點 (i-node)、共享節點 (x-node)、受害節點 (v-node)等。如圖所示，藍色節點為 s-node、黃色為 d-node，紅色為 v-node。一個節點可以同時具有多種類型，如某個節點可能同時是目的節點 (d-node)與共享節點 (x-node)，如圖 4-26 所示。

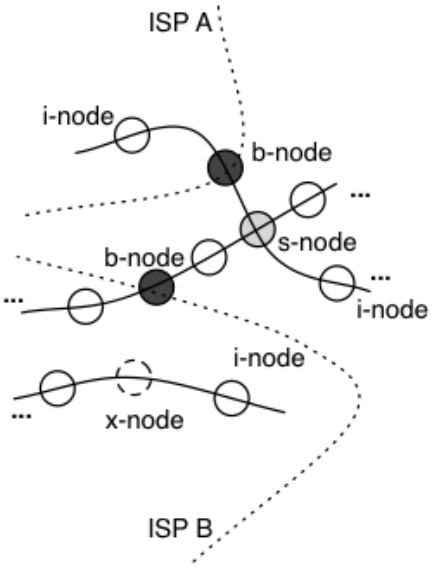


圖 4-26、利用 jtracert 所分析得到之區域拓樸圖及其節點特性分析結果

透過本工具所評估的資訊，系統管理人員可依據節點資訊與其類型進行分類，找出網路區域拓樸圖中可能的數個受害節點，並針對這些弱點節點進行安全功能補強，或改變整個網路的路由機制，提昇整體網路的安全度。使用者者可進一步透過現有的滲透分析工具 (nmap、nessus、metasploit 等)對這些受害節點進行滲透分析。藉由滲透分析之結果，可進一步地評估出此區域網路的安全等級。這些評估結果將可提供相關 ISP 業者或系統管理員參考，以茲作為加強其網路安全等級之依據。

- **2009 年開發並完成之工具（2010 年主要工作為增強功能與維護）**
  - 無線網路金鑰強度檢測系統

    無線網路金鑰強度檢測系統主要用來檢測一無線網路基地台所設定的金鑰是否安全。此系統利用竊聽無線網路 ARP reply 封包的方式取得所需的 IV (Initial vector)資料。為加速取得 IV 資料，我們利用竊得的 ARP request 封包進行反覆傳送。當蒐集到足夠的 IV 資訊後即可破解出正確的金鑰。透過本系統可以成功破解 WEP 128bit 加密方式的金鑰，而破解時間最快為半小時。無線網路金鑰強度檢測系統操作畫面如圖 4-27。

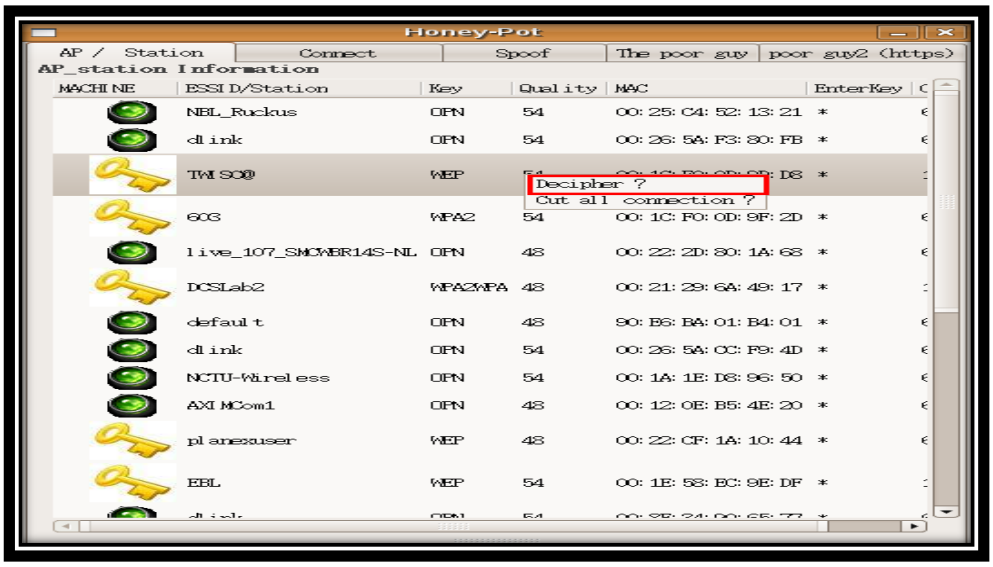


圖 4-27、無線網路金鑰強度檢測系統操作畫面

- 無線網路使用者安全意識檢測系統

無線網路使用者安全意識檢測系統主要用來檢測使用者在使用無線網路時是否具有安全意識。本系統建置不需要帳號密碼的無線基地台來吸引使用者連線，若有使用者因為便利而進行連線可知其安全意識並不佳。此外，本系統也會攔截經過此無線基地台的網路封包來觀察使用者是否會連線至不具有合法網路憑證的網站。藉此可進一步得知該使用者的網站安全意識。無線網路使用者安全意識檢測系統操作畫面如圖 4-28。

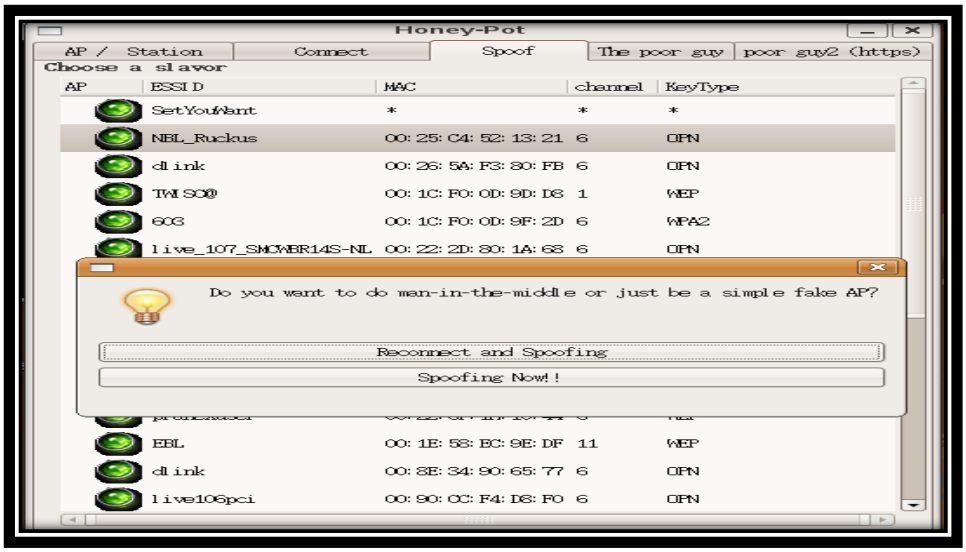


圖 4-28、無線網路使用者安全意識檢測系統操作畫面

- 大規模無線網路安全即時監控系統(WiMon)

WiMon 使用主動式監控與被動式掃描來保護 Wi-Fi 無線區域網路並防禦攻擊。若裝有 WiMon 系統的 AP 若遭受攻擊，WiMon 可利用 GPS 定位出 WiMon 範圍內的攻擊者與被攻擊者的正確位置，亦可清楚的標示出攻擊的類型。WiMon

也提供入侵預防的功能。WiMon 可提供由大範圍至小區域的監控畫面，圖 4-29 是 WiMon 系統初始時出現的地理位置的空照圖，圖 4-30 挑選該地建築物並選取樓層，圖 4-31 顯示出該環境中攻擊者的所在位置。

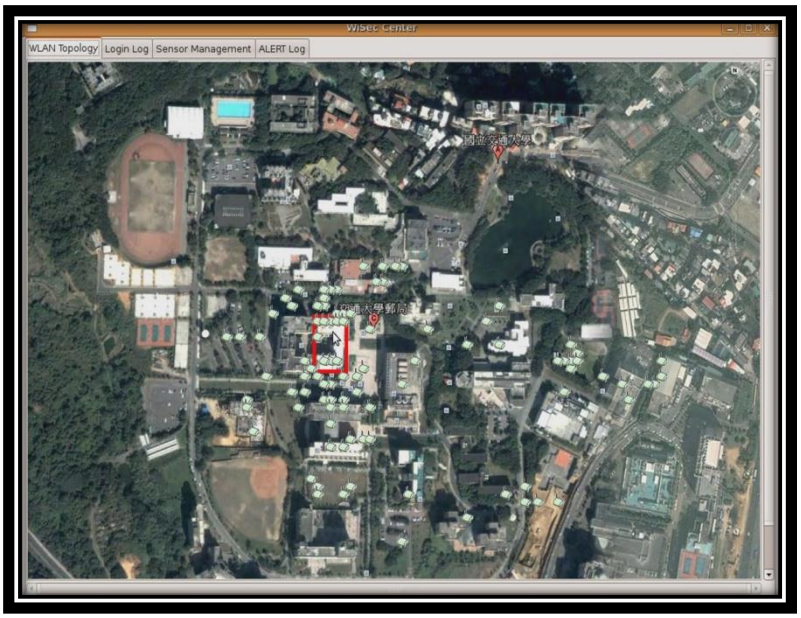


圖 4-29、WiMon 空照圖

圖 4-30、挑選該地建築物並選取樓層

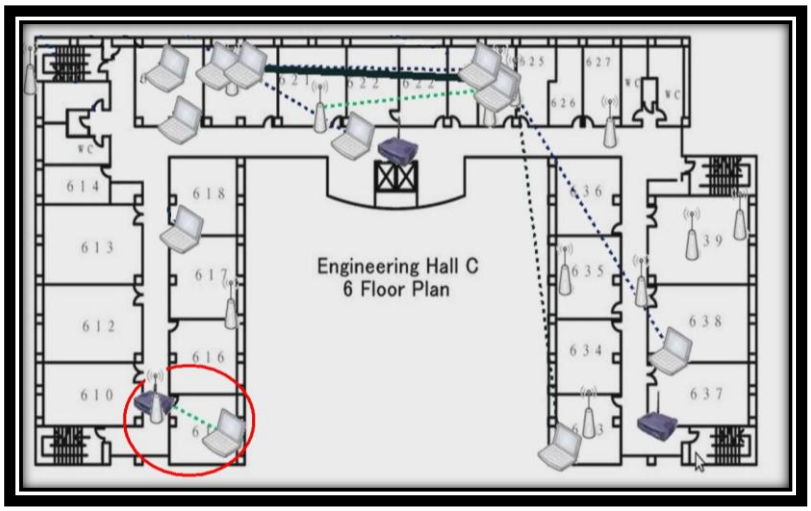


圖 4-31、顯示出該環境中攻擊者的所在位置

- 入侵偵測系統強度評估系統

  入侵偵測系統為核心網路其中一個重要的元件。我們開發入侵偵測系統強度評估系統來檢測與評估入侵偵測系統(IDS)的強度，以及探索是否有可能規避受測 IDS 的方法。它能夠輕易的編造出畸形封包，改變封包中 Layer 2 到 Layer 7 任何的欄位的能力，並且獨立發送。藉由它我們可以進行任意的 IDS Evasion Test 或是 Attack。一般的無線 DUT 在設計上經常在以下路徑上有安全性的漏洞，這些路徑分別是 LAN – LAN、LAN – WLAN 以及 WLAN – WLAN (以下我們用 critical paths 表示這三條路徑)。圖 4-32 為入侵偵測系統強度評估系統實驗架構圖。

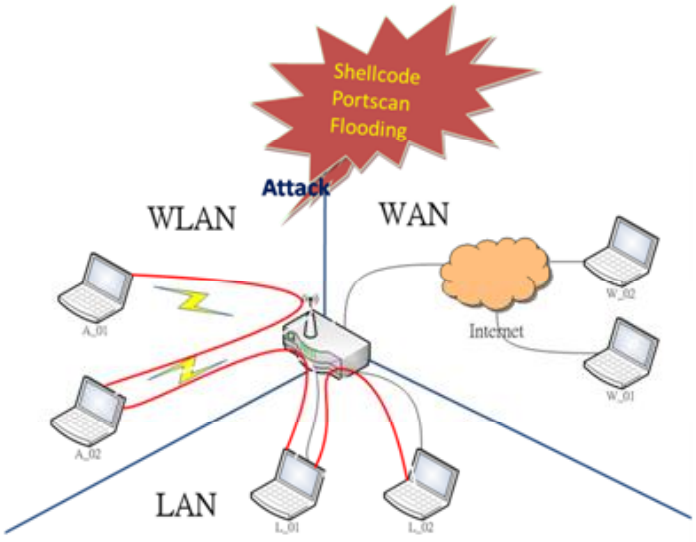


圖 4-32、入侵偵測系統強度評估系統實驗架構圖

五、 系統效能評估成果

在此章節中，我們將分別說明每項在 2010 年新開發之工具的效能評估成果，接著說明每項在 2009 年開發而 2010 年完成之工具的效能評估成果。

■ **2010 年新開發並完成之工具**

- Wimax 使用者之頻寬檢測及基礎弱點掃描系統

WSBW 是透過流量檢測的方式來判斷使用者是否遭受 DoS 攻擊，因此我們透過模擬網路攻擊的方式來對本系統進行測試。首先我們先對一般情況進行測試，在沒有受到 DoS 攻擊時對使用者進行檢測，以下是實驗中受測者的環境設定。

- ◆ 作業系統 : Winodws XP
- ◆ 網路介面 : WiMAX
- ◆ 網路速度 : 下行 4Mbps/上行 1Mbps

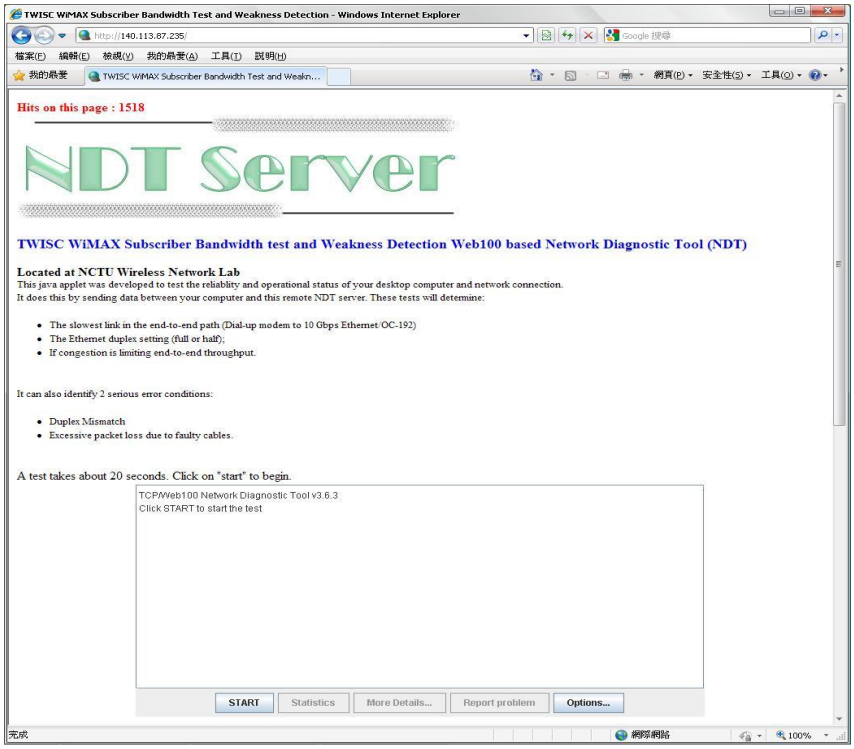


圖 5- 1、WSBW 首頁

首先，受測者進入 WSBW(如圖 5- 1)的主畫面，等待中間的 Java Applet 載入完成後點擊「Start」按鈕開始進行檢測動作，檢測完畢後會在 Java Applet 中顯示結果，檢測結果如圖 5-2。

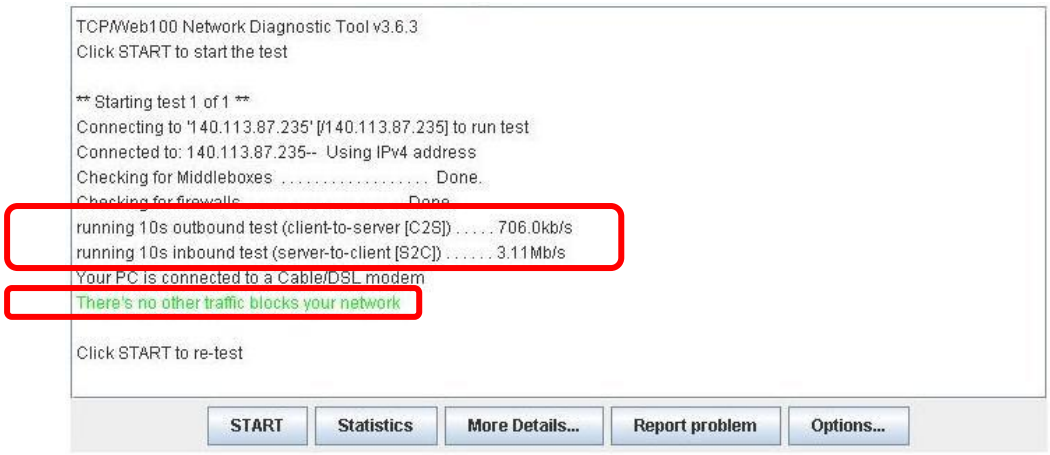


圖 5-2、測試結果(1)

在這個測試中，我們使用的是下行 4Mbps、下行 1Mbps 的 WiMAX 帳戶，由上述圖表測得的結果可看出在使用者未受到攻擊的情況下，上行與下行的速度是很接近系統廠商提供的速度上限值，因此 WSBW 也根據此數據判斷目前並沒有其他網路流量阻擋了使用者的網路頻寬。接下來我們對相同的使用者進行 DoS 的攻擊，並且進行檢測，測試結果如圖 5-3。

圖 5-3、測試結果(2)

由於受到 DoS 的攻擊，從圖中可以看出上行與下行的速度明顯降低，與使用者的速度上限值 4Mbps/1Mbps 有顯著的差距，而且在測試時間結束時，Server 端還有封包在 Queue 內尚未傳送完畢，WSBW 根據這個資訊判定目前有其他網路流量阻擋了使用者的網路傳輸，很有可能是來自網路上的 DoS 攻擊。透過 WSBW 系統可檢測出此類攻擊，提醒使用者該對此攻擊進行防禦措施。

- 網站伺服器安全滲透檢測系統

本計劃已於 2010 年完成網站伺服器安全滲透檢測系統，此系統會針對現有網站安全漏洞進行偵測，透過遠端掃描以及比對網站回傳之封包來判斷是否具有

系統漏洞。為了說明我們的系統可有效檢測網站伺服器的安全性，我們利用 Linux 2.6.45-22 來架設網站伺服器安全滲透檢測系統，另外我們架設一台用來測試的網站伺服器於 linux 2.6.32-26，並同時安裝 Blog 套件 WordPress 1.2 版。

在此測試用的網站伺服器上有一已知漏洞(即瀏覽器可能會執行由攻擊者所插入惡意 JavaScript 語法)。表 5-1 顯示從 WSS 系統產生的檢測報告中擷取的片段資訊。我們可以發現此網站伺服器具有 XSS 弱點、其根目錄底下具有可疑資料夾、以及發現 PHP Easter Egg (攻擊者可藉由 PHP 開發者名單來推測 php 版本，如圖 5- 4)。圖 5-5 顯示一位使用者連上此具有漏洞的網站伺服器，跳出視窗顯示此網頁的確有執行 javascript，在這個情況下，使用者的 cookie 資訊將可能經由惡意的 javascript 傳送給惡意人士，造成使用者資訊外洩。

表 5- 1、測試網站伺服器的分析報告節錄

URI	/index.php/"><script><script>alert(document.cookie)</script><
HTTP Method	GET
Description	/index.php/"><script><script>alert(document.cookie)</script><: eZ publish v3 and prior allow Cross Site Scripting (XSS). CA-2000-02.
URI	/admin/index.php
HTTP Method	GET
Description	/admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
URI	/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
HTTP Method	GET
Description	/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests which contain specific QUERY strings.

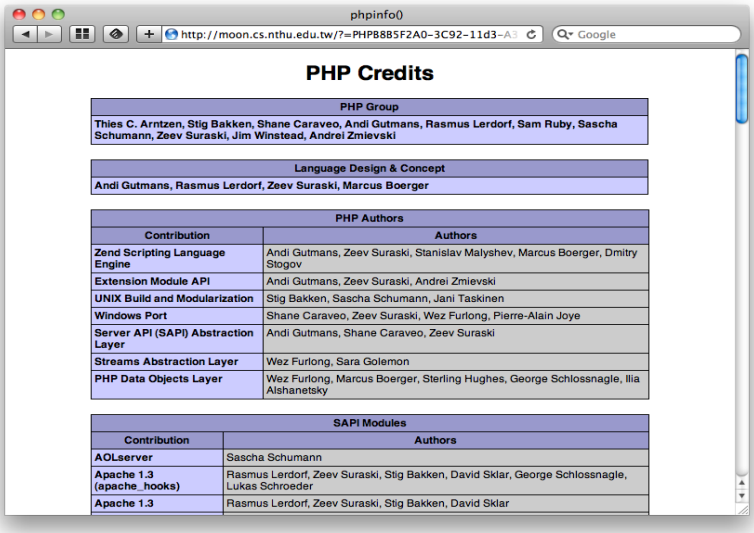


圖 5- 4、PHP Easter Egg 開發者名單

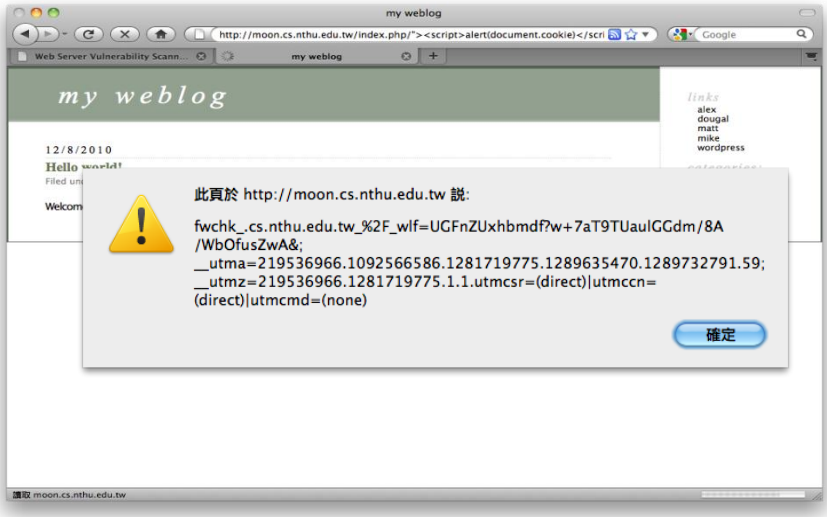


圖 5- 5、受測網頁 xss 漏洞

- Android 行動裝置惡意網頁檢測工具

Android 行動裝置惡意網頁檢測工具可即時檢測使用者欲瀏覽的網頁是否含有惡意行為，該工具藉由建置規則、建立黑白名單、增強 JavaScript 函式的保護來避免網頁上的惡意語法產生危害，並明確地提供給使用者安全等級評估及惡意行為描述，並結合 Google SafeBrowsing 提供互補性的資訊給使用者參考。此工具實作於 Android 瀏覽器(WebKit)及提供網頁版本給瀏覽者使用。其中，安全等級的評估如下(如圖 5-6)：

1. Low: 安全無慮，是評等中最安全的等級。
2. Fair: 發現有存取如 cookie、reference 等隱私資訊，但未發現不當使用，仍屬安全範圍中。
3. Medium: 發現有存取如 cookie、reference 等隱私資訊，且含有不當使用的可能性，請謹慎考慮是否瀏覽或再度確認。

4. High: 明確發現惡意語法，請勿瀏覽。
5. Extremely High: 明確發現大量惡意語法，或該網站已被列入惡意網頁，請勿瀏覽。

每個等級皆有詳細的描述提供使用者參考以了解該等級所代表的意義。在等級的區分上，我們也用了不同的顏色提醒使用者，即便使用者無資安方面的相關背景知識也能輕易判讀檢測結果，了解所要瀏覽的網頁是否含有惡意行為。

圖 5- 6、系統簡介及安全評估

此工具能夠發現的惡意行為包含以下 6 種：

1. Sensitive data access - Cookie
2. Potential XSS attack
3. Write after sensitive data read
4. Alert is disallowed
5. URL is forbidden
6. And so on

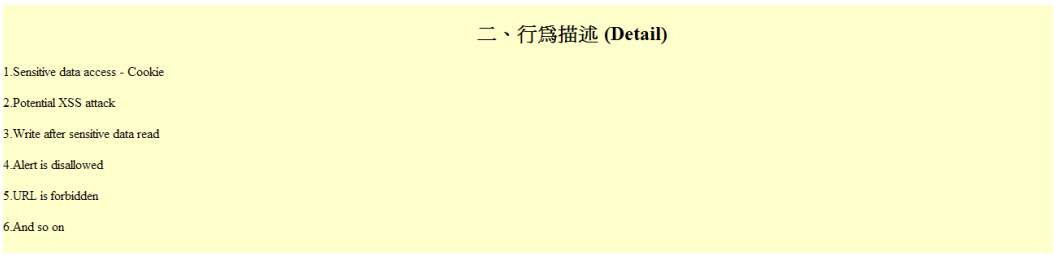


圖 5- 7、惡意行為描述

我們以一個我們自行架設的惡意網頁來做為檢測樣本，其網址為 http://140.113.210.231/~whitescars/android/malicious.php ，檢測結果如圖 5- 8 所示。檢測結果顯示該網頁的安全評估等級為 medium，且被列為可疑的惡意網頁，而它所包含的惡意行為有 sensitive data access (cookie)、write after sentive data read、javascript function is disallowed 等，可供進階的 android 使用者參考。

圖 5- 8、惡意網站分析結果

另外我們再以使用者經常瀏覽的 Yahoo 網頁作為檢測對象，從圖 5- 9 的檢測結果可以發現它的等級評估是屬於 Low，且不為可疑的惡意網頁。當然在該網頁中也沒有檢測出任何的惡意行為。

圖 5- 9、Yahoo 網站檢測結果

- Android/Java 應用軟體安全漏洞檢測工具(G-exploit)

G-exploit 旨在檢測 Android 上應用程式之弱點，幫助程式開發人員彌補程式開發中不經意發生的錯誤或是修補隱藏的安全性漏洞。由於 Java 本身就是一個以安全為優先考量的程式開發語言，因此常見的錯誤都是寫作壞習慣或是寫作規則的錯誤，較少發現可能造成重大傷害的安全性漏洞，但是仍隨著 Android 之普遍和日趨強大的功能，Android 之應用軟體安全性也更加值得注意。目前 G-exploit 可以檢測到的 java 問題包含以下類型:

1) 正確性的問題(correctness)：檢測程式設計人員沒注意到之寫作上的錯誤，避免此類寫作錯誤成為真實程式的臭蟲 (bug)。
2) 寫作壞習慣(bad practice)：檢測程式設計人員寫作時的壞習慣，例如解構子的濫用，避免不必要的錯誤。
3) 異常的程式碼(dodgy)：檢測不確定的程式行為，如未被確認的轉型等。

我們以 Snake 這個 Android 應用程式為例來介紹 G-exploit 之操作流程並驗證 G-exploit 之可行性。首先，我們將 Snake.dex 檔上傳至 G-exploit 網頁平台，並勾選檢測功能來進行靜態偵測 (見圖 5- 10)。

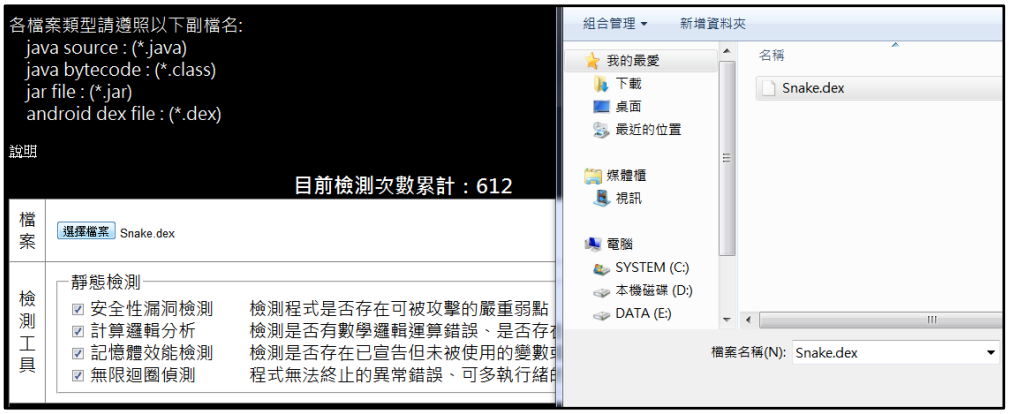


圖 5- 10、G-exploit 線上檢測平台

G-exploit 的檢測報告如圖 5-11 所示。由檢測報告可以看出，此應用程式大小為 14 kb，含有 59 個臭蟲。此檢測報告亦會提供安全漏洞的危險等級，其中 Bugs p1 之危險等級最高，Bugs p2 其次，依此類推。而報告中的 Ratio 則表示安全性漏洞的存在比例。此次實驗偵測到的安全性漏洞為 MS (見圖 5- 11)，這表示在 Snake 程式中存在一塊可被惡意程式或是經由人為的不小心而被更動的靜態區塊；MS 安全漏洞將可能造成 Snake 程式被惡意程式所控制而執行非預期之惡意行為，其解決辦法為將 Snake 程式封裝成套裝軟體 (package)。

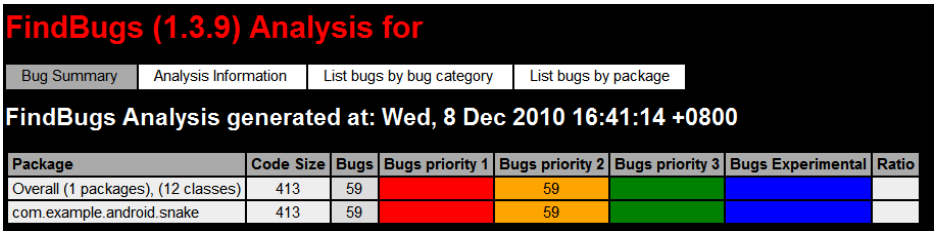


圖 5-11、G-exploit 之檢測報告

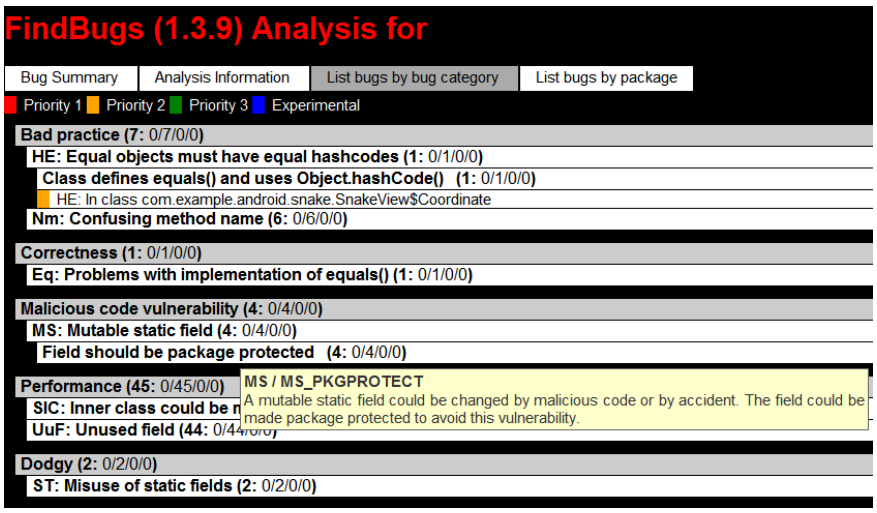


圖 5- 11、檢測結果之詳細說明

- 網路釣魚安全意識檢測

網路釣魚安全意識檢測工具 (PAT) 為本計畫所開發的個人化人員安全意識檢測工具。PAT 藉由模擬真實的網路釣魚郵件，來檢測使用者使否具備足以防範網路釣魚郵件攻擊的安全知識。PAT 的檢測流程如圖 5- 12 所示：

(1) 使用者在 PAT 網頁上申請註冊。

(2) 經由 E-mail 認證啟動帳號，即可取得讓 PAT 發送釣魚郵件的權限。

(3) PAT 提供了多樣化的釣魚郵件範本，讓使用者可全面性的檢驗自身對不同種類的釣魚攻擊是否具備足夠的判定能力。下圖分別為 PAT 所提供的檢測郵件之範例：圖 5- 13 為本開發團隊複製常見的「好康道相報」郵件，在信件中加入受測者感興趣的商品優惠訊息，吸引受測者點擊信件中隱藏之惡意連結；圖 5- 為本開發團隊針對交通大學校園內的學生信箱系統的使用者設計的測試郵件，藉由冒充學校行政單位所發出的正式公告，以測試交通大學學生對釣魚信件的防範能力。

圖 5- 12、網路釣魚安全意識檢測工具 (PAT) 的檢測流程


Dell又出包啦~~~要下單趁現在!
dell [dell@hotmail.com]
寄件日期: 2010/12/3 (週五) 下午 07:11

好康又來囉!

Dell 線上購物網站又出包啦~~~懊惱上次來不及下單嗎?沒關係，這次還有機會。

8,499 元的 22 吋液晶螢幕，只賣你 3,499 元。

要搶購要快喔，詳情請至 Dell 線上購物網站

好東西要與好朋友分享，趕快將這封信再轉寄出去。

圖 5- 13、常見釣魚郵件內容


D2系統密碼重新設定要求確認
d2 [d2@nctu.edu.tw]
寄件日期: 2010/12/3 (週五) 下午 07:11

國立交通大學資訊技術服務中心
National Chiao Tung University Information Technology Service Center

王小明 您好

近日，**國立交通大學資訊技術服務中心**收到您的重設 D2 密碼要求，為確認是本人申請，請先下載 D2 密碼系統變更申請表，填寫完畢後再將表格帶至中心變更密碼，請攜帶身份證明文件(如學生證、校友證)。

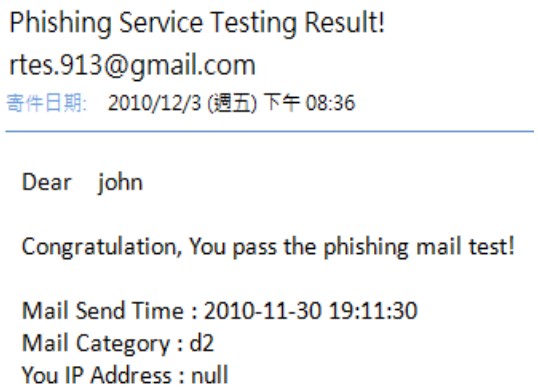
若不需要重設 D2 系統密碼，請至 D2.NCTU.edu.tw 取消密碼重設要求。

注意：請不要回覆此郵件，郵件是系統自動寄出，因此將無法收到回覆。

National Chiao Tung University 資訊技術服務中心

圖 5- 15、PAT 所使用之釣魚郵件範本

測試完畢後，PAT 會提供使用者一份詳盡的安全意識檢測報告，幫助使用者快速了解自身安全觀念之弱點，降低遭受釣魚攻擊之可能性。該檢測報告包含了釣魚信件的範本類別，釣魚信件的寄送時間等資訊，如圖 5- 14 所示。當受測者點擊釣魚信件中之惡意連結後，PAT server 端會紀錄受測者點擊連結的時間，以及受測者的 IP 位址等資訊。這些資訊將一併檢附在寄送給使用者的檢測報告中 (如圖 5- 15 所示)，以利使用者了解自身安全意識之弱點，降低日後遭受同類型釣魚信件攻擊的可能性。


Phishing Service Testing Result!
rtes.913@gmail.com
寄件日期: 2010/12/3 (週五) 下午 08:36

Dear john

Congratulation, You pass the phishing mail test!

Mail Send Time : 2010-11-30 19:11:30
Mail Category : d2
You IP Address : null

圖 5- 14、安全意識檢測報告(1)


Phishing Service Testing Result!
rtes.913@gmail.com
寄件日期: 2010/12/3 (週五) 下午 08:39

Dear john

Sorry! You don't pass the phishing mail test!

Mail Send Time : 2010-11-30 20:38:30
Mail Click Time : 2010-12-03 20:38:19
Mail Category : yahoo
You IP Address : 140.113.151.67

圖 5- 15、安全意識檢測報告(2)

- 使用者網路攻防能力評估系統 (Wargame)

由於現實生活中所發動的網路攻擊事件、軟體破解之行為都是不合法的，所以一般使用者難以了解到實際上的網路攻擊。因此我們建立起了一個 Wargame 模擬平台，旨在加強人們在意識到資訊安全問題的存在與相關能力的培養。在我們的平台上我們建立起了許多的遊戲關卡，透過闖關的模式，讓使用者在闖關的過程中一步一步的了解和學習。關卡中包含了許多已知的漏洞或是人為設計出來的程式安全問題，使用者可以在我們所建立的平台上模擬日常生活中常可見到的實際網路攻擊，進而對於資訊安全方面的概念更加了解，並了解到網路攻擊背後實際上的原理，進而得知如何開發出安全的程式抑或保護自己的電腦。

Wargame 平台目前擁有 34 個關卡，擁有了 500 多位使用者。平台上的能力檢測部分可分成三大類：Attack(攻擊)、Crack(破解)、Forensics(鑑識)。Attack(攻擊)是以公開現有的程式及程式碼，讓使用者嘗試去找出程式中可能的弱點及漏洞，並針對這些潛在的問題進行 I/O(Input/Output)的攻擊行為，這類型的關卡可以讓使用者了解到撰寫程式碼上可能會造成程式漏洞的問題，進而訓練使用者在撰寫程式碼時避免犯下同樣的錯誤。Crack(破解)是提供已編譯好的執行檔程式，讓使用者透過逆向工程及反組譯來猜測、修改及破解執行程式，從而改變執行結果，在這些關卡中，使用者可以學習到逆向工程方面的能力，藉以了解程式實際上運作的流程。Forensics(鑑識)則是透過資料隱藏法、資料偽裝法、資料加密等手段，將訊息隱藏起來，讓使用者透過各種方法來分析可疑的內容，從這類關卡中可以讓使用者知道運用在程式上常見的加殼、加密手法。當使用者完成此三大類的每一個關卡，都可於闖關結束後獲得一組金鑰(key)，並將得到的金鑰輸入到網頁中進入下一關。

而在 Wargame 平台的每個關卡都有提供解題提示，透過這種方式引導使用者找到解題的方向，以降低初學者的入門門檻。Wargame 平台也設有使用者論壇討論區，讓使用者及出題者可以互相討論切磋，也是新手諮詢的好地方。Wargame 平台已對外開放了半年多，已有眾多學生群及專業人士一同參與學習和競爭排名。目前已有 92 位使用者成功闖 3 關(含)以上、53 位使用者成功 5 關(含)以上，及

23 位使用者成功闖 10 關(含)以上。最高成功闖關數為 29 關(使用者代號為：cb520、mtk)，並無人把 34 關全數通過。圖 5- 16 為我們的 Wargame 平台首頁。

圖 5- 16Wargame 平台首頁

■ **2009 年起開發，2010 完成之工具**

● 大規模遠端系統安全滲透檢測網

大規模遠端系統安全滲透檢測網是一網頁介面的線上服務，服務對象從個人到企業團體均適用。使用者可透過瀏覽器連上滲透測試網，對使用者電腦進行系統滲透檢測。除了提供易讀的檢測結果之外，對於滲透成功的項目，也會提供給修正建議，讓使用者能夠提升其電腦的安全性。

使用者透過瀏覽器連上 RSPTN 首頁（圖 5- 179），點選上方選單中的“Security Test”項目，將會呈現滲透檢測的使用條約，向使用者說明 RSPTN 系統以及滲透檢測的使用限制。使用者若同意進行檢測，點選使用條約下方的 “I Accept”按鈕即可立刻進行系統滲透檢測（如圖 5-20）；否則，點選 “I Decline”按鈕回到首頁。

圖 5- 17RSPTN 首頁

圖 5- 18、選擇是否接受檢測的畫面

RSPTN 將開始對使用者的系統進行滲透檢測。首先進行收集系統資訊，偵測使用者 IPAddress 以及作業系統版本；接下來進行連接阜掃描的動作，偵測使用者系統開啟了哪些網路連接阜；最後根據開啟的連接阜清單，進行對應的系統滲透攻擊。因為進行系統安全滲透檢測需要花費不少的時間，檢測的進度將會同步顯現於網頁上，告知使用者目前檢測完成的程度（如圖 5-21）。

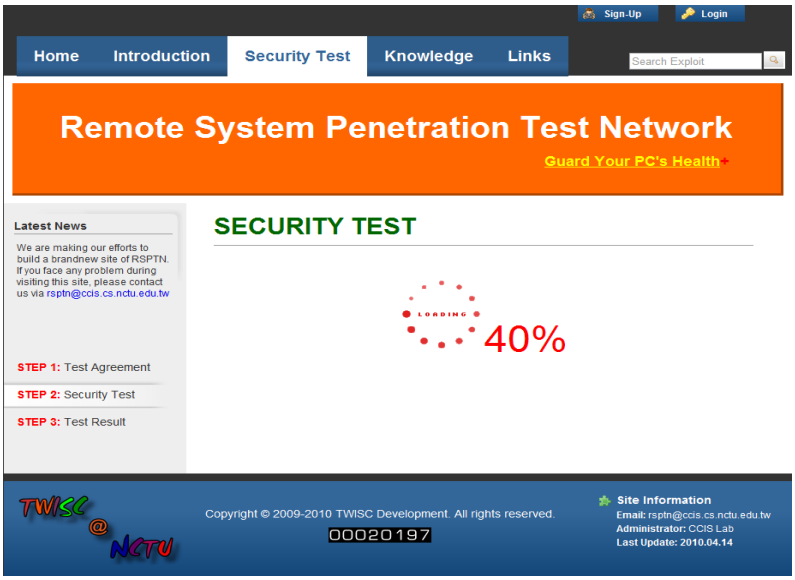


圖 5- 191、檢測進度示意圖

根據使用者網路狀態及系統防火牆設定，滲透檢測通常需要約五分鐘到十分鐘左右（根據網路狀況而定）才能完成檢測。待滲透檢測完畢後，會顯示出檢測結果(如圖 5-22 所示)，以提供使用者系統資訊、網路連接阜開啟狀態、以及滲透檢測的結果。使用者如果需要進一步的漏洞資訊，可以點選漏洞旁的 "Click!"連結，此系統會提供更詳細的漏洞資訊及相關建議（請見圖 5-23）。

在圖 5-22 中，我們以剛灌好的 Windows XP SP3 系統為檢測對象（此系統上並無任何防毒軟體、以及無防火牆設定）。 此工具發現該系統並開啟了 6 個網路連接阜（分別是 135、139、445、3389、16992、16993），滲透檢測總共花費 312 秒，總

共發動 132 種滲透測試，其中兩種滲透測試都可成功取得檢測對象的操作權限，此兩種攻擊都建立在 Windows/smb/ms08_067_netapi 這個系統漏洞。因此，利用 RSPTN，使用者可輕鬆地進行電腦安全檢測，讓使用者能夠提升其電腦的安全性。

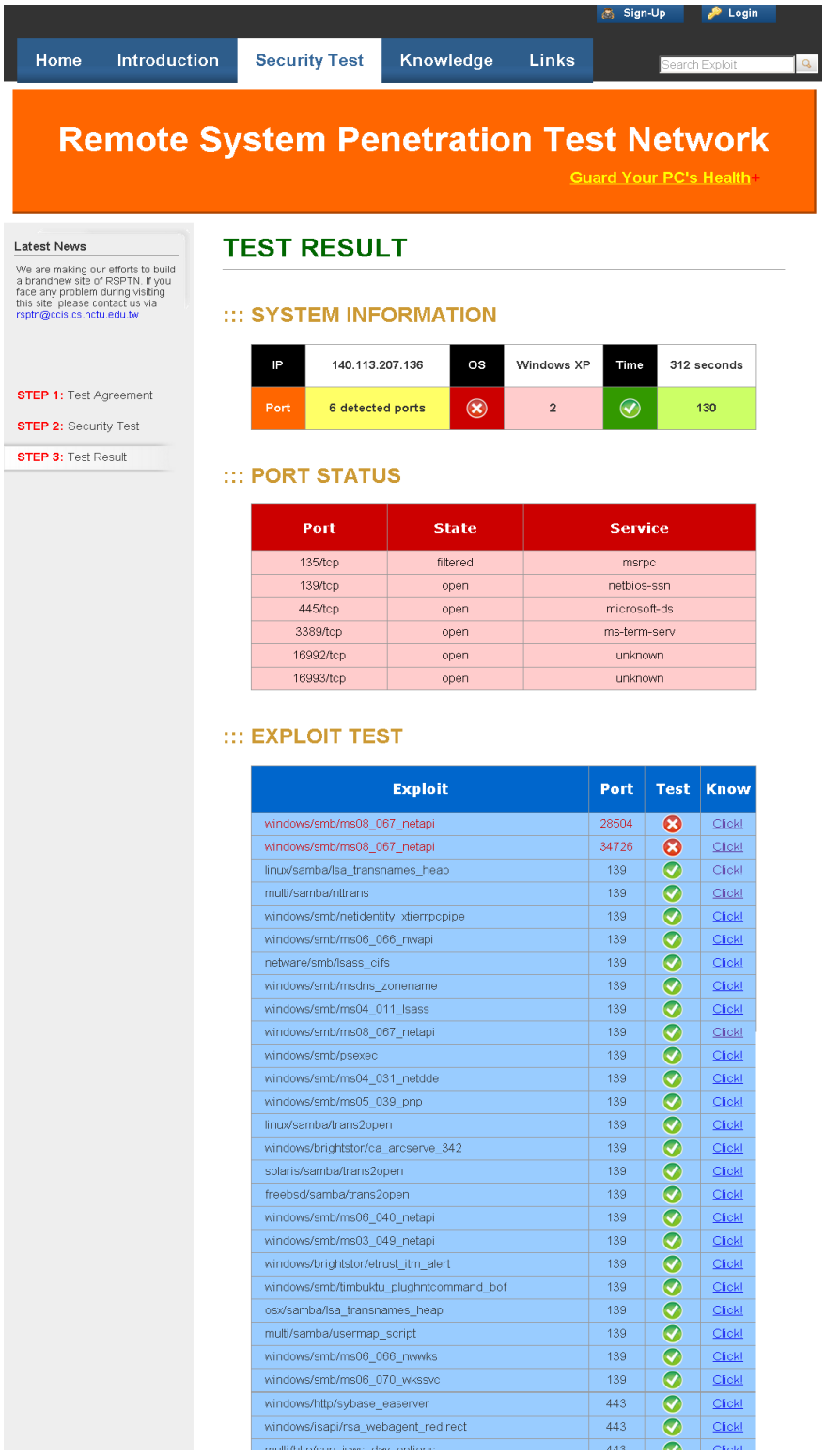


圖 5- 20、檢測結果

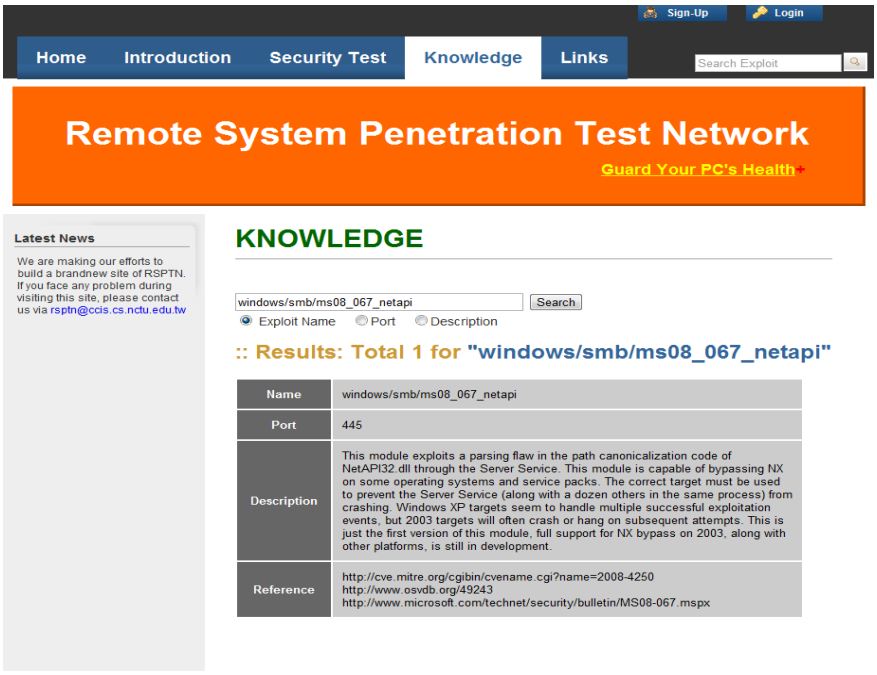


圖 5- 213、漏洞資訊示意圖

- 異質多網擬真模擬平台

異質多網擬真模擬平台可用於進行異質多網的安全測試。此平台支援異質網路之特性，可協助測試新的安全機制和產品在異質無線網路下之效能和表現。使用者可以於此平台上進行 Wired、Wi-Fi、WiMAX 異質網路實驗，毋需重新建置實體實驗環境。以下將介紹二項實驗來展示異質多網擬真模擬平台的可行性和應用性。第一是無線竊聽攻擊實驗，第二是分散式阻絕服務 (Distributed Denial of Service，簡稱 DDoS)攻擊實驗。

1. 無線竊聽攻擊：

相較於有線網路，無線網路以空氣為傳送介質的特性使其更易於遭受攻擊，竊聽攻擊是無線網路中常見的攻擊之一。我們的開發團隊實作了 WiMAX 的虛擬驅動程式，該驅動程式完全符合 IEEE 802.16 標準，因此在這個實驗中，我們除了呈現此平台北對於網路攻防實驗的支援度之外，也可檢驗 WiMAX 虛擬驅動程式之正確性與此平台監控功能的有效性。此外，我們的開發團隊亦修改了 Wireshark 網路封包檢視軟體，使其支援 WiMAX 封包的格式判斷，增加此平台的應用性。從圖 5-24 中可以看到我們正進行無線竊聽來擷取 WiMAX 封包。

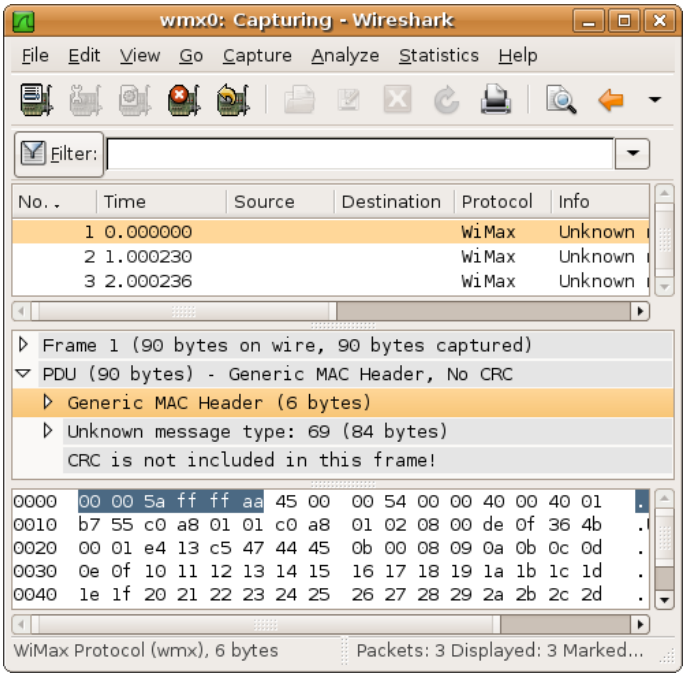


圖 5- 22、以 WiMAX 為例之無線竊聽攻擊實驗

2. DDoS 攻擊實驗：

DDoS 攻擊實驗除了能測試此模擬平台對於網路攻防實驗之支援度之外，亦可用於測試此平台之穩定性。圖 5- 23 為利用此模擬平台架設的模擬網路環境，在此環境中，攻擊者 (Attacker)透過其他機器 (Zombie1、Zombie2)對受害者 (Victim)進行的 DDoS 攻擊；在 DDoS 攻擊之下，受害者電腦的 CPU 使用率與網路接收封包量將劇增。此模擬平台的 DDoS 偵測模組則在 DDoS 攻擊啟動後偵測到此一攻擊行為，當封包數量劇增超過定義的臨界值時，如圖 5- 24 所示，偵測模組則會發出紅色警示。如果攻擊者停止攻擊，則此模擬平台中的 DDoS 偵測模組將會得到新的系統資訊。明顯地，受害端的系統 CPU 使用率將回到正常狀態(見圖 5- 25)。

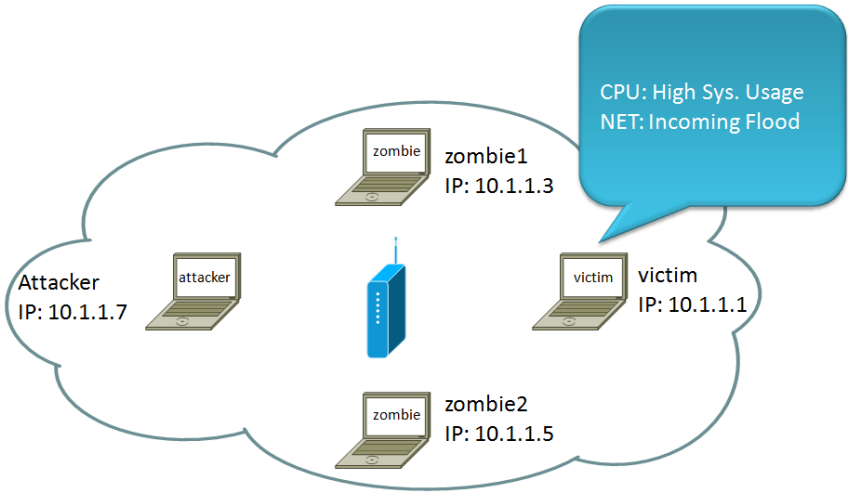


圖 5- 23、模擬網路環境

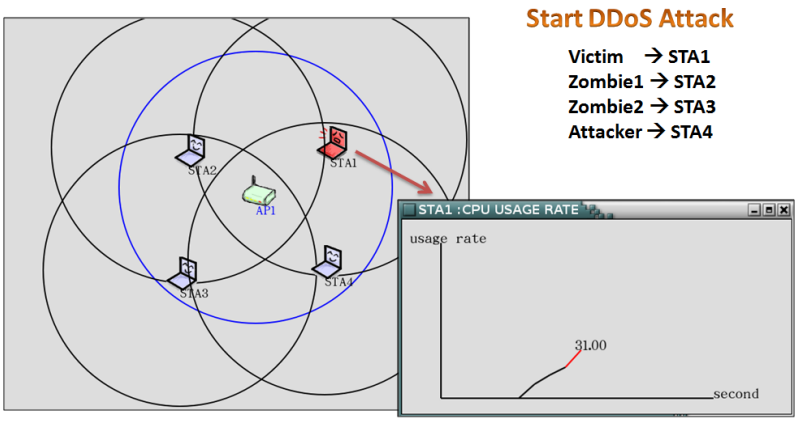


圖 5- 24、異質多網擬真模擬平台偵測到 DDoS 攻擊

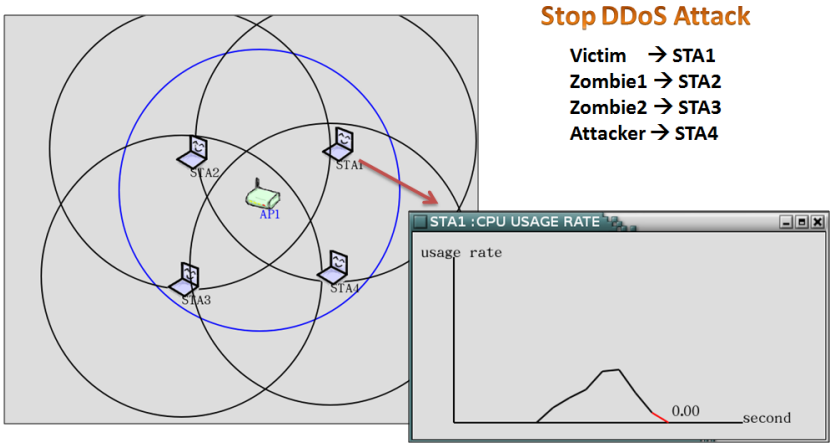


圖 5- 257、DDoS 攻擊停止

除了以上二個攻擊實驗，表 5- 2 亦條列異質多網擬真模擬平台所能支援的網路攻擊實驗，並且比較與 DETER 之間的差異。以駕駛攻擊 (war driving) 為例，該實驗需能夠仿真可搜尋無線網路且蒐集封包之行動代理人 (mobile agent)，然而 DETER 是專為有線網路設計的安全實驗平台，無法支援專屬於無線網路的駕駛攻擊。而此模擬平台的「虛擬天線–虛擬驅動程式」之設計能仿真模擬無線訊號之衰減，並且此模擬平台監測模組能解析收到的無線封包，因此此模擬平台能有效地支援駕駛攻擊實驗。

表 5- 2、可仿真的網路攻擊實驗比較表

網路攻擊	DETER	異質多網擬真模擬平台
駕駛攻擊 (War driving)	No	Yes
MAC 欺騙 (MAC spoofing)	No	Yes
IP 欺騙 (IP spoofing)	Yes	Yes
有線竊聽 (Wired eavesdropping)	Yes	Yes
無線竊聽 (Wireless eavesdropping)	No	Yes
中間人攻擊 (Man-in-the-Middle)	Yes	Yes
邪惡雙生 (Evil Twin)	No	Yes
分散式阻絕服務 (DDoS)	Yes	Yes

- 惡意執行檔案檢測系統

本工具針對惡意軟體的分析進行開發，所分析的內容包含了是否使用加殼保護、是否在引用的外部函式庫中使用了敏感的函式、副檔名是否與檔案實際的內容不合及是否含有可疑字串等。以下我們將針對兩個項目進行實驗：加殼保護以及外部函式庫的偵測。首先檢測的是一個未知使用何種加殼方式的加殼病毒，接著是一個用來與之比較的已知加殼方式的加殼程式。

一、未知加殼方式的加殼病毒

測試檔案為一隻名為 0C9C4681802F.exe 的病毒，它會竊取中毒使用者的帳號密碼。在圖 5- 的檢測報告中可以看到，在 PE File Format Anaylsis 中含有 encrypted executable 及 packed or encrypted executable 兩項，代表這隻程式已經透過加殼將自己的執行行為隱藏起來，藉此躲避防毒軟體的掃描，藉由本工具可以偵測出這樣的行為並且告訴使用者。

```
========== Suspicious String Analysis ==========
IP :
URI :
Windows UNC Path :
Unix Path :
IFrame :
Embed :
Executable Filename :
========== File Format Analysis ==========
FIle Format : MS-DOS executable PE  for MS Windows (GUI) Intel 80386 32-bit
FIle Exename : exe
========== PE File Format Analysis ==========
Suspicious imported APIs:
Entropy Analysis:
ju2       0.0 Text     MEM_WRITE,CNT_UNINTIALIZED_DATA, MEM_EXECUTE, MEM_READ
p5        7.982 Encrypted ExecutableMEM_WRITE,CNT_CODE,
```

```
MEM_EXECUTE, CNT_UNINTIALIZED_DATA, MEM_READ
7i      7.241 Packed or Encrypted ExecutableMEM_WRITE, CNT_UNINTIALIZ
========== Code Obfuscation Analysis ==========
Unknown packer found.



========== End of Analysis ==========
```

圖 5- 28、未知加殼方式的加殼病毒檢測報告

二、已知加殼方法的加殼程式

測試檔案為”sendsrv.exe”這個執行檔，從圖 5- 29 的檢測報告可以看出該執行檔呼叫了許多系統的 kernel API，此外還做了 ThreadInjection。在報告的最後我們還可以看到這個程式使用了「Safeguard 1.03 -> Simonzh」進行加殼。透過本工具可以很容易看出程式呼叫了哪些 API，藉此來判斷出這個程式是否有可能是一個惡意程式。

```
========== Suspicious String Analysis ==========
IP :
URI :
Windows UNC Path :
Unix Path :
IFrame :
Embed :
Executable Filename :
========== File Format Analysis ==========
FIle Format : MS-DOS executable PE  for MS Windows (GUI) Intel 8038632-bit
FIle Exename : exe
========== PE File Format Analysis ==========
Suspicious imported APIs:
Process Manipulation
   ReadProcessMemory            KERNEL32.DLL
   OpenProcess                  KERNEL32.DLL
   Process32Next                KERNEL32.DLL
   Process32First               KERNEL32.DLL
   WriteProcessMemory           KERNEL32.DLL
Thread Injection
   CreateRemoteThread           KERNEL32.DLL
Window Manipulation
   FindWindow                     USER32.DLL
Entropy Analysis:
.text       7.992 Encrypted Executable      MEM_WRITE,          CNT_CODE,
MEM_EXECUTE, MEM_READ
.idata      4.220 Text                      MEM_WRITE, CNT_UNINTIALIZED
========== Code Obfuscation Analysis ==========
Target may be obfuscated(or written) by :
Safeguard 1.03 -> Simonzh
```

```
========== End of Analysis ==========
```

圖 5- 29、已知加殼方法的加殼程式檢測報告

從以上兩項檢測報告可得知一個惡意軟體就算意圖使用加殼程式來規避防毒軟體的偵測，也可以被我們開發的惡意執行檔案檢測系統偵測出來，此系統也可以補足一般防毒軟體使用特徵值檢測所不足的地方。

- 動態惡意軟體行為分析檢測工具(MBA@TWISC)

本工具的主要目標為分析惡意軟體在執行期間的所有行為，包含了修改哪些檔案、新增了哪些系統登錄值以及對系統核心所做的修改等。以下我們針對三個在網路上或是生活中流傳甚廣的真實惡意程式的分析結果：

1. 隨身碟病毒 KAVO

KAVO 是一個非常有名的隨身碟病毒，會在電腦中常駐並且感染所有新插進來的隨身碟，並在隨身碟中寫入新的感染程式感染其他電腦。

我們利用 MBA@TWISC 來檢測 KAVO。圖 5- 30 是本工具的分析報告，根據分析到的惡意行為可分成多個項目，其中「Registry Diff Scanning」是 Windows 系統登錄值遭到變更的項目，「Disk Diff Scanning」則是檔案系統遭到變更的項目，包含了新增、刪除或修改檔案等行為，「Driver Diff Scanning」則是系統驅動程式遭到變更的項目。由分析報告可以看到 KAVO 病毒會修改系統登錄值有關開機啟動的部分，使得系統在一開機時就會啟動病毒主程式，藉此達成持續感染新插入的隨身碟的目的。此外 KAVO 病毒也會在檔案系統中新增幾個可疑檔案，並且在系統核心中加上新的驅動程式，在分析報告上可以很明顯的看出。

```
HKCU/Software/Microsoft/Windows/CurrentVersio
n/Run/kava C:\WINDOWS\system32\kavo.exe
===== Disk Diff Scanning =====
/WINDOWS/system32/kavo.exe
/WINDOWS/system32/kavo0.dll
/Documents and Settings/dsns/Local
Settings/Temp/wdagnb7.dll
===== Driver Diff Scanning =====
0x00f8928000 0x006000 wincab.sys
```

圖 5- 30、KAVO 病毒的檢測報告

2. Stoned bootkit

Stoned bootkit 是一隻會去修改系統開機磁區的程式，藉由修改開機磁區使得他能夠在 Windows 之前就啟動並留在記憶體中，如此可以取得存取整個系統的權力。我們接著利用 MBA@TWISC 來檢測 Stoned bootkit。在檢測報告(如圖 5- 31

所示)的「MBR Modification Scanning」中可以清楚看到這隻程式會修改 MBR 開機磁區。

===== Disk Diff Scanning =====
/Stoned/Drivers/Sinowal Extractor.sys /Stoned/Master Boot Record.bak /Stoned/Applications/Sinowal Loader.sys /Stoned/Applications/Hibernation File Attack.sys /Stoned/Applications/Forensic Lockdown Software.sys /Stoned/Applications/Windows.sys //$Secure:$SDH //$Secure:$SDS /Stoned/Drivers/Sinowal.sys /Stoned/Drivers/Black Hat Europe 2007 Vipin Kumar POC.sys
===== MBR Modification Scanning =====
MBR Modified

圖 5- 31、Stoned bootkit 的檢測報告

3. FUTO rootkit

FUTO rootkit 其實並不是一隻惡意程式，而是一個用來隱藏其他 Process 的工具。圖 5- 32 的檢測報告是我們用 FUTO rookit 來隱藏 notepad.exe 時產生的的分析結果。要特別提的是，隱藏一個 Process 這件事有非常大的可能性是個惡意行為，因為只有惡意程式會想要隱藏自己，來達成在使用者不知情的情況下進行攻擊。一個正常的程式並沒有權力隱藏自己，就連系統管理者都無法察覺到他的存在。因此若偵測到一個程式會隱藏 Pcocess 的話，有很高的機率可以斷定他是個惡意程式。圖 5- 32 的檢測報告中，可以在「Process Diff Scanning」項目中看到這個程式修改了系統的 Process Table，意圖隱藏一個程式。

===== Driver Diff Scanning =====
0x00f7a40000 0x010000 msdirectx.sys
===== Process Diff Scanning =====
notepad.exe

圖 5- 32、FUTO rootkit 的檢測報告

由上面的分析報告可以看出，相較於其他分析工具，本工具並不需要事先知道任何惡意手法或者程式碼及病毒碼的特徵，只要這個惡意程式會對系統進行修改，或是新增一些可疑的檔案，MBA@TWISC 都可以偵測並且列出其所有行為。

- 使用者敲鍵行為辨識系統

使用者敲鍵行為辨識系統利用使用者的敲鍵行為來進行使用者身分的識別。為了有效評估系統效能，我們首先建構一個由 JavaScript 所寫成的網頁來進行樣

本收集，時間單位為微秒。收集對象共有 53 位志願者，這些志願者每天提供 10~20 個樣本，樣本採取為期兩個月，同時也請了 103 位匿名使用者試著去輸入他們的帳號密碼，用來測試系統對非法使用者的拒絕率，每個帳號會遭到 50~200 次的攻擊，總共為 3126 次。此外，我們亦利用 AR Model 分別取 order 1 至 5 進行比較，其中 AR Model 的參數是由 Burg's Algorithm 算出。最後，列出各個 EER (equal error rate)進行比較。EER 的比較結果如表 5- 。而 Digraph 以及 Trigraph 則分別為不同的馬可夫鏈的建立方式，我們可發現在 AR model = 1 的時候，系統的 EER 可降低至 2.19%。

表 5- 3、COMPARATIVE RESULTS OF EER IN EXPERIMENT

	Analysis with Digraph	Analysis with Trigraph
AR(1)	2.19%	2.93%
AR(2)	2.37%	2.81%
AR(3)	2.37%	2.68%
AR(4)	2.49%	3.08%
AR(5)	2.64%	3.08%

我們也分析了將生物行為改變趨勢作為生物特徵時所增加的效益，發現有超過一半的使用者的準確率上升 (見表 5-)。而平均增進效益如表表 5-。

表 5- 4、THE RATIOS OF USERS HAVING IMPROVED EER

	Analysis with Digraph	Analysis with Trigraph
AR(1)	41.18%	50.00%
AR(2)	50.00%	55.88%
AR(3)	44.12%	44.12%
AR(4)	55.88%	52.94%
AR(5)	52.94%	55.88%
Average	***48.82%***	***51.76%***

表 5-5、THE AVERAGE PROMOTION OF EER WITH DIFFERENT ORDER OF AR MODEL IN THE EXPERIMENT

	Analysis with Digraph	Analysis with Trigraph
AR(1)	6.21%	5.79%
AR(2)	5.17%	5.69%
AR(3)	5.84%	5.49%
AR(4)	5.73%	6.76%

AR(5)	4.27%	6.64%
Average	***5.44%***	***6.07%***

圖 5-1 列出我們的系統與其他各研究的比較。在實驗結果中可以發現本系統產生的 EER 範圍在 2.19%~3.08%，就目前而言，比其他研究要來的準確，之前研究出現最佳的 EER 是 2.54%，這些研究大多未將生物行為改變列入考慮。

雖然在本次實驗中只增進大約 50%使用者的準確率，但如果我們把採取樣本的時間拉長，生物行為的改變將更為明顯，同時也會明顯地提升辨識的準確率，而本次實驗也針對 digraph 以及 trigraph 來做比較，結果顯示大多時候 digraph 的表現比 trigraph 好，因此本系統採取 digraph。

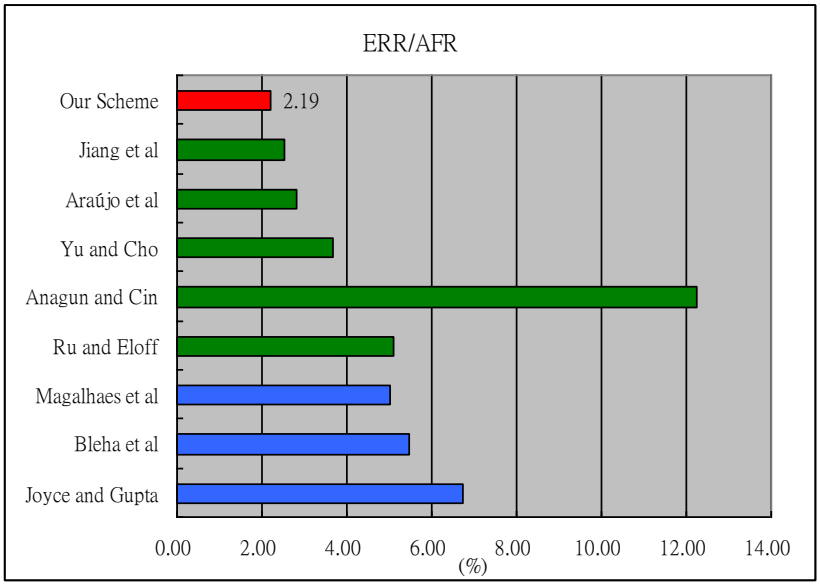


圖 5-33、EPR/AFR 比較

綜合上述，可以發現利用容易改變的生物行為模式來進行辨識，才是有效辨識的方法。我們結合自回歸模型、高斯模型、馬可夫鍊模型以及數學統計方法，於每次使用者合法登入時微調舊模型，使之一直可以維持良好的準確率。

- 3.5G 核心網路拓樸檢測工具

jtracert 為一網路拓樸的探索工具，該工具可讓使用者任意指定兩個以上的網路節點，透過各種網路協定，找出網路節點之間的路由路徑。本工具之特色包括：

1. 圖形化使用者介面：可通訊網路中的弱鏈結與可能成為攻擊目標的受害節點。
2. 快速追蹤法：藉由改善路由路徑追蹤方法可以比一般路徑追蹤法更快得到相關節點之間的路由資訊。
3. 多協定支援：本工具支援多種網路協定，包括 ICMP、TCP 等。使用者可以依據當時的網路設定與狀況選擇適用的網路協定來收集路由資訊。
4. 網路區域拓樸圖：本工具可提供單一路由路徑之圖形化顯示介面，亦可

整併多筆路由路徑，建構出涵蓋所指定之多個來源/目的節點的區域網路拓樸圖。

5. 拓樸分析：透過路由路徑的合併與內/外分支度的分析，本工具可找出該區域拓樸之中最可能成為攻擊目標的受害節點。

本工具的快速追蹤、多協定支援、網路區域拓樸圖與拓樸分析等都是新設計開發的方法與功能，這些都是傳統的 tracert (trace route 公用程式)中所尚未提供的。

本計畫研究人員針對台灣數家 ISP 業者的 3.5G 網路進行拓樸探索，透過拓樸探索實驗可瞭解 ISP 業者在某些定點的網路拓樸結構，以規劃滲透測試之流程。在本實驗中，我們使用一台安裝 jtracert 的主機作為來源節點，與一台透過 3.5G 上網的智慧型手機當作目的節點，來進行拓樸探索實驗，智慧型手機會不斷的嚐試和 ISP 業者的網路進行連線，以取得不同的 3.5G 網路的 IP 位址。其實驗結果如**錯誤! 找不到參照來源**。所示：

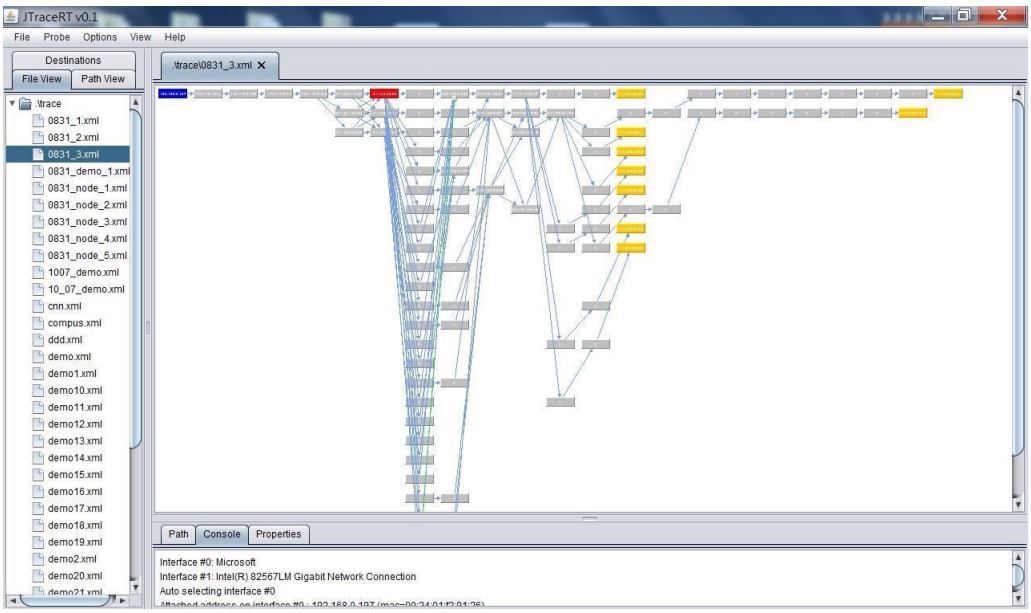


圖 5- 34、使用 jtracert 探索 3.5G 網路架構

圖 5- 34 中，藍色的節點代表安裝 jtracert 之主機的 IP 位址，黃色的節點為智慧型手機取得的 3.5G 網路的 IP 位址，灰色的節點為路由經過之中間節點。由實驗結果可發現，從主機端發送封包至不同智慧型手機取得 3.5G 的 IP 位址時，其路由路徑都會經過圖中標為紅色之受害節點 (其 IP 位址為 211.22.38.66)。我們可進一步透過 WHOIS/IPWHOIS **錯誤! 找不到參照來源**。或是 WhatIsMyIPAddress.com[28]等網站服務，查出此 IP 的公開資訊，例如此 IP 之設備為中華電信公司架設寬頻網際網路 (Broadband Internet access) 之伺服器等，作為之後進行滲透測試時的參考資料。

六、 整體計畫成果

本計畫在 2009 年執行初期便邀請研考會、國家資通安全會報技術服務中心、工研院、資策會、國安局、中科院、中華電信、友訊科技、明泰科技、宏碁科技等單位共同協助規劃合作。在 2010 年，我們持續與中華電信、友訊科技、工研院、資策會、中科院共同合作開發多種安全檢測工具。目前此平台可分成四大檢測類別：網路安全檢測、系統安全檢測、軟體安全檢測以及人員安全意識檢測。從 2009 年到 2010 年，我們在此平台上共累計建置與開發 16 個工具以及 1 個異質多網擬真模擬平台(詳細列表請見表 6-1，詳細功能說明請見第四章)。藉由這些檢測工具的開發，我們可提供政府機關、財團法人及高科技廠商多樣化的安全檢測的服務，幫助上述單位發現漏洞及弱點。

表 6-1 檢測工具開發清單

2010 年新開發並完成	Wimax 使用者之頻寬檢測及基礎弱點掃描系統
	網站伺服器安全滲透檢測系統
	Android 行動裝置惡意網頁檢測工具
	Android/Java 應用軟體安全漏洞檢測工具(G-exploit)
	網路釣魚安全意識檢測
	使用者網路攻防能力評估系統 (Wargame)
	3.5G 行動裝置滲透檢測工具
2009 年起開發，2010 完成之工具	大規模遠端系統安全滲透檢測網
	異質多網擬真模擬平台
	惡意執行檔案檢測系統
	動態惡意軟體行為分析檢測工具(MBA@TWISC)
	使用者敲鍵行為辨識系統
	3.5G 核心網路拓樸檢測工具 (jtracert)
2009 年開發並完成之具（2010 年主要工作為強功能與維護）	無線網路金鑰強度檢測系統
	無線網路使用者安全意識檢測系統
	大規模無線網路安全即時監控系統
	入侵偵測系統強度評估系統

此外為擴大服務對象給更多網際網路使用者，我們將安全檢測跳脫實驗室的限制，將部份合適的工具進一步提供線上服務(此為新加入之服務，在原 2010 計劃書中未包含)，以提供網際網路使用者更為即時性的安全檢測服務。我們所建構的線上安全檢測平台(http://www.twisc.nctu.edu.tw/)提供四大類別的安全檢測服務，包括網路安全檢測、系統安全檢測、軟體安全檢測以及人員安全意識檢測。舉例說明，在網路檢測方面，WiMAX mobile users 可經由連線到我們開發的線上檢測網站來檢測其網路現況，可測得其是否遭受 DoS 攻擊；在系統安全檢測方面，網路使用者可經由 VPN 連線到我們開發的大規模遠端系統滲透檢測網，自行檢測其系統是否有漏洞以及被滲透的可能，網路管理人員也可透過網站伺服器安全滲透檢測系統來檢測其管理的網站伺服器是否有安全問題；在軟體弱點檢測方面，Android 應用程式使用 Java 撰寫，programmer 若想知道他的程式是否有漏洞，可將原始檔或執行檔上傳至我們的線上檢測網站，該網站會立即將檢測結果回傳，藉此發現軟體安全弱點；在惡意程式檢測方面，使用者可將可疑程式上傳至我們的線上檢測網站，利用平行運算以及虛擬機器觀測程式行為，可偵測防毒軟體所偵測不到的惡意程式加殼、變形等行為，在人員安全意識檢測方面，我們開發的 Wargame 經由遊戲破關的方式，可測試

並且培育資訊人員對網路安全的知識，另外我們也開發系統可測試人員對於網路安全的警覺性。藉此，我們不但可以解決行動裝置上計算資源不足以執行各樣的檢測工具的問題，更可有效的推廣安全檢測服務給一般社會大眾。本年度（2010）迄今，使用我們建置的線上安全檢測服務的人次已突破 15 萬人次。對象包含各教育機構(例如台灣大學、清華大學、中央大學、成功大學、中山大學、交通大學...等)、政府或研究機構(如行政院研考會、中研院、資策會、國家資通安全會報技服中心、法務部調查局...等)、以及海外連線(如北京清華大學、河南師範大學、中國科學技術大學...等)，隨著本服務規模的擴大，預計未來將有更多人可因而受惠。

● 計畫績效

在 2010 年計畫執行期間，我們分別發表於國際重要期刊 7 篇、國際研討會 5 篇以及國內研討會 4 篇之論文(詳細列表請見本章中 “學術成就”小節)。在專利方面，我們共有 3 件國外專利申請以及 3 件國內專利(詳細列表請見本章中 “學術成就”小節)。

表 6-2 詳列了本計畫在本年度預期成果與達成成果。由該表可知，本計畫 100%皆已達成並且超越 2010 年預期成果。**錯誤! 找不到參照來源。**及**錯誤! 找不到參照來源。**4 列出本計畫在 2010 年之技術服務與產學合作細項。技術服務對象包括友訊科技、中華電信以及洪先生(個人委託)。產學合作對象包括中科院、中華電信、微軟、資策會以及教育部。技術服務與產學合作總金額達 702.8 萬。

表 6-2、2010 預期成果與實際達成比較表(KPI)

	2010 預期成果	2010 實際達成
建置異質多網安全檢測平台	1	1
累計工具數量(包含 2009 與 2010 開發之工具)	13	15
技術服務	0 項	3 項 (見表 6-3)
技術服務與產學合作總金額	400 萬	702.8 萬
線上安全檢測服務	N/A (原計劃未包含)	超過 15 萬使用人次
網路安全線上實驗教材	N/A (原計劃未包含)	10

表 6-3、2010 年技術服務項目清單

項目名稱	對象	年度	簽訂金額(萬)

委託 Open D-Link Routers Forum 建置、維護與測試技術與諮詢服務	友訊科技	2009/12 ~2010/11	150*
自動化惡意程式檢測系統	中華電信	2009/9 ~2010/9	84.5*
未知方式自我加密軟體檔案破解與還原	洪先生 (個人委託)	2010	15
總金額			**15**

*跨年度服務項目金額不列入本年度計算

表 6-4、2010 年產學合作項目清單

項目名稱	對象	年度	簽訂金額 (萬)
資訊產品安全檢測技術整合型研究 2/2	中科院	2010	171.4
動態惡意程式行為側錄與污染分析	中華電信	2010	98.4
行動平台資通訊安全問題的研究	中華電信	2010	94.5
iNCTU-iPhone 校園生活服務研製	中華電信	2010	93.5
使用者敲鍵行為辨識系統	微軟	2010	0
惡意軟體行為分析與檢測技術	資策會	2010	60
DNSsec 推動先期型計畫	教育部	2010	170
總金額			**687.8**

● 學術成就

以下列出本計畫在 2010 年所發表及已被接受的國際期刊論文、國際會議論文以及國內會議論文，以及國外專利申請、國內專利申請項目。

■ 國際期刊論文

1. H.Y. Lin and W.G. Tzeng, "A Secure Decentralized Erasure Code for Networked Storage Systems," *IEEE Transactions on Parallel and Distributed Systems, (accepted*), 2010.
2. T. Klove, T.T. Lin, S.C. Tsai, and W.G. Tzeng, "Permutation Arrays Under the Chebyshev Distance, " *IEEE Transactions on Information Theory* 56(6), pp.2611-2617, 2010.
3. C.L. Hou, C. Lu, S.C. Tsai, and W.G. Tzeng, "An Optimal Data Hiding Scheme with Tree-Based Parity Check," *IEEE Transactions on Image Processing, (accepted)*, 2010.

4. Ming Hour Yang, Shiuhpyng Shieh, "Tracing Anonymous Mobile Attackers in Wireless Network," JDCTA: International Journal of Digital Content Technology and its Applications, Vol. 4, No. 4, pp. 161-174, 2010.
5. Shih-I Huang and Shiuhpyng Shieh, "Secure Encrypted-Data Aggregation for Wireless Sensor Networks," accepted for publication, ACM Journal of Wireless Networks.
6. Chi-Wei Wang and Shiuhpyng Shieh, "The Evolution of Fine-Grain Malware Behavior Analysis -From Static to Dynamic," IEEE ATR, 2010.
7. Shih-I Huang and Shiuhpyng Shieh, "Secret Search Mechanism for Wireless Sensor Networks with Passive RFIDs," accepted for publication, International Journal of Security and Networks.

■ **國際會議論文**

1. Shih-Fan Chou, Jen-I Liu, I-Lu Chao, Tzu-Chi Guo, Chia-Lung Liu, and Feng-Jie Tsai, "Analytical Modeling of Timeout for Contention-Based Bandwidth Request Mechanism in IEEE 802.16 WiMAX Networks," *IEEE LCN*, 2010.
2. Shih-Fan Chou, Jen-I Liu, I-Lu Chao, Tzu-Chi Guo, Chia-Lung Liu, and Feng-Jie Tsai, "Performance Enhancement of Contention-Based Bandwidth Request Mechanism in IEEE 802.16 WiMAX Networks," *IEEE PIMRC*, 2010.
3. Ming-Pei Hsu and I-Lu Chao, "Positioning with Reusability Improvement for Millimeter Wave Based Wireless Personal Area Networks," *IEEE ICC*, 2010.
4. Shuhua Jiang and I-Lu Chao, "Linear Cooperative Detection for Alarm Messages in Vehicular Ad Hoc Networks,"*IEEE WCNC*, 2010.
5. Wei Shi-Sue, Shiuhpyng Shieh, Chin-Wei Tien, "A Framework Using Fingerprinting for Signal Overlapping-Based Method in WLAN," accepted for publication, International Computer Symposium, 2010.

■ **國內會議論文**

1. Chia-Wei Hsu, Shiuhpyng Shieh, "FREE: A Fine-grain Replaying Executions by Using Emulation," *The 20th Cryptology and Information Security Conference (CISC 2010)*, Taiwan, 2010. (Best Student Paper Award)
2. B.T. Chen and Y.L. Huang, "The Design and Implementation of a Multi-core Supported Network Intrusion Detection System", *The 20th Cryptology and Information Security Conference (CISC 2010)*, Taiwan, 2010.
3. 蔡欣宜、王繼偉、陳柏廷、黃育綸、謝續平, 平基於虛擬裝置之無線網路安全測試平台", *The 20th Cryptology and Information Security Conference (CISC 2010)*, Taiwan, 2010.
4. 王繼偉、王嘉偉、許家維、謝續平, "基於虛擬機器外部觀察與映像檔比對的惡意程式分析,對 *The 20th Cryptology and Information Security Conference (CISC 2010)*, Taiwan, 2010.

● **專利**

以下列出目前申請的專利，其中國內專利申請共有三件、國內專利申請共有四件。

■ **國外專利**

1. S.I. Huang, S.P. Shieh, and C.W. Wang, "Light-Weight Authentication and Secret Retrieval Scheme and Its Applications," USA patent pending.
2. S.I. Huang and S.P. Shieh, "Method and System for Secure Data Aggregation in Wireless Sensor Networks," USA patent pending.
3. S.I. Huang and S.P. Shieh, "無線感測器網路中安全資料聚合的方法和系統," 大陸專利申請中。

■ **國內專利**

1. 劉家隆、邱碧貞、趙禧綠、周詩梵，" 長程演進技術網路的量測回報機制"，臺灣專利申請中。
2. 黃士一、謝續平、王繼偉，"輕量網路安全認證機制及秘密資料擷取方法與其應用"，臺灣專利申請中。
3. 黃士一、謝續平，"無線感測器網路中安全資料聚合的方法和系統"，臺灣專利申請中。

七、 重大突破

本計畫的重大突破可就學術成就、線上安全檢測服務以及產學效益三方面來敘述。

- 學術成就

參與本計畫之成員於 2010 年發表於國際重要期刊之論文數共 7 篇，發表於國際研討會之論文數共 5 篇以及國內研討會之論文共 4 篇，由此可知本計畫之相關成員學術研究成果相當豐碩。在我們所發表的國際期刊中，有兩篇論文的 impact factor 高於達 2.357 與 2.848，分別是 IEEE Transactions on Information Theory 與 IEEE Transactions on Image Processing。在國內研討會之論文方面，有一篇在 Cryptography and Information Security Conference 2010 得到最佳學生論文獎的殊榮。

- 線上安全檢測服務

為提供普羅大眾更為便利的安全檢測服務，我們於 2010 年將部份適合的工具轉為線上版本，來提供線上安全服務 (此為新加入之服務，原計劃書中未包含)。在網路安全檢測方面，WiMAX mobile users 可經由連線到我們的線上檢測網站來檢測其網路現況，可測得其是否遭受 DoS 攻擊；在系統安全檢測方面，網路使用者可經由 VPN 連線到雲端，自行檢測其系統是否有漏洞以及被滲透的可能，網路管理人員也可透過網站伺服器安全滲透檢測系統來檢測其管理的網站伺服器是否有安全問題；在軟體弱點檢測方面，Android 應用程式使用 Java 撰寫，programmer 若想知道他的程式是否有漏洞，可將原始檔或執行檔上傳至我們的線上檢測網站，該網站會立即將檢測結果回傳，藉此發現軟體安全弱點；在惡意程式檢測方面，使用者可將可疑程式上傳至我們的線上檢測網站，利用平行運算以及虛擬機器觀測程式行為，可

偵測防毒軟體所偵測不到的惡意程式加殼、變形等行為，在人員安全意識檢測方面，我們開發的 Wargame 經由遊戲破關的方式，可測試並且培育資訊人員對網路安全的知識，另外我們也開發系統可測試人員對於網路安全的警覺性。本年度（2010）迄今，目前使用我們建置的線上安全檢測（http://www.twisc.nctu.edu.tw, 網站首頁如圖 7-1 所示）服務的人次已突破 15 萬人次。對象包含各教育機構(如台灣大學、清華大學、中央大學、成功大學、中山大學...等)、政府或研究機構(如行政院研考會、中研院、資策會...等)、以及海外連線(如北京清華大學、河南師範大學、中國科學技術大學...等)，隨著本服務規模的擴大，預計未來將有更多人可因而受惠。

圖 7-1、twisc@nctu 網站首頁

目前線上安全檢測服務所提供的工具包含：

- **網路安全檢測**
  - Wimax 使用者之頻寬檢測及基礎弱點掃描系統 (WSBW)
- **系統安全檢測**
  - 大規模遠端系統安全滲透檢測網 (RSPTN)
  - 網站伺服器安全滲透檢測系統(WSS)
- **軟體安全檢測**
  - Android/Java 應用軟體安全漏洞檢測工具 (G-exploit)
  - 惡意執行檔案檢測系統
- **人員安全意識檢測**
  - 使用者網路攻防能力評估系統 (Wargame)
  - 使用者敲鍵行為辨識系統

- 產學效益

在 2010 年，本計畫分別與中科院、中華電信、教育部、微軟、資策會等官產學研單位進行合作，將本計畫所開發出之安全檢測工具(如：動態惡意軟體行為分析檢測工具、使用者敲鍵行為辨識系統、惡意執行檔案檢測系統等)提供給各單位參考，並進一步合作修改調整這些工具以符合上述單位之需求。除此之外，本計畫也提供開發安全相關之服務予多個單位，例如：將入侵偵測系統(IDS)移植至 Android 手機、基於 iPhone 手機開發 iNCTU 服務來推動校園生活服務、與推動 DNSsec 建置計畫，來達成產業與學術合作的互利關係。表 6-3 及 6-4 列出本計畫在 2010 年之技術服務與產學合作細項。技術服務對象包括友訊科技、中華電信以及洪先生(個人委託)。產學合作對象包括中科院、中華電信、微軟、資策會以及教育部。技術服務與產學合作總金額達 702.8 萬。

以下列出本計畫在 2010 年之技術服務與產學合作清單 (總金額為 702.8 萬元)。

- 技術服務【共 3 件，15 萬元(跨年度服務項目第一項與友訊科技第二項與中華電信合作總金額 234.5 萬，不列入本年度計算) 】
  - ◆ 友訊科技 D-link－委託 Open D-Link Routers Forum 建置、維護與測試技術與諮詢服務；無線網路設備開放程式碼網站（社群）建置與安全性分析(此為跨年度延續去年的技術服務項目)
  - ◆ 中華電信－自動化惡意程式檢測系統(此為跨年度延續去年的項目)
  - ◆ 洪先生（科技公司個人委託）─受委託執行特殊未知自我加殼（加密）執行檔 2.exe 之軟體破解、密碼解密與原始文件還原。本委託難度極高，該軟體僅容許輸入不知位元長度之 password，所有資料皆隱藏在軟體執行檔內，執行檔程式架構與內容完全未知，需經過反組譯，分析執行檔的架構，再將軟體切割後，分離出 password 軟體模組、加殼軟體模組、被加殼模組後，再經過平行運算破解程序，分析 key 的產生程序，破解與還原原始文件。

- 產學合作 (共 7 件，共 687.8 萬)
  - ◆ 中科院－資訊產品安全檢測技術整合型研究
    合作項目：針對「動態惡意軟體行為分析檢測工具」進行客製化，以符合中科院資訊產品安全檢測之軟體安全分析需求。
  - ◆ 中華電信－動態惡意程式行為側錄與汙染分析
    合作項目：針對「動態惡意軟體行為分析檢測工具」進行客製化，以符合中華電信用於 ISP 端分析檔案、電子郵件附件之需求。
  - ◆ 中華電信－行動平台資通訊安全問題的研究
    合作項目：針對中華電信為行動平台服務的需求，客製化將入侵偵測系統(IDS)移植至 Android 手機。
  - ◆ 中華電信－iNCTU-iPhone 校園生活服務研製
    合作項目：中華電信為推動校園生活服務，合作進行基於 iPhone 手機開發 iNCTU 服務。
  - ◆ 教育部－DNSsec 推動先期型計畫
    合作項目：教育部為了減少傳統 DNS 安全性問題，合作推動 DNSsec 建置計畫，於本年度進行先期全面評估與研究 DNSsec 相關安全議題。
  - ◆ 微軟－使用者敲鍵行為辨識系統
    合作項目：針對「使用者敲鍵行為辨識系統」進行客製化，以利微軟用於增強使用者登入的安全性。

◆ 資策會－惡意軟體行為分析與檢測技術

合作項目：針對「惡意執行檔案檢測系統」進行客製化，提供資策會進行惡意軟體行為分析與檢測。

藉由我們所建置的異質多網安全檢測平台與開發的安全檢測工具，我們可提供政府機關、財團法人及高科技廠商無線網路安全檢測的服務，以幫助上述單位發現漏洞及弱點。如此一來將可提高產業的經濟效益、提升無線產品附加價值、節省因網路攻擊或系統弱點所消耗的產值、節省專業檢測人力並且有效減少無線網路環境的攻擊。

八、 結論與展望

隨著網路技術的進步，異質多網通訊日漸普及，許多通訊廠以及高科技廠商紛紛投入研發新一代的行動裝置、硬體設備以及應用軟體，提供使用者更多元化的需求。然而，伴隨新一代高科技產品的便利性以及產業成長的同時，具有危害性的安全漏洞也開始因應而生。許多政府機關、財團法人以及一般大眾常因為系統、網路、軟體的安全性不足以及人員安全意識的缺乏而蒙受重大的財物損失以及機密資料的損失。由此可知，異質多網的全面性檢測有相當的急迫性與重要性。然而，目前市面上缺乏完善且全面性的安全檢測的工具可供使用。為了檢測異質多網環境之下眾多的安全風險，TWISC@NCTU 在 2009 以及 2010 年已開發了一異質多網安全檢測平台。本平台提供一個完整的安全檢測服務，包括四大檢測類別：網路安全檢測、系統安全檢測、軟體安全檢測以及人員安全意識檢測，服務對象包括政府機關、財團法人、產業界、高科技廠商以及一般的網際網路使用者。

為推廣以及服務擴大的對象，我們在2010年已將適合的部分工具進一步轉為線上服務或是提供線上下載功能，讓所有的網際網路使用者都可方便使用。藉由此線上安全檢測平台系統，使用者毋須安裝額外或是未知風險的軟體來輔助檢測，即可進行即時安全檢測。在2011年，我們也將持續開發更新安全檢測工具並且將繼續把更多適切的檢測工具轉成線上服務，以提供更為完整的安全檢測服務。為促進與產業界、政府單位，與學術界合作的機會，我們也將針對各單位的檢測需要來開發客製化的安全檢測工具以提升其產業效益。

參考文獻

[1]. 卡巴斯基實驗室，http://www.kaspersky.com.tw/

[2]. 諾頓(賽門鐵克)，http://tw.norton.com/

[3]. W. Visser, C. Pasareanu, and S. Khurshid, " Test Input Generation with Java PathFinder," *In Proceedings of the ISSTA*, Boston, MA, 2004.

[4]. S. Koushik, and A. Gul, "jCUTE : Automated Testing of Multithreaded Programs UsingRace-Detection and Flipping," Submitted for Publication.

[5]. S. Koushik, and A. Gul, "CUTE and jCUTE: Concolic Unit Testing and Explicit Path Model-Checking Tools," *In Proceedings of the 18th International Conference on Computer Aided Verification (CAV'06)*, Lecture Notes in Computer Science, Seattle, Washington,

USA, 2006.

[6]. S. Koushik, “Concolic Testing,” *In Proceedings of the EECS Department*, UC Berkeley, CA, USA. ASE’07, 2007.

[7]. S. Koushik, and A. GUL, “Concolic Testing of Multithreaded Programs and Its Application to Testing Security Protocols,” *In Proceedings of the Department of Computer Science University of Illinois at UrbanaChampaign*, USA.

[8]. S. Khurshid, C. S. Pasareanu, and W. Visser, “Generalized Symbolic Execution for Model Checking and Testing,” *In Proceedings of the TACAS*, Warsaw, Poland, 2003.

[9]. Min Gyung Kang, Pongsin Poosankam, and Heng Yin, “Renovo: A Hidden Code Extractor for Packed Executables,” *In Proceedings of the 5th ACM Workshop on Recurring Malcode (WORM)*, October 2007.

[10]. S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, “Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish,” *In Proceedings of the 3rd Symposium on Usable Privacy and Security*, pp. 88–99, 2007.

[11]. P. Kumaraguru, Y. Rhee, S. Sheng, S. Hasan, A. Acquisti, L. F. Cranor, and J. Hong, “Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer,” *In Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, pp. 70–81, 2007.

[12]. S. Garera, N. Provos, M. Chew, and A. D. Rubin, “A framework for detection and measurement of phishing attacks,” *In Proceedings of the 2007 ACM Workshop on Recurring Malcode*, pp. 1–8, 2007.

[13]. M. Sharifi, and S. H. Siadati, “A phishing sites blacklist generator. In Proceedings of the Computer Systems and Applications,” *AICCSA IEEE/ACS International Conference*, pp. 840–843, 2008.

[14]. C. Karlof, U. Shankar, J. Tygar, and D. Wagner, “Dynamic pharming attacks and locked same-origin policies for web browsers,” *In Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 58–71, 2007.

[15]. Botnet, http://192.83.193.18/dorm/know-botnet.html

[16]. D.M. Taverira, O.C.M. Duarte, “A monitor Tool for Anti-spam Mechanisams and Spammers Behavior,” *In Proceedings of the Network Operations and Management Symposium Workshops*, pp. 101–108, 2008.

[17]. SpamAssassin, http://spamassassin.org

[18]. P.J. Sandford, J.M. Sandford, and D.J. Parish, “Analysis of SMTP Connection Characteristics for Detecting Spam Relays,” *In Proceedings of the ICCGI '06*, pp. 68–68, 2006.

[19]. 張僩鈞，“兩階層式垃圾郵件過濾機制之研究”，私立銘傳大學資訊傳播工程所 (2006)。

[20]. ORBD, http://www.coolacid.net/the-news/99-orbdorg-marks-all-as-spam

[21]. I. Biju, J.J. Wendy, and H.S. Jofry, “Improved Bayesian Anti-Spam Filter – Implementation and Analysis onIndependent Spam Corpuses,” *In Proceedings of the ICCET '08*, pp. 326–330, 2009.

[22]. 資安之眼，全球企業被駭去年平均每家損失 200 萬美元(2010)。http://www.itis.tw/node/3641

[23]. R.K. Singh, and T. Ramanujam, “Intrusion Detection System Using Advanced Honeypots,” *In Proceedings of the Internatilnal Journal of Computer Science and Information Security*, Volume 2, no. 1, 2009.

[24]. K. Shishir, and P. Durgesh, “Detection and Prevention of New and Unknown Malware using Honeypots,” *In Proceedings of the International Journal on Computer Science and Engineering* ,Volume 1, no. 2, pp. 56–61, 2009.

[25]. M. Christodorescu, and S. Jha, “Testing malware detectors,” *In Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis*, 2004.

[26]. 張智翔，中央研究院計算中心通訊電子報: 淺談網路應用程式安全(二)。http://newsletter.ascc.sinica.edu.tw/news/readnews.php?nid=1294

[27]. Dnsstuff, http://www.dnsstuff.com/tools/

[28]. WhatIsMyIPAddress.com, http://whatismyipaddress.com/ip-lookup

[29]. zInternet2 – Network Diagnostic Tools. http://www.internet2.edu/performance/ndt/

出國短期訪問報告書

撰寫時間： 99 年 10 月 1 日

報告人： 交通大學謝續平

一、出國目的：

TWISC@NCTU（Taiwan Information Security Center at NCTU）執行國科會異質多網安全檢測平台建置計畫，出國參訪美國加州大學洛杉磯分校電機與資訊學系（Department of Electrical and Computer Engineering, UCLA）、華盛頓大學西雅圖分校電機與資訊工程系（Department of Electrical and Computer Engineering, University of Washington at Seattle），國際交流。美國加州大學洛杉磯分校電機與資訊學系 Professor Lixia Zhang 是資訊安全界的權威，近年獲得美國國家科學基金會的 Future Internet Architecture (FIA)跨校的最大型計畫，該計畫的重點在於補足現有網際網路整體安全架構的不足，提出以 DNSSEC 來補強安全，這與本研究計畫高度相關，也與台灣網際網路整體安全息息相關，希望藉此機會瞭解未來網際網路安全的發展規劃，獲得第一手的資訊，另外 University of Washington at Seattle 位於西雅圖，接近美國微軟的總部，該校許多的研究都與最新的網路網路、行動網路的發展有關，經由 Professor Jenq-Neng Hwang 的安排，藉此機會參

觀該校的網路安全相關的研究，該校在行動網路方面的研究令人印象深刻，例如在 distributed operating system 的研究就是放在 high availability，與我們研究的重點有許多相關之處。

二、參訪期間：

短期參訪期間為九十九年九月四日至九十九年九月月二十二日止，於期間內赴美國加州大學洛杉磯分校電機與資訊學系（Department of Electrical and Computer Engineering, UCLA)、華盛頓大學西雅圖分校電機與資訊工程系（Department of Electrical and Computer Engineering, University of Washington at Seattle）國際合作參觀訪問。詳細參訪行程如下：

9/3 Taipei to L.A.

9/4-9/13 短期研究 Professor Lixia Zhang of UCLA

9/14 L.A. to Seattle

9/15 - 9/21 短期研究訪問 Professor Jenq-Neng Hwang of University of Washington at Seattle.

9/22 返抵台灣

三、出國人員：

謝續平現任交通大學資訊工程系教授暨 TWISC@NCTU(Taiwan

Information Security Center at NCTU)主任，曾任交通大學資訊工程系系主任、交通大學計算機與網路中心主任、中華民國資訊安全學會理事長。謝教授積極參與國際活動，目前擔任 IEEE Reliability Society Ad Com 議員，Taipei/Tainan Chapter 主席，並榮獲榮譽獎項 ACM Distinguished Scientist。在國際期刊編輯方面，現在擔任 IEEE Reliability Society Newsletter 總編輯、IEEE Tran. On Dependable and Secure Computing、IEEE Trans. On Reliability、Journal of Computer Security 副編輯。會國際會議活動方面，現在創立並擔任 ACM Symposium on Information, Computer and Communications Security （ASIACCS） 推動委員會主席（steering committee chair)，該會議為 ACM 旗艦會議，論文接受率僅約有 15%。

四、參訪經過及重要結果：

美國加州大學洛杉磯分校電機與資訊學系 Professor Lixia Zhang 是資訊安全界的權威，近年獲得美國國家科學基金會的 Future Internet Architecture (FIA)跨校的最大型計畫，該計畫的重點在於補足現有網際網路整體安全架構的不足，提出以 DNSSEC 來補強安全，這與本研究計畫高度相關，也與台灣網際網路整體安全息息相關，

DNS（Domain Name Service)，為現今全世界最重要的服務之一，

舉凡網路相關之事便離不開 DNS，即使是內部封閉網路，電腦間的溝通也需要透過 DNS 來解析。而 DNS 在最初設計時並沒有考慮到身分認證的功能，也造成了近年來 DNS 遭受攻擊的資安事件層出不窮，特別在 Kaminsky 發現 DNS 緩衝區漏洞攻擊後，DNS 安全性問題逐漸開始受到關注，追究其根本原因實為 DNS 協定本身之問題。

為了解決 DNS 本質上的不安全性，IETF 組織（Internet Engineering Task Force）定義了一套 DNSSEC 協定（Domain Name System Security Extensions），可被視為 DNS 的安全性升級版。DNSSEC 導入了數位簽章的概念，能提供 DNS 資料驗證、資料完整性、資料存在性驗證等，藉此抵擋 Man-in-middle、DNS cache poisoning、DNS hijacking 等形式的攻擊，更進一步能安全的傳遞憑證等重要資料，應用到其他網路服務如電子郵件，提昇各種網路應用的安全性。

DNSSEC 協定在發展數年後的今日逐漸成熟並得到支持，國際組織與各國政府也開始著手進行部署。以目前的態勢來看，DNSSEC 已確定成為 DNS 的後繼標準，相關的國際標準制定已經成熟完備，不會再有太大的變動，各國政府與機構也積極進入 DNSSEC 佈署維運階段。

DNSSEC 的部署將被網路服務提供商視為未來網路基礎建設的重要目標，另一方面它在近年熱門的雲端運算(Cloud Computing)技術中也扮演著重要的角色，一旦所有服務都遷移到雲端，使用者獲得服

務的首要步驟即是透過 DNS 服務轉譯，因此 DNS 的攻擊將造成服務中斷或惡意服務轉向。可見將傳統 DNS 升級為 DNSSEC，已成刻不容緩的任務。

為瞭解美國網路科技學術研發與技術發展現況，特別安排此次實地參訪活動，經由密集的實地參訪，深切的瞭解到美國對軟體技術的重視與投入，尤其在重點大學投資更是驚人，目前美國重點大學與產業之合作明顯超越台灣重點大學，且經由校內設立研究中心，使得學術研究已經與產業所需密切的結合，大學的研究真正的達到提升產業技術的目的。

美國目前電腦網路頻寬已經遠超過台灣，網路電話也較台灣更為普遍，而全世界一流的高科技公司也紛紛在各重點大學設立研發中心，對產業技術發展具有催化作用，可以預見美國將在軟體技術持續保持領先。台灣過去教育頗為成功，創造了經濟奇蹟，現在因應大陸強力的競爭，台灣亦應大力投資教育，厚植我國高科技基礎。

「ACM Symposium on Information, Computer and Communications Security（ASIACCS）國際學術會議」出國報告書

報告人： 交通大學謝續平

日期：2010 年 04 月 30 日

一、 出國目的

ACM Symposium on Information, Computer and Communications Security （ASIACCS）為 ACM Special Interest Group on Security, Audit, and Control（SIGSAC）所贊助與主辦的兩大頂尖會議之一，接受率約為 10%一頂尖會議為 ACM Conference on Computer and Communications Security（CCS）， 接受率也約為 10%。本人擔任 ACM ASIACCS steering committee chair, 負責推動該會議，並且召集 steering committee meeting，遴選每年執行單位。此次參加該國際學術會議，並審查 2011 年主辦單位進度，與 2012 年主辦國家與單位，並討論會議場地與籌辦流程。

二、 行程

參加 ACM Symposium on Information, Computer and Communications Security 擔任 Steering Committee Chair。

4/9 Taipei – Beijing

4/10 受 ACM ASIACCS steering committee member 以及 Mozilla Online Ltd. CEO Li Gong 博士邀請訪問 Mozilla Online Ltd. (該公司為開發 Firefox web browser 的公司，Firefox 瀏覽器為全球最受歡迎的瀏覽器之一)

4/12 受大會以及 Chinese Academy of Sciences, Deputy Director Jiwu Jing 邀請訪問中科院並演講 “Cloud Computing Security”

4/13-16 ACM Symposium on Information, Computer and Communications Security 會議

4/17-18 ASIACCS steering committee 會議擔任主席

4/19 返台

三、 出國人員：

謝續平現任交通大學資訊工程系教授暨 TWISC@NCTU 主任，曾任交通大學資訊工程系系主任、交通大學計算機與網路中心主任、中華民國資訊安全學會理事長，現在擔任 IEEE Tran. On Dependable and Secure Computing、IEEE Trans. On Reliability、Journal of Computer Security 副編輯、IEEE RS Newsletter 總編輯。由於現在擔任 ACM Symposium on Information, Computer and Communications Security （ASIACCS） 推動委員會主席（steering committee chair)。負責遴選籌辦國家單位，並督導籌辦進度。

四、 工作內容摘要

由於擔任 ACM Special Interest Group on Security, Audit, and Control (SIGSAC) 的推動委員會委員（Steering Committee member)，並且擔任 ACM Symposium on Information, Computer and

Communications Security （ASIACCS） 推動委員會主席（steering committee chair)，被 ACM 賦予：

a）觀察本年度會議執行成果，

b）審查下年度執行單位籌備現況，

c）並甄選兩年後會議執行單位。

本次出國為了推動 SIGSAC 的未來發展，赴大陸北京友誼賓館，參加本年度會議，觀察 ASIACCS 本年度會議主辦單位美國賓州州立大學、瑞士 ETH、北京中國科學研究院成果，並審查 2011 會議舉辦單位香港大學、香港城市大學籌備進度，與 2012 年申請舉辦單位上海交通大學等單位的提案。

此次大會由北京中國科學研究院 Dengguo Feng 主任擔任大會主席，David Basin(basin@inf.ethz.ch, ETH Zurich, Switzerland)
Peng Liu(pliu@ist.psu.edu, Pennsylvania State University, USA)
擔任議程主席，會議接受率僅約 10%，相較於 IEEE INFOCOMM 等頂級國際會議的接受率 25%，顯得更為難得。

本次會議前、後分別受到本會議的推動委員會委員 Mozilla 的 CEO Li Gong 的邀請訪問以及本會議的大會邀請至中國科學研究院演講，而國際會議後的推動委員會也決議 2012 年的主辦單位延至下次會議討論。

五、　結語

本次大會由有來自全世界三十餘國作者投稿，稿件水準極高，接受率極低，約為 10%，會議圓滿成功。會議組織與會議議程如下：

CONFERENCE ORGANIZING COMMITTEE

General Chair	Dengguo Feng (feng@is.iscas.ac.cn, Chinese Academy of Sciences, China)
Program Committee Chair	David Basin(basin@inf.ethz.ch, ETH Zurich, Switzerland) Peng Liu(pliu@ist.psu.edu, Pennsylvania State University, USA)
Local Arrangements Committee Chair	Jiwu Jing (jing@lois.cn, Chinese Academy of Sciences, China)
Publication Chair	Peng Ning (pning@ncsu.edu, NC State University, USA)
Publicity Chair	Jie Li (lijie@cs.tsukuba.ac.jp, University of Tsukuba, Japan)
Workshop Chair	Dongdai Lin (ddlin@is.iscas.ac.cn, Chinese Academy of Sciences, China)
Tutorial Chair	Zhong Chen (chen@cs.pku.edu.cn, Peking University, China)

Treasurer	Sencun Zhu (szhu@cse.psu.edu, Pennsylvania State University, USA)
Web Chair	Ji Xiang (xiangji2008@gmail.com, Chinese Academy of Sciences, China)
Secretary	Daren Zha (zdr@lois.cn) Zongbin Liu (liuufo85@gmail.com)

STEERING COMMITTEE

Shiuhpyng Shieh(Chair), Chiao Tung University, Chinese Taipei
David Basin, ETH Zurich, Switzerland
Robert Deng, Singapore Management University, Singapore
Virgil Gligor, Carnegie Mellon University, USA
Hideki Imai, National Institute of Advanced Industrial Science and Technology, Japan
Sushil Jajodia, George Mason University, USA
Pierangela Samarati, University of Milan, Italy
Elisa Bertino, Purdue University, USA
Mike Reiter, University of North Carolina at Chapel Hill, USA
Li Gong, Mozilla Online Ltd., USA
Ninghui Li, Purdue University, USA
Eiji Okamoto, University of Tsukuba, Japan
Vijay Varadharajan, Macquarie University, Australia

六、會議議程

ASIACCS 2010: Beijing, China

Program Sketch

12 April	**13:30-18:00**	Registration	Lobby of Building 2
13 April	**8:00-8:50**	Registration	Meeting Room1, Building 8
	8:50-9:00	Welcoming Remarks	Meeting Room1, Building 8
	9:00-10:00	Invited Talk	Meeting Room1, Building 8
	10:00-10:30	Coffee-break	Meeting Room1, Building 8
	10:30-12:00	Session 1:Privacy	Meeting Room1, Building 8
	12:00-13:30	Lunch	Cafeteria in Friendship Palace
	13:30-15:00	Session 2:Applied Cryptography	Meeting Room1, Building 8
	15:00-15:30	Coffee Break	Meeting Room1, Building 8
	15:30-17:00	Session 3: Network Security	Meeting Room1, Building 8
	17:30-19:00	Dinner	Cafeteria in Friendship Palace
	19:00-21:00	Steering Committee Meeting (Steering committee members only)	Second Floor meeting Room, Building 2
14 April	**8:00-8:50**	Registration	Meeting Room1, Building 8
	9:00-10:00	Invited Talk	Meeting Room1, Building 8
	10:00-10:30	Coffee Break	Meeting Room1, Building 8
	10:30-12:00	Session 4: Systems Security – I	Meeting Room1, Building 8
	12:00-13:30	Lunch	Cafeteria in Friendship Palace
	13:30-15:00	Session 5: Access Control – I	Meeting Room1, Building 8
	15:00-15:30	Coffee Break	Meeting Room1, Building 8
	15:30-17:30	Session 6: Security Protocols	Meeting Room1, Building 8
	18:30-20:30	Banquet	Ju Xiu Yuan Friendship Palace
	8:00-8:45	Registration	Meeting Room1, Building 8
	8:45-10:15	Session 7: Access Control – II	Meeting Room1, Building 8

15 April	**10:10-10:35**	Coffee Break	Meeting Room1 Building 8
	10:35-12:05	Session 8: Systems Security - II	Meeting Room1, Building 8
	12:05-13:30	Lunch	Cafeteria in Friendship Palace
	13:30-15:10	Session 9: Short Papers – I	Meeting Room1, Building 8
	13:10-15:30	Coffee Break	Meeting Room1, Building 8
	15:30-17:10	Session 10: Short Papers – II	Meeting Room1, Building 8
	17:30-19:00	Dinner	Cafeteria in Friendship Palace

Advanced Program

The 5th ACM Symposium on Information, Computer and Communications Security

(ASIACCS 2010)

（Beijing Friendship Hotel）

April 13, 2010	
8:00 - 8:50	**Registration**
8:50 - 9:00	**Welcoming Remarks**
9:00 - 10:00	**INVITED TALK:** **Pierangela Samarati, Universita` degli Studi di Milano** **Session Chair: Peng Liu**
10:00 - 10:30	**Coffee Break**
Session 1: Privacy **Session Chair: Adam Lee**	
10:30 - 11:00	**Towards Publishing Recommendation Data With Predictive Anonymization** Chih-Cheng Chang, Rutgers University Brian Thompson, Rutgers University Hui Wang, Stevens Institute of Technology Danfeng Yao, Rutgers University
11:00 - 11:30	**Restoring Compromised Privacy in Micro-data Disclosure** Lei Zhang, George Mason University Alexander Brodsky, George Mason University Sushil Jajodia, George Mason University
11:30 - 12:00	**Securely Outsourcing Linear Algebra Computations** Mikhail Atallah, Purdue University Keith Frikken, Miami University
12:00 - 13:30	**Lunch**
Session 2: Applied Cryptography **Session Chair: Dongdai Lin**	
13:30 - 14:00	**Attribute-based Signature and its Application** Jin Li, Illinois Institute of Technology Man Ho Au, University of Wollongong Willy Susilo, University of Wollongong Dongqing Xie, Guangzhou University

	Kui Ren, Illinois Institute of Technology
14:00 - 14:30	**Dynamic Fully Forward-Secure Group Signatures** Benoit Libert, Universite Catholique de Louvain Moti Yung, Google & Columbia University
14:30 - 15:00	**Identity-Based Encryption based on ElGamal** Yu Chen, Peking University Manuel Charlemagne, Dublin City University, Ireland Zhi Guan, Peking University Jianbin Hu, Peking University Zhong Chen, Peking University
15:00 - 15:30	**Coffee Break**
Session 3: Network Security Session Chair: Kui Ren	
15:30 - 16:00	**Region-based BGP Announcement Filtering for Improved BGP Security** Fernando Sanchez, Zhenhai Duan Florida State University
16:00 - 16:30	**Fast-flux Service Network Detection Based on Spatial Snapshot Mechanism for Delay-free Detection** Si-Yu Huang, Taiwan Tech Ching-Hao Mao, Taiwan Tech Hahn-Ming Lee, Taiwan Tech
16:30 - 17:00	**Securing Wireless Sensor Networks against Large-scale Node Capture Attacks** Tuan Vu, University of Calgary Reihaneh Safavi-Naini, University of Calgary Carey Williamson, University of Calgary
17:30 - 19:00	**Dinner**
April 14, 2010	
8:00 - 9:00	**Registration**
9:00 – 10:00	**INVITED TALK:** **Andrei Sabelfeld, Chalmers University of Technology** **Session Chair: David Basin**
10:00 - 10:30	**Coffee Break**

Session 4: Systems Security – I Session Chair: Andrei Sabelfeld	
10:30 - 11:00	**Preventing Drive-by Download via Inter-Module Communication Monitoring** Chengyu Song, Peking University Jianwei Zhuge, Peking University Xinhui Han, Peking University Zhiyuan Ye, Peking University
11:00 - 11:30	**A Solution for the Automated Detection of Clickjacking Attacks** Marco Balduzzi, Eurecom Manuel Egele, University of California, Santa Barbara Engin Kirda, Eurecom Davide Balzarotti, Eurecom Christopher Kruegel, University of California, Santa Barbara
11:30 - 12:00	**PAriCheck: An Efficient Pointer Arithmetic Checker for C Programs** Yves Younan, Katholieke Universiteit Leuven Pieter Philippaerts, Katholieke Universiteit Leuven Lorenzo Cavallaro, University of California, Santa Barbara R. Sekar, Stony Brook University Frank Piessens, Katholieke Universiteit Leuven Wouter Joosen, Katholieke Universiteit Leuven
12:00 - 13:30	**Lunch**
Session 5: Access Control – I **Session Chair: Robert Deng**	
13:30 - 14:00	**An Opportunistic Authority Evaluation Scheme for Data Security in Crisis Management Scenarios** Enrico Scalavino, Imperial College London Giovanni Russello, Create-Net Rudi Ball, Imperial College London Vaibhav Gowadia, Imperial College London Emil Lupu, Imperial College London
14:00 - 14:30	**Effective Trust Management Through a Hybrid Logical and Relational Approach** Adam J. Lee, University of Pittsburgh

	Ting Yu, North Carolina State University Yann Le Gall, University of Pittsburgh
14:30 - 15:00	**Toward Practical Authorization-dependent User Obligation Systems** Murillo Pontual, University of Texas at San Antonio Omar Chowdhury, University of Texas at San Antonio William H. Winsborough, University of Texas at San Antonio Ting Yu, North Carolina State University Keith Irwin, Winston-Salem State University
15:00 – 15:20	**Coffee-break**
Session 6: Security Protocols **Session Chair: Kanta MATSUURA**	
15:30 - 16:00	**Cap Unification: Application to Protocol Security modulo Homomorphic Encryption** Siva Anantharaman, LIFO, University of Orleans Hai Lin, Clarkson University Christopher Lynch, Clarkson University Paliath Narendran, University at Albany--SUNY Michael Rusinowitch, LORIA - INRIA Lorraine
16:00 - 16:30	**SSLOCK: Sustaining the Trust on Entities Brought by SSL** Adonis P.H. Fung, The Chinese University of Hong Kong K.W. Cheung, The Chinese University of Hong Kong
16:30 - 17:00	**Computationally Secure Two-Round Authenticated Message Exchange** Klaas Ole Kürtz, Christian-Albrechts-Universität Kiel Henning Schnoor, Christian-Albrechts-Universität Kiel Thomas Wilke, Christian-Albrechts-Universität Kiel
17:00 – 17:30	**Bureaucratic Protocols for Secure Two-Party Sorting, Selection, and Permuting** Guan Wang, Syracuse University Tongbo Luo, Syracuse University Michael T. Goodrich, Univ. of California, Irvine Wenliang Du, Syracuse University Zutao Zhu, Syracuse University

18:30 - 20:30	**Conference Banquet**
April 15, 2010	
8:00 - 8:45	**Registration**
Session 7: Access Control – II **Session Chair: Ting Yu**	
8:45 - 9:15	**A Logic for Authorization Provenance** Jinwei Hu, Huazhong University of Science and Technology Yan Zhang, University of Western Sydney Ruixuan Li, Huazhong University of Science and Technology Zhengding Lu, Huazhong University of Science and Technology
9:15 - 9:45	**Risk-based Access Control Systems Built on Fuzzy Inferences** Qun Ni, Purdue University Elisa Bertino, Purdue University Jorge Lobo, IBM T. J. Watson Research Center
9:45 - 10:15	**Attribute Based Data Sharing with Attribute Revocation** Shucheng Yu, Worcester Polytechnic Institute Cong Wang, Illinois Institute of Technology Kui Ren, Illinois Institute of Technology Wenjing Lou, Worcester Polytechnic Institute
10:15 – 10:35	**Coffee-break**
Session 8: Systems Security - II **Session Chair: Engin Kirda**	
10:35 – 11:05	**binOb+: A Framework for Potent and Stealthy Binary Obfuscation** **Byoungyoung Lee, POSTECH** Yuna Kim, POSTECH Jong KIM, POSTECH
11:05 – 11:35	**Secure Provenance: The Essential of Bread and Buffer of Data Forensics in Cloud Computing** Rongxing Lu, University of Waterloo Xiaodong Lin, University of Ontario Institute of Technology Xiaohui Liang, University of Waterloo Xuemin (Sherman) Shen, University of Waterloo

11:35 – 12:05	**RunTest: Assuring Integrity of Dataflow Processing in Cloud Computing Infrastructures** Juan Du, Wei Wei, Xiaohui Gu, Ting Yu North Carolina State University
12:05 – 13:30	**Lunch**
Session 9: Short Papers – I Session Chair: Sencun Zhu	
13:30 – 13:50	**K-anonymous Association Rule Hiding** Zutao Zhu, Wenliang Du Syracuse University
13:50 – 14:10	**Controlling Data Disclosure in Computational PIR Protocols** Ning Shang, Gabriel Ghinita, Yongbin Zhou, Elisa Bertino Purdue University
14:10 – 14:30	**Cryptographic Role-based Security Mechanisms based on Role-Key Hierarchy** Yan Zhu, Arizona State University Gail-Joon Ahn, Arizona State University Hongxin Hu, Arizona State University Huaixi Wang, Peking University
14:30 – 14:50	**PriMa: An Effective Privacy Protection Mechanism for Social Networks** Anna Squicciarini, The Pennsylvania State University Federica Paci, University of Trento Smitha Sundareswaran, The Pennsylvania State University
14:50 – 15:10	**Oblivious Enforcement of Hidden Information Release Policies** Brian Wongchaowart, Adam Lee University of Pittsburgh
15:10 – 15:30	**Coffee-break**
Session 10: Short Papers – II Session Chair: Cliff Zou	
15:30 – 15:50	**Apex: Extending Android Permission Model and Enforcement with User-defined Runtime Constraints** Mohammad Nauman, Institute of Management Sciences, Pakistan Sohail Khan, Institute of Management Sciences, Pakistan Masoom Alam, Austria Xinwen Zhang, Samsung Information Systems America

15:50 – 16:10	**A Hotspot-based Protocol for Attack Traceback in Mobile Ad Hoc Networks** Hungyuan Hsu, Penn State University Sencun Zhu, Penn State University Ali Hurson, Missouri University of Science and Technology
16:10 – 16:30	**Practical ID-based Encryption for Wireless Sensor Network** Cheng-Kang Chu, Singapore Management University Joseph K. Liu, Institute for Infocomm Research, Singapore Jianying Zhou, Institute for Infocomm Research, Singapore Feng Bao, Institute for Infocomm Research, Singapore Robert H. Deng, Singapore Management University
16:30 – 16:50	**A Game Theoretic Model for Digital Identity and Trust in Online Communities** Tansu Alpcan, Deutsche Telekom Laboratories Cengiz Orencik, Sabanci University Albert Levi, Sabanci University Erkay Savas, Sabanci University
16:50 – 17:10	**Scene Tagging: Image-Based CAPTCHA Using Image Composition and Object Relationships** Peter Matthews, Cliff Zou University of Central Florida
17:30 - 19:00	**Dinner**
End of the conference	

出席 2010 International Dependable Systems and Networks 會議與參訪美國 Purdue University 報告

出國人員姓名/服務機關/單位/職稱/電話
吳育松/國立交通大學/資工系/助理教授/0975225901

出國期間：99/6/23-99/7/7

出國地區：美國/芝加哥、印第安那州西拉法葉市

報告日期：99/6/23-99/7/7

內容摘要：

本次出國的主要目的是出席於美國芝加哥所舉辦的第 40 屆 International Conference on Dependable Systems and Networks (DSN)。該會議囊闊了系統可靠度、性能表現、安全性等各個層面的相關 workshop、tutorial、以及最新的研究成果發表。該會議與本人目前所正執行之對於分散是系統環境中零時攻擊的反制研究以及所參與的 TWISC 相關研究計畫有非常高的相關性。出席該會議具有獲取新知、參考國外相關研究、自我檢討目前計畫執行進程等功效。

在會議結束後，我順道南下位於芝加哥南部約一百英里遠的印第安那西拉法葉市參訪 Purdue University。在 Purdue 我給了一個 talk，並與 ECE Department 的 Prof. Saurabh Bagchi 及其學生進行短暫的晤談，並尋求未來可能的相關研究合作之可能性。

壹、 參訪過程紀要

一、 出席 2010 DSN Conference 經過

DSN (International Conference on Dependable Systems and Networks)為系統可靠性的旗艦級會議。今年為第 40 屆，於美國芝加哥舉辦。主辦單位為美國密西跟大學安那堡分校（General Chair 為 U of Michigan 資訊科學工程系 Farnam Jahanian 教授）。其中 Intrusion-Tolerant Systems Workshop 以及 Security 議題的 Tracks 跟本計畫具高度相關性。其餘的 Tracks 則著墨於系統相關的性能、可靠性等議題，亦與本計畫有一定程度的相關性。

會議的第一天我出席了 Workshop on Recent Advances in Intrusion-Tolerant Systems。該 workshop 一開始是由 Cornell CS 的 Robert L. Constable 教授所給的 keynote speech。題目是"Using Formal Methods to Build Systems that Survive Attacks"。另外之後的 session 中有 MIT 的 O. Patrick Kreidl 博士所給的講題 "Analysis of a Markov Decision Process Model for Intrusion Tolerance"，以及 Lockheed Martin 的 Melvin Greer 所給的講題 "Survivability and Information Assurance in the Cloud" 這三個部分正好囊闊了從系統設計面、系統運作面、以及展望未來雲端環境中面對潛在攻擊的因應之道，與研究方向。我覺得受益方常良多。

第二天會議由 VeriSign 的研發副董 Danny McPherson 所給的 keynote speech "Availability in the Face of Evolving Internet Threats" 所展開。VeriSign 掌控全球主要的 DNS root server，而他的演講側重在透過 ATLAS 全球網路監控系統對於 distributed denial-of-service attack 的觀測以及相關見解。第二天我後半段主要是出席 Fast Abstracts Session，聽取一些最新的初步研究成果。比如說 Michigan 大學 Kang G. Shin 教授研究群的"How to Construct a Mobile Botnet"、伊利諾大學 Ravi K. Iyer 教授研究群的 "Analysis of Security Data from a Large Computing Organization"、伊利諾大學 William H. Sanders 教授研究群的 "Characterizing the Behavior of Cyber Adversaries: The Means, Motive, and Opportunity of Cyber Attacks" 等研究。

第三天的會議由分散式計算大師 MIT Nancy Lynch 教授所給的 keynote speech "Distributed Computing Theory Through the Ages" 所展開。這個演講一開始論及了分散式計算中的一些古典問題 (atomicity、mutual exclusion...)，基本上有點類似 Nancy Lynch 教授的那本 Distributed Algorithms 裡面的重點提要，當然由原作者親自講授的感覺就是不一樣。Lynch 教授的演講後來有提一些他比較近期的一些 research work。由於這部分跟我專長有些距離，部分精要之處比較無法完全領會。之後我聽了 EPFL 的一篇關於程式驗證的論文報告 "iProve: A Scalable Technique for Consumer-Verifiable Software Guarantees"。由於系統弱點(vulnerabilities)很大一部分均是由於程式內部的某些 property 沒有被滿足（比如說緩衝區溢位）所造成的，也因此如何能對一個真實世

界中的複雜程式去做驗證也就是欲解決系統弱點所需要面對的一個很重要的研究課題。第三天後來的時間我都在聽 fast abstracts，這天的 fast abstracts 較少跟本計畫研究課題有直接相關的題目，所以純粹是以增廣見聞，瞭解一下其他研究題目最近的一些進展狀況這樣。

第四天的會議有比較多跟 Security 相關的論文發表，比如說 Purdue 大學 Dongyan Xu 教授研究群的發表 "Reuse-Oriented Camouflaging Trojan: Vulnerability Detection and Attack Construction"、密西跟大學 Kang G. Shin 教授研究群的發表 " "Detection of Botnets Using Combined Host- and Network-Level Information" 以及 CMU 大學 Virgil D. Gligor 教授研究群的發表 "Dependable Connection Setup for Network Capabilities" 等。雖然這些研究根本計畫的入侵反制課題沒有直接關係，但對於激發新的研究方法還是很有幫助的。

二、 Purdue 大學參訪

此次 DSN 會議正巧是在芝加哥舉辦 。芝加哥距離 Purdue University 不過一百多英里遠，開車兩小時多便可到達。我正好把握此一難得機會南下 Purdue University 拜訪我的指導教授 Prof. Saurabh Bagchi，並在 ECE Department 給一個關於我目前在入侵反制上研究的一個 talk。此行目的之一是見見老同學，Purdue 的一些師長，維持聯繫關係，另一方面是尋求未來研究上可能的一些合作。

貳、 心得與結論

總地來說，有機會出席國際會議對於增廣見聞、見見老朋友、認識新朋友是非常有幫助的。尤其我國近年欲推動大學邁向國際一流，其中很重要的一環便是要讓國外一流大學的師生們能看到我們的學校、知道我們的學校也是有在做不錯的 research、甚至可以在國際重要會議上與他們相爭鋒。另外如果經費許可，我是覺得亦能多鼓勵學生出國參加這些重要會議，親自見識一下國外一流大學的學生、老師、以及人家的研究成果。我相信這比透過我們老師所傳遞給他們的二手資訊會對他們有更直接、更深遠的影響。

這次出席 DSN 會議所得到的訊息是入侵反制仍是一個很重要的研究課題。一方面對於驗證程式的安全性，去除弱點等問題就現實生活中的複雜系統仍尚未有完美的解決方案。二方面不斷推成出新的攻擊型態更彰顯了入侵反制機制之存在必要性。在我所原本設想的反制動作中，多半是以阻擋攻擊進程為首要目標。這次參與 DSN 讓我想起了傳統容錯計算上的 checkpoint 和 recovery 等技巧或也可用為反制動作的選項之一。另外整體而言，對於會議中 VeriSign、Lockheed Martin 等業界講者所提供的一些業界在網路攻擊、雲端運算上的看法，對於檢討本計畫之入侵反制系統設計架構在

實務面上的合理性亦有相當程度的助益。

DSN 明年將於香港舉辦，另外像 SIGCOMM 今年在印度舉辦、INFOCOM 明年將在中國上海辦。感覺起來這些大學發展原本落後台灣的國家近幾年在國際會議上的著力程度似乎相對比台灣都還來得深。當然不可否認的是中國、印度有其綜合國力的優勢存在，這些重要會議在那邊舉辦並不代表中、印兩國在相關領域的學術研究已經具有國際一流水準。但以客觀角度來說，人家把握了這些與國際頂尖學者互動的機會，假以時日他們在這些領域的發展肯定會有很大的進步。在這個問題上，我們必須要更認真地去看待，更積極地去應對。

出席國際學術會議心得報告

計畫編號	99-2219-E-009-013-
出國人員姓名 服務機關及職稱	趙禧綠 交通大學資工系助理教授
會議時間地點	2010/9/26~2010/9/29, Istanbul, Turkey
會議名稱	The 21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2010**)**
發表論文題目	Analytical Modeling of Timeout for Contention-Based Bandwidth Request Mechanism in IEEE 802.16 WiMAX Networks

一、參加會議經過

此次國際研討會共計四天，報告人的論文屬 track 2 的 MAC and cross layer design，technical session 則是排在九月二十八日上午。該篇論文的主題是針對頻譜設定在 60GHz 的 IEEE 802.15.3c 之排程演算法。由於 PIMRC 是通訊網路領域主要的國際研討會之一，再加上伊斯坦堡是個旅遊勝地，與會人數很多。

二、與會心得

依據報告人研究興趣，在此次研討會主要聆聽的研究議題有：

(1) Cognitive networks（感知網路）：這個範圍的研究在近期 IEEE 國際研討會議非常熱門，PIMRC 亦安排一場 panel discussion。在這場 panel discussion，他們提出感知無線電網路應有一大型資料庫，供 secondary users 以及 cognitive radio access points (CR APs) 查詢附近區域 primary users 或 primary base stations (BSs) / access points (APs) 的位置以及發射功率，進一步由 CR APs 分配頻道以及頻道可使用時間給 secondary users，避免對 primary users 造成干擾，同時減輕 secondary users 所需要執行的運算。此大型資料庫的需求恰與目前正紅的雲端運算相呼應。利用雲端伺服器所提供的強大運算功能與地域性的資訊查詢，將實現感知無線電網路的進程往前推一大步。由於報告者目前參與一項國科會的橋接計畫，該計畫內容正是實作感知無線電網路。藉由聆聽此 panel discussion，對我們的實作開發助益很大。

(2) Radio Resource Management(RRM)以及 scheduling：偏向跨層的最優化設計(Cross-Layer Optimization)。

(3) LTE：在此次會議中，大多數此範圍的研究仍然是以 OFDM 或者 OFDMA 技術為主，比如 OFDM 所使用通道估測及 Joint CFO and CE 的設計等等。RRM 以及 scheduling 的文章不多見。

(4) Cooperative/relay communications：cooperative communication 這幾年來廣受注意，相關的

論文亦很多。多數論文均以 PHY 的角度來決定 relay 的選擇與數量。

藉由在國際間分享研究與國內外學者交流，並聽取世界各地的研究報告以獲取新知，可以說是非常有收穫的一次行程。報告之論文全文收錄於後。

Performance Enhancement of Contention-Based Bandwidth Request Mechanism in IEEE 802.16 WiMAX Networks

Shih-Fan Chou[1], Jen-Hsi Liu[1], Hsi-Lu Chao[1], Tzu-Chi Guo[1], Chia-Lung Liu[2], and Feng-Jie Tsai[2]
[1]Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan
[2]Information & Communications Research Labs, Industrial Technology Research Institute, Hsinchu, Taiwan

***Abstract*—The IEEE 802.16 standard is a promising technology for 4G mobile networks. Though supporting versatile service classes, best effort (BE) service class is expected to dominate WiMAX networks, due to operational simplicity. One of bandwidth request mechanisms that subscriber stations (SS) can utilize to issue bandwidth requests (BW-REQ) for BE connections is contention-based random access. An SS starts a timer *T*16 when transmitting a BW-REQ. If getting a grant before timer expiration, the SS transmits data packets at the allocated time slots; otherwise it performs truncated binary exponential backoff process for BW-REQ retransmission. The default value of *T*16 is one frame time. However, *T*16 impacts on contention and request collision significantly. In the paper, we develop an analytical model for *T*16 timer setting. Besides, we derive analytical expressions for the average number of tries per BW-REQ and the average packet delay. We compare the theoretical results of fixed and adjustable timers. The results show that adjusting timer reduces both the number of collision and the average packet delay.**

***Keywords*—WiMAX, best effort, bandwidth request, contention**

I. INTRODUCTION

IEEE 802.16 protocol has been standardized for metropolitan broadband wireless access (BWA) systems, and it is a viable technology to be used for connecting local area networks (e.g., IEEE 802.11-bassed WLAN) to the Internet, due to the characteristics of high transmission rate and flexible quality-of-service (QoS). [1]. The IEEE 802.16 MAC layer supports a mandatory PMP architecture, which consists of a base station (BS) serving a number of subscriber stations (SS). There are two types of duplex scheme, i.e. FDD (Frequency Division Duplexing) and TDD (Time Division Duplexing). In this paper, we focus on TDD mode. TDD mode requires only one channel for transmitting downlink (DL) and uplink (UL) sub-frames at two distinct time slots. Moreover, the DL and UL ratio can be adjusted dynamically.

In order to support multimedia services, the IEEE 802.16 standard [1][2] defines five service classes to accommodate versatile QoS-demand applications (such as VoIP, and MPEG video). These service classes are unsolicited grant service (UGS), extended real-time polling service (ertPS), real-time polling service (rtPS), non-real-time polling service (nrtPS), and best-effort (BE) service. Due to the fact that "*how to perform resource reservation to meet applications' QoS demands*" is not within the scope of the standard, it is possible that even VoIP flows would be treated as BE service class. Therefore, in this paper, we focus on the BE service class.

A BS has the full control of slot allocation. To avoid collisions, SSs should get permission before their data transmission. According to the IEEE 802.16 standard, such an exclusive channel access is achieved by requiring SSs to send bandwidth requests first. For this purpose, the IEEE 802.16 standard specifies three bandwidth request mechanisms: contention-based random access and contention free-based polling are two suggested approaches, and piggyback mechanism is optional. These three request mechanisms are applicable to BE service class, and our focus is on the contention-based approach.

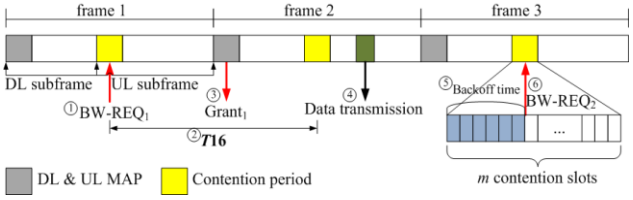


Figure 1 Illustration of contention-based bandwidth request mechanism

The random access contention resolution adopted in WiMAX is based on a truncated binary exponential backoff scheme without carrier sensing. Before each attempt of BW-REQ transmission, an SS randomly selects a backoff timer from [0, W_i-1], where W_i is the contention window size of the i^{th} retry. The backoff time indicates the number of slots that the SS should wait before its BW-REQ transmission. For the first attempt, the contention window size is the minimum value W_{min}; the window size after the i^{th} retry is 2^iW_{min}. The window size keeps doubling till it reaches the maximum value $W_{max}=2^rW_{min}$, where r is the maximum backoff stage. For a BW-REQ, an SS can try at most 16 times. Both W_{min} and W_{max} are defined by BSs, while the WiMAX standard does not provide optimal/suggested values.

When using contention, no explicit acknowledgment (ACK) frame is sent back to indicate whether a bandwidth request (BW-REQ) message is successfully transmitted or not. Instead, a timeout *T*16 is set to determine whether requiring retransmission or not. The default setting of *T*16 is one frame time. An illustrative example of contention-based bandwidth request mechanism is shown in Fig. 1. BW-REQs are sent in the contention period of a frame (Fig. 1-①), and *T*16 is set simultaneously (Fig. 1-②). If a grant is given within *T*16 timeout (Fig. 1-③), the SS stops contention resolution and use the allocated bandwidth for uplink transmission (Fig. 1-④). Otherwise the SS believes that its BW-REQ was corrupted, and then restarts a contention resolution process. The SS randomly selects a backoff timer (Fig. 1-⑤), and counts down that timer. When the timer is zero, the SS retransmits the BW-REQ (Fig. 1-⑥), and same processes repeat.

Recent research of request mechanisms include [3][4][5][6][7]. In [3], the authors conclude that the best size of contention period is (2*N*-1), and *N* is the number of SSs. However, upon heavy traffic load, the number of data slots of an UL subframe decrease as *N* increases, and a BS may not issue grants to all received BW-REQs. For those refused and collided BW-REQs, the SSs will run the contention resolution mechanism again, and thus delay time increases.

In [4], the authors introduce a new algorithm, called Multi-FS-ALOHA, which divides the contention period into two parts. The first is used by SSs to issue first-try BW-REQs, while the second part is dedicated for retransmission of BW-REQ messages. These two parts are dynamically fixed on a frame by frame basis. The drawback of [4] is that it requires a dedicated feedback channel for operation.

A modified contention resolution process is proposed in [5] to improve the system performance. Its main idea is assigning different initial window sizes to different scheduling classes. However, based on the presented simulation results, this algorithm performs similarly to the contention mechanism defined in the standard.

An analytical model of the contention-based bandwidth request mechanism, defined in [1], in a saturated WiMAX network was developed in [6][7]. [8] took the number of contending SSs into account to determine the optimal window size.

Briefly summarizing the introduced literature, performance of the contention-based request mechanism can be improved by (1) reducing the collision probability, (2) dynamically adjusting the contention period according to the number of SSs, (3) assigning different minimum contention window sizes to service classes, and (4) integrating/implementing both piggyback and contention mechanisms. However, these solutions may incur the problem of compatibility.

Two possible reasons that a BW-REQ cannot be granted and need retransmission are: collision, and insufficient UL data slots. The former is due to multiple BW-REQs are transmitted at the same contention slot; the latter is due to the UL data slots cannot accommodate the total demand of received BW-REQs. However, SSs cannot identify the exact reason why they do not get resource grants, and just perform contention resolution procedure. Upon heavy traffic load, more contentions in a fixed contention period results in more collisions and worse system performance. Thus our idea is to dynamically adjust *T*16 timeout. BW-REQs may wait longer before perform contention resolution process. The objective of this paper is to develop an analytical mode for *T*16 derivation.

The rest of this paper is organized as follows. The analytical model of timeout derivation is introduced in Section II. Numerical results are presented and discussed in Section III. This paper is concluded in Section IV.

II. Analytical Model

In this section, we explain the developed analytical model. Since we focus on the retransmission caused by insufficient UL bandwidth, $T16_{ib}$ is used to represent the desired timeout. In addition, we analyze the average tries of a BW-REQ to get a resource grant, and the average packet delay.

In this analytical model, there are N BE connections, and their packet arrival is in Poisson distribution with λ_{packet}. t_{frame} and d are the frame time duration and the number of data slots of a UL subframe. r_{be} is the percentage of UL data slots which are allocated to BE service class.

A. $T16_{ib}$

Let n be the number of frames that a successfully transmitted BW-REQ can be preserved by a BS at most. Therefore,

$$T16_{ib} \geq (1+n)t_{frame} \tag{1}$$

To derive a proper $T16_{ib}$ is to determine an adequate *n* value.

In our analysis, we assume there are *m* slots in a contention period, and each slot can accommodate one BW-REQ message.

Considering a BW-REQ, the probabilities of request collision and insufficient UL bandwidth of its i^{th} retransmission (i.e., the $(i+1)^{th}$ try) are denoted as $p_c^{(i)}$ and $p_{ib}^{(i)}$ respectively. Since unsuccessful BW-REQs are only due to collisions in the modified mechanism, the probability of the i^{th} contention for an unsuccessful BW-REQ (denoted as $p_{modified}^{(i)}$) is

$$p_{modified}^{(i)} = p_c^{(i)} \tag{2}$$

According to [9], the probability that an SS attempts to transmit a BW-REQ at a contention slot for the i^{th} retry $\tau^{(i)}$ is

$$\tau^{(i)} = \frac{2}{W_i + 1} \qquad 0 \leq i \leq R-1, \tag{3}$$

where *R* is the maximum number of tries.

Given the number of transmitted BW-REQs in frame $\left\lceil \frac{W_i-1}{m} \right\rceil$, denoted as $N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}$, suppose the observed BW-REQ is retransmitted at the last contention slot in frame $\left\lceil \frac{W_i-1}{m} \right\rceil$, $p_c^{(i)}$ is

$$p_c^{(i)} = 1 - \left[1-\tau^{(i)}\right]^{N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}-1}, \quad 0 \leq i \leq R-1 \tag{4}$$

Furthermore, for $0 \leq i \leq R-1$,

$$p_{ib}{}^{(i)} = \frac{N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}\left(1-p_c^{(i)}\right) - N_{request\_served}}{N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}\left(1-p_c^{(i)}\right)} \tag{5}$$

where $N_{request\_served}$ is the number of served requests in a superframe.

We then derive the number of transmitted BW-REQs in a specific frame, say frame *j*. Connections either incurring BW-REQ collision or having packet arrivals in frame (*j*-1) will send their BW-REQs in frame *j*. We assume all BE connections have queued packets initially, i.e., $N^{(1)} = N$. Thus for frame 2,

$$N^{(2)} = N^{(1)}(1-P_0)\left(1-P_c{}^{(0)}\right)\left(1-P_{ib}{}^{(0)}\right) + N^{(1)}P_c{}^{(0)}\frac{m}{W_{min}} \tag{6}$$

where P_0 is the probability that an SS has no packet arrivals in t_{frame} time, and $P_0 = 1 - \mathrm{e}^{-(\lambda_{packet})(t_{frame})}$. Through iterative derivation, for $j \geq 1$

$$N^{(j+1)} = N^{(j)}(1-P_0)\left(1-p_c{}^{\left(log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor\right)}\right)\left(1-p_{ib}{}^{\left(log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor\right)}\right) + N^{(j)}p_c{}^{\left(log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor\right)}\frac{m}{W_{log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor}} \tag{7}$$

In (7), we use the backoff stage to get the number of retransmitted requests occur at this frame and $\frac{m}{W_{\log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor}}$ is the probability that a collided request would transmit again in frame j.

On the other hand, the number of requests a BS can serve in a UL subframe is

$$N_{request\_served} = \left\lfloor \frac{dr_{be}}{\lambda_{packet} t_{frame}} \right\rfloor. \quad (8)$$

Thus considering the worst case, a successfully transmitted BW-REQ at frame j can be served at most after n frames, and n is

$$n = \left\lceil \frac{N^{(j)}(1-p_c^{(j)}) - N_{request\_served}}{N_{request\_served}} \right\rceil. \quad (9)$$

Substituting (4), (7), (8), and (9) into (1), we obtain a theoretical $T16_{ib}$.

B. Average Number of Tries

Again in the original contention-based bandwidth request mechanism, a BW-REQ is retransmitted when either the BW-REQ experiences a collision, or the BS has no sufficient UL bandwidth to give it a grant. Let X be the number of tries for a BW-REQ to get granted. Since a request can be sent at most R times, the average number of tries is

$$E[X]_{original} = \sum_{i=1}^{R} \left[i p_c^{(i)} + i(1-p_c^{(i)}) p_{ib}^{(i)} \right] \quad (10)$$

However, in the modified mechanism, the BW-REQ retransmission is only caused by collisions, thus the average number of tries is as listed in (11).

$$E[X]_{modified} = \sum_{i=1}^{R} i p_c^{(i)} \quad (11)$$

C. Packet Delay

We define the packet delay being the time duration from the first try of a BW-REQ to the time of successful data packet transmission. In the IEEE 802.16 standard, the frame structure of TDD mode includes a downlink subframe (Fig. 2 ①) and an uplink subframe. An uplink subframe consists of a contention period $t_{contention}$ (Fig. 2 ②) and a data interval t_{DA} (Fig. 2 ③). The time gap between two consecutive frames is called guard time t_{guard}(Fig. 2 ④). Let $t_{request}$ and t_{data}be the time of a contention slot and an uplink data slot respectively. Thus $t_{contention} = mt_{request}$, and $t_{DA} = dt_{data}$. Let $D^{(i)}$ indicate the packet delay that a BW-REQ is granted at its i^{th} retry. Note that i=0 means the BW-REQ gets grant at its first try. An example to calculate $D^{(i)}$ is shown in Fig. 2. U and V are the time durations from sending the first BW-REQ to the end of the contention period (t_u) and from the beginning of the uplink data interval (t_v) to the time that the first packet has been transmitted, respectively. Using i=0 as an example, the first possibility is that a first-try BW-REQ is successfully transmitted and gets served immediately, its packet delay is

$$D^{(0)} = U + Y^{(0)} + V, \quad (12)$$

where

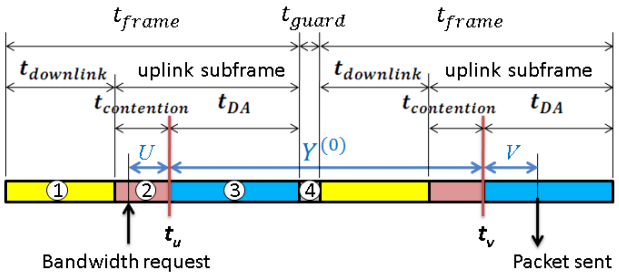


Figure 2 An illustrative example of packet delay calculation

$$\begin{cases} U = it_{request} & w.p.\ \frac{1}{m}, i = 1,2,\dots,m \\ V = it_{data} & w.p.\ \frac{1}{dr_{be}}, i = 1,2,\dots,dr_{be} \\ Y^{(0)} = t_{DA} + t_{guard} + t_{downlink} + t_{contention} \\ \quad = t_{frame} + t_{guard} = c \end{cases}$$

and *w.p.* stands for "with probability".

The second possibility is this first-try BW-REQ is successfully transmitted but preserved for later grant. In such a case, the packet delay is the same as (12) while with a different $Y^{(0)}$, and

$$Y^{(0)} = (1 + \tfrac{1}{2}\left\lceil \frac{T16_{ib}}{t_{frame}} \right\rceil)c.$$

$\frac{1}{2}\left\lceil \frac{T16_{ib}}{t_{frame}} \right\rceil$ is the waiting time in a frame for a preserved BW-REQ to get a grant, and it is uniformly distributed within $T16_{ib}$ time duration.

The last possibility is that this BW-REQ is collided with other requests, and thus the SS doubles the contention window size, randomly selects a backoff value, and retransmits this BW-REQ. If this 2nd try immediately gets a grant, the corresponding packet delay $D^{(1)}$ is

$$D^{(1)} = U + Y^{(1)} + V, \quad (13)$$

where $Y^{(1)}$ is the waiting time (and its unit is frame) between t_u and t_v and is given as

$$Y^{(1)} = c \sum_{i=0}^{1} K^{(i)} Y^{(0)}.$$

$K^{(i)}$ is the waiting time in a frame for packet transmission at the i^{th} contention. Since the SS uniformly selects its backoff counter from [0,W_i-1]. According to [10], the probability mass function of random variable $K^{(i)}$ is

$$K^{(i)} = \begin{cases} 1, & i = 0 \\ j, & w.p.\ \frac{m}{W_i}, \quad i \neq 0,\ j = 1,2,\dots,\left\lfloor \frac{W_i}{m} \right\rfloor - 1 \\ \left\lceil \frac{W_i}{m} \right\rceil, & w.p.\ 1 - \frac{(\left\lfloor \frac{W_i}{m} \right\rfloor - 1)m}{W_i}, i \neq 0 \end{cases} \quad (14)$$

If this 2nd-try BW-REQ is successfully transmitted while been preserved, it packet delay is

$$D^{(1)} = U + \left(K^{(0)} + K^{(1)} + \frac{1}{2}\left\lceil \frac{T16_{ib}}{t_{frame}} \right\rceil \right) c + V.$$

In general, for the i^{th} attempt, the average packet delay $D^{(i)}$ is

$$\begin{cases} \mathrm{E}\left[D^{(i)}\right] = E[U] + \mathrm{E}\left[Y^{(i)}\right] + E[V] \\ \mathrm{E}\left[Y^{(i)}\right] = c\sum_{j=0}^{i} \mathrm{E}\left[Z^{(j)}\right] \end{cases}, 0 \le i < R \quad (15)$$

where $Z^{(j)}$ is the waiting time in a frame for a j^{th}-retry BW-REQ and its mean is

$$\mathrm{E}\left[Z^{(j)}\right] = \begin{cases} 1, & j = 0 \\ p_c^{(j)}\mathrm{E}[K^{(j)}] + (1 - p_c^{(j)})p_{ib}^{(j)}\left(\frac{1}{2}\left\lceil\frac{T16_{ib}}{t_{frame}}\right\rceil\right), & j \ge 1 \end{cases} \quad (16)$$

Since

$$\mathrm{E}\left[K^{(j)}\right] = \begin{cases} 1, & j = 0 \\ \left\lceil\frac{W_j}{m}\right\rceil - \left\lceil\frac{W_j}{m}\right\rceil\left(\left\lceil\frac{W_j}{m}\right\rceil - 1\right)\frac{m}{2^{j+1}W_{min}}, & j = 1, \dots, r-1 \\ \left\lceil\frac{W_j}{m}\right\rceil - \left\lceil\frac{W_j}{m}\right\rceil\left(\left\lceil\frac{W_j}{m}\right\rceil - 1\right)\frac{m}{2^{r+1}W_{min}}, & j = r, \dots, R-1 \end{cases} \quad (17)$$

and

$$\begin{cases} E[U] = \dfrac{(m+1)t_{request}}{2} \\ E[V] = \dfrac{(dr_{be}+1)t_{data}}{2} \end{cases} \quad (18)$$

we obtain $\mathrm{E}\left[D^{(i)}\right]$ by substituting (16), (17) and (18) into (15). Further, the mean total packet delay of the modified mechanism $\mathrm{E}[D]_{\text{modified}}$ is

$$\mathrm{E}[D]_{\text{modified}} = (1 - p_{modified}^{(R)})\sum_{i=0}^{R-1}\left\{\left(\prod_{k=0}^{i} p_{modified}^{(k)}\right)\mathrm{E}\left[D^{(i)}\right]\right\}. \quad (19)$$

For comparison purpose, we also derive the mean total packet delay of the original mechanism, i.e., $\mathrm{E}[D]_{\text{original}}$. The expression of $\mathrm{E}[D]_{\text{original}}$ is same as (19), while the probability for a BW-REQ to fail at its i^{th} contention is $p_{original}^{(i)} = 1 - \left(1 - p_c{}^{(i)}\right)\left(1 - p_{ib}{}^{(i)}\right)$.

III. Numerical Results

In this section, we develop a simulation program to validate the analytical model, and compare and discuss the performance of the original and modified contention request mechanisms. Parameter settings are listed in Table 1.

Fig. 3 shows the $T16_{ib}$ settings upon various numbers of BW-REQs. As the number of requests increases, $T16_{ib}$ also linearly increases. Besides, upon a specific N value, as λ_{packet} increases, $T16_{ib}$ increases, too. The reason is, in average, the number of required time slots increases, and thus a BS can only serves few requests in a UL subframe. Consequently successfully transmitted BW-REQs will be preserved longer before getting grants.

In the following experiment, we set λ_{packet} be 3, and $T16_{ib}$ setting is based on the results in Fig. 3. We investigated the performance of p_c and p_{ib}, as shown in Fig. 4. It is intuitive that both p_c and p_{ib} increase as the number of requests increases. Moreover, we observed that when properly setting W_{min} (e.g., W_{min}=64), p_c is significantly reduced to 1.2×10^{-3}, and p_{ib} maintains at the smallest value among all.

The performance of average number of tries is in Fig. 5 (a) and (b). If a BW-REQ is transmitted successfully to the BS, it may be preserved for future grant. In such a case, the SS does not need to retransmit this request and thus the number of tries per request reduces, compared with the original contention request mechanism. Note that the average number of tries for both original and modified mechanisms of $W_{min} = 8$ is more than that of $W_{min} = 16$. The reason is that a small contention window size results in a high collision probability.

Table 1. Parameter settings

Parameter	Value
W_{min}	8/16/32/64
Maximum backoff stage, r	10
Maximum number of tries, R	16
Number of request slots, m	10
Number of data slots per uplink subframe, d	20
Ratio of data slots for BE, r_{be}	0.5
Time of a request slot, $t_{request}$	0.024 ms (6 slots)
Time for a uplink data slot, t_{data}	0.0376 ms (94 slots)
Guard time duration, t_{guard}	0.004 ms (1 slot)
Frame duration, t_{frame}	1 ms
Packet arrival rate, λ_{packet}	3/5/7

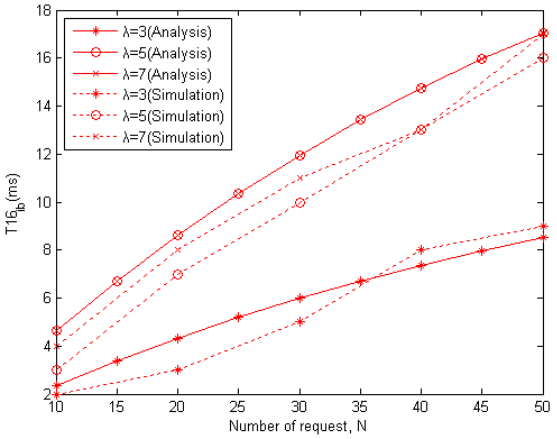


Figure 3. $T16_{ib}$ settings vs. the number of requests N upon various packet arrival rates

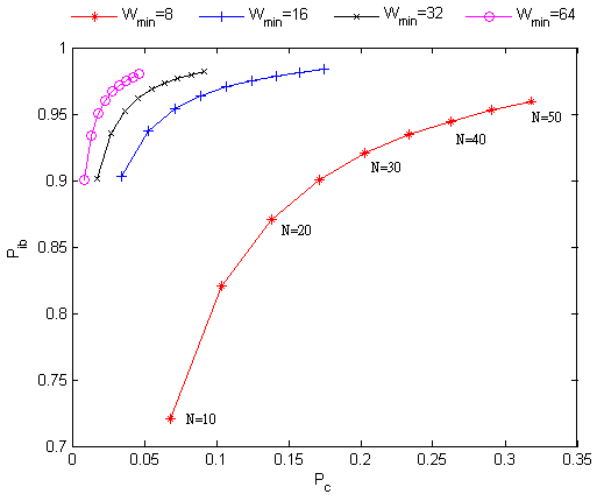
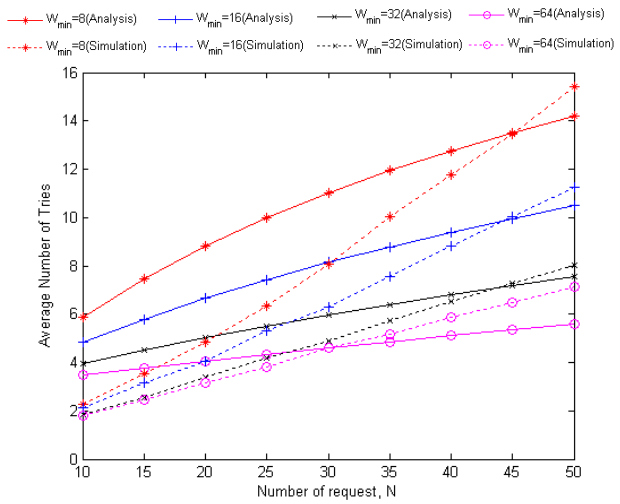
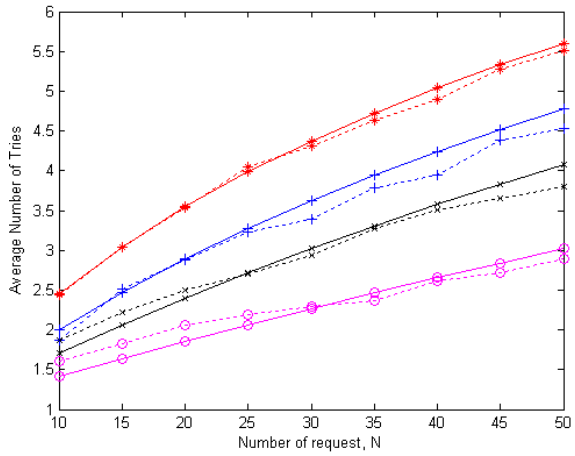


Figure 4 Probabilities of collision and insufficient bandwidth upon various W_{min} settings

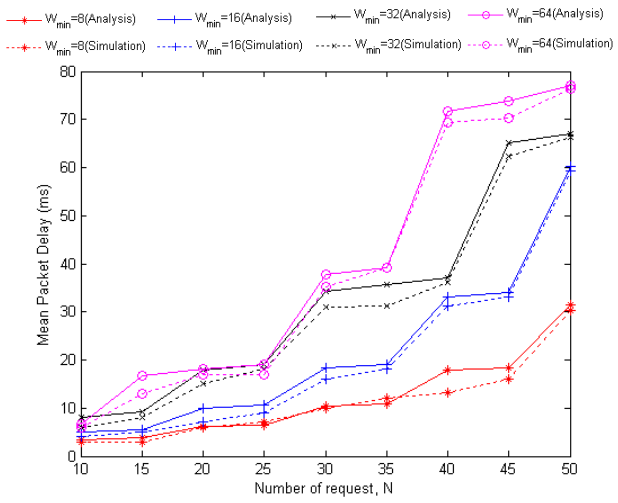


(a) Original

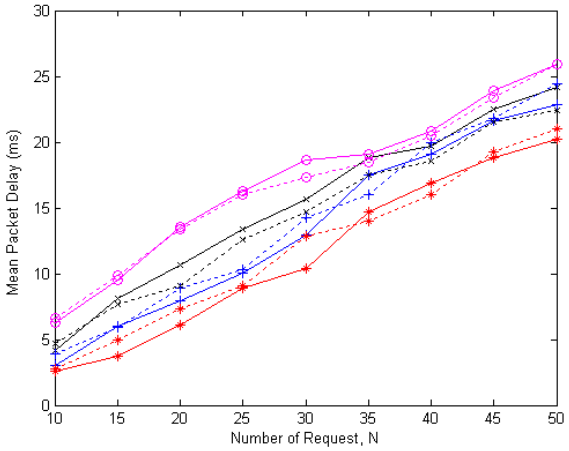


(b) Modified

Figure 5 The performance of average number of tries of the two contention-based bandwidth request mechanisms



(a) Original



(b) Modified

Figure 6 The performance of mean packet delay of the two contention-based bandwidth request mechanisms

Fig. 6 depicts the mean packet delay of both request mechanisms as the number of requests increases from 10 to 50, upon various W_{min} settings. For both mechanisms, when given a W_{min}, a large N value results in long delay due to high collision probability and more retries. On the other hand, for a specific N value, the window size of each backoff stage increases, and the average packet delay increases accordingly. The reason is that when collision occurs, the range of the backoff value becomes larger (0 to W_i -1). An SS is delayed much more frames when using a larger backoff value. The mean packet delay of the modified mechanism is significantly smaller than that of the original mechanism. The reason is that the modified request mechanism preserves successfully transmitted BW-REQs at most (n+1) frames without performing binary exponential backoff process and thus the contention window size is intact. Therefore, it has rather small delay, compared to the original mechanism.

IV. Conclusion

In this paper, focused on BE service class and contention-based request mechanism, we developed an analytical model to derive a theoretical $T16_{ib}$ timeout. Dissimilar to the original contention-based request mechanism that all unsuccessfully transmitted BW-REQs must perform the truncated binary exponential backoff process, the modified mechanism achieves reduction of collisions and tries by adjusts timeout properly for those successfully transmitted BW-REQs while cannot get grants in the next frame. The modeled timeout is a function of (1) number of BE connections, (2) traffic load, (3) retransmission, (4) collision probability, and (5) bandwidth insufficient probability. Numerical results showed that a suitable timeout does reduce the number of tries, and the average packet delay. Since the failure probability of transmitting BW-REQ decreases and the probability of a BW-REQ being hold increases, the number of tries is reduced. In addition, the range of the backoff value grows exponentially when retry occurs. An SS does not need to wait for the backoff counter counting down to zero for BW-REQ transmission when the BW-REQ is hold by the BS. The average packet delay is lower accordingly. From the numeral and simulation results, when the size of initial contention window approaches the number of contention slots, we could get better average packet delay performance. In our case, we suggest that the contention window size is 8.

Acknowledgment

This work was supported in part by NCTU-MTK Research Center under grant 99Q583, in part by National Science Council under grant NSC 99-2219-E-009-013- and in part by Ministry of Economic Affairs and Industrial Technology Research Institute under grant 99-EC-17-A-03-01-0620.

REFERENCES

[1] IEEE Std. 802.16-2004, "Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems".

[2] IEEE 802.16e-2005, IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, 2006.

[3] Taleb T., Fernandez J.C., Hashimoto K., Nemoto Y., Kato N., "A Bandwidth Aggregation-aware QoS Negotiation Mechanism for Next-Generation Wireless Networks", *IEEE Global Telecommunications Conference*, November 2007, pp.1912-1916.

[4] Lidong Lin, Bo Han and Lizhuo Zhang, "Performance Improvement using Dynamic Contention Window Adjustment for Initial Ranging in IEEE 802.16 P2MP Networks", IEEE Wireless Communications & Networking Conference (WCNC), 2007, pp.11-15.

[5] Jianhua He, Ken Guild, Kun Yang, and Hsiao-Hwa Chen, "Modeling Contention Based Bandwidth Request Scheme for IEEE 802.16 Networks", *IEEE Communications Letters*, Volume 11, August 2007 pp.689-700.

[6] Vinel A., Ying Zhang, Qiang Ni, Lyakhov A., "Efficient Request Mechanism Usage in IEEE 802.16", *Global Telecommunications Conference*, December 2006, pp.1-5.

[7] Wenyan Lu, Weijia Jia, Wenfeng Du, Lizhuo Zhang, "Performance analysis of the contention resolution scheme in IEEE 802.16". Journal of Software, Volume 18, No. 9, pp.2259-2270, 2007.

[8] Sung-Min Oh, Jae-Hyun Kim, "The Analysis of the Optimal Contention Period for Broadband Wireless Access Network", *Pervasive Computing and Communications Workshops*, March 2005, pp.215-219..

[9] Giuseppe Bianchi, Luigi Fratta, and Matteo Oliveri, "Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs," in Proc. IEEE PIMRC, Taipei, Taiwan, Sept. 1996, pp. 392–396.

[10] Hai L. Vu, Sammy Chan, and Lachlan L. H. Andrew, "Performance analysis of Best-Effort Service in Saturated IEEE 802.16 Networks," *Proc. IEEE Vehicular Technology*, Volume 59, No. 1, January 2010, pp.460-472.

[11] Q. Ni, L. Hu. "An Unsaturated Model for Request Mechanisms in WiMAX". IEEE Communications Letters, Vol. 14, No. 1, Jan 2010, pp. 45-47.

[12] Q. Ni, A. Vinel, Y. Xiao, A. Turlikov, T. Jiang. "Investigation of Bandwidth Request Mechanisms under Point-to-Multipoint Mode of WiMAX Networks". IEEE Communications Magazine, Vol. 45, No. 5, May 2007, pp. 132-138.

「ACM Symposium on Information, Computer and Communications Security（ASIACCS）國際學術會議」出國報告書

報告人： 交通大學謝續平

日期：2010 年 04 月 30 日

一、 出國目的

ACM Symposium on Information, Computer and Communications Security （ASIACCS）為 ACM Special Interest Group on Security, Audit, and Control（SIGSAC）所贊助與主辦的兩大頂尖會議之一，接受率約為 10%一頂尖會議為 ACM Conference on Computer and Communications Security（CCS）， 接受率也約為 10%。本人擔任 ACM ASIACCS steering committee chair, 負責推動該會議，並且召集 steering committee meeting，遴選每年執行單位。此次參加該國際學術會議，並審查 2011 年主辦單位進度，與 2012 年主辦國家與單位，並討論會議場地與籌辦流程。

二、 行程

參加 ACM Symposium on Information, Computer and Communications Security 擔任 Steering Committee Chair。

4/9 Taipei – Beijing

4/10 受 ACM ASIACCS steering committee member 以及 Mozilla Online Ltd. CEO Li Gong 博士邀請訪問 Mozilla Online Ltd. (該公司為開發 Firefox web browser 的公司，Firefox 瀏覽器為全球最受歡迎的瀏覽器之一)

4/12 受大會以及 Chinese Academy of Sciences, Deputy Director Jiwu Jing 邀請訪問中科院並演講 “Cloud Computing Security”

4/13-16 ACM Symposium on Information, Computer and Communications Security 會議

4/17-18 ASIACCS steering committee 會議擔任主席

4/19 返台

三、 出國人員：

謝續平現任交通大學資訊工程系教授暨 TWISC@NCTU 主任，曾任交通大學資訊工程系系主任、交通大學計算機與網路中心主任、中華民國資訊安全學會理事長，現在擔任 IEEE Tran. On Dependable and Secure Computing、IEEE Trans. On Reliability、Journal of Computer Security 副編輯、IEEE RS Newsletter 總編輯。由於現在擔任 ACM Symposium on Information, Computer and Communications Security （ASIACCS） 推動委員會主席（steering committee chair)。負責遴選籌辦國家單位，並督導籌辦進度。

四、 工作內容摘要

由於擔任 ACM Special Interest Group on Security, Audit, and Control (SIGSAC) 的推動委員會委員（Steering Committee member)，並且擔任 ACM Symposium on Information, Computer and

Communications Security （ASIACCS） 推動委員會主席（steering committee chair)，被 ACM 賦予：

a）觀察本年度會議執行成果，

b）審查下年度執行單位籌備現況，

c）並甄選兩年後會議執行單位。

本次出國為了推動 SIGSAC 的未來發展，赴大陸北京友誼賓館，參加本年度會議，觀察 ASIACCS 本年度會議主辦單位美國賓州州立大學、瑞士 ETH、北京中國科學研究院成果，並審查 2011 會議舉辦單位香港大學、香港城市大學籌備進度，與 2012 年申請舉辦單位上海交通大學等單位的提案。

此次大會由北京中國科學研究院 Dengguo Feng 主任擔任大會主席，David Basin(basin@inf.ethz.ch, ETH Zurich, Switzerland)
Peng Liu(pliu@ist.psu.edu, Pennsylvania State University, USA)
擔任議程主席，會議接受率僅約 10%，相較於 IEEE INFOCOMM 等頂級國際會議的接受率 25%，顯得更為難得。

本次會議前、後分別受到本會議的推動委員會委員 Mozilla 的 CEO Li Gong 的邀請訪問以及本會議的大會邀請至中國科學研究院演講，而國際會議後的推動委員會也決議 2012 年的主辦單位延至下次會議討論。

五、　結語

本次大會由有來自全世界三十餘國作者投稿，稿件水準極高，接受率極低，約為 10%，會議圓滿成功。會議組織與會議議程如下：

CONFERENCE ORGANIZING COMMITTEE

General Chair	Dengguo Feng (feng@is.iscas.ac.cn, Chinese Academy of Sciences, China)
Program Committee Chair	David Basin(basin@inf.ethz.ch, ETH Zurich, Switzerland) Peng Liu(pliu@ist.psu.edu, Pennsylvania State University, USA)
Local Arrangements Committee Chair	Jiwu Jing (jing@lois.cn, Chinese Academy of Sciences, China)
Publication Chair	Peng Ning (pning@ncsu.edu, NC State University, USA)
Publicity Chair	Jie Li (lijie@cs.tsukuba.ac.jp, University of Tsukuba, Japan)
Workshop Chair	Dongdai Lin (ddlin@is.iscas.ac.cn, Chinese Academy of Sciences, China)
Tutorial Chair	Zhong Chen (chen@cs.pku.edu.cn, Peking University, China)

Treasurer	Sencun Zhu (szhu@cse.psu.edu, Pennsylvania State University, USA)
Web Chair	Ji Xiang (xiangji2008@gmail.com, Chinese Academy of Sciences, China)
Secretary	Daren Zha (zdr@lois.cn) Zongbin Liu (liuufo85@gmail.com)

STEERING COMMITTEE

Shiuhpyng Shieh(Chair), Chiao Tung University, Chinese Taipei
David Basin, ETH Zurich, Switzerland
Robert Deng, Singapore Management University, Singapore
Virgil Gligor, Carnegie Mellon University, USA
Hideki Imai, National Institute of Advanced Industrial Science and Technology, Japan
Sushil Jajodia, George Mason University, USA
Pierangela Samarati, University of Milan, Italy
Elisa Bertino, Purdue University, USA
Mike Reiter, University of North Carolina at Chapel Hill, USA
Li Gong, Mozilla Online Ltd., USA
Ninghui Li, Purdue University, USA
Eiji Okamoto, University of Tsukuba, Japan
Vijay Varadharajan, Macquarie University, Australia

六、會議議程

ASIACCS 2010: Beijing, China

Program Sketch

12 April	**13:30-18:00**	Registration	Lobby of Building 2
13 April	**8:00-8:50**	Registration	Meeting Room1, Building 8
	8:50-9:00	Welcoming Remarks	Meeting Room1, Building 8
	9:00-10:00	Invited Talk	Meeting Room1, Building 8
	10:00-10:30	Coffee-break	Meeting Room1, Building 8
	10:30-12:00	Session 1:Privacy	Meeting Room1, Building 8
	12:00-13:30	Lunch	Cafeteria in Friendship Palace
	13:30-15:00	Session 2:Applied Cryptography	Meeting Room1, Building 8
	15:00-15:30	Coffee Break	Meeting Room1, Building 8
	15:30-17:00	Session 3: Network Security	Meeting Room1, Building 8
	17:30-19:00	Dinner	Cafeteria in Friendship Palace
	19:00-21:00	Steering Committee Meeting (Steering committee members only)	Second Floor meeting Room, Building 2
14 April	**8:00-8:50**	Registration	Meeting Room1, Building 8
	9:00-10:00	Invited Talk	Meeting Room1, Building 8
	10:00-10:30	Coffee Break	Meeting Room1, Building 8
	10:30-12:00	Session 4: Systems Security – I	Meeting Room1, Building 8
	12:00-13:30	Lunch	Cafeteria in Friendship Palace
	13:30-15:00	Session 5: Access Control – I	Meeting Room1, Building 8
	15:00-15:30	Coffee Break	Meeting Room1, Building 8
	15:30-17:30	Session 6: Security Protocols	Meeting Room1, Building 8
	18:30-20:30	Banquet	Ju Xiu Yuan Friendship Palace
	8:00-8:45	Registration	Meeting Room1, Building 8
	8:45-10:15	Session 7: Access Control – II	Meeting Room1, Building 8

15 April	**10:10-10:35**	Coffee Break	Meeting Room1 Building 8
	10:35-12:05	Session 8: Systems Security - II	Meeting Room1, Building 8
	12:05-13:30	Lunch	Cafeteria in Friendship Palace
	13:30-15:10	Session 9: Short Papers – I	Meeting Room1, Building 8
	13:10-15:30	Coffee Break	Meeting Room1, Building 8
	15:30-17:10	Session 10: Short Papers – II	Meeting Room1, Building 8
	17:30-19:00	Dinner	Cafeteria in Friendship Palace

Advanced Program

The 5th ACM Symposium on Information, Computer and Communications Security

(ASIACCS 2010)

（Beijing Friendship Hotel）

April 13, 2010	
8:00 - 8:50	**Registration**
8:50 - 9:00	**Welcoming Remarks**
9:00 - 10:00	**INVITED TALK:** **Pierangela Samarati, Universita` degli Studi di Milano** **Session Chair: Peng Liu**
10:00 - 10:30	**Coffee Break**
Session 1: Privacy **Session Chair: Adam Lee**	
10:30 - 11:00	**Towards Publishing Recommendation Data With Predictive Anonymization** Chih-Cheng Chang, Rutgers University Brian Thompson, Rutgers University Hui Wang, Stevens Institute of Technology Danfeng Yao, Rutgers University
11:00 - 11:30	**Restoring Compromised Privacy in Micro-data Disclosure** Lei Zhang, George Mason University Alexander Brodsky, George Mason University Sushil Jajodia, George Mason University
11:30 - 12:00	**Securely Outsourcing Linear Algebra Computations** Mikhail Atallah, Purdue University Keith Frikken, Miami University
12:00 - 13:30	**Lunch**
Session 2: Applied Cryptography **Session Chair: Dongdai Lin**	
13:30 - 14:00	**Attribute-based Signature and its Application** Jin Li, Illinois Institute of Technology Man Ho Au, University of Wollongong Willy Susilo, University of Wollongong Dongqing Xie, Guangzhou University

	Kui Ren, Illinois Institute of Technology
14:00 - 14:30	**Dynamic Fully Forward-Secure Group Signatures** Benoit Libert, Universite Catholique de Louvain Moti Yung, Google & Columbia University
14:30 - 15:00	**Identity-Based Encryption based on ElGamal** Yu Chen, Peking University Manuel Charlemagne, Dublin City University, Ireland Zhi Guan, Peking University Jianbin Hu, Peking University Zhong Chen, Peking University
15:00 - 15:30	**Coffee Break**
Session 3: Network Security Session Chair: Kui Ren	
15:30 - 16:00	**Region-based BGP Announcement Filtering for Improved BGP Security** Fernando Sanchez, Zhenhai Duan Florida State University
16:00 - 16:30	**Fast-flux Service Network Detection Based on Spatial Snapshot Mechanism for Delay-free Detection** Si-Yu Huang, Taiwan Tech Ching-Hao Mao, Taiwan Tech Hahn-Ming Lee, Taiwan Tech
16:30 - 17:00	**Securing Wireless Sensor Networks against Large-scale Node Capture Attacks** Tuan Vu, University of Calgary Reihaneh Safavi-Naini, University of Calgary Carey Williamson, University of Calgary
17:30 - 19:00	**Dinner**
April 14, 2010	
8:00 - 9:00	**Registration**
9:00 – 10:00	**INVITED TALK:** **Andrei Sabelfeld, Chalmers University of Technology** **Session Chair: David Basin**
10:00 - 10:30	**Coffee Break**

Session 4: Systems Security – I Session Chair: Andrei Sabelfeld	
10:30 - 11:00	**Preventing Drive-by Download via Inter-Module Communication Monitoring** Chengyu Song, Peking University Jianwei Zhuge, Peking University Xinhui Han, Peking University Zhiyuan Ye, Peking University
11:00 - 11:30	**A Solution for the Automated Detection of Clickjacking Attacks** Marco Balduzzi, Eurecom Manuel Egele, University of California, Santa Barbara Engin Kirda, Eurecom Davide Balzarotti, Eurecom Christopher Kruegel, University of California, Santa Barbara
11:30 - 12:00	**PAriCheck: An Efficient Pointer Arithmetic Checker for C Programs** Yves Younan, Katholieke Universiteit Leuven Pieter Philippaerts, Katholieke Universiteit Leuven Lorenzo Cavallaro, University of California, Santa Barbara R. Sekar, Stony Brook University Frank Piessens, Katholieke Universiteit Leuven Wouter Joosen, Katholieke Universiteit Leuven
12:00 - 13:30	**Lunch**
Session 5: Access Control – I **Session Chair: Robert Deng**	
13:30 - 14:00	**An Opportunistic Authority Evaluation Scheme for Data Security in Crisis Management Scenarios** Enrico Scalavino, Imperial College London Giovanni Russello, Create-Net Rudi Ball, Imperial College London Vaibhav Gowadia, Imperial College London Emil Lupu, Imperial College London
14:00 - 14:30	**Effective Trust Management Through a Hybrid Logical and Relational Approach** Adam J. Lee, University of Pittsburgh

	Ting Yu, North Carolina State University Yann Le Gall, University of Pittsburgh
14:30 - 15:00	**Toward Practical Authorization-dependent User Obligation Systems** Murillo Pontual, University of Texas at San Antonio Omar Chowdhury, University of Texas at San Antonio William H. Winsborough, University of Texas at San Antonio Ting Yu, North Carolina State University Keith Irwin, Winston-Salem State University
15:00 – 15:20	**Coffee-break**
Session 6: Security Protocols **Session Chair: Kanta MATSUURA**	
15:30 - 16:00	**Cap Unification: Application to Protocol Security modulo Homomorphic Encryption** Siva Anantharaman, LIFO, University of Orleans Hai Lin, Clarkson University Christopher Lynch, Clarkson University Paliath Narendran, University at Albany--SUNY Michael Rusinowitch, LORIA - INRIA Lorraine
16:00 - 16:30	**SSLOCK: Sustaining the Trust on Entities Brought by SSL** Adonis P.H. Fung, The Chinese University of Hong Kong K.W. Cheung, The Chinese University of Hong Kong
16:30 - 17:00	**Computationally Secure Two-Round Authenticated Message Exchange** Klaas Ole Kürtz, Christian-Albrechts-Universität Kiel Henning Schnoor, Christian-Albrechts-Universität Kiel Thomas Wilke, Christian-Albrechts-Universität Kiel
17:00 – 17:30	**Bureaucratic Protocols for Secure Two-Party Sorting, Selection, and Permuting** Guan Wang, Syracuse University Tongbo Luo, Syracuse University Michael T. Goodrich, Univ. of California, Irvine Wenliang Du, Syracuse University Zutao Zhu, Syracuse University

18:30 - 20:30	**Conference Banquet**
April 15, 2010	
8:00 - 8:45	**Registration**
Session 7: Access Control – II **Session Chair: Ting Yu**	
8:45 - 9:15	**A Logic for Authorization Provenance** Jinwei Hu, Huazhong University of Science and Technology Yan Zhang, University of Western Sydney Ruixuan Li, Huazhong University of Science and Technology Zhengding Lu, Huazhong University of Science and Technology
9:15 - 9:45	**Risk-based Access Control Systems Built on Fuzzy Inferences** Qun Ni, Purdue University Elisa Bertino, Purdue University Jorge Lobo, IBM T. J. Watson Research Center
9:45 - 10:15	**Attribute Based Data Sharing with Attribute Revocation** Shucheng Yu, Worcester Polytechnic Institute Cong Wang, Illinois Institute of Technology Kui Ren, Illinois Institute of Technology Wenjing Lou, Worcester Polytechnic Institute
10:15 – 10:35	**Coffee-break**
Session 8: Systems Security - II **Session Chair: Engin Kirda**	
10:35 – 11:05	**binOb+: A Framework for Potent and Stealthy Binary Obfuscation** **Byoungyoung Lee, POSTECH** Yuna Kim, POSTECH Jong KIM, POSTECH
11:05 – 11:35	**Secure Provenance: The Essential of Bread and Buffer of Data Forensics in Cloud Computing** Rongxing Lu, University of Waterloo Xiaodong Lin, University of Ontario Institute of Technology Xiaohui Liang, University of Waterloo Xuemin (Sherman) Shen, University of Waterloo

11:35 – 12:05	**RunTest: Assuring Integrity of Dataflow Processing in Cloud Computing Infrastructures** Juan Du, Wei Wei, Xiaohui Gu, Ting Yu North Carolina State University
12:05 – 13:30	**Lunch**
Session 9: Short Papers – I Session Chair: Sencun Zhu	
13:30 – 13:50	**K-anonymous Association Rule Hiding** Zutao Zhu, Wenliang Du Syracuse University
13:50 – 14:10	**Controlling Data Disclosure in Computational PIR Protocols** Ning Shang, Gabriel Ghinita, Yongbin Zhou, Elisa Bertino Purdue University
14:10 – 14:30	**Cryptographic Role-based Security Mechanisms based on Role-Key Hierarchy** Yan Zhu, Arizona State University Gail-Joon Ahn, Arizona State University Hongxin Hu, Arizona State University Huaixi Wang, Peking University
14:30 – 14:50	**PriMa: An Effective Privacy Protection Mechanism for Social Networks** Anna Squicciarini, The Pennsylvania State University Federica Paci, University of Trento Smitha Sundareswaran, The Pennsylvania State University
14:50 – 15:10	**Oblivious Enforcement of Hidden Information Release Policies** Brian Wongchaowart, Adam Lee University of Pittsburgh
15:10 – 15:30	**Coffee-break**
Session 10: Short Papers – II Session Chair: Cliff Zou	
15:30 – 15:50	**Apex: Extending Android Permission Model and Enforcement with User-defined Runtime Constraints** Mohammad Nauman, Institute of Management Sciences, Pakistan Sohail Khan, Institute of Management Sciences, Pakistan Masoom Alam, Austria Xinwen Zhang, Samsung Information Systems America

15:50 – 16:10	**A Hotspot-based Protocol for Attack Traceback in Mobile Ad Hoc Networks** Hungyuan Hsu, Penn State University Sencun Zhu, Penn State University Ali Hurson, Missouri University of Science and Technology
16:10 – 16:30	**Practical ID-based Encryption for Wireless Sensor Network** Cheng-Kang Chu, Singapore Management University Joseph K. Liu, Institute for Infocomm Research, Singapore Jianying Zhou, Institute for Infocomm Research, Singapore Feng Bao, Institute for Infocomm Research, Singapore Robert H. Deng, Singapore Management University
16:30 – 16:50	**A Game Theoretic Model for Digital Identity and Trust in Online Communities** Tansu Alpcan, Deutsche Telekom Laboratories Cengiz Orencik, Sabanci University Albert Levi, Sabanci University Erkay Savas, Sabanci University
16:50 – 17:10	**Scene Tagging: Image-Based CAPTCHA Using Image Composition and Object Relationships** Peter Matthews, Cliff Zou University of Central Florida
17:30 - 19:00	**Dinner**
End of the conference	

出席 2010 International Dependable Systems and Networks 會議與參訪美國 Purdue University 報告

出國人員姓名/服務機關/單位/職稱/電話
吳育松/國立交通大學/資工系/助理教授/0975225901

出國期間：99/6/23-99/7/7

出國地區：美國/芝加哥、印第安那州西拉法葉市

報告日期：99/6/23-99/7/7

內容摘要：

本次出國的主要目的是出席於美國芝加哥所舉辦的第 40 屆 International Conference on Dependable Systems and Networks (DSN)。該會議囊闊了系統可靠度、性能表現、安全性等各個層面的相關 workshop、tutorial、以及最新的研究成果發表。該會議與本人目前所正執行之對於分散是系統環境中零時攻擊的反制研究以及所參與的 TWISC 相關研究計畫有非常高的相關性。出席該會議具有獲取新知、參考國外相關研究、自我檢討目前計畫執行進程等功效。

在會議結束後，我順道南下位於芝加哥南部約一百英里遠的印第安那西拉法葉市參訪 Purdue University。在 Purdue 我給了一個 talk，並與 ECE Department 的 Prof. Saurabh Bagchi 及其學生進行短暫的晤談，並尋求未來可能的相關研究合作之可能性。

壹、 參訪過程紀要

一、 出席 2010 DSN Conference 經過

DSN (International Conference on Dependable Systems and Networks)為系統可靠性的旗艦級會議。今年為第 40 屆，於美國芝加哥舉辦。主辦單位為美國密西跟大學安那堡分校（General Chair 為 U of Michigan 資訊科學工程系 Farnam Jahanian 教授）。其中 Intrusion-Tolerant Systems Workshop 以及 Security 議題的 Tracks 跟本計畫具高度相關性。其餘的 Tracks 則著墨於系統相關的性能、可靠性等議題，亦與本計畫有一定程度的相關性。

會議的第一天我出席了 Workshop on Recent Advances in Intrusion-Tolerant Systems。該 workshop 一開始是由 Cornell CS 的 Robert L. Constable 教授所給的 keynote speech。題目是"Using Formal Methods to Build Systems that Survive Attacks"。另外之後的 session 中有 MIT 的 O. Patrick Kreidl 博士所給的講題 "Analysis of a Markov Decision Process Model for Intrusion Tolerance"，以及 Lockheed Martin 的 Melvin Greer 所給的講題 "Survivability and Information Assurance in the Cloud" 這三個部分正好囊闊了從系統設計面、系統運作面、以及展望未來雲端環境中面對潛在攻擊的因應之道，與研究方向。我覺得受益方常良多。

第二天會議由 VeriSign 的研發副董 Danny McPherson 所給的 keynote speech "Availability in the Face of Evolving Internet Threats" 所展開。VeriSign 掌控全球主要的 DNS root server，而他的演講側重在透過 ATLAS 全球網路監控系統對於 distributed denial-of-service attack 的觀測以及相關見解。第二天我後半段主要是出席 Fast Abstracts Session，聽取一些最新的初步研究成果。比如說 Michigan 大學 Kang G. Shin 教授研究群的"How to Construct a Mobile Botnet"、伊利諾大學 Ravi K. Iyer 教授研究群的 "Analysis of Security Data from a Large Computing Organization"、伊利諾大學 William H. Sanders 教授研究群的 "Characterizing the Behavior of Cyber Adversaries: The Means, Motive, and Opportunity of Cyber Attacks" 等研究。

第三天的會議由分散式計算大師 MIT Nancy Lynch 教授所給的 keynote speech "Distributed Computing Theory Through the Ages" 所展開。這個演講一開始論及了分散式計算中的一些古典問題 (atomicity、mutual exclusion...)，基本上有點類似 Nancy Lynch 教授的那本 Distributed Algorithms 裡面的重點提要，當然由原作者親自講授的感覺就是不一樣。Lynch 教授的演講後來有提一些他比較近期的一些 research work。由於這部分跟我專長有些距離，部分精要之處比較無法完全領會。之後我聽了 EPFL 的一篇關於程式驗證的論文報告 "iProve: A Scalable Technique for Consumer-Verifiable Software Guarantees"。由於系統弱點(vulnerabilities)很大一部分均是由於程式內部的某些 property 沒有被滿足（比如說緩衝區溢位）所造成的，也因此如何能對一個真實世

界中的複雜程式去做驗證也就是欲解決系統弱點所需要面對的一個很重要的研究課題。第三天後來的時間我都在聽 fast abstracts，這天的 fast abstracts 較少跟本計畫研究課題有直接相關的題目，所以純粹是以增廣見聞，瞭解一下其他研究題目最近的一些進展狀況這樣。

第四天的會議有比較多跟 Security 相關的論文發表，比如說 Purdue 大學 Dongyan Xu 教授研究群的發表 "Reuse-Oriented Camouflaging Trojan: Vulnerability Detection and Attack Construction"、密西跟大學 Kang G. Shin 教授研究群的發表 " "Detection of Botnets Using Combined Host- and Network-Level Information" 以及 CMU 大學 Virgil D. Gligor 教授研究群的發表 "Dependable Connection Setup for Network Capabilities" 等。雖然這些研究根本計畫的入侵反制課題沒有直接關係，但對於激發新的研究方法還是很有幫助的。

二、 Purdue 大學參訪

此次 DSN 會議正巧是在芝加哥舉辦 。芝加哥距離 Purdue University 不過一百多英里遠，開車兩小時多便可到達。我正好把握此一難得機會南下 Purdue University 拜訪我的指導教授 Prof. Saurabh Bagchi，並在 ECE Department 給一個關於我目前在入侵反制上研究的一個 talk。此行目的之一是見見老同學，Purdue 的一些師長，維持聯繫關係，另一方面是尋求未來研究上可能的一些合作。

貳、 心得與結論

總地來說，有機會出席國際會議對於增廣見聞、見見老朋友、認識新朋友是非常有幫助的。尤其我國近年欲推動大學邁向國際一流，其中很重要的一環便是要讓國外一流大學的師生們能看到我們的學校、知道我們的學校也是有在做不錯的 research、甚至可以在國際重要會議上與他們相爭鋒。另外如果經費許可，我是覺得亦能多鼓勵學生出國參加這些重要會議，親自見識一下國外一流大學的學生、老師、以及人家的研究成果。我相信這比透過我們老師所傳遞給他們的二手資訊會對他們有更直接、更深遠的影響。

這次出席 DSN 會議所得到的訊息是入侵反制仍是一個很重要的研究課題。一方面對於驗證程式的安全性，去除弱點等問題就現實生活中的複雜系統仍尚未有完美的解決方案。二方面不斷推成出新的攻擊型態更彰顯了入侵反制機制之存在必要性。在我所原本設想的反制動作中，多半是以阻擋攻擊進程為首要目標。這次參與 DSN 讓我想起了傳統容錯計算上的 checkpoint 和 recovery 等技巧或也可用為反制動作的選項之一。另外整體而言，對於會議中 VeriSign、Lockheed Martin 等業界講者所提供的一些業界在網路攻擊、雲端運算上的看法，對於檢討本計畫之入侵反制系統設計架構在

實務面上的合理性亦有相當程度的助益。

DSN 明年將於香港舉辦，另外像 SIGCOMM 今年在印度舉辦、INFOCOM 明年將在中國上海辦。感覺起來這些大學發展原本落後台灣的國家近幾年在國際會議上的著力程度似乎相對比台灣都還來得深。當然不可否認的是中國、印度有其綜合國力的優勢存在，這些重要會議在那邊舉辦並不代表中、印兩國在相關領域的學術研究已經具有國際一流水準。但以客觀角度來說，人家把握了這些與國際頂尖學者互動的機會，假以時日他們在這些領域的發展肯定會有很大的進步。在這個問題上，我們必須要更認真地去看待，更積極地去應對。

出席國際學術會議心得報告

計畫編號	99-2219-E-009-013-
出國人員姓名 服務機關及職稱	趙禧綠 交通大學資工系助理教授
會議時間地點	2010/9/26~2010/9/29, Istanbul, Turkey
會議名稱	The 21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2010**)**
發表論文題目	Analytical Modeling of Timeout for Contention-Based Bandwidth Request Mechanism in IEEE 802.16 WiMAX Networks

一、參加會議經過

此次國際研討會共計四天，報告人的論文屬 track 2 的 MAC and cross layer design，technical session 則是排在九月二十八日上午。該篇論文的主題是針對頻譜設定在 60GHz 的 IEEE 802.15.3c 之排程演算法。由於 PIMRC 是通訊網路領域主要的國際研討會之一，再加上伊斯坦堡是個旅遊勝地，與會人數很多。

二、與會心得

依據報告人研究興趣，在此次研討會主要聆聽的研究議題有：

(1) Cognitive networks（感知網路）：這個範圍的研究在近期 IEEE 國際研討會議非常熱門，PIMRC 亦安排一場 panel discussion。在這場 panel discussion，他們提出感知無線電網路應有一大型資料庫，供 secondary users 以及 cognitive radio access points (CR APs) 查詢附近區域 primary users 或 primary base stations (BSs) / access points (APs) 的位置以及發射功率，進一步由 CR APs 分配頻道以及頻道可使用時間給 secondary users，避免對 primary users 造成干擾，同時減輕 secondary users 所需要執行的運算。此大型資料庫的需求恰與目前正紅的雲端運算相呼應。利用雲端伺服器所提供的強大運算功能與地域性的資訊查詢，將實現感知無線電網路的進程往前推一大步。由於報告者目前參與一項國科會的橋接計畫，該計畫內容正是實作感知無線電網路。藉由聆聽此 panel discussion，對我們的實作開發助益很大。

(2) Radio Resource Management(RRM)以及 scheduling：偏向跨層的最優化設計(Cross-Layer Optimization)。

(3) LTE：在此次會議中，大多數此範圍的研究仍然是以 OFDM 或者 OFDMA 技術為主，比如 OFDM 所使用通道估測及 Joint CFO and CE 的設計等等。RRM 以及 scheduling 的文章不多見。

(4) Cooperative/relay communications：cooperative communication 這幾年來廣受注意，相關的

論文亦很多。多數論文均以 PHY 的角度來決定 relay 的選擇與數量。

藉由在國際間分享研究與國內外學者交流，並聽取世界各地的研究報告以獲取新知，可以說是非常有收穫的一次行程。報告之論文全文收錄於後。

Performance Enhancement of Contention-Based Bandwidth Request Mechanism in IEEE 802.16 WiMAX Networks

Shih-Fan Chou[1], Jen-Hsi Liu[1], Hsi-Lu Chao[1], Tzu-Chi Guo[1], Chia-Lung Liu[2], and Feng-Jie Tsai[2]
[1]Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan
[2]Information & Communications Research Labs, Industrial Technology Research Institute, Hsinchu, Taiwan

***Abstract*—The IEEE 802.16 standard is a promising technology for 4G mobile networks. Though supporting versatile service classes, best effort (BE) service class is expected to dominate WiMAX networks, due to operational simplicity. One of bandwidth request mechanisms that subscriber stations (SS) can utilize to issue bandwidth requests (BW-REQ) for BE connections is contention-based random access. An SS starts a timer *T*16 when transmitting a BW-REQ. If getting a grant before timer expiration, the SS transmits data packets at the allocated time slots; otherwise it performs truncated binary exponential backoff process for BW-REQ retransmission. The default value of *T*16 is one frame time. However, *T*16 impacts on contention and request collision significantly. In the paper, we develop an analytical model for *T*16 timer setting. Besides, we derive analytical expressions for the average number of tries per BW-REQ and the average packet delay. We compare the theoretical results of fixed and adjustable timers. The results show that adjusting timer reduces both the number of collision and the average packet delay.**

***Keywords*—WiMAX, best effort, bandwidth request, contention**

I. INTRODUCTION

IEEE 802.16 protocol has been standardized for metropolitan broadband wireless access (BWA) systems, and it is a viable technology to be used for connecting local area networks (e.g., IEEE 802.11-bassed WLAN) to the Internet, due to the characteristics of high transmission rate and flexible quality-of-service (QoS). [1]. The IEEE 802.16 MAC layer supports a mandatory PMP architecture, which consists of a base station (BS) serving a number of subscriber stations (SS). There are two types of duplex scheme, i.e. FDD (Frequency Division Duplexing) and TDD (Time Division Duplexing). In this paper, we focus on TDD mode. TDD mode requires only one channel for transmitting downlink (DL) and uplink (UL) sub-frames at two distinct time slots. Moreover, the DL and UL ratio can be adjusted dynamically.

In order to support multimedia services, the IEEE 802.16 standard [1][2] defines five service classes to accommodate versatile QoS-demand applications (such as VoIP, and MPEG video). These service classes are unsolicited grant service (UGS), extended real-time polling service (ertPS), real-time polling service (rtPS), non-real-time polling service (nrtPS), and best-effort (BE) service. Due to the fact that "*how to perform resource reservation to meet applications' QoS demands*" is not within the scope of the standard, it is possible that even VoIP flows would be treated as BE service class. Therefore, in this paper, we focus on the BE service class.

A BS has the full control of slot allocation. To avoid collisions, SSs should get permission before their data transmission. According to the IEEE 802.16 standard, such an exclusive channel access is achieved by requiring SSs to send bandwidth requests first. For this purpose, the IEEE 802.16 standard specifies three bandwidth request mechanisms: contention-based random access and contention free-based polling are two suggested approaches, and piggyback mechanism is optional. These three request mechanisms are applicable to BE service class, and our focus is on the contention-based approach.

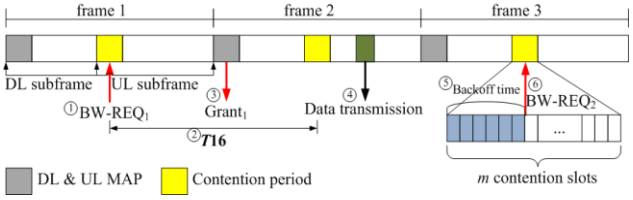


Figure 1 Illustration of contention-based bandwidth request mechanism

The random access contention resolution adopted in WiMAX is based on a truncated binary exponential backoff scheme without carrier sensing. Before each attempt of BW-REQ transmission, an SS randomly selects a backoff timer from [0, W_i-1], where W_i is the contention window size of the i^{th} retry. The backoff time indicates the number of slots that the SS should wait before its BW-REQ transmission. For the first attempt, the contention window size is the minimum value W_{min}; the window size after the i^{th} retry is 2^iW_{min}. The window size keeps doubling till it reaches the maximum value $W_{max}=2^rW_{min}$, where r is the maximum backoff stage. For a BW-REQ, an SS can try at most 16 times. Both W_{min} and W_{max} are defined by BSs, while the WiMAX standard does not provide optimal/suggested values.

When using contention, no explicit acknowledgment (ACK) frame is sent back to indicate whether a bandwidth request (BW-REQ) message is successfully transmitted or not. Instead, a timeout *T*16 is set to determine whether requiring retransmission or not. The default setting of *T*16 is one frame time. An illustrative example of contention-based bandwidth request mechanism is shown in Fig. 1. BW-REQs are sent in the contention period of a frame (Fig. 1-①), and *T*16 is set simultaneously (Fig. 1-②). If a grant is given within *T*16 timeout (Fig. 1-③), the SS stops contention resolution and use the allocated bandwidth for uplink transmission (Fig. 1-④). Otherwise the SS believes that its BW-REQ was corrupted, and then restarts a contention resolution process. The SS randomly selects a backoff timer (Fig. 1-⑤), and counts down that timer. When the timer is zero, the SS retransmits the BW-REQ (Fig. 1-⑥), and same processes repeat.

Recent research of request mechanisms include [3][4][5][6][7]. In [3], the authors conclude that the best size of contention period is (2*N*-1), and *N* is the number of SSs. However, upon heavy traffic load, the number of data slots of an UL subframe decrease as *N* increases, and a BS may not issue grants to all received BW-REQs. For those refused and collided BW-REQs, the SSs will run the contention resolution mechanism again, and thus delay time increases.

In [4], the authors introduce a new algorithm, called Multi-FS-ALOHA, which divides the contention period into two parts. The first is used by SSs to issue first-try BW-REQs, while the second part is dedicated for retransmission of BW-REQ messages. These two parts are dynamically fixed on a frame by frame basis. The drawback of [4] is that it requires a dedicated feedback channel for operation.

A modified contention resolution process is proposed in [5] to improve the system performance. Its main idea is assigning different initial window sizes to different scheduling classes. However, based on the presented simulation results, this algorithm performs similarly to the contention mechanism defined in the standard.

An analytical model of the contention-based bandwidth request mechanism, defined in [1], in a saturated WiMAX network was developed in [6][7]. [8] took the number of contending SSs into account to determine the optimal window size.

Briefly summarizing the introduced literature, performance of the contention-based request mechanism can be improved by (1) reducing the collision probability, (2) dynamically adjusting the contention period according to the number of SSs, (3) assigning different minimum contention window sizes to service classes, and (4) integrating/implementing both piggyback and contention mechanisms. However, these solutions may incur the problem of compatibility.

Two possible reasons that a BW-REQ cannot be granted and need retransmission are: collision, and insufficient UL data slots. The former is due to multiple BW-REQs are transmitted at the same contention slot; the latter is due to the UL data slots cannot accommodate the total demand of received BW-REQs. However, SSs cannot identify the exact reason why they do not get resource grants, and just perform contention resolution procedure. Upon heavy traffic load, more contentions in a fixed contention period results in more collisions and worse system performance. Thus our idea is to dynamically adjust *T*16 timeout. BW-REQs may wait longer before perform contention resolution process. The objective of this paper is to develop an analytical mode for *T*16 derivation.

The rest of this paper is organized as follows. The analytical model of timeout derivation is introduced in Section II. Numerical results are presented and discussed in Section III. This paper is concluded in Section IV.

II. Analytical Model

In this section, we explain the developed analytical model. Since we focus on the retransmission caused by insufficient UL bandwidth, $T16_{ib}$ is used to represent the desired timeout. In addition, we analyze the average tries of a BW-REQ to get a resource grant, and the average packet delay.

In this analytical model, there are N BE connections, and their packet arrival is in Poisson distribution with λ_{packet}. t_{frame} and d are the frame time duration and the number of data slots of a UL subframe. r_{be} is the percentage of UL data slots which are allocated to BE service class.

A. $T16_{ib}$

Let n be the number of frames that a successfully transmitted BW-REQ can be preserved by a BS at most. Therefore,

$$T16_{ib} \geq (1+n)t_{frame} \tag{1}$$

To derive a proper $T16_{ib}$ is to determine an adequate *n* value.

In our analysis, we assume there are *m* slots in a contention period, and each slot can accommodate one BW-REQ message.

Considering a BW-REQ, the probabilities of request collision and insufficient UL bandwidth of its i^{th} retransmission (i.e., the $(i+1)^{th}$ try) are denoted as $p_c^{(i)}$ and $p_{ib}^{(i)}$ respectively. Since unsuccessful BW-REQs are only due to collisions in the modified mechanism, the probability of the i^{th} contention for an unsuccessful BW-REQ (denoted as $p_{modified}^{(i)}$) is

$$p_{modified}^{(i)} = p_c^{(i)} \tag{2}$$

According to [9], the probability that an SS attempts to transmit a BW-REQ at a contention slot for the i^{th} retry $\tau^{(i)}$ is

$$\tau^{(i)} = \frac{2}{W_i + 1} \qquad 0 \leq i \leq R-1, \tag{3}$$

where *R* is the maximum number of tries.

Given the number of transmitted BW-REQs in frame $\left\lceil \frac{W_i-1}{m} \right\rceil$, denoted as $N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}$, suppose the observed BW-REQ is retransmitted at the last contention slot in frame $\left\lceil \frac{W_i-1}{m} \right\rceil$, $p_c^{(i)}$ is

$$p_c^{(i)} = 1 - \left[1-\tau^{(i)}\right]^{N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}-1}, \quad 0 \leq i \leq R-1 \tag{4}$$

Furthermore, for $0 \leq i \leq R-1$,

$$p_{ib}{}^{(i)} = \frac{N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}\left(1-p_c^{(i)}\right) - N_{request\_served}}{N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}\left(1-p_c^{(i)}\right)} \tag{5}$$

where $N_{request\_served}$ is the number of served requests in a superframe.

We then derive the number of transmitted BW-REQs in a specific frame, say frame *j*. Connections either incurring BW-REQ collision or having packet arrivals in frame (*j*-1) will send their BW-REQs in frame *j*. We assume all BE connections have queued packets initially, i.e., $N^{(1)} = N$. Thus for frame 2,

$$N^{(2)} = N^{(1)}(1-P_0)\left(1-P_c{}^{(0)}\right)\left(1-P_{ib}{}^{(0)}\right) + N^{(1)}P_c{}^{(0)}\frac{m}{W_{min}} \tag{6}$$

where P_0 is the probability that an SS has no packet arrivals in t_{frame} time, and $P_0 = 1 - \mathrm{e}^{-(\lambda_{packet})(t_{frame})}$. Through iterative derivation, for $j \geq 1$

$$N^{(j+1)} = N^{(j)}(1-P_0)\left(1-p_c{}^{\left(log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor\right)}\right)\left(1-p_{ib}{}^{\left(log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor\right)}\right) + N^{(j)}p_c{}^{\left(log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor\right)}\frac{m}{W_{log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor}} \tag{7}$$

In (7), we use the backoff stage to get the number of retransmitted requests occur at this frame and $\frac{m}{W_{\log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor}}$ is the probability that a collided request would transmit again in frame j.

On the other hand, the number of requests a BS can serve in a UL subframe is

$$N_{request\_served} = \left\lfloor \frac{dr_{be}}{\lambda_{packet} t_{frame}} \right\rfloor. \quad (8)$$

Thus considering the worst case, a successfully transmitted BW-REQ at frame j can be served at most after n frames, and n is

$$n = \left\lceil \frac{N^{(j)}(1-p_c^{(j)}) - N_{request\_served}}{N_{request\_served}} \right\rceil. \quad (9)$$

Substituting (4), (7), (8), and (9) into (1), we obtain a theoretical $T16_{ib}$.

B. Average Number of Tries

Again in the original contention-based bandwidth request mechanism, a BW-REQ is retransmitted when either the BW-REQ experiences a collision, or the BS has no sufficient UL bandwidth to give it a grant. Let X be the number of tries for a BW-REQ to get granted. Since a request can be sent at most R times, the average number of tries is

$$E[X]_{original} = \sum_{i=1}^{R} \left[i p_c^{(i)} + i(1-p_c^{(i)}) p_{ib}^{(i)} \right] \quad (10)$$

However, in the modified mechanism, the BW-REQ retransmission is only caused by collisions, thus the average number of tries is as listed in (11).

$$E[X]_{modified} = \sum_{i=1}^{R} i p_c^{(i)} \quad (11)$$

C. Packet Delay

We define the packet delay being the time duration from the first try of a BW-REQ to the time of successful data packet transmission. In the IEEE 802.16 standard, the frame structure of TDD mode includes a downlink subframe (Fig. 2 ①) and an uplink subframe. An uplink subframe consists of a contention period $t_{contention}$ (Fig. 2 ②) and a data interval t_{DA} (Fig. 2 ③). The time gap between two consecutive frames is called guard time t_{guard}(Fig. 2 ④). Let $t_{request}$ and t_{data}be the time of a contention slot and an uplink data slot respectively. Thus $t_{contention} = mt_{request}$, and $t_{DA} = dt_{data}$. Let $D^{(i)}$ indicate the packet delay that a BW-REQ is granted at its i^{th} retry. Note that i=0 means the BW-REQ gets grant at its first try. An example to calculate $D^{(i)}$ is shown in Fig. 2. U and V are the time durations from sending the first BW-REQ to the end of the contention period (t_u) and from the beginning of the uplink data interval (t_v) to the time that the first packet has been transmitted, respectively. Using i=0 as an example, the first possibility is that a first-try BW-REQ is successfully transmitted and gets served immediately, its packet delay is

$$D^{(0)} = U + Y^{(0)} + V, \quad (12)$$

where

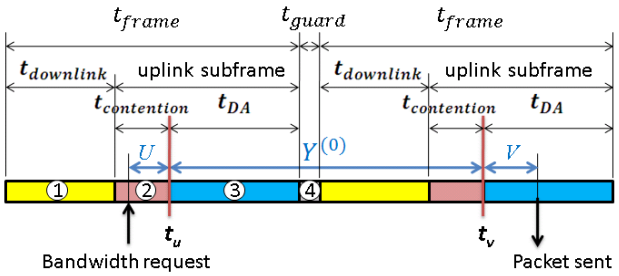


Figure 2 An illustrative example of packet delay calculation

$$\begin{cases} U = it_{request} & w.p.\ \frac{1}{m}, i = 1,2,\dots,m \\ V = it_{data} & w.p.\ \frac{1}{dr_{be}}, i = 1,2,\dots,dr_{be} \\ Y^{(0)} = t_{DA} + t_{guard} + t_{downlink} + t_{contention} \\ \quad = t_{frame} + t_{guard} = c \end{cases}$$

and *w.p.* stands for "with probability".

The second possibility is this first-try BW-REQ is successfully transmitted but preserved for later grant. In such a case, the packet delay is the same as (12) while with a different $Y^{(0)}$, and

$$Y^{(0)} = (1 + \tfrac{1}{2}\left\lceil \frac{T16_{ib}}{t_{frame}} \right\rceil)c.$$

$\frac{1}{2}\left\lceil \frac{T16_{ib}}{t_{frame}} \right\rceil$ is the waiting time in a frame for a preserved BW-REQ to get a grant, and it is uniformly distributed within $T16_{ib}$ time duration.

The last possibility is that this BW-REQ is collided with other requests, and thus the SS doubles the contention window size, randomly selects a backoff value, and retransmits this BW-REQ. If this 2nd try immediately gets a grant, the corresponding packet delay $D^{(1)}$ is

$$D^{(1)} = U + Y^{(1)} + V, \quad (13)$$

where $Y^{(1)}$ is the waiting time (and its unit is frame) between t_u and t_v and is given as

$$Y^{(1)} = c \sum_{i=0}^{1} K^{(i)} Y^{(0)}.$$

$K^{(i)}$ is the waiting time in a frame for packet transmission at the i^{th} contention. Since the SS uniformly selects its backoff counter from [0,W_i-1]. According to [10], the probability mass function of random variable $K^{(i)}$ is

$$K^{(i)} = \begin{cases} 1, & i = 0 \\ j, & w.p.\ \frac{m}{W_i}, \quad i \neq 0,\ j = 1,2,\dots,\left\lfloor \frac{W_i}{m} \right\rfloor - 1 \\ \left\lceil \frac{W_i}{m} \right\rceil, & w.p.\ 1 - \frac{(\left\lfloor \frac{W_i}{m} \right\rfloor - 1)m}{W_i}, i \neq 0 \end{cases} \quad (14)$$

If this 2nd-try BW-REQ is successfully transmitted while been preserved, it packet delay is

$$D^{(1)} = U + \left(K^{(0)} + K^{(1)} + \frac{1}{2}\left\lceil \frac{T16_{ib}}{t_{frame}} \right\rceil \right) c + V.$$

In general, for the i^{th} attempt, the average packet delay $D^{(i)}$ is

$$\begin{cases} \mathrm{E}\left[D^{(i)}\right] = E[U] + \mathrm{E}\left[Y^{(i)}\right] + E[V] \\ \mathrm{E}\left[Y^{(i)}\right] = c\sum_{j=0}^{i} \mathrm{E}\left[Z^{(j)}\right] \end{cases}, 0 \le i < R \quad (15)$$

where $Z^{(j)}$ is the waiting time in a frame for a j^{th}-retry BW-REQ and its mean is

$$\mathrm{E}\left[Z^{(j)}\right] = \begin{cases} 1, & j = 0 \\ p_c^{(j)}\mathrm{E}[K^{(j)}] + (1 - p_c^{(j)})p_{ib}^{(j)}\left(\frac{1}{2}\left\lceil\frac{T16_{ib}}{t_{frame}}\right\rceil\right), & j \ge 1 \end{cases} \quad (16)$$

Since

$$\mathrm{E}\left[K^{(j)}\right] = \begin{cases} 1, & j = 0 \\ \left\lceil\frac{W_j}{m}\right\rceil - \left\lceil\frac{W_j}{m}\right\rceil\left(\left\lceil\frac{W_j}{m}\right\rceil - 1\right)\frac{m}{2^{j+1}W_{min}}, & j = 1, \dots, r-1 \\ \left\lceil\frac{W_j}{m}\right\rceil - \left\lceil\frac{W_j}{m}\right\rceil\left(\left\lceil\frac{W_j}{m}\right\rceil - 1\right)\frac{m}{2^{r+1}W_{min}}, & j = r, \dots, R-1 \end{cases} \quad (17)$$

and

$$\begin{cases} E[U] = \dfrac{(m+1)t_{request}}{2} \\ E[V] = \dfrac{(dr_{be}+1)t_{data}}{2} \end{cases} \quad (18)$$

we obtain $\mathrm{E}\left[D^{(i)}\right]$ by substituting (16), (17) and (18) into (15). Further, the mean total packet delay of the modified mechanism $\mathrm{E}[D]_{\text{modified}}$ is

$$\mathrm{E}[D]_{\text{modified}} = (1 - p_{modified}^{(R)})\sum_{i=0}^{R-1}\left\{\left(\prod_{k=0}^{i} p_{modified}^{(k)}\right)\mathrm{E}\left[D^{(i)}\right]\right\}. \quad (19)$$

For comparison purpose, we also derive the mean total packet delay of the original mechanism, i.e., $\mathrm{E}[D]_{\text{original}}$. The expression of $\mathrm{E}[D]_{\text{original}}$ is same as (19), while the probability for a BW-REQ to fail at its i^{th} contention is $p_{original}^{(i)} = 1 - \left(1 - p_c{}^{(i)}\right)\left(1 - p_{ib}{}^{(i)}\right)$.

III. Numerical Results

In this section, we develop a simulation program to validate the analytical model, and compare and discuss the performance of the original and modified contention request mechanisms. Parameter settings are listed in Table 1.

Fig. 3 shows the $T16_{ib}$ settings upon various numbers of BW-REQs. As the number of requests increases, $T16_{ib}$ also linearly increases. Besides, upon a specific N value, as λ_{packet} increases, $T16_{ib}$ increases, too. The reason is, in average, the number of required time slots increases, and thus a BS can only serves few requests in a UL subframe. Consequently successfully transmitted BW-REQs will be preserved longer before getting grants.

In the following experiment, we set λ_{packet} be 3, and $T16_{ib}$ setting is based on the results in Fig. 3. We investigated the performance of p_c and p_{ib}, as shown in Fig. 4. It is intuitive that both p_c and p_{ib} increase as the number of requests increases. Moreover, we observed that when properly setting W_{min} (e.g., W_{min}=64), p_c is significantly reduced to 1.2×10^{-3}, and p_{ib} maintains at the smallest value among all.

The performance of average number of tries is in Fig. 5 (a) and (b). If a BW-REQ is transmitted successfully to the BS, it may be preserved for future grant. In such a case, the SS does not need to retransmit this request and thus the number of tries per request reduces, compared with the original contention request mechanism. Note that the average number of tries for both original and modified mechanisms of $W_{min} = 8$ is more than that of $W_{min} = 16$. The reason is that a small contention window size results in a high collision probability.

Table 1. Parameter settings

Parameter	Value
W_{min}	8/16/32/64
Maximum backoff stage, r	10
Maximum number of tries, R	16
Number of request slots, m	10
Number of data slots per uplink subframe, d	20
Ratio of data slots for BE, r_{be}	0.5
Time of a request slot, $t_{request}$	0.024 ms (6 slots)
Time for a uplink data slot, t_{data}	0.0376 ms (94 slots)
Guard time duration, t_{guard}	0.004 ms (1 slot)
Frame duration, t_{frame}	1 ms
Packet arrival rate, λ_{packet}	3/5/7

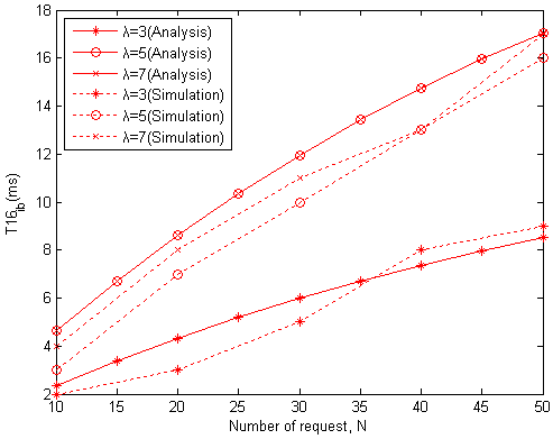


Figure 3. $T16_{ib}$ settings vs. the number of requests N upon various packet arrival rates

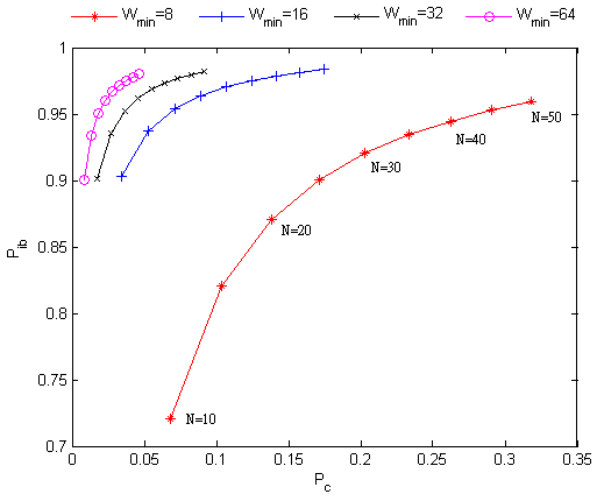
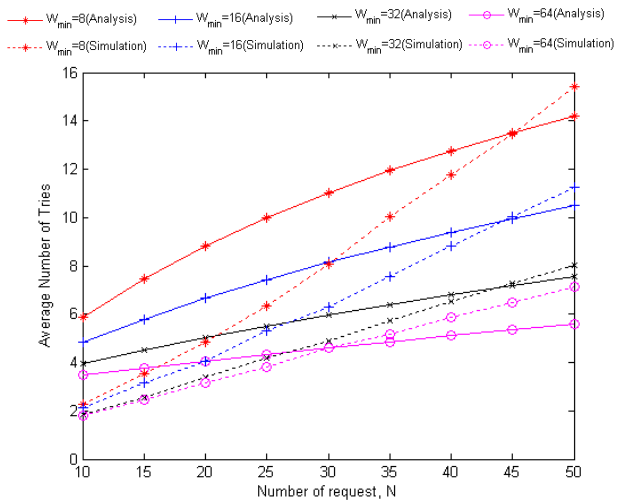
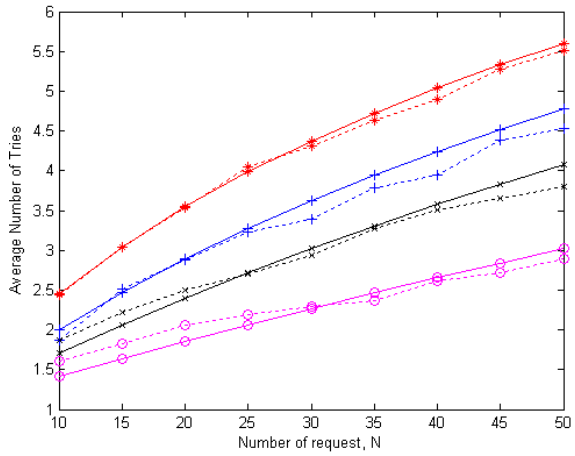


Figure 4 Probabilities of collision and insufficient bandwidth upon various W_{min} settings

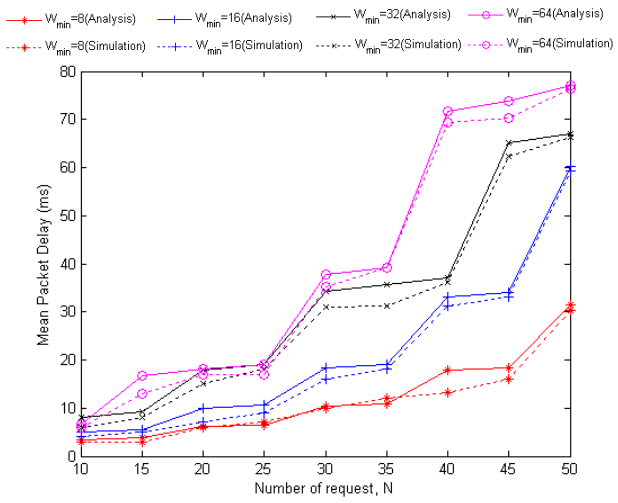


(a) Original

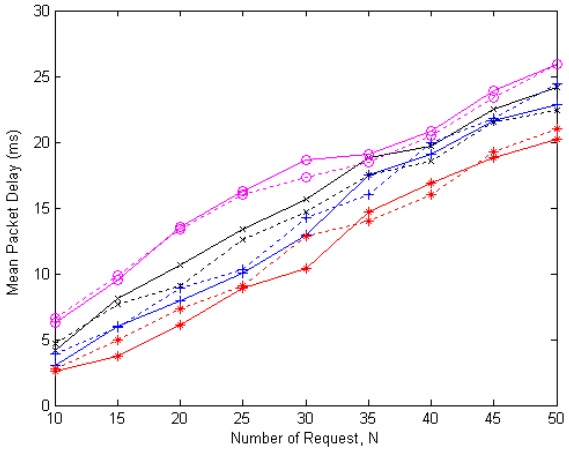


(b) Modified

Figure 5 The performance of average number of tries of the two contention-based bandwidth request mechanisms



(a) Original



(b) Modified

Figure 6 The performance of mean packet delay of the two contention-based bandwidth request mechanisms

Fig. 6 depicts the mean packet delay of both request mechanisms as the number of requests increases from 10 to 50, upon various W_{min} settings. For both mechanisms, when given a W_{min}, a large N value results in long delay due to high collision probability and more retries. On the other hand, for a specific N value, the window size of each backoff stage increases, and the average packet delay increases accordingly. The reason is that when collision occurs, the range of the backoff value becomes larger (0 to W_i -1). An SS is delayed much more frames when using a larger backoff value. The mean packet delay of the modified mechanism is significantly smaller than that of the original mechanism. The reason is that the modified request mechanism preserves successfully transmitted BW-REQs at most (n+1) frames without performing binary exponential backoff process and thus the contention window size is intact. Therefore, it has rather small delay, compared to the original mechanism.

IV. Conclusion

In this paper, focused on BE service class and contention-based request mechanism, we developed an analytical model to derive a theoretical $T16_{ib}$ timeout. Dissimilar to the original contention-based request mechanism that all unsuccessfully transmitted BW-REQs must perform the truncated binary exponential backoff process, the modified mechanism achieves reduction of collisions and tries by adjusts timeout properly for those successfully transmitted BW-REQs while cannot get grants in the next frame. The modeled timeout is a function of (1) number of BE connections, (2) traffic load, (3) retransmission, (4) collision probability, and (5) bandwidth insufficient probability. Numerical results showed that a suitable timeout does reduce the number of tries, and the average packet delay. Since the failure probability of transmitting BW-REQ decreases and the probability of a BW-REQ being hold increases, the number of tries is reduced. In addition, the range of the backoff value grows exponentially when retry occurs. An SS does not need to wait for the backoff counter counting down to zero for BW-REQ transmission when the BW-REQ is hold by the BS. The average packet delay is lower accordingly. From the numeral and simulation results, when the size of initial contention window approaches the number of contention slots, we could get better average packet delay performance. In our case, we suggest that the contention window size is 8.

Acknowledgment

This work was supported in part by NCTU-MTK Research Center under grant 99Q583, in part by National Science Council under grant NSC 99-2219-E-009-013- and in part by Ministry of Economic Affairs and Industrial Technology Research Institute under grant 99-EC-17-A-03-01-0620.

REFERENCES

[1] IEEE Std. 802.16-2004, "Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems".

[2] IEEE 802.16e-2005, IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, 2006.

[3] Taleb T., Fernandez J.C., Hashimoto K., Nemoto Y., Kato N., "A Bandwidth Aggregation-aware QoS Negotiation Mechanism for Next-Generation Wireless Networks", *IEEE Global Telecommunications Conference*, November 2007, pp.1912-1916.

[4] Lidong Lin, Bo Han and Lizhuo Zhang, "Performance Improvement using Dynamic Contention Window Adjustment for Initial Ranging in IEEE 802.16 P2MP Networks", IEEE Wireless Communications & Networking Conference (WCNC), 2007, pp.11-15.

[5] Jianhua He, Ken Guild, Kun Yang, and Hsiao-Hwa Chen, "Modeling Contention Based Bandwidth Request Scheme for IEEE 802.16 Networks", *IEEE Communications Letters*, Volume 11, August 2007 pp.689-700.

[6] Vinel A., Ying Zhang, Qiang Ni, Lyakhov A., "Efficient Request Mechanism Usage in IEEE 802.16", *Global Telecommunications Conference*, December 2006, pp.1-5.

[7] Wenyan Lu, Weijia Jia, Wenfeng Du, Lizhuo Zhang, "Performance analysis of the contention resolution scheme in IEEE 802.16". Journal of Software, Volume 18, No. 9, pp.2259-2270, 2007.

[8] Sung-Min Oh, Jae-Hyun Kim, "The Analysis of the Optimal Contention Period for Broadband Wireless Access Network", *Pervasive Computing and Communications Workshops*, March 2005, pp.215-219..

[9] Giuseppe Bianchi, Luigi Fratta, and Matteo Oliveri, "Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs," in Proc. IEEE PIMRC, Taipei, Taiwan, Sept. 1996, pp. 392–396.

[10] Hai L. Vu, Sammy Chan, and Lachlan L. H. Andrew, "Performance analysis of Best-Effort Service in Saturated IEEE 802.16 Networks," *Proc. IEEE Vehicular Technology*, Volume 59, No. 1, January 2010, pp.460-472.

[11] Q. Ni, L. Hu. "An Unsaturated Model for Request Mechanisms in WiMAX". IEEE Communications Letters, Vol. 14, No. 1, Jan 2010, pp. 45-47.

[12] Q. Ni, A. Vinel, Y. Xiao, A. Turlikov, T. Jiang. "Investigation of Bandwidth Request Mechanisms under Point-to-Multipoint Mode of WiMAX Networks". IEEE Communications Magazine, Vol. 45, No. 5, May 2007, pp. 132-138.

「ACM Symposium on Information, Computer and Communications Security（ASIACCS）國際學術會議」出國報告書

報告人： 交通大學謝續平

日期：2010 年 04 月 30 日

一、 出國目的

ACM Symposium on Information, Computer and Communications Security （ASIACCS）為 ACM Special Interest Group on Security, Audit, and Control（SIGSAC）所贊助與主辦的兩大頂尖會議之一，接受率約為 10%一頂尖會議為 ACM Conference on Computer and Communications Security（CCS）， 接受率也約為 10%。本人擔任 ACM ASIACCS steering committee chair, 負責推動該會議，並且召集 steering committee meeting，遴選每年執行單位。此次參加該國際學術會議，並審查 2011 年主辦單位進度，與 2012 年主辦國家與單位，並討論會議場地與籌辦流程。

二、 行程

參加 ACM Symposium on Information, Computer and Communications Security 擔任 Steering Committee Chair。

4/9 Taipei – Beijing

4/10 受 ACM ASIACCS steering committee member 以及 Mozilla Online Ltd. CEO Li Gong 博士邀請訪問 Mozilla Online Ltd. (該公司為開發 Firefox web browser 的公司，Firefox 瀏覽器為全球最受歡迎的瀏覽器之一)

4/12 受大會以及 Chinese Academy of Sciences, Deputy Director Jiwu Jing 邀請訪問中科院並演講 “Cloud Computing Security”

4/13-16 ACM Symposium on Information, Computer and Communications Security 會議

4/17-18 ASIACCS steering committee 會議擔任主席

4/19 返台

三、 出國人員：

謝續平現任交通大學資訊工程系教授暨 TWISC@NCTU 主任，曾任交通大學資訊工程系系主任、交通大學計算機與網路中心主任、中華民國資訊安全學會理事長，現在擔任 IEEE Tran. On Dependable and Secure Computing、IEEE Trans. On Reliability、Journal of Computer Security 副編輯、IEEE RS Newsletter 總編輯。由於現在擔任 ACM Symposium on Information, Computer and Communications Security （ASIACCS） 推動委員會主席（steering committee chair)。負責遴選籌辦國家單位，並督導籌辦進度。

四、 工作內容摘要

由於擔任 ACM Special Interest Group on Security, Audit, and Control (SIGSAC) 的推動委員會委員（Steering Committee member)，並且擔任 ACM Symposium on Information, Computer and

Communications Security （ASIACCS） 推動委員會主席（steering committee chair)，被 ACM 賦予：

a）觀察本年度會議執行成果，

b）審查下年度執行單位籌備現況，

c）並甄選兩年後會議執行單位。

本次出國為了推動 SIGSAC 的未來發展，赴大陸北京友誼賓館，參加本年度會議，觀察 ASIACCS 本年度會議主辦單位美國賓州州立大學、瑞士 ETH、北京中國科學研究院成果，並審查 2011 會議舉辦單位香港大學、香港城市大學籌備進度，與 2012 年申請舉辦單位上海交通大學等單位的提案。

此次大會由北京中國科學研究院 Dengguo Feng 主任擔任大會主席，David Basin(basin@inf.ethz.ch, ETH Zurich, Switzerland)
Peng Liu(pliu@ist.psu.edu, Pennsylvania State University, USA)
擔任議程主席，會議接受率僅約 10%，相較於 IEEE INFOCOMM 等頂級國際會議的接受率 25%，顯得更為難得。

本次會議前、後分別受到本會議的推動委員會委員 Mozilla 的 CEO Li Gong 的邀請訪問以及本會議的大會邀請至中國科學研究院演講，而國際會議後的推動委員會也決議 2012 年的主辦單位延至下次會議討論。

五、　結語

本次大會由有來自全世界三十餘國作者投稿，稿件水準極高，接受率極低，約為 10%，會議圓滿成功。會議組織與會議議程如下：

CONFERENCE ORGANIZING COMMITTEE

General Chair	Dengguo Feng (feng@is.iscas.ac.cn, Chinese Academy of Sciences, China)
Program Committee Chair	David Basin(basin@inf.ethz.ch, ETH Zurich, Switzerland) Peng Liu(pliu@ist.psu.edu, Pennsylvania State University, USA)
Local Arrangements Committee Chair	Jiwu Jing (jing@lois.cn, Chinese Academy of Sciences, China)
Publication Chair	Peng Ning (pning@ncsu.edu, NC State University, USA)
Publicity Chair	Jie Li (lijie@cs.tsukuba.ac.jp, University of Tsukuba, Japan)
Workshop Chair	Dongdai Lin (ddlin@is.iscas.ac.cn, Chinese Academy of Sciences, China)
Tutorial Chair	Zhong Chen (chen@cs.pku.edu.cn, Peking University, China)

Treasurer	Sencun Zhu (szhu@cse.psu.edu, Pennsylvania State University, USA)
Web Chair	Ji Xiang (xiangji2008@gmail.com, Chinese Academy of Sciences, China)
Secretary	Daren Zha (zdr@lois.cn) Zongbin Liu (liuufo85@gmail.com)

STEERING COMMITTEE

Shiuhpyng Shieh(Chair), Chiao Tung University, Chinese Taipei
David Basin, ETH Zurich, Switzerland
Robert Deng, Singapore Management University, Singapore
Virgil Gligor, Carnegie Mellon University, USA
Hideki Imai, National Institute of Advanced Industrial Science and Technology, Japan
Sushil Jajodia, George Mason University, USA
Pierangela Samarati, University of Milan, Italy
Elisa Bertino, Purdue University, USA
Mike Reiter, University of North Carolina at Chapel Hill, USA
Li Gong, Mozilla Online Ltd., USA
Ninghui Li, Purdue University, USA
Eiji Okamoto, University of Tsukuba, Japan
Vijay Varadharajan, Macquarie University, Australia

六、會議議程

ASIACCS 2010: Beijing, China

Program Sketch

12 April	**13:30-18:00**	Registration	Lobby of Building 2
13 April	**8:00-8:50**	Registration	Meeting Room1, Building 8
	8:50-9:00	Welcoming Remarks	Meeting Room1, Building 8
	9:00-10:00	Invited Talk	Meeting Room1, Building 8
	10:00-10:30	Coffee-break	Meeting Room1, Building 8
	10:30-12:00	Session 1:Privacy	Meeting Room1, Building 8
	12:00-13:30	Lunch	Cafeteria in Friendship Palace
	13:30-15:00	Session 2:Applied Cryptography	Meeting Room1, Building 8
	15:00-15:30	Coffee Break	Meeting Room1, Building 8
	15:30-17:00	Session 3: Network Security	Meeting Room1, Building 8
	17:30-19:00	Dinner	Cafeteria in Friendship Palace
	19:00-21:00	Steering Committee Meeting (Steering committee members only)	Second Floor meeting Room, Building 2
14 April	**8:00-8:50**	Registration	Meeting Room1, Building 8
	9:00-10:00	Invited Talk	Meeting Room1, Building 8
	10:00-10:30	Coffee Break	Meeting Room1, Building 8
	10:30-12:00	Session 4: Systems Security – I	Meeting Room1, Building 8
	12:00-13:30	Lunch	Cafeteria in Friendship Palace
	13:30-15:00	Session 5: Access Control – I	Meeting Room1, Building 8
	15:00-15:30	Coffee Break	Meeting Room1, Building 8
	15:30-17:30	Session 6: Security Protocols	Meeting Room1, Building 8
	18:30-20:30	Banquet	Ju Xiu Yuan Friendship Palace
	8:00-8:45	Registration	Meeting Room1, Building 8
	8:45-10:15	Session 7: Access Control – II	Meeting Room1, Building 8

15 April	**10:10-10:35**	Coffee Break	Meeting Room1 Building 8
	10:35-12:05	Session 8: Systems Security - II	Meeting Room1, Building 8
	12:05-13:30	Lunch	Cafeteria in Friendship Palace
	13:30-15:10	Session 9: Short Papers – I	Meeting Room1, Building 8
	13:10-15:30	Coffee Break	Meeting Room1, Building 8
	15:30-17:10	Session 10: Short Papers – II	Meeting Room1, Building 8
	17:30-19:00	Dinner	Cafeteria in Friendship Palace

Advanced Program

The 5th ACM Symposium on Information, Computer and Communications Security

(ASIACCS 2010)

（Beijing Friendship Hotel）

April 13, 2010	
8:00 - 8:50	**Registration**
8:50 - 9:00	**Welcoming Remarks**
9:00 - 10:00	**INVITED TALK:** **Pierangela Samarati, Universita` degli Studi di Milano** **Session Chair: Peng Liu**
10:00 - 10:30	**Coffee Break**
Session 1: Privacy **Session Chair: Adam Lee**	
10:30 - 11:00	**Towards Publishing Recommendation Data With Predictive Anonymization** Chih-Cheng Chang, Rutgers University Brian Thompson, Rutgers University Hui Wang, Stevens Institute of Technology Danfeng Yao, Rutgers University
11:00 - 11:30	**Restoring Compromised Privacy in Micro-data Disclosure** Lei Zhang, George Mason University Alexander Brodsky, George Mason University Sushil Jajodia, George Mason University
11:30 - 12:00	**Securely Outsourcing Linear Algebra Computations** Mikhail Atallah, Purdue University Keith Frikken, Miami University
12:00 - 13:30	**Lunch**
Session 2: Applied Cryptography **Session Chair: Dongdai Lin**	
13:30 - 14:00	**Attribute-based Signature and its Application** Jin Li, Illinois Institute of Technology Man Ho Au, University of Wollongong Willy Susilo, University of Wollongong Dongqing Xie, Guangzhou University

	Kui Ren, Illinois Institute of Technology
14:00 - 14:30	**Dynamic Fully Forward-Secure Group Signatures** Benoit Libert, Universite Catholique de Louvain Moti Yung, Google & Columbia University
14:30 - 15:00	**Identity-Based Encryption based on ElGamal** Yu Chen, Peking University Manuel Charlemagne, Dublin City University, Ireland Zhi Guan, Peking University Jianbin Hu, Peking University Zhong Chen, Peking University
15:00 - 15:30	**Coffee Break**
Session 3: Network Security Session Chair: Kui Ren	
15:30 - 16:00	**Region-based BGP Announcement Filtering for Improved BGP Security** Fernando Sanchez, Zhenhai Duan Florida State University
16:00 - 16:30	**Fast-flux Service Network Detection Based on Spatial Snapshot Mechanism for Delay-free Detection** Si-Yu Huang, Taiwan Tech Ching-Hao Mao, Taiwan Tech Hahn-Ming Lee, Taiwan Tech
16:30 - 17:00	**Securing Wireless Sensor Networks against Large-scale Node Capture Attacks** Tuan Vu, University of Calgary Reihaneh Safavi-Naini, University of Calgary Carey Williamson, University of Calgary
17:30 - 19:00	**Dinner**
April 14, 2010	
8:00 - 9:00	**Registration**
9:00 – 10:00	**INVITED TALK:** **Andrei Sabelfeld, Chalmers University of Technology** **Session Chair: David Basin**
10:00 - 10:30	**Coffee Break**

Session 4: Systems Security – I Session Chair: Andrei Sabelfeld	
10:30 - 11:00	**Preventing Drive-by Download via Inter-Module Communication Monitoring** Chengyu Song, Peking University Jianwei Zhuge, Peking University Xinhui Han, Peking University Zhiyuan Ye, Peking University
11:00 - 11:30	**A Solution for the Automated Detection of Clickjacking Attacks** Marco Balduzzi, Eurecom Manuel Egele, University of California, Santa Barbara Engin Kirda, Eurecom Davide Balzarotti, Eurecom Christopher Kruegel, University of California, Santa Barbara
11:30 - 12:00	**PAriCheck: An Efficient Pointer Arithmetic Checker for C Programs** Yves Younan, Katholieke Universiteit Leuven Pieter Philippaerts, Katholieke Universiteit Leuven Lorenzo Cavallaro, University of California, Santa Barbara R. Sekar, Stony Brook University Frank Piessens, Katholieke Universiteit Leuven Wouter Joosen, Katholieke Universiteit Leuven
12:00 - 13:30	**Lunch**
Session 5: Access Control – I **Session Chair: Robert Deng**	
13:30 - 14:00	**An Opportunistic Authority Evaluation Scheme for Data Security in Crisis Management Scenarios** Enrico Scalavino, Imperial College London Giovanni Russello, Create-Net Rudi Ball, Imperial College London Vaibhav Gowadia, Imperial College London Emil Lupu, Imperial College London
14:00 - 14:30	**Effective Trust Management Through a Hybrid Logical and Relational Approach** Adam J. Lee, University of Pittsburgh

	Ting Yu, North Carolina State University Yann Le Gall, University of Pittsburgh
14:30 - 15:00	**Toward Practical Authorization-dependent User Obligation Systems** Murillo Pontual, University of Texas at San Antonio Omar Chowdhury, University of Texas at San Antonio William H. Winsborough, University of Texas at San Antonio Ting Yu, North Carolina State University Keith Irwin, Winston-Salem State University
15:00 – 15:20	**Coffee-break**
Session 6: Security Protocols **Session Chair: Kanta MATSUURA**	
15:30 - 16:00	**Cap Unification: Application to Protocol Security modulo Homomorphic Encryption** Siva Anantharaman, LIFO, University of Orleans Hai Lin, Clarkson University Christopher Lynch, Clarkson University Paliath Narendran, University at Albany--SUNY Michael Rusinowitch, LORIA - INRIA Lorraine
16:00 - 16:30	**SSLOCK: Sustaining the Trust on Entities Brought by SSL** Adonis P.H. Fung, The Chinese University of Hong Kong K.W. Cheung, The Chinese University of Hong Kong
16:30 - 17:00	**Computationally Secure Two-Round Authenticated Message Exchange** Klaas Ole Kürtz, Christian-Albrechts-Universität Kiel Henning Schnoor, Christian-Albrechts-Universität Kiel Thomas Wilke, Christian-Albrechts-Universität Kiel
17:00 – 17:30	**Bureaucratic Protocols for Secure Two-Party Sorting, Selection, and Permuting** Guan Wang, Syracuse University Tongbo Luo, Syracuse University Michael T. Goodrich, Univ. of California, Irvine Wenliang Du, Syracuse University Zutao Zhu, Syracuse University

18:30 - 20:30	**Conference Banquet**
April 15, 2010	
8:00 - 8:45	**Registration**
Session 7: Access Control – II **Session Chair: Ting Yu**	
8:45 - 9:15	**A Logic for Authorization Provenance** Jinwei Hu, Huazhong University of Science and Technology Yan Zhang, University of Western Sydney Ruixuan Li, Huazhong University of Science and Technology Zhengding Lu, Huazhong University of Science and Technology
9:15 - 9:45	**Risk-based Access Control Systems Built on Fuzzy Inferences** Qun Ni, Purdue University Elisa Bertino, Purdue University Jorge Lobo, IBM T. J. Watson Research Center
9:45 - 10:15	**Attribute Based Data Sharing with Attribute Revocation** Shucheng Yu, Worcester Polytechnic Institute Cong Wang, Illinois Institute of Technology Kui Ren, Illinois Institute of Technology Wenjing Lou, Worcester Polytechnic Institute
10:15 – 10:35	**Coffee-break**
Session 8: Systems Security - II **Session Chair: Engin Kirda**	
10:35 – 11:05	**binOb+: A Framework for Potent and Stealthy Binary Obfuscation** **Byoungyoung Lee, POSTECH** Yuna Kim, POSTECH Jong KIM, POSTECH
11:05 – 11:35	**Secure Provenance: The Essential of Bread and Buffer of Data Forensics in Cloud Computing** Rongxing Lu, University of Waterloo Xiaodong Lin, University of Ontario Institute of Technology Xiaohui Liang, University of Waterloo Xuemin (Sherman) Shen, University of Waterloo

11:35 – 12:05	**RunTest: Assuring Integrity of Dataflow Processing in Cloud Computing Infrastructures** Juan Du, Wei Wei, Xiaohui Gu, Ting Yu North Carolina State University
12:05 – 13:30	**Lunch**
Session 9: Short Papers – I Session Chair: Sencun Zhu	
13:30 – 13:50	**K-anonymous Association Rule Hiding** Zutao Zhu, Wenliang Du Syracuse University
13:50 – 14:10	**Controlling Data Disclosure in Computational PIR Protocols** Ning Shang, Gabriel Ghinita, Yongbin Zhou, Elisa Bertino Purdue University
14:10 – 14:30	**Cryptographic Role-based Security Mechanisms based on Role-Key Hierarchy** Yan Zhu, Arizona State University Gail-Joon Ahn, Arizona State University Hongxin Hu, Arizona State University Huaixi Wang, Peking University
14:30 – 14:50	**PriMa: An Effective Privacy Protection Mechanism for Social Networks** Anna Squicciarini, The Pennsylvania State University Federica Paci, University of Trento Smitha Sundareswaran, The Pennsylvania State University
14:50 – 15:10	**Oblivious Enforcement of Hidden Information Release Policies** Brian Wongchaowart, Adam Lee University of Pittsburgh
15:10 – 15:30	**Coffee-break**
Session 10: Short Papers – II Session Chair: Cliff Zou	
15:30 – 15:50	**Apex: Extending Android Permission Model and Enforcement with User-defined Runtime Constraints** Mohammad Nauman, Institute of Management Sciences, Pakistan Sohail Khan, Institute of Management Sciences, Pakistan Masoom Alam, Austria Xinwen Zhang, Samsung Information Systems America

15:50 – 16:10	**A Hotspot-based Protocol for Attack Traceback in Mobile Ad Hoc Networks** Hungyuan Hsu, Penn State University Sencun Zhu, Penn State University Ali Hurson, Missouri University of Science and Technology
16:10 – 16:30	**Practical ID-based Encryption for Wireless Sensor Network** Cheng-Kang Chu, Singapore Management University Joseph K. Liu, Institute for Infocomm Research, Singapore Jianying Zhou, Institute for Infocomm Research, Singapore Feng Bao, Institute for Infocomm Research, Singapore Robert H. Deng, Singapore Management University
16:30 – 16:50	**A Game Theoretic Model for Digital Identity and Trust in Online Communities** Tansu Alpcan, Deutsche Telekom Laboratories Cengiz Orencik, Sabanci University Albert Levi, Sabanci University Erkay Savas, Sabanci University
16:50 – 17:10	**Scene Tagging: Image-Based CAPTCHA Using Image Composition and Object Relationships** Peter Matthews, Cliff Zou University of Central Florida
17:30 - 19:00	**Dinner**
End of the conference	

出席 2010 International Dependable Systems and Networks 會議與參訪美國 Purdue University 報告

出國人員姓名/服務機關/單位/職稱/電話
吳育松/國立交通大學/資工系/助理教授/0975225901

出國期間：99/6/23-99/7/7

出國地區：美國/芝加哥、印第安那州西拉法葉市

報告日期：99/6/23-99/7/7

內容摘要：

本次出國的主要目的是出席於美國芝加哥所舉辦的第 40 屆 International Conference on Dependable Systems and Networks (DSN)。該會議囊闊了系統可靠度、性能表現、安全性等各個層面的相關 workshop、tutorial、以及最新的研究成果發表。該會議與本人目前所正執行之對於分散是系統環境中零時攻擊的反制研究以及所參與的 TWISC 相關研究計畫有非常高的相關性。出席該會議具有獲取新知、參考國外相關研究、自我檢討目前計畫執行進程等功效。

在會議結束後，我順道南下位於芝加哥南部約一百英里遠的印第安那西拉法葉市參訪 Purdue University。在 Purdue 我給了一個 talk，並與 ECE Department 的 Prof. Saurabh Bagchi 及其學生進行短暫的晤談，並尋求未來可能的相關研究合作之可能性。

壹、 參訪過程紀要

一、 出席 2010 DSN Conference 經過

DSN (International Conference on Dependable Systems and Networks)為系統可靠性的旗艦級會議。今年為第 40 屆，於美國芝加哥舉辦。主辦單位為美國密西跟大學安那堡分校（General Chair 為 U of Michigan 資訊科學工程系 Farnam Jahanian 教授）。其中 Intrusion-Tolerant Systems Workshop 以及 Security 議題的 Tracks 跟本計畫具高度相關性。其餘的 Tracks 則著墨於系統相關的性能、可靠性等議題，亦與本計畫有一定程度的相關性。

會議的第一天我出席了 Workshop on Recent Advances in Intrusion-Tolerant Systems。該 workshop 一開始是由 Cornell CS 的 Robert L. Constable 教授所給的 keynote speech。題目是"Using Formal Methods to Build Systems that Survive Attacks"。另外之後的 session 中有 MIT 的 O. Patrick Kreidl 博士所給的講題 "Analysis of a Markov Decision Process Model for Intrusion Tolerance"，以及 Lockheed Martin 的 Melvin Greer 所給的講題 "Survivability and Information Assurance in the Cloud" 這三個部分正好囊闊了從系統設計面、系統運作面、以及展望未來雲端環境中面對潛在攻擊的因應之道，與研究方向。我覺得受益方常良多。

第二天會議由 VeriSign 的研發副董 Danny McPherson 所給的 keynote speech "Availability in the Face of Evolving Internet Threats" 所展開。VeriSign 掌控全球主要的 DNS root server，而他的演講側重在透過 ATLAS 全球網路監控系統對於 distributed denial-of-service attack 的觀測以及相關見解。第二天我後半段主要是出席 Fast Abstracts Session，聽取一些最新的初步研究成果。比如說 Michigan 大學 Kang G. Shin 教授研究群的"How to Construct a Mobile Botnet"、伊利諾大學 Ravi K. Iyer 教授研究群的 "Analysis of Security Data from a Large Computing Organization"、伊利諾大學 William H. Sanders 教授研究群的 "Characterizing the Behavior of Cyber Adversaries: The Means, Motive, and Opportunity of Cyber Attacks" 等研究。

第三天的會議由分散式計算大師 MIT Nancy Lynch 教授所給的 keynote speech "Distributed Computing Theory Through the Ages" 所展開。這個演講一開始論及了分散式計算中的一些古典問題 (atomicity、mutual exclusion...)，基本上有點類似 Nancy Lynch 教授的那本 Distributed Algorithms 裡面的重點提要，當然由原作者親自講授的感覺就是不一樣。Lynch 教授的演講後來有提一些他比較近期的一些 research work。由於這部分跟我專長有些距離，部分精要之處比較無法完全領會。之後我聽了 EPFL 的一篇關於程式驗證的論文報告 "iProve: A Scalable Technique for Consumer-Verifiable Software Guarantees"。由於系統弱點(vulnerabilities)很大一部分均是由於程式內部的某些 property 沒有被滿足（比如說緩衝區溢位）所造成的，也因此如何能對一個真實世

界中的複雜程式去做驗證也就是欲解決系統弱點所需要面對的一個很重要的研究課題。第三天後來的時間我都在聽 fast abstracts，這天的 fast abstracts 較少跟本計畫研究課題有直接相關的題目，所以純粹是以增廣見聞，瞭解一下其他研究題目最近的一些進展狀況這樣。

第四天的會議有比較多跟 Security 相關的論文發表，比如說 Purdue 大學 Dongyan Xu 教授研究群的發表 "Reuse-Oriented Camouflaging Trojan: Vulnerability Detection and Attack Construction"、密西跟大學 Kang G. Shin 教授研究群的發表 " "Detection of Botnets Using Combined Host- and Network-Level Information" 以及 CMU 大學 Virgil D. Gligor 教授研究群的發表 "Dependable Connection Setup for Network Capabilities" 等。雖然這些研究根本計畫的入侵反制課題沒有直接關係，但對於激發新的研究方法還是很有幫助的。

二、 Purdue 大學參訪

此次 DSN 會議正巧是在芝加哥舉辦 。芝加哥距離 Purdue University 不過一百多英里遠，開車兩小時多便可到達。我正好把握此一難得機會南下 Purdue University 拜訪我的指導教授 Prof. Saurabh Bagchi，並在 ECE Department 給一個關於我目前在入侵反制上研究的一個 talk。此行目的之一是見見老同學，Purdue 的一些師長，維持聯繫關係，另一方面是尋求未來研究上可能的一些合作。

貳、 心得與結論

總地來說，有機會出席國際會議對於增廣見聞、見見老朋友、認識新朋友是非常有幫助的。尤其我國近年欲推動大學邁向國際一流，其中很重要的一環便是要讓國外一流大學的師生們能看到我們的學校、知道我們的學校也是有在做不錯的 research、甚至可以在國際重要會議上與他們相爭鋒。另外如果經費許可，我是覺得亦能多鼓勵學生出國參加這些重要會議，親自見識一下國外一流大學的學生、老師、以及人家的研究成果。我相信這比透過我們老師所傳遞給他們的二手資訊會對他們有更直接、更深遠的影響。

這次出席 DSN 會議所得到的訊息是入侵反制仍是一個很重要的研究課題。一方面對於驗證程式的安全性，去除弱點等問題就現實生活中的複雜系統仍尚未有完美的解決方案。二方面不斷推成出新的攻擊型態更彰顯了入侵反制機制之存在必要性。在我所原本設想的反制動作中，多半是以阻擋攻擊進程為首要目標。這次參與 DSN 讓我想起了傳統容錯計算上的 checkpoint 和 recovery 等技巧或也可用為反制動作的選項之一。另外整體而言，對於會議中 VeriSign、Lockheed Martin 等業界講者所提供的一些業界在網路攻擊、雲端運算上的看法，對於檢討本計畫之入侵反制系統設計架構在

實務面上的合理性亦有相當程度的助益。

DSN 明年將於香港舉辦，另外像 SIGCOMM 今年在印度舉辦、INFOCOM 明年將在中國上海辦。感覺起來這些大學發展原本落後台灣的國家近幾年在國際會議上的著力程度似乎相對比台灣都還來得深。當然不可否認的是中國、印度有其綜合國力的優勢存在，這些重要會議在那邊舉辦並不代表中、印兩國在相關領域的學術研究已經具有國際一流水準。但以客觀角度來說，人家把握了這些與國際頂尖學者互動的機會，假以時日他們在這些領域的發展肯定會有很大的進步。在這個問題上，我們必須要更認真地去看待，更積極地去應對。

出席國際學術會議心得報告

計畫編號	99-2219-E-009-013-
出國人員姓名 服務機關及職稱	趙禧綠 交通大學資工系助理教授
會議時間地點	2010/9/26~2010/9/29, Istanbul, Turkey
會議名稱	The 21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2010**)**
發表論文題目	Analytical Modeling of Timeout for Contention-Based Bandwidth Request Mechanism in IEEE 802.16 WiMAX Networks

一、參加會議經過

此次國際研討會共計四天，報告人的論文屬 track 2 的 MAC and cross layer design，technical session 則是排在九月二十八日上午。該篇論文的主題是針對頻譜設定在 60GHz 的 IEEE 802.15.3c 之排程演算法。由於 PIMRC 是通訊網路領域主要的國際研討會之一，再加上伊斯坦堡是個旅遊勝地，與會人數很多。

二、與會心得

依據報告人研究興趣，在此次研討會主要聆聽的研究議題有：

(1) Cognitive networks（感知網路）：這個範圍的研究在近期 IEEE 國際研討會議非常熱門，PIMRC 亦安排一場 panel discussion。在這場 panel discussion，他們提出感知無線電網路應有一大型資料庫，供 secondary users 以及 cognitive radio access points (CR APs) 查詢附近區域 primary users 或 primary base stations (BSs) / access points (APs) 的位置以及發射功率，進一步由 CR APs 分配頻道以及頻道可使用時間給 secondary users，避免對 primary users 造成干擾，同時減輕 secondary users 所需要執行的運算。此大型資料庫的需求恰與目前正紅的雲端運算相呼應。利用雲端伺服器所提供的強大運算功能與地域性的資訊查詢，將實現感知無線電網路的進程往前推一大步。由於報告者目前參與一項國科會的橋接計畫，該計畫內容正是實作感知無線電網路。藉由聆聽此 panel discussion，對我們的實作開發助益很大。

(2) Radio Resource Management(RRM)以及 scheduling：偏向跨層的最優化設計(Cross-Layer Optimization)。

(3) LTE：在此次會議中，大多數此範圍的研究仍然是以 OFDM 或者 OFDMA 技術為主，比如 OFDM 所使用通道估測及 Joint CFO and CE 的設計等等。RRM 以及 scheduling 的文章不多見。

(4) Cooperative/relay communications：cooperative communication 這幾年來廣受注意，相關的

論文亦很多。多數論文均以 PHY 的角度來決定 relay 的選擇與數量。

藉由在國際間分享研究與國內外學者交流，並聽取世界各地的研究報告以獲取新知，可以說是非常有收穫的一次行程。報告之論文全文收錄於後。

Performance Enhancement of Contention-Based Bandwidth Request Mechanism in IEEE 802.16 WiMAX Networks

Shih-Fan Chou[1], Jen-Hsi Liu[1], Hsi-Lu Chao[1], Tzu-Chi Guo[1], Chia-Lung Liu[2], and Feng-Jie Tsai[2]
[1]Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan
[2]Information & Communications Research Labs, Industrial Technology Research Institute, Hsinchu, Taiwan

***Abstract*—The IEEE 802.16 standard is a promising technology for 4G mobile networks. Though supporting versatile service classes, best effort (BE) service class is expected to dominate WiMAX networks, due to operational simplicity. One of bandwidth request mechanisms that subscriber stations (SS) can utilize to issue bandwidth requests (BW-REQ) for BE connections is contention-based random access. An SS starts a timer *T*16 when transmitting a BW-REQ. If getting a grant before timer expiration, the SS transmits data packets at the allocated time slots; otherwise it performs truncated binary exponential backoff process for BW-REQ retransmission. The default value of *T*16 is one frame time. However, *T*16 impacts on contention and request collision significantly. In the paper, we develop an analytical model for *T*16 timer setting. Besides, we derive analytical expressions for the average number of tries per BW-REQ and the average packet delay. We compare the theoretical results of fixed and adjustable timers. The results show that adjusting timer reduces both the number of collision and the average packet delay.**

***Keywords*—WiMAX, best effort, bandwidth request, contention**

I. INTRODUCTION

IEEE 802.16 protocol has been standardized for metropolitan broadband wireless access (BWA) systems, and it is a viable technology to be used for connecting local area networks (e.g., IEEE 802.11-bassed WLAN) to the Internet, due to the characteristics of high transmission rate and flexible quality-of-service (QoS). [1]. The IEEE 802.16 MAC layer supports a mandatory PMP architecture, which consists of a base station (BS) serving a number of subscriber stations (SS). There are two types of duplex scheme, i.e. FDD (Frequency Division Duplexing) and TDD (Time Division Duplexing). In this paper, we focus on TDD mode. TDD mode requires only one channel for transmitting downlink (DL) and uplink (UL) sub-frames at two distinct time slots. Moreover, the DL and UL ratio can be adjusted dynamically.

In order to support multimedia services, the IEEE 802.16 standard [1][2] defines five service classes to accommodate versatile QoS-demand applications (such as VoIP, and MPEG video). These service classes are unsolicited grant service (UGS), extended real-time polling service (ertPS), real-time polling service (rtPS), non-real-time polling service (nrtPS), and best-effort (BE) service. Due to the fact that "*how to perform resource reservation to meet applications' QoS demands*" is not within the scope of the standard, it is possible that even VoIP flows would be treated as BE service class. Therefore, in this paper, we focus on the BE service class.

A BS has the full control of slot allocation. To avoid collisions, SSs should get permission before their data transmission. According to the IEEE 802.16 standard, such an exclusive channel access is achieved by requiring SSs to send bandwidth requests first. For this purpose, the IEEE 802.16 standard specifies three bandwidth request mechanisms: contention-based random access and contention free-based polling are two suggested approaches, and piggyback mechanism is optional. These three request mechanisms are applicable to BE service class, and our focus is on the contention-based approach.

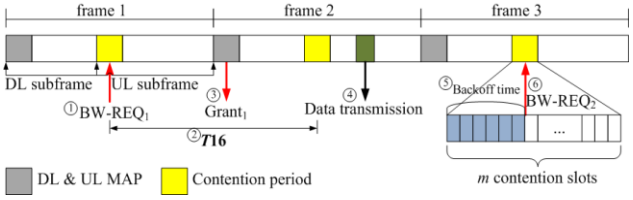


Figure 1 Illustration of contention-based bandwidth request mechanism

The random access contention resolution adopted in WiMAX is based on a truncated binary exponential backoff scheme without carrier sensing. Before each attempt of BW-REQ transmission, an SS randomly selects a backoff timer from [0, W_i-1], where W_i is the contention window size of the i^{th} retry. The backoff time indicates the number of slots that the SS should wait before its BW-REQ transmission. For the first attempt, the contention window size is the minimum value W_{min}; the window size after the i^{th} retry is 2^iW_{min}. The window size keeps doubling till it reaches the maximum value $W_{max}=2^rW_{min}$, where r is the maximum backoff stage. For a BW-REQ, an SS can try at most 16 times. Both W_{min} and W_{max} are defined by BSs, while the WiMAX standard does not provide optimal/suggested values.

When using contention, no explicit acknowledgment (ACK) frame is sent back to indicate whether a bandwidth request (BW-REQ) message is successfully transmitted or not. Instead, a timeout *T*16 is set to determine whether requiring retransmission or not. The default setting of *T*16 is one frame time. An illustrative example of contention-based bandwidth request mechanism is shown in Fig. 1. BW-REQs are sent in the contention period of a frame (Fig. 1-①), and *T*16 is set simultaneously (Fig. 1-②). If a grant is given within *T*16 timeout (Fig. 1-③), the SS stops contention resolution and use the allocated bandwidth for uplink transmission (Fig. 1-④). Otherwise the SS believes that its BW-REQ was corrupted, and then restarts a contention resolution process. The SS randomly selects a backoff timer (Fig. 1-⑤), and counts down that timer. When the timer is zero, the SS retransmits the BW-REQ (Fig. 1-⑥), and same processes repeat.

Recent research of request mechanisms include [3][4][5][6][7]. In [3], the authors conclude that the best size of contention period is (2*N*-1), and *N* is the number of SSs. However, upon heavy traffic load, the number of data slots of an UL subframe decrease as *N* increases, and a BS may not issue grants to all received BW-REQs. For those refused and collided BW-REQs, the SSs will run the contention resolution mechanism again, and thus delay time increases.

In [4], the authors introduce a new algorithm, called Multi-FS-ALOHA, which divides the contention period into two parts. The first is used by SSs to issue first-try BW-REQs, while the second part is dedicated for retransmission of BW-REQ messages. These two parts are dynamically fixed on a frame by frame basis. The drawback of [4] is that it requires a dedicated feedback channel for operation.

A modified contention resolution process is proposed in [5] to improve the system performance. Its main idea is assigning different initial window sizes to different scheduling classes. However, based on the presented simulation results, this algorithm performs similarly to the contention mechanism defined in the standard.

An analytical model of the contention-based bandwidth request mechanism, defined in [1], in a saturated WiMAX network was developed in [6][7]. [8] took the number of contending SSs into account to determine the optimal window size.

Briefly summarizing the introduced literature, performance of the contention-based request mechanism can be improved by (1) reducing the collision probability, (2) dynamically adjusting the contention period according to the number of SSs, (3) assigning different minimum contention window sizes to service classes, and (4) integrating/implementing both piggyback and contention mechanisms. However, these solutions may incur the problem of compatibility.

Two possible reasons that a BW-REQ cannot be granted and need retransmission are: collision, and insufficient UL data slots. The former is due to multiple BW-REQs are transmitted at the same contention slot; the latter is due to the UL data slots cannot accommodate the total demand of received BW-REQs. However, SSs cannot identify the exact reason why they do not get resource grants, and just perform contention resolution procedure. Upon heavy traffic load, more contentions in a fixed contention period results in more collisions and worse system performance. Thus our idea is to dynamically adjust *T*16 timeout. BW-REQs may wait longer before perform contention resolution process. The objective of this paper is to develop an analytical mode for *T*16 derivation.

The rest of this paper is organized as follows. The analytical model of timeout derivation is introduced in Section II. Numerical results are presented and discussed in Section III. This paper is concluded in Section IV.

II. Analytical Model

In this section, we explain the developed analytical model. Since we focus on the retransmission caused by insufficient UL bandwidth, $T16_{ib}$ is used to represent the desired timeout. In addition, we analyze the average tries of a BW-REQ to get a resource grant, and the average packet delay.

In this analytical model, there are N BE connections, and their packet arrival is in Poisson distribution with λ_{packet}. t_{frame} and d are the frame time duration and the number of data slots of a UL subframe. r_{be} is the percentage of UL data slots which are allocated to BE service class.

A. $T16_{ib}$

Let n be the number of frames that a successfully transmitted BW-REQ can be preserved by a BS at most. Therefore,

$$T16_{ib} \geq (1+n)t_{frame} \tag{1}$$

To derive a proper $T16_{ib}$ is to determine an adequate *n* value.

In our analysis, we assume there are *m* slots in a contention period, and each slot can accommodate one BW-REQ message.

Considering a BW-REQ, the probabilities of request collision and insufficient UL bandwidth of its i^{th} retransmission (i.e., the $(i+1)^{th}$ try) are denoted as $p_c^{(i)}$ and $p_{ib}^{(i)}$ respectively. Since unsuccessful BW-REQs are only due to collisions in the modified mechanism, the probability of the i^{th} contention for an unsuccessful BW-REQ (denoted as $p_{modified}^{(i)}$) is

$$p_{modified}^{(i)} = p_c^{(i)} \tag{2}$$

According to [9], the probability that an SS attempts to transmit a BW-REQ at a contention slot for the i^{th} retry $\tau^{(i)}$ is

$$\tau^{(i)} = \frac{2}{W_i + 1} \qquad 0 \leq i \leq R-1, \tag{3}$$

where *R* is the maximum number of tries.

Given the number of transmitted BW-REQs in frame $\left\lceil \frac{W_i-1}{m} \right\rceil$, denoted as $N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}$, suppose the observed BW-REQ is retransmitted at the last contention slot in frame $\left\lceil \frac{W_i-1}{m} \right\rceil$, $p_c^{(i)}$ is

$$p_c^{(i)} = 1 - \left[1-\tau^{(i)}\right]^{N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}-1}, \quad 0 \leq i \leq R-1 \tag{4}$$

Furthermore, for $0 \leq i \leq R-1$,

$$p_{ib}{}^{(i)} = \frac{N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}\left(1-p_c^{(i)}\right) - N_{request\_served}}{N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}\left(1-p_c^{(i)}\right)} \tag{5}$$

where $N_{request\_served}$ is the number of served requests in a superframe.

We then derive the number of transmitted BW-REQs in a specific frame, say frame *j*. Connections either incurring BW-REQ collision or having packet arrivals in frame (*j*-1) will send their BW-REQs in frame *j*. We assume all BE connections have queued packets initially, i.e., $N^{(1)} = N$. Thus for frame 2,

$$N^{(2)} = N^{(1)}(1-P_0)\left(1-P_c{}^{(0)}\right)\left(1-P_{ib}{}^{(0)}\right) + N^{(1)}P_c{}^{(0)}\frac{m}{W_{min}} \tag{6}$$

where P_0 is the probability that an SS has no packet arrivals in t_{frame} time, and $P_0 = 1 - \mathrm{e}^{-(\lambda_{packet})(t_{frame})}$. Through iterative derivation, for $j \geq 1$

$$N^{(j+1)} = N^{(j)}(1-P_0)\left(1-p_c{}^{\left(log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor\right)}\right)\left(1-p_{ib}{}^{\left(log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor\right)}\right) + N^{(j)}p_c{}^{\left(log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor\right)}\frac{m}{W_{log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor}} \tag{7}$$

In (7), we use the backoff stage to get the number of retransmitted requests occur at this frame and $\frac{m}{W_{\log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor}}$ is the probability that a collided request would transmit again in frame j.

On the other hand, the number of requests a BS can serve in a UL subframe is

$$N_{request\_served} = \left\lfloor \frac{dr_{be}}{\lambda_{packet} t_{frame}} \right\rfloor. \quad (8)$$

Thus considering the worst case, a successfully transmitted BW-REQ at frame j can be served at most after n frames, and n is

$$n = \left\lceil \frac{N^{(j)}(1-p_c^{(j)}) - N_{request\_served}}{N_{request\_served}} \right\rceil. \quad (9)$$

Substituting (4), (7), (8), and (9) into (1), we obtain a theoretical $T16_{ib}$.

B. Average Number of Tries

Again in the original contention-based bandwidth request mechanism, a BW-REQ is retransmitted when either the BW-REQ experiences a collision, or the BS has no sufficient UL bandwidth to give it a grant. Let X be the number of tries for a BW-REQ to get granted. Since a request can be sent at most R times, the average number of tries is

$$E[X]_{original} = \sum_{i=1}^{R} \left[i p_c^{(i)} + i(1-p_c^{(i)}) p_{ib}^{(i)} \right] \quad (10)$$

However, in the modified mechanism, the BW-REQ retransmission is only caused by collisions, thus the average number of tries is as listed in (11).

$$E[X]_{modified} = \sum_{i=1}^{R} i p_c^{(i)} \quad (11)$$

C. Packet Delay

We define the packet delay being the time duration from the first try of a BW-REQ to the time of successful data packet transmission. In the IEEE 802.16 standard, the frame structure of TDD mode includes a downlink subframe (Fig. 2 ①) and an uplink subframe. An uplink subframe consists of a contention period $t_{contention}$ (Fig. 2 ②) and a data interval t_{DA} (Fig. 2 ③). The time gap between two consecutive frames is called guard time t_{guard}(Fig. 2 ④). Let $t_{request}$ and t_{data}be the time of a contention slot and an uplink data slot respectively. Thus $t_{contention} = mt_{request}$, and $t_{DA} = dt_{data}$. Let $D^{(i)}$ indicate the packet delay that a BW-REQ is granted at its i^{th} retry. Note that i=0 means the BW-REQ gets grant at its first try. An example to calculate $D^{(i)}$ is shown in Fig. 2. U and V are the time durations from sending the first BW-REQ to the end of the contention period (t_u) and from the beginning of the uplink data interval (t_v) to the time that the first packet has been transmitted, respectively. Using i=0 as an example, the first possibility is that a first-try BW-REQ is successfully transmitted and gets served immediately, its packet delay is

$$D^{(0)} = U + Y^{(0)} + V, \quad (12)$$

where

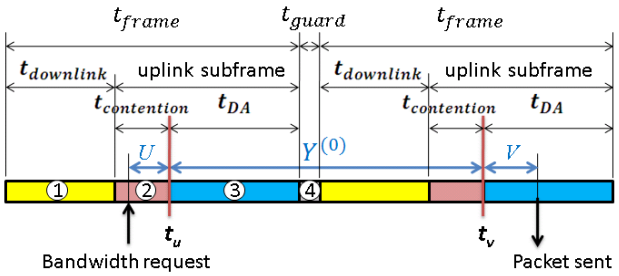


Figure 2 An illustrative example of packet delay calculation

$$\begin{cases} U = it_{request} & w.p.\ \frac{1}{m}, i = 1,2,\dots,m \\ V = it_{data} & w.p.\ \frac{1}{dr_{be}}, i = 1,2,\dots,dr_{be} \\ Y^{(0)} = t_{DA} + t_{guard} + t_{downlink} + t_{contention} \\ \quad = t_{frame} + t_{guard} = c \end{cases}$$

and *w.p.* stands for "with probability".

The second possibility is this first-try BW-REQ is successfully transmitted but preserved for later grant. In such a case, the packet delay is the same as (12) while with a different $Y^{(0)}$, and

$$Y^{(0)} = (1 + \tfrac{1}{2}\left\lceil \frac{T16_{ib}}{t_{frame}} \right\rceil)c.$$

$\frac{1}{2}\left\lceil \frac{T16_{ib}}{t_{frame}} \right\rceil$ is the waiting time in a frame for a preserved BW-REQ to get a grant, and it is uniformly distributed within $T16_{ib}$ time duration.

The last possibility is that this BW-REQ is collided with other requests, and thus the SS doubles the contention window size, randomly selects a backoff value, and retransmits this BW-REQ. If this 2nd try immediately gets a grant, the corresponding packet delay $D^{(1)}$ is

$$D^{(1)} = U + Y^{(1)} + V, \quad (13)$$

where $Y^{(1)}$ is the waiting time (and its unit is frame) between t_u and t_v and is given as

$$Y^{(1)} = c \sum_{i=0}^{1} K^{(i)} Y^{(0)}.$$

$K^{(i)}$ is the waiting time in a frame for packet transmission at the i^{th} contention. Since the SS uniformly selects its backoff counter from [0,W_i-1]. According to [10], the probability mass function of random variable $K^{(i)}$ is

$$K^{(i)} = \begin{cases} 1, & i = 0 \\ j, & w.p.\ \frac{m}{W_i}, \quad i \neq 0,\ j = 1,2,\dots,\left\lfloor \frac{W_i}{m} \right\rfloor - 1 \\ \left\lceil \frac{W_i}{m} \right\rceil, & w.p.\ 1 - \frac{(\left\lfloor \frac{W_i}{m} \right\rfloor - 1)m}{W_i}, i \neq 0 \end{cases} \quad (14)$$

If this 2nd-try BW-REQ is successfully transmitted while been preserved, it packet delay is

$$D^{(1)} = U + \left(K^{(0)} + K^{(1)} + \frac{1}{2}\left\lceil \frac{T16_{ib}}{t_{frame}} \right\rceil \right) c + V.$$

In general, for the i^{th} attempt, the average packet delay $D^{(i)}$ is

$$\begin{cases} \mathrm{E}\left[D^{(i)}\right] = E[U] + \mathrm{E}\left[Y^{(i)}\right] + E[V] \\ \mathrm{E}\left[Y^{(i)}\right] = c\sum_{j=0}^{i} \mathrm{E}\left[Z^{(j)}\right] \end{cases}, 0 \le i < R \quad (15)$$

where $Z^{(j)}$ is the waiting time in a frame for a j^{th}-retry BW-REQ and its mean is

$$\mathrm{E}\left[Z^{(j)}\right] = \begin{cases} 1, & j = 0 \\ p_c^{(j)}\mathrm{E}[K^{(j)}] + (1 - p_c^{(j)})p_{ib}^{(j)}\left(\frac{1}{2}\left\lceil\frac{T16_{ib}}{t_{frame}}\right\rceil\right), & j \ge 1 \end{cases} \quad (16)$$

Since

$$\mathrm{E}\left[K^{(j)}\right] = \begin{cases} 1, & j = 0 \\ \left\lceil\frac{W_j}{m}\right\rceil - \left\lceil\frac{W_j}{m}\right\rceil\left(\left\lceil\frac{W_j}{m}\right\rceil - 1\right)\frac{m}{2^{j+1}W_{min}}, & j = 1, \dots, r-1 \\ \left\lceil\frac{W_j}{m}\right\rceil - \left\lceil\frac{W_j}{m}\right\rceil\left(\left\lceil\frac{W_j}{m}\right\rceil - 1\right)\frac{m}{2^{r+1}W_{min}}, & j = r, \dots, R-1 \end{cases} \quad (17)$$

and

$$\begin{cases} E[U] = \dfrac{(m+1)t_{request}}{2} \\ E[V] = \dfrac{(dr_{be}+1)t_{data}}{2} \end{cases} \quad (18)$$

we obtain $\mathrm{E}\left[D^{(i)}\right]$ by substituting (16), (17) and (18) into (15). Further, the mean total packet delay of the modified mechanism $\mathrm{E}[D]_{\text{modified}}$ is

$$\mathrm{E}[D]_{\text{modified}} = (1 - p_{modified}^{(R)})\sum_{i=0}^{R-1}\left\{\left(\prod_{k=0}^{i} p_{modified}^{(k)}\right)\mathrm{E}\left[D^{(i)}\right]\right\}. \quad (19)$$

For comparison purpose, we also derive the mean total packet delay of the original mechanism, i.e., $\mathrm{E}[D]_{\text{original}}$. The expression of $\mathrm{E}[D]_{\text{original}}$ is same as (19), while the probability for a BW-REQ to fail at its i^{th} contention is $p_{original}^{(i)} = 1 - \left(1 - p_c{}^{(i)}\right)\left(1 - p_{ib}{}^{(i)}\right)$.

III. Numerical Results

In this section, we develop a simulation program to validate the analytical model, and compare and discuss the performance of the original and modified contention request mechanisms. Parameter settings are listed in Table 1.

Fig. 3 shows the $T16_{ib}$ settings upon various numbers of BW-REQs. As the number of requests increases, $T16_{ib}$ also linearly increases. Besides, upon a specific N value, as λ_{packet} increases, $T16_{ib}$ increases, too. The reason is, in average, the number of required time slots increases, and thus a BS can only serves few requests in a UL subframe. Consequently successfully transmitted BW-REQs will be preserved longer before getting grants.

In the following experiment, we set λ_{packet} be 3, and $T16_{ib}$ setting is based on the results in Fig. 3. We investigated the performance of p_c and p_{ib}, as shown in Fig. 4. It is intuitive that both p_c and p_{ib} increase as the number of requests increases. Moreover, we observed that when properly setting W_{min} (e.g., W_{min}=64), p_c is significantly reduced to 1.2×10^{-3}, and p_{ib} maintains at the smallest value among all.

The performance of average number of tries is in Fig. 5 (a) and (b). If a BW-REQ is transmitted successfully to the BS, it may be preserved for future grant. In such a case, the SS does not need to retransmit this request and thus the number of tries per request reduces, compared with the original contention request mechanism. Note that the average number of tries for both original and modified mechanisms of $W_{min} = 8$ is more than that of $W_{min} = 16$. The reason is that a small contention window size results in a high collision probability.

Table 1. Parameter settings

Parameter	Value
W_{min}	8/16/32/64
Maximum backoff stage, r	10
Maximum number of tries, R	16
Number of request slots, m	10
Number of data slots per uplink subframe, d	20
Ratio of data slots for BE, r_{be}	0.5
Time of a request slot, $t_{request}$	0.024 ms (6 slots)
Time for a uplink data slot, t_{data}	0.0376 ms (94 slots)
Guard time duration, t_{guard}	0.004 ms (1 slot)
Frame duration, t_{frame}	1 ms
Packet arrival rate, λ_{packet}	3/5/7

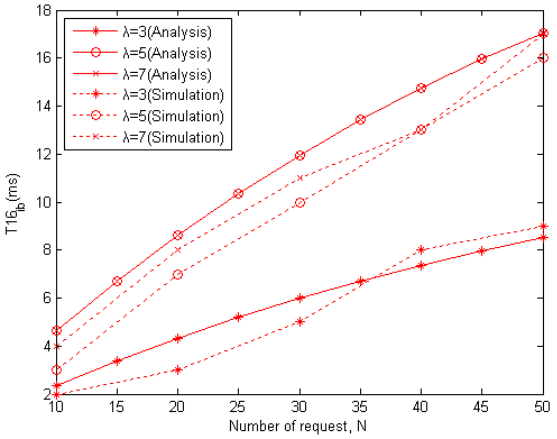


Figure 3. $T16_{ib}$ settings vs. the number of requests N upon various packet arrival rates

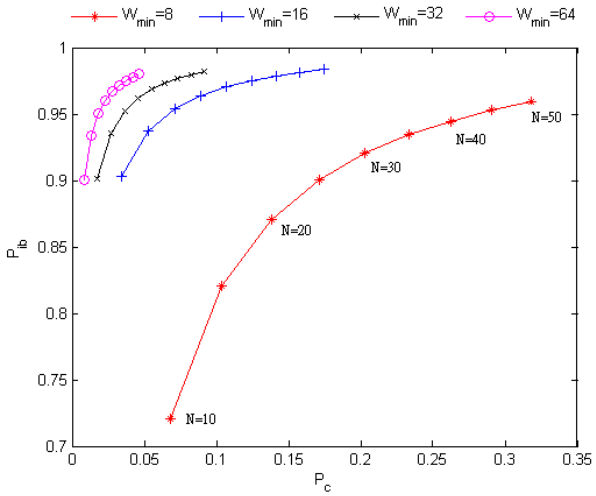
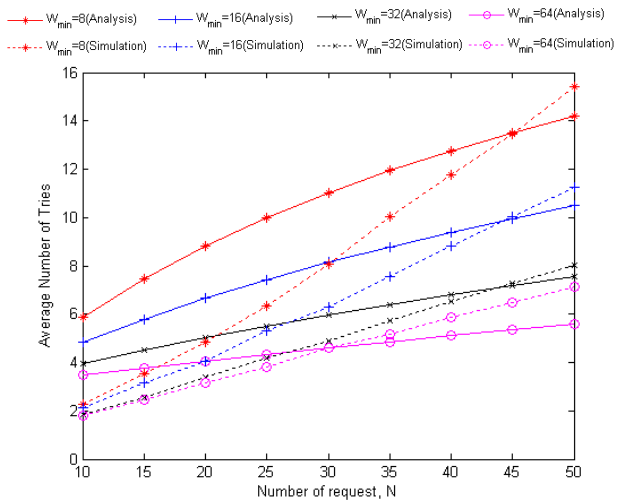
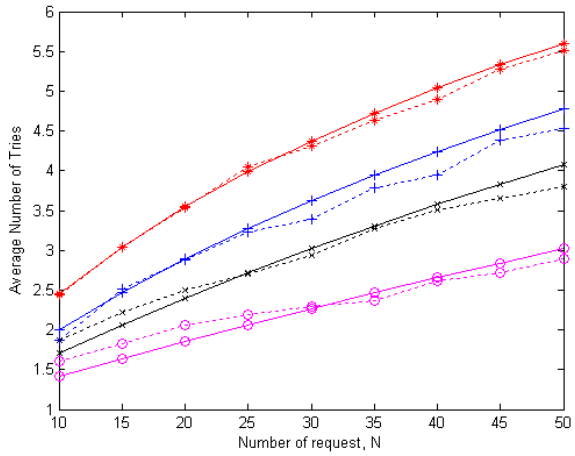


Figure 4 Probabilities of collision and insufficient bandwidth upon various W_{min} settings

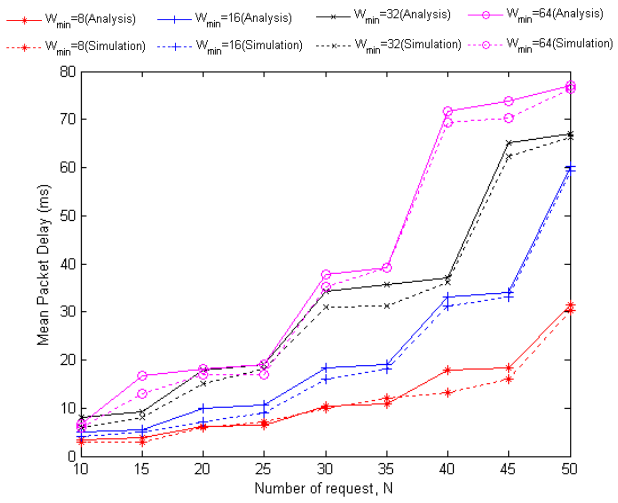


(a) Original

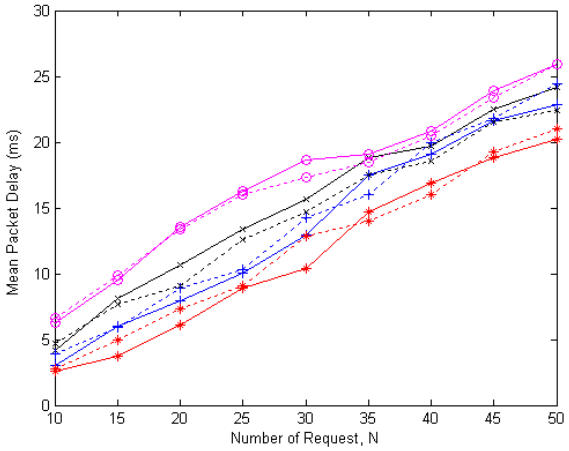


(b) Modified

Figure 5 The performance of average number of tries of the two contention-based bandwidth request mechanisms



(a) Original



(b) Modified

Figure 6 The performance of mean packet delay of the two contention-based bandwidth request mechanisms

Fig. 6 depicts the mean packet delay of both request mechanisms as the number of requests increases from 10 to 50, upon various W_{min} settings. For both mechanisms, when given a W_{min}, a large N value results in long delay due to high collision probability and more retries. On the other hand, for a specific N value, the window size of each backoff stage increases, and the average packet delay increases accordingly. The reason is that when collision occurs, the range of the backoff value becomes larger (0 to W_i -1). An SS is delayed much more frames when using a larger backoff value. The mean packet delay of the modified mechanism is significantly smaller than that of the original mechanism. The reason is that the modified request mechanism preserves successfully transmitted BW-REQs at most (n+1) frames without performing binary exponential backoff process and thus the contention window size is intact. Therefore, it has rather small delay, compared to the original mechanism.

IV. Conclusion

In this paper, focused on BE service class and contention-based request mechanism, we developed an analytical model to derive a theoretical $T16_{ib}$ timeout. Dissimilar to the original contention-based request mechanism that all unsuccessfully transmitted BW-REQs must perform the truncated binary exponential backoff process, the modified mechanism achieves reduction of collisions and tries by adjusts timeout properly for those successfully transmitted BW-REQs while cannot get grants in the next frame. The modeled timeout is a function of (1) number of BE connections, (2) traffic load, (3) retransmission, (4) collision probability, and (5) bandwidth insufficient probability. Numerical results showed that a suitable timeout does reduce the number of tries, and the average packet delay. Since the failure probability of transmitting BW-REQ decreases and the probability of a BW-REQ being hold increases, the number of tries is reduced. In addition, the range of the backoff value grows exponentially when retry occurs. An SS does not need to wait for the backoff counter counting down to zero for BW-REQ transmission when the BW-REQ is hold by the BS. The average packet delay is lower accordingly. From the numeral and simulation results, when the size of initial contention window approaches the number of contention slots, we could get better average packet delay performance. In our case, we suggest that the contention window size is 8.

Acknowledgment

This work was supported in part by NCTU-MTK Research Center under grant 99Q583, in part by National Science Council under grant NSC 99-2219-E-009-013- and in part by Ministry of Economic Affairs and Industrial Technology Research Institute under grant 99-EC-17-A-03-01-0620.

REFERENCES

[1] IEEE Std. 802.16-2004, "Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems".

[2] IEEE 802.16e-2005, IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, 2006.

[3] Taleb T., Fernandez J.C., Hashimoto K., Nemoto Y., Kato N., "A Bandwidth Aggregation-aware QoS Negotiation Mechanism for Next-Generation Wireless Networks", *IEEE Global Telecommunications Conference*, November 2007, pp.1912-1916.

[4] Lidong Lin, Bo Han and Lizhuo Zhang, "Performance Improvement using Dynamic Contention Window Adjustment for Initial Ranging in IEEE 802.16 P2MP Networks", IEEE Wireless Communications & Networking Conference (WCNC), 2007, pp.11-15.

[5] Jianhua He, Ken Guild, Kun Yang, and Hsiao-Hwa Chen, "Modeling Contention Based Bandwidth Request Scheme for IEEE 802.16 Networks", *IEEE Communications Letters*, Volume 11, August 2007 pp.689-700.

[6] Vinel A., Ying Zhang, Qiang Ni, Lyakhov A., "Efficient Request Mechanism Usage in IEEE 802.16", *Global Telecommunications Conference*, December 2006, pp.1-5.

[7] Wenyan Lu, Weijia Jia, Wenfeng Du, Lizhuo Zhang, "Performance analysis of the contention resolution scheme in IEEE 802.16". Journal of Software, Volume 18, No. 9, pp.2259-2270, 2007.

[8] Sung-Min Oh, Jae-Hyun Kim, "The Analysis of the Optimal Contention Period for Broadband Wireless Access Network", *Pervasive Computing and Communications Workshops*, March 2005, pp.215-219..

[9] Giuseppe Bianchi, Luigi Fratta, and Matteo Oliveri, "Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs," in Proc. IEEE PIMRC, Taipei, Taiwan, Sept. 1996, pp. 392–396.

[10] Hai L. Vu, Sammy Chan, and Lachlan L. H. Andrew, "Performance analysis of Best-Effort Service in Saturated IEEE 802.16 Networks," *Proc. IEEE Vehicular Technology*, Volume 59, No. 1, January 2010, pp.460-472.

[11] Q. Ni, L. Hu. "An Unsaturated Model for Request Mechanisms in WiMAX". IEEE Communications Letters, Vol. 14, No. 1, Jan 2010, pp. 45-47.

[12] Q. Ni, A. Vinel, Y. Xiao, A. Turlikov, T. Jiang. "Investigation of Bandwidth Request Mechanisms under Point-to-Multipoint Mode of WiMAX Networks". IEEE Communications Magazine, Vol. 45, No. 5, May 2007, pp. 132-138.

「ACM Symposium on Information, Computer and Communications Security（ASIACCS）國際學術會議」出國報告書

報告人： 交通大學謝續平

日期：2010 年 04 月 30 日

一、 出國目的

ACM Symposium on Information, Computer and Communications Security （ASIACCS）為 ACM Special Interest Group on Security, Audit, and Control（SIGSAC）所贊助與主辦的兩大頂尖會議之一，接受率約為 10%一頂尖會議為 ACM Conference on Computer and Communications Security（CCS）， 接受率也約為 10%。本人擔任 ACM ASIACCS steering committee chair, 負責推動該會議，並且召集 steering committee meeting，遴選每年執行單位。此次參加該國際學術會議，並審查 2011 年主辦單位進度，與 2012 年主辦國家與單位，並討論會議場地與籌辦流程。

二、 行程

參加 ACM Symposium on Information, Computer and Communications Security 擔任 Steering Committee Chair。

4/9 Taipei – Beijing

4/10 受 ACM ASIACCS steering committee member 以及 Mozilla Online Ltd. CEO Li Gong 博士邀請訪問 Mozilla Online Ltd. (該公司為開發 Firefox web browser 的公司，Firefox 瀏覽器為全球最受歡迎的瀏覽器之一)

4/12 受大會以及 Chinese Academy of Sciences, Deputy Director Jiwu Jing 邀請訪問中科院並演講 “Cloud Computing Security”

4/13-16 ACM Symposium on Information, Computer and Communications Security 會議

4/17-18 ASIACCS steering committee 會議擔任主席

4/19 返台

三、 出國人員：

謝續平現任交通大學資訊工程系教授暨 TWISC@NCTU 主任，曾任交通大學資訊工程系系主任、交通大學計算機與網路中心主任、中華民國資訊安全學會理事長，現在擔任 IEEE Tran. On Dependable and Secure Computing、IEEE Trans. On Reliability、Journal of Computer Security 副編輯、IEEE RS Newsletter 總編輯。由於現在擔任 ACM Symposium on Information, Computer and Communications Security （ASIACCS） 推動委員會主席（steering committee chair)。負責遴選籌辦國家單位，並督導籌辦進度。

四、 工作內容摘要

由於擔任 ACM Special Interest Group on Security, Audit, and Control (SIGSAC) 的推動委員會委員（Steering Committee member)，並且擔任 ACM Symposium on Information, Computer and

Communications Security （ASIACCS） 推動委員會主席（steering committee chair)，被 ACM 賦予：

a）觀察本年度會議執行成果，

b）審查下年度執行單位籌備現況，

c）並甄選兩年後會議執行單位。

本次出國為了推動 SIGSAC 的未來發展，赴大陸北京友誼賓館，參加本年度會議，觀察 ASIACCS 本年度會議主辦單位美國賓州州立大學、瑞士 ETH、北京中國科學研究院成果，並審查 2011 會議舉辦單位香港大學、香港城市大學籌備進度，與 2012 年申請舉辦單位上海交通大學等單位的提案。

此次大會由北京中國科學研究院 Dengguo Feng 主任擔任大會主席，David Basin(basin@inf.ethz.ch, ETH Zurich, Switzerland)
Peng Liu(pliu@ist.psu.edu, Pennsylvania State University, USA)
擔任議程主席，會議接受率僅約 10%，相較於 IEEE INFOCOMM 等頂級國際會議的接受率 25%，顯得更為難得。

本次會議前、後分別受到本會議的推動委員會委員 Mozilla 的 CEO Li Gong 的邀請訪問以及本會議的大會邀請至中國科學研究院演講，而國際會議後的推動委員會也決議 2012 年的主辦單位延至下次會議討論。

五、　結語

本次大會由有來自全世界三十餘國作者投稿，稿件水準極高，接受率極低，約為 10%，會議圓滿成功。會議組織與會議議程如下：

CONFERENCE ORGANIZING COMMITTEE

General Chair	Dengguo Feng (feng@is.iscas.ac.cn, Chinese Academy of Sciences, China)
Program Committee Chair	David Basin(basin@inf.ethz.ch, ETH Zurich, Switzerland) Peng Liu(pliu@ist.psu.edu, Pennsylvania State University, USA)
Local Arrangements Committee Chair	Jiwu Jing (jing@lois.cn, Chinese Academy of Sciences, China)
Publication Chair	Peng Ning (pning@ncsu.edu, NC State University, USA)
Publicity Chair	Jie Li (lijie@cs.tsukuba.ac.jp, University of Tsukuba, Japan)
Workshop Chair	Dongdai Lin (ddlin@is.iscas.ac.cn, Chinese Academy of Sciences, China)
Tutorial Chair	Zhong Chen (chen@cs.pku.edu.cn, Peking University, China)

Treasurer	Sencun Zhu (szhu@cse.psu.edu, Pennsylvania State University, USA)
Web Chair	Ji Xiang (xiangji2008@gmail.com, Chinese Academy of Sciences, China)
Secretary	Daren Zha (zdr@lois.cn) Zongbin Liu (liuufo85@gmail.com)

STEERING COMMITTEE

Shiuhpyng Shieh(Chair), Chiao Tung University, Chinese Taipei
David Basin, ETH Zurich, Switzerland
Robert Deng, Singapore Management University, Singapore
Virgil Gligor, Carnegie Mellon University, USA
Hideki Imai, National Institute of Advanced Industrial Science and Technology, Japan
Sushil Jajodia, George Mason University, USA
Pierangela Samarati, University of Milan, Italy
Elisa Bertino, Purdue University, USA
Mike Reiter, University of North Carolina at Chapel Hill, USA
Li Gong, Mozilla Online Ltd., USA
Ninghui Li, Purdue University, USA
Eiji Okamoto, University of Tsukuba, Japan
Vijay Varadharajan, Macquarie University, Australia

六、會議議程

ASIACCS 2010: Beijing, China

Program Sketch

12 April	**13:30-18:00**	Registration	Lobby of Building 2
13 April	**8:00-8:50**	Registration	Meeting Room1, Building 8
	8:50-9:00	Welcoming Remarks	Meeting Room1, Building 8
	9:00-10:00	Invited Talk	Meeting Room1, Building 8
	10:00-10:30	Coffee-break	Meeting Room1, Building 8
	10:30-12:00	Session 1:Privacy	Meeting Room1, Building 8
	12:00-13:30	Lunch	Cafeteria in Friendship Palace
	13:30-15:00	Session 2:Applied Cryptography	Meeting Room1, Building 8
	15:00-15:30	Coffee Break	Meeting Room1, Building 8
	15:30-17:00	Session 3: Network Security	Meeting Room1, Building 8
	17:30-19:00	Dinner	Cafeteria in Friendship Palace
	19:00-21:00	Steering Committee Meeting (Steering committee members only)	Second Floor meeting Room, Building 2
14 April	**8:00-8:50**	Registration	Meeting Room1, Building 8
	9:00-10:00	Invited Talk	Meeting Room1, Building 8
	10:00-10:30	Coffee Break	Meeting Room1, Building 8
	10:30-12:00	Session 4: Systems Security – I	Meeting Room1, Building 8
	12:00-13:30	Lunch	Cafeteria in Friendship Palace
	13:30-15:00	Session 5: Access Control – I	Meeting Room1, Building 8
	15:00-15:30	Coffee Break	Meeting Room1, Building 8
	15:30-17:30	Session 6: Security Protocols	Meeting Room1, Building 8
	18:30-20:30	Banquet	Ju Xiu Yuan Friendship Palace
	8:00-8:45	Registration	Meeting Room1, Building 8
	8:45-10:15	Session 7: Access Control – II	Meeting Room1, Building 8

15 April	**10:10-10:35**	Coffee Break	Meeting Room1 Building 8
	10:35-12:05	Session 8: Systems Security - II	Meeting Room1, Building 8
	12:05-13:30	Lunch	Cafeteria in Friendship Palace
	13:30-15:10	Session 9: Short Papers – I	Meeting Room1, Building 8
	13:10-15:30	Coffee Break	Meeting Room1, Building 8
	15:30-17:10	Session 10: Short Papers – II	Meeting Room1, Building 8
	17:30-19:00	Dinner	Cafeteria in Friendship Palace

Advanced Program

The 5th ACM Symposium on Information, Computer and Communications Security

(ASIACCS 2010)

（Beijing Friendship Hotel）

April 13, 2010	
8:00 - 8:50	**Registration**
8:50 - 9:00	**Welcoming Remarks**
9:00 - 10:00	**INVITED TALK:** **Pierangela Samarati, Universita` degli Studi di Milano** **Session Chair: Peng Liu**
10:00 - 10:30	**Coffee Break**
Session 1: Privacy **Session Chair: Adam Lee**	
10:30 - 11:00	**Towards Publishing Recommendation Data With Predictive Anonymization** Chih-Cheng Chang, Rutgers University Brian Thompson, Rutgers University Hui Wang, Stevens Institute of Technology Danfeng Yao, Rutgers University
11:00 - 11:30	**Restoring Compromised Privacy in Micro-data Disclosure** Lei Zhang, George Mason University Alexander Brodsky, George Mason University Sushil Jajodia, George Mason University
11:30 - 12:00	**Securely Outsourcing Linear Algebra Computations** Mikhail Atallah, Purdue University Keith Frikken, Miami University
12:00 - 13:30	**Lunch**
Session 2: Applied Cryptography **Session Chair: Dongdai Lin**	
13:30 - 14:00	**Attribute-based Signature and its Application** Jin Li, Illinois Institute of Technology Man Ho Au, University of Wollongong Willy Susilo, University of Wollongong Dongqing Xie, Guangzhou University

	Kui Ren, Illinois Institute of Technology
14:00 - 14:30	**Dynamic Fully Forward-Secure Group Signatures** Benoit Libert, Universite Catholique de Louvain Moti Yung, Google & Columbia University
14:30 - 15:00	**Identity-Based Encryption based on ElGamal** Yu Chen, Peking University Manuel Charlemagne, Dublin City University, Ireland Zhi Guan, Peking University Jianbin Hu, Peking University Zhong Chen, Peking University
15:00 - 15:30	**Coffee Break**
Session 3: Network Security Session Chair: Kui Ren	
15:30 - 16:00	**Region-based BGP Announcement Filtering for Improved BGP Security** Fernando Sanchez, Zhenhai Duan Florida State University
16:00 - 16:30	**Fast-flux Service Network Detection Based on Spatial Snapshot Mechanism for Delay-free Detection** Si-Yu Huang, Taiwan Tech Ching-Hao Mao, Taiwan Tech Hahn-Ming Lee, Taiwan Tech
16:30 - 17:00	**Securing Wireless Sensor Networks against Large-scale Node Capture Attacks** Tuan Vu, University of Calgary Reihaneh Safavi-Naini, University of Calgary Carey Williamson, University of Calgary
17:30 - 19:00	**Dinner**
April 14, 2010	
8:00 - 9:00	**Registration**
9:00 – 10:00	**INVITED TALK:** **Andrei Sabelfeld, Chalmers University of Technology** **Session Chair: David Basin**
10:00 - 10:30	**Coffee Break**

Session 4: Systems Security – I Session Chair: Andrei Sabelfeld	
10:30 - 11:00	**Preventing Drive-by Download via Inter-Module Communication Monitoring** Chengyu Song, Peking University Jianwei Zhuge, Peking University Xinhui Han, Peking University Zhiyuan Ye, Peking University
11:00 - 11:30	**A Solution for the Automated Detection of Clickjacking Attacks** Marco Balduzzi, Eurecom Manuel Egele, University of California, Santa Barbara Engin Kirda, Eurecom Davide Balzarotti, Eurecom Christopher Kruegel, University of California, Santa Barbara
11:30 - 12:00	**PAriCheck: An Efficient Pointer Arithmetic Checker for C Programs** Yves Younan, Katholieke Universiteit Leuven Pieter Philippaerts, Katholieke Universiteit Leuven Lorenzo Cavallaro, University of California, Santa Barbara R. Sekar, Stony Brook University Frank Piessens, Katholieke Universiteit Leuven Wouter Joosen, Katholieke Universiteit Leuven
12:00 - 13:30	**Lunch**
Session 5: Access Control – I **Session Chair: Robert Deng**	
13:30 - 14:00	**An Opportunistic Authority Evaluation Scheme for Data Security in Crisis Management Scenarios** Enrico Scalavino, Imperial College London Giovanni Russello, Create-Net Rudi Ball, Imperial College London Vaibhav Gowadia, Imperial College London Emil Lupu, Imperial College London
14:00 - 14:30	**Effective Trust Management Through a Hybrid Logical and Relational Approach** Adam J. Lee, University of Pittsburgh

	Ting Yu, North Carolina State University Yann Le Gall, University of Pittsburgh
14:30 - 15:00	**Toward Practical Authorization-dependent User Obligation Systems** Murillo Pontual, University of Texas at San Antonio Omar Chowdhury, University of Texas at San Antonio William H. Winsborough, University of Texas at San Antonio Ting Yu, North Carolina State University Keith Irwin, Winston-Salem State University
15:00 – 15:20	**Coffee-break**
Session 6: Security Protocols **Session Chair: Kanta MATSUURA**	
15:30 - 16:00	**Cap Unification: Application to Protocol Security modulo Homomorphic Encryption** Siva Anantharaman, LIFO, University of Orleans Hai Lin, Clarkson University Christopher Lynch, Clarkson University Paliath Narendran, University at Albany--SUNY Michael Rusinowitch, LORIA - INRIA Lorraine
16:00 - 16:30	**SSLOCK: Sustaining the Trust on Entities Brought by SSL** Adonis P.H. Fung, The Chinese University of Hong Kong K.W. Cheung, The Chinese University of Hong Kong
16:30 - 17:00	**Computationally Secure Two-Round Authenticated Message Exchange** Klaas Ole Kürtz, Christian-Albrechts-Universität Kiel Henning Schnoor, Christian-Albrechts-Universität Kiel Thomas Wilke, Christian-Albrechts-Universität Kiel
17:00 – 17:30	**Bureaucratic Protocols for Secure Two-Party Sorting, Selection, and Permuting** Guan Wang, Syracuse University Tongbo Luo, Syracuse University Michael T. Goodrich, Univ. of California, Irvine Wenliang Du, Syracuse University Zutao Zhu, Syracuse University

18:30 - 20:30	**Conference Banquet**
April 15, 2010	
8:00 - 8:45	**Registration**
Session 7: Access Control – II **Session Chair: Ting Yu**	
8:45 - 9:15	**A Logic for Authorization Provenance** Jinwei Hu, Huazhong University of Science and Technology Yan Zhang, University of Western Sydney Ruixuan Li, Huazhong University of Science and Technology Zhengding Lu, Huazhong University of Science and Technology
9:15 - 9:45	**Risk-based Access Control Systems Built on Fuzzy Inferences** Qun Ni, Purdue University Elisa Bertino, Purdue University Jorge Lobo, IBM T. J. Watson Research Center
9:45 - 10:15	**Attribute Based Data Sharing with Attribute Revocation** Shucheng Yu, Worcester Polytechnic Institute Cong Wang, Illinois Institute of Technology Kui Ren, Illinois Institute of Technology Wenjing Lou, Worcester Polytechnic Institute
10:15 – 10:35	**Coffee-break**
Session 8: Systems Security - II **Session Chair: Engin Kirda**	
10:35 – 11:05	**binOb+: A Framework for Potent and Stealthy Binary Obfuscation** **Byoungyoung Lee, POSTECH** Yuna Kim, POSTECH Jong KIM, POSTECH
11:05 – 11:35	**Secure Provenance: The Essential of Bread and Buffer of Data Forensics in Cloud Computing** Rongxing Lu, University of Waterloo Xiaodong Lin, University of Ontario Institute of Technology Xiaohui Liang, University of Waterloo Xuemin (Sherman) Shen, University of Waterloo

11:35 – 12:05	**RunTest: Assuring Integrity of Dataflow Processing in Cloud Computing Infrastructures** Juan Du, Wei Wei, Xiaohui Gu, Ting Yu North Carolina State University
12:05 – 13:30	**Lunch**
Session 9: Short Papers – I Session Chair: Sencun Zhu	
13:30 – 13:50	**K-anonymous Association Rule Hiding** Zutao Zhu, Wenliang Du Syracuse University
13:50 – 14:10	**Controlling Data Disclosure in Computational PIR Protocols** Ning Shang, Gabriel Ghinita, Yongbin Zhou, Elisa Bertino Purdue University
14:10 – 14:30	**Cryptographic Role-based Security Mechanisms based on Role-Key Hierarchy** Yan Zhu, Arizona State University Gail-Joon Ahn, Arizona State University Hongxin Hu, Arizona State University Huaixi Wang, Peking University
14:30 – 14:50	**PriMa: An Effective Privacy Protection Mechanism for Social Networks** Anna Squicciarini, The Pennsylvania State University Federica Paci, University of Trento Smitha Sundareswaran, The Pennsylvania State University
14:50 – 15:10	**Oblivious Enforcement of Hidden Information Release Policies** Brian Wongchaowart, Adam Lee University of Pittsburgh
15:10 – 15:30	**Coffee-break**
Session 10: Short Papers – II Session Chair: Cliff Zou	
15:30 – 15:50	**Apex: Extending Android Permission Model and Enforcement with User-defined Runtime Constraints** Mohammad Nauman, Institute of Management Sciences, Pakistan Sohail Khan, Institute of Management Sciences, Pakistan Masoom Alam, Austria Xinwen Zhang, Samsung Information Systems America

15:50 – 16:10	**A Hotspot-based Protocol for Attack Traceback in Mobile Ad Hoc Networks** Hungyuan Hsu, Penn State University Sencun Zhu, Penn State University Ali Hurson, Missouri University of Science and Technology
16:10 – 16:30	**Practical ID-based Encryption for Wireless Sensor Network** Cheng-Kang Chu, Singapore Management University Joseph K. Liu, Institute for Infocomm Research, Singapore Jianying Zhou, Institute for Infocomm Research, Singapore Feng Bao, Institute for Infocomm Research, Singapore Robert H. Deng, Singapore Management University
16:30 – 16:50	**A Game Theoretic Model for Digital Identity and Trust in Online Communities** Tansu Alpcan, Deutsche Telekom Laboratories Cengiz Orencik, Sabanci University Albert Levi, Sabanci University Erkay Savas, Sabanci University
16:50 – 17:10	**Scene Tagging: Image-Based CAPTCHA Using Image Composition and Object Relationships** Peter Matthews, Cliff Zou University of Central Florida
17:30 - 19:00	**Dinner**
End of the conference	

出席 2010 International Dependable Systems and Networks 會議與參訪美國 Purdue University 報告

出國人員姓名/服務機關/單位/職稱/電話
吳育松/國立交通大學/資工系/助理教授/0975225901

出國期間：99/6/23-99/7/7

出國地區：美國/芝加哥、印第安那州西拉法葉市

報告日期：99/6/23-99/7/7

內容摘要：

本次出國的主要目的是出席於美國芝加哥所舉辦的第 40 屆 International Conference on Dependable Systems and Networks (DSN)。該會議囊闊了系統可靠度、性能表現、安全性等各個層面的相關 workshop、tutorial、以及最新的研究成果發表。該會議與本人目前所正執行之對於分散是系統環境中零時攻擊的反制研究以及所參與的 TWISC 相關研究計畫有非常高的相關性。出席該會議具有獲取新知、參考國外相關研究、自我檢討目前計畫執行進程等功效。

在會議結束後，我順道南下位於芝加哥南部約一百英里遠的印第安那西拉法葉市參訪 Purdue University。在 Purdue 我給了一個 talk，並與 ECE Department 的 Prof. Saurabh Bagchi 及其學生進行短暫的晤談，並尋求未來可能的相關研究合作之可能性。

壹、 參訪過程紀要

一、 出席 2010 DSN Conference 經過

DSN (International Conference on Dependable Systems and Networks)為系統可靠性的旗艦級會議。今年為第 40 屆，於美國芝加哥舉辦。主辦單位為美國密西跟大學安那堡分校（General Chair 為 U of Michigan 資訊科學工程系 Farnam Jahanian 教授）。其中 Intrusion-Tolerant Systems Workshop 以及 Security 議題的 Tracks 跟本計畫具高度相關性。其餘的 Tracks 則著墨於系統相關的性能、可靠性等議題，亦與本計畫有一定程度的相關性。

會議的第一天我出席了 Workshop on Recent Advances in Intrusion-Tolerant Systems。該 workshop 一開始是由 Cornell CS 的 Robert L. Constable 教授所給的 keynote speech。題目是"Using Formal Methods to Build Systems that Survive Attacks"。另外之後的 session 中有 MIT 的 O. Patrick Kreidl 博士所給的講題 "Analysis of a Markov Decision Process Model for Intrusion Tolerance"，以及 Lockheed Martin 的 Melvin Greer 所給的講題 "Survivability and Information Assurance in the Cloud" 這三個部分正好囊闊了從系統設計面、系統運作面、以及展望未來雲端環境中面對潛在攻擊的因應之道，與研究方向。我覺得受益方常良多。

第二天會議由 VeriSign 的研發副董 Danny McPherson 所給的 keynote speech "Availability in the Face of Evolving Internet Threats" 所展開。VeriSign 掌控全球主要的 DNS root server，而他的演講側重在透過 ATLAS 全球網路監控系統對於 distributed denial-of-service attack 的觀測以及相關見解。第二天我後半段主要是出席 Fast Abstracts Session，聽取一些最新的初步研究成果。比如說 Michigan 大學 Kang G. Shin 教授研究群的"How to Construct a Mobile Botnet"、伊利諾大學 Ravi K. Iyer 教授研究群的 "Analysis of Security Data from a Large Computing Organization"、伊利諾大學 William H. Sanders 教授研究群的 "Characterizing the Behavior of Cyber Adversaries: The Means, Motive, and Opportunity of Cyber Attacks" 等研究。

第三天的會議由分散式計算大師 MIT Nancy Lynch 教授所給的 keynote speech "Distributed Computing Theory Through the Ages" 所展開。這個演講一開始論及了分散式計算中的一些古典問題 (atomicity、mutual exclusion...)，基本上有點類似 Nancy Lynch 教授的那本 Distributed Algorithms 裡面的重點提要，當然由原作者親自講授的感覺就是不一樣。Lynch 教授的演講後來有提一些他比較近期的一些 research work。由於這部分跟我專長有些距離，部分精要之處比較無法完全領會。之後我聽了 EPFL 的一篇關於程式驗證的論文報告 "iProve: A Scalable Technique for Consumer-Verifiable Software Guarantees"。由於系統弱點(vulnerabilities)很大一部分均是由於程式內部的某些 property 沒有被滿足（比如說緩衝區溢位）所造成的，也因此如何能對一個真實世

界中的複雜程式去做驗證也就是欲解決系統弱點所需要面對的一個很重要的研究課題。第三天後來的時間我都在聽 fast abstracts，這天的 fast abstracts 較少跟本計畫研究課題有直接相關的題目，所以純粹是以增廣見聞，瞭解一下其他研究題目最近的一些進展狀況這樣。

第四天的會議有比較多跟 Security 相關的論文發表，比如說 Purdue 大學 Dongyan Xu 教授研究群的發表 "Reuse-Oriented Camouflaging Trojan: Vulnerability Detection and Attack Construction"、密西跟大學 Kang G. Shin 教授研究群的發表 " "Detection of Botnets Using Combined Host- and Network-Level Information" 以及 CMU 大學 Virgil D. Gligor 教授研究群的發表 "Dependable Connection Setup for Network Capabilities" 等。雖然這些研究根本計畫的入侵反制課題沒有直接關係，但對於激發新的研究方法還是很有幫助的。

二、 Purdue 大學參訪

此次 DSN 會議正巧是在芝加哥舉辦 。芝加哥距離 Purdue University 不過一百多英里遠，開車兩小時多便可到達。我正好把握此一難得機會南下 Purdue University 拜訪我的指導教授 Prof. Saurabh Bagchi，並在 ECE Department 給一個關於我目前在入侵反制上研究的一個 talk。此行目的之一是見見老同學，Purdue 的一些師長，維持聯繫關係，另一方面是尋求未來研究上可能的一些合作。

貳、 心得與結論

總地來說，有機會出席國際會議對於增廣見聞、見見老朋友、認識新朋友是非常有幫助的。尤其我國近年欲推動大學邁向國際一流，其中很重要的一環便是要讓國外一流大學的師生們能看到我們的學校、知道我們的學校也是有在做不錯的 research、甚至可以在國際重要會議上與他們相爭鋒。另外如果經費許可，我是覺得亦能多鼓勵學生出國參加這些重要會議，親自見識一下國外一流大學的學生、老師、以及人家的研究成果。我相信這比透過我們老師所傳遞給他們的二手資訊會對他們有更直接、更深遠的影響。

這次出席 DSN 會議所得到的訊息是入侵反制仍是一個很重要的研究課題。一方面對於驗證程式的安全性，去除弱點等問題就現實生活中的複雜系統仍尚未有完美的解決方案。二方面不斷推成出新的攻擊型態更彰顯了入侵反制機制之存在必要性。在我所原本設想的反制動作中，多半是以阻擋攻擊進程為首要目標。這次參與 DSN 讓我想起了傳統容錯計算上的 checkpoint 和 recovery 等技巧或也可用為反制動作的選項之一。另外整體而言，對於會議中 VeriSign、Lockheed Martin 等業界講者所提供的一些業界在網路攻擊、雲端運算上的看法，對於檢討本計畫之入侵反制系統設計架構在

實務面上的合理性亦有相當程度的助益。

DSN 明年將於香港舉辦，另外像 SIGCOMM 今年在印度舉辦、INFOCOM 明年將在中國上海辦。感覺起來這些大學發展原本落後台灣的國家近幾年在國際會議上的著力程度似乎相對比台灣都還來得深。當然不可否認的是中國、印度有其綜合國力的優勢存在，這些重要會議在那邊舉辦並不代表中、印兩國在相關領域的學術研究已經具有國際一流水準。但以客觀角度來說，人家把握了這些與國際頂尖學者互動的機會，假以時日他們在這些領域的發展肯定會有很大的進步。在這個問題上，我們必須要更認真地去看待，更積極地去應對。

出席國際學術會議心得報告

計畫編號	99-2219-E-009-013-
出國人員姓名 服務機關及職稱	趙禧綠 交通大學資工系助理教授
會議時間地點	2010/9/26~2010/9/29, Istanbul, Turkey
會議名稱	The 21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2010**)**
發表論文題目	Analytical Modeling of Timeout for Contention-Based Bandwidth Request Mechanism in IEEE 802.16 WiMAX Networks

一、參加會議經過

此次國際研討會共計四天，報告人的論文屬 track 2 的 MAC and cross layer design，technical session 則是排在九月二十八日上午。該篇論文的主題是針對頻譜設定在 60GHz 的 IEEE 802.15.3c 之排程演算法。由於 PIMRC 是通訊網路領域主要的國際研討會之一，再加上伊斯坦堡是個旅遊勝地，與會人數很多。

二、與會心得

依據報告人研究興趣，在此次研討會主要聆聽的研究議題有：

(1) Cognitive networks（感知網路）：這個範圍的研究在近期 IEEE 國際研討會議非常熱門，PIMRC 亦安排一場 panel discussion。在這場 panel discussion，他們提出感知無線電網路應有一大型資料庫，供 secondary users 以及 cognitive radio access points (CR APs) 查詢附近區域 primary users 或 primary base stations (BSs) / access points (APs) 的位置以及發射功率，進一步由 CR APs 分配頻道以及頻道可使用時間給 secondary users，避免對 primary users 造成干擾，同時減輕 secondary users 所需要執行的運算。此大型資料庫的需求恰與目前正紅的雲端運算相呼應。利用雲端伺服器所提供的強大運算功能與地域性的資訊查詢，將實現感知無線電網路的進程往前推一大步。由於報告者目前參與一項國科會的橋接計畫，該計畫內容正是實作感知無線電網路。藉由聆聽此 panel discussion，對我們的實作開發助益很大。

(2) Radio Resource Management(RRM)以及 scheduling：偏向跨層的最優化設計(Cross-Layer Optimization)。

(3) LTE：在此次會議中，大多數此範圍的研究仍然是以 OFDM 或者 OFDMA 技術為主，比如 OFDM 所使用通道估測及 Joint CFO and CE 的設計等等。RRM 以及 scheduling 的文章不多見。

(4) Cooperative/relay communications：cooperative communication 這幾年來廣受注意，相關的

論文亦很多。多數論文均以 PHY 的角度來決定 relay 的選擇與數量。

藉由在國際間分享研究與國內外學者交流，並聽取世界各地的研究報告以獲取新知，可以說是非常有收穫的一次行程。報告之論文全文收錄於後。

Performance Enhancement of Contention-Based Bandwidth Request Mechanism in IEEE 802.16 WiMAX Networks

Shih-Fan Chou[1], Jen-Hsi Liu[1], Hsi-Lu Chao[1], Tzu-Chi Guo[1], Chia-Lung Liu[2], and Feng-Jie Tsai[2]
[1]Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan
[2]Information & Communications Research Labs, Industrial Technology Research Institute, Hsinchu, Taiwan

***Abstract*—The IEEE 802.16 standard is a promising technology for 4G mobile networks. Though supporting versatile service classes, best effort (BE) service class is expected to dominate WiMAX networks, due to operational simplicity. One of bandwidth request mechanisms that subscriber stations (SS) can utilize to issue bandwidth requests (BW-REQ) for BE connections is contention-based random access. An SS starts a timer *T*16 when transmitting a BW-REQ. If getting a grant before timer expiration, the SS transmits data packets at the allocated time slots; otherwise it performs truncated binary exponential backoff process for BW-REQ retransmission. The default value of *T*16 is one frame time. However, *T*16 impacts on contention and request collision significantly. In the paper, we develop an analytical model for *T*16 timer setting. Besides, we derive analytical expressions for the average number of tries per BW-REQ and the average packet delay. We compare the theoretical results of fixed and adjustable timers. The results show that adjusting timer reduces both the number of collision and the average packet delay.**

***Keywords*—WiMAX, best effort, bandwidth request, contention**

I. INTRODUCTION

IEEE 802.16 protocol has been standardized for metropolitan broadband wireless access (BWA) systems, and it is a viable technology to be used for connecting local area networks (e.g., IEEE 802.11-bassed WLAN) to the Internet, due to the characteristics of high transmission rate and flexible quality-of-service (QoS). [1]. The IEEE 802.16 MAC layer supports a mandatory PMP architecture, which consists of a base station (BS) serving a number of subscriber stations (SS). There are two types of duplex scheme, i.e. FDD (Frequency Division Duplexing) and TDD (Time Division Duplexing). In this paper, we focus on TDD mode. TDD mode requires only one channel for transmitting downlink (DL) and uplink (UL) sub-frames at two distinct time slots. Moreover, the DL and UL ratio can be adjusted dynamically.

In order to support multimedia services, the IEEE 802.16 standard [1][2] defines five service classes to accommodate versatile QoS-demand applications (such as VoIP, and MPEG video). These service classes are unsolicited grant service (UGS), extended real-time polling service (ertPS), real-time polling service (rtPS), non-real-time polling service (nrtPS), and best-effort (BE) service. Due to the fact that "*how to perform resource reservation to meet applications' QoS demands*" is not within the scope of the standard, it is possible that even VoIP flows would be treated as BE service class. Therefore, in this paper, we focus on the BE service class.

A BS has the full control of slot allocation. To avoid collisions, SSs should get permission before their data transmission. According to the IEEE 802.16 standard, such an exclusive channel access is achieved by requiring SSs to send bandwidth requests first. For this purpose, the IEEE 802.16 standard specifies three bandwidth request mechanisms: contention-based random access and contention free-based polling are two suggested approaches, and piggyback mechanism is optional. These three request mechanisms are applicable to BE service class, and our focus is on the contention-based approach.

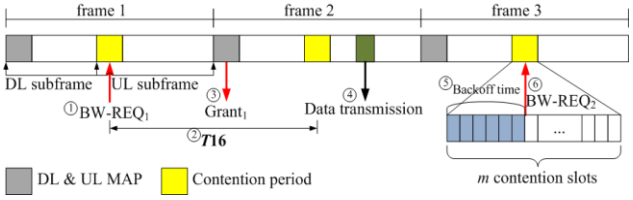


Figure 1 Illustration of contention-based bandwidth request mechanism

The random access contention resolution adopted in WiMAX is based on a truncated binary exponential backoff scheme without carrier sensing. Before each attempt of BW-REQ transmission, an SS randomly selects a backoff timer from [0, W_i-1], where W_i is the contention window size of the i^{th} retry. The backoff time indicates the number of slots that the SS should wait before its BW-REQ transmission. For the first attempt, the contention window size is the minimum value W_{min}; the window size after the i^{th} retry is 2^iW_{min}. The window size keeps doubling till it reaches the maximum value $W_{max}=2^rW_{min}$, where r is the maximum backoff stage. For a BW-REQ, an SS can try at most 16 times. Both W_{min} and W_{max} are defined by BSs, while the WiMAX standard does not provide optimal/suggested values.

When using contention, no explicit acknowledgment (ACK) frame is sent back to indicate whether a bandwidth request (BW-REQ) message is successfully transmitted or not. Instead, a timeout *T*16 is set to determine whether requiring retransmission or not. The default setting of *T*16 is one frame time. An illustrative example of contention-based bandwidth request mechanism is shown in Fig. 1. BW-REQs are sent in the contention period of a frame (Fig. 1-①), and *T*16 is set simultaneously (Fig. 1-②). If a grant is given within *T*16 timeout (Fig. 1-③), the SS stops contention resolution and use the allocated bandwidth for uplink transmission (Fig. 1-④). Otherwise the SS believes that its BW-REQ was corrupted, and then restarts a contention resolution process. The SS randomly selects a backoff timer (Fig. 1-⑤), and counts down that timer. When the timer is zero, the SS retransmits the BW-REQ (Fig. 1-⑥), and same processes repeat.

Recent research of request mechanisms include [3][4][5][6][7]. In [3], the authors conclude that the best size of contention period is (2*N*-1), and *N* is the number of SSs. However, upon heavy traffic load, the number of data slots of an UL subframe decrease as *N* increases, and a BS may not issue grants to all received BW-REQs. For those refused and collided BW-REQs, the SSs will run the contention resolution mechanism again, and thus delay time increases.

In [4], the authors introduce a new algorithm, called Multi-FS-ALOHA, which divides the contention period into two parts. The first is used by SSs to issue first-try BW-REQs, while the second part is dedicated for retransmission of BW-REQ messages. These two parts are dynamically fixed on a frame by frame basis. The drawback of [4] is that it requires a dedicated feedback channel for operation.

A modified contention resolution process is proposed in [5] to improve the system performance. Its main idea is assigning different initial window sizes to different scheduling classes. However, based on the presented simulation results, this algorithm performs similarly to the contention mechanism defined in the standard.

An analytical model of the contention-based bandwidth request mechanism, defined in [1], in a saturated WiMAX network was developed in [6][7]. [8] took the number of contending SSs into account to determine the optimal window size.

Briefly summarizing the introduced literature, performance of the contention-based request mechanism can be improved by (1) reducing the collision probability, (2) dynamically adjusting the contention period according to the number of SSs, (3) assigning different minimum contention window sizes to service classes, and (4) integrating/implementing both piggyback and contention mechanisms. However, these solutions may incur the problem of compatibility.

Two possible reasons that a BW-REQ cannot be granted and need retransmission are: collision, and insufficient UL data slots. The former is due to multiple BW-REQs are transmitted at the same contention slot; the latter is due to the UL data slots cannot accommodate the total demand of received BW-REQs. However, SSs cannot identify the exact reason why they do not get resource grants, and just perform contention resolution procedure. Upon heavy traffic load, more contentions in a fixed contention period results in more collisions and worse system performance. Thus our idea is to dynamically adjust *T*16 timeout. BW-REQs may wait longer before perform contention resolution process. The objective of this paper is to develop an analytical mode for *T*16 derivation.

The rest of this paper is organized as follows. The analytical model of timeout derivation is introduced in Section II. Numerical results are presented and discussed in Section III. This paper is concluded in Section IV.

II. Analytical Model

In this section, we explain the developed analytical model. Since we focus on the retransmission caused by insufficient UL bandwidth, $T16_{ib}$ is used to represent the desired timeout. In addition, we analyze the average tries of a BW-REQ to get a resource grant, and the average packet delay.

In this analytical model, there are N BE connections, and their packet arrival is in Poisson distribution with λ_{packet}. t_{frame} and d are the frame time duration and the number of data slots of a UL subframe. r_{be} is the percentage of UL data slots which are allocated to BE service class.

A. $T16_{ib}$

Let n be the number of frames that a successfully transmitted BW-REQ can be preserved by a BS at most. Therefore,

$$T16_{ib} \geq (1+n)t_{frame} \tag{1}$$

To derive a proper $T16_{ib}$ is to determine an adequate *n* value.

In our analysis, we assume there are *m* slots in a contention period, and each slot can accommodate one BW-REQ message.

Considering a BW-REQ, the probabilities of request collision and insufficient UL bandwidth of its i^{th} retransmission (i.e., the $(i+1)^{th}$ try) are denoted as $p_c^{(i)}$ and $p_{ib}^{(i)}$ respectively. Since unsuccessful BW-REQs are only due to collisions in the modified mechanism, the probability of the i^{th} contention for an unsuccessful BW-REQ (denoted as $p_{modified}^{(i)}$) is

$$p_{modified}^{(i)} = p_c^{(i)} \tag{2}$$

According to [9], the probability that an SS attempts to transmit a BW-REQ at a contention slot for the i^{th} retry $\tau^{(i)}$ is

$$\tau^{(i)} = \frac{2}{W_i + 1} \qquad 0 \leq i \leq R-1, \tag{3}$$

where *R* is the maximum number of tries.

Given the number of transmitted BW-REQs in frame $\left\lceil \frac{W_i-1}{m} \right\rceil$, denoted as $N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}$, suppose the observed BW-REQ is retransmitted at the last contention slot in frame $\left\lceil \frac{W_i-1}{m} \right\rceil$, $p_c^{(i)}$ is

$$p_c^{(i)} = 1 - \left[1-\tau^{(i)}\right]^{N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}-1}, \quad 0 \leq i \leq R-1 \tag{4}$$

Furthermore, for $0 \leq i \leq R-1$,

$$p_{ib}{}^{(i)} = \frac{N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}\left(1-p_c^{(i)}\right) - N_{request\_served}}{N^{\left(\left\lceil \frac{W_i-1}{m} \right\rceil\right)}\left(1-p_c^{(i)}\right)} \tag{5}$$

where $N_{request\_served}$ is the number of served requests in a superframe.

We then derive the number of transmitted BW-REQs in a specific frame, say frame *j*. Connections either incurring BW-REQ collision or having packet arrivals in frame (*j*-1) will send their BW-REQs in frame *j*. We assume all BE connections have queued packets initially, i.e., $N^{(1)} = N$. Thus for frame 2,

$$N^{(2)} = N^{(1)}(1-P_0)\left(1-P_c{}^{(0)}\right)\left(1-P_{ib}{}^{(0)}\right) + N^{(1)}P_c{}^{(0)}\frac{m}{W_{min}} \tag{6}$$

where P_0 is the probability that an SS has no packet arrivals in t_{frame} time, and $P_0 = 1 - \mathrm{e}^{-(\lambda_{packet})(t_{frame})}$. Through iterative derivation, for $j \geq 1$

$$N^{(j+1)} = N^{(j)}(1-P_0)\left(1-p_c{}^{\left(log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor\right)}\right)\left(1-p_{ib}{}^{\left(log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor\right)}\right) + N^{(j)}p_c{}^{\left(log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor\right)}\frac{m}{W_{log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor}} \tag{7}$$

In (7), we use the backoff stage to get the number of retransmitted requests occur at this frame and $\frac{m}{W_{\log_2\left\lfloor\frac{mj+1}{W_{min}}\right\rfloor}}$ is the probability that a collided request would transmit again in frame j.

On the other hand, the number of requests a BS can serve in a UL subframe is

$$N_{request\_served} = \left\lfloor \frac{dr_{be}}{\lambda_{packet} t_{frame}} \right\rfloor. \quad (8)$$

Thus considering the worst case, a successfully transmitted BW-REQ at frame j can be served at most after n frames, and n is

$$n = \left\lceil \frac{N^{(j)}(1-p_c^{(j)}) - N_{request\_served}}{N_{request\_served}} \right\rceil. \quad (9)$$

Substituting (4), (7), (8), and (9) into (1), we obtain a theoretical $T16_{ib}$.

B. Average Number of Tries

Again in the original contention-based bandwidth request mechanism, a BW-REQ is retransmitted when either the BW-REQ experiences a collision, or the BS has no sufficient UL bandwidth to give it a grant. Let X be the number of tries for a BW-REQ to get granted. Since a request can be sent at most R times, the average number of tries is

$$E[X]_{original} = \sum_{i=1}^{R} \left[i p_c^{(i)} + i(1-p_c^{(i)}) p_{ib}^{(i)} \right] \quad (10)$$

However, in the modified mechanism, the BW-REQ retransmission is only caused by collisions, thus the average number of tries is as listed in (11).

$$E[X]_{modified} = \sum_{i=1}^{R} i p_c^{(i)} \quad (11)$$

C. Packet Delay

We define the packet delay being the time duration from the first try of a BW-REQ to the time of successful data packet transmission. In the IEEE 802.16 standard, the frame structure of TDD mode includes a downlink subframe (Fig. 2 ①) and an uplink subframe. An uplink subframe consists of a contention period $t_{contention}$ (Fig. 2 ②) and a data interval t_{DA} (Fig. 2 ③). The time gap between two consecutive frames is called guard time t_{guard}(Fig. 2 ④). Let $t_{request}$ and t_{data}be the time of a contention slot and an uplink data slot respectively. Thus $t_{contention} = mt_{request}$, and $t_{DA} = dt_{data}$. Let $D^{(i)}$ indicate the packet delay that a BW-REQ is granted at its i^{th} retry. Note that i=0 means the BW-REQ gets grant at its first try. An example to calculate $D^{(i)}$ is shown in Fig. 2. U and V are the time durations from sending the first BW-REQ to the end of the contention period (t_u) and from the beginning of the uplink data interval (t_v) to the time that the first packet has been transmitted, respectively. Using i=0 as an example, the first possibility is that a first-try BW-REQ is successfully transmitted and gets served immediately, its packet delay is

$$D^{(0)} = U + Y^{(0)} + V, \quad (12)$$

where

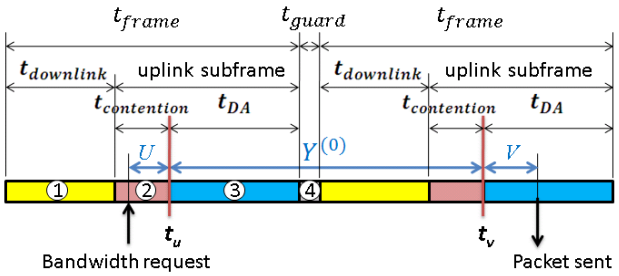


Figure 2 An illustrative example of packet delay calculation

$$\begin{cases} U = it_{request} & w.p.\ \frac{1}{m}, i = 1,2,\dots,m \\ V = it_{data} & w.p.\ \frac{1}{dr_{be}}, i = 1,2,\dots,dr_{be} \\ Y^{(0)} = t_{DA} + t_{guard} + t_{downlink} + t_{contention} \\ \quad = t_{frame} + t_{guard} = c \end{cases}$$

and *w.p.* stands for "with probability".

The second possibility is this first-try BW-REQ is successfully transmitted but preserved for later grant. In such a case, the packet delay is the same as (12) while with a different $Y^{(0)}$, and

$$Y^{(0)} = (1 + \tfrac{1}{2}\left\lceil \frac{T16_{ib}}{t_{frame}} \right\rceil)c.$$

$\frac{1}{2}\left\lceil \frac{T16_{ib}}{t_{frame}} \right\rceil$ is the waiting time in a frame for a preserved BW-REQ to get a grant, and it is uniformly distributed within $T16_{ib}$ time duration.

The last possibility is that this BW-REQ is collided with other requests, and thus the SS doubles the contention window size, randomly selects a backoff value, and retransmits this BW-REQ. If this 2nd try immediately gets a grant, the corresponding packet delay $D^{(1)}$ is

$$D^{(1)} = U + Y^{(1)} + V, \quad (13)$$

where $Y^{(1)}$ is the waiting time (and its unit is frame) between t_u and t_v and is given as

$$Y^{(1)} = c \sum_{i=0}^{1} K^{(i)} Y^{(0)}.$$

$K^{(i)}$ is the waiting time in a frame for packet transmission at the i^{th} contention. Since the SS uniformly selects its backoff counter from [0,W_i-1]. According to [10], the probability mass function of random variable $K^{(i)}$ is

$$K^{(i)} = \begin{cases} 1, & i = 0 \\ j, & w.p.\ \frac{m}{W_i}, \quad i \neq 0,\ j = 1,2,\dots,\left\lfloor \frac{W_i}{m} \right\rfloor - 1 \\ \left\lceil \frac{W_i}{m} \right\rceil, & w.p.\ 1 - \frac{(\left\lfloor \frac{W_i}{m} \right\rfloor - 1)m}{W_i}, i \neq 0 \end{cases} \quad (14)$$

If this 2nd-try BW-REQ is successfully transmitted while been preserved, it packet delay is

$$D^{(1)} = U + \left(K^{(0)} + K^{(1)} + \frac{1}{2}\left\lceil \frac{T16_{ib}}{t_{frame}} \right\rceil \right) c + V.$$

In general, for the i^{th} attempt, the average packet delay $D^{(i)}$ is

$$\begin{cases} \mathrm{E}\left[D^{(i)}\right] = E[U] + \mathrm{E}\left[Y^{(i)}\right] + E[V] \\ \mathrm{E}\left[Y^{(i)}\right] = c\sum_{j=0}^{i} \mathrm{E}\left[Z^{(j)}\right] \end{cases}, 0 \le i < R \quad (15)$$

where $Z^{(j)}$ is the waiting time in a frame for a j^{th}-retry BW-REQ and its mean is

$$\mathrm{E}\left[Z^{(j)}\right] = \begin{cases} 1, & j = 0 \\ p_c^{(j)}\mathrm{E}[K^{(j)}] + (1 - p_c^{(j)})p_{ib}^{(j)}\left(\frac{1}{2}\left\lceil\frac{T16_{ib}}{t_{frame}}\right\rceil\right), & j \ge 1 \end{cases} \quad (16)$$

Since

$$\mathrm{E}\left[K^{(j)}\right] = \begin{cases} 1, & j = 0 \\ \left\lceil\frac{W_j}{m}\right\rceil - \left\lceil\frac{W_j}{m}\right\rceil\left(\left\lceil\frac{W_j}{m}\right\rceil - 1\right)\frac{m}{2^{j+1}W_{min}}, & j = 1, \dots, r-1 \\ \left\lceil\frac{W_j}{m}\right\rceil - \left\lceil\frac{W_j}{m}\right\rceil\left(\left\lceil\frac{W_j}{m}\right\rceil - 1\right)\frac{m}{2^{r+1}W_{min}}, & j = r, \dots, R-1 \end{cases} \quad (17)$$

and

$$\begin{cases} E[U] = \dfrac{(m+1)t_{request}}{2} \\ E[V] = \dfrac{(dr_{be}+1)t_{data}}{2} \end{cases} \quad (18)$$

we obtain $\mathrm{E}\left[D^{(i)}\right]$ by substituting (16), (17) and (18) into (15). Further, the mean total packet delay of the modified mechanism $\mathrm{E}[D]_{\text{modified}}$ is

$$\mathrm{E}[D]_{\text{modified}} = (1 - p_{modified}^{(R)})\sum_{i=0}^{R-1}\left\{\left(\prod_{k=0}^{i} p_{modified}^{(k)}\right)\mathrm{E}\left[D^{(i)}\right]\right\}. \quad (19)$$

For comparison purpose, we also derive the mean total packet delay of the original mechanism, i.e., $\mathrm{E}[D]_{\text{original}}$. The expression of $\mathrm{E}[D]_{\text{original}}$ is same as (19), while the probability for a BW-REQ to fail at its i^{th} contention is $p_{original}^{(i)} = 1 - \left(1 - p_c{}^{(i)}\right)\left(1 - p_{ib}{}^{(i)}\right)$.

III. Numerical Results

In this section, we develop a simulation program to validate the analytical model, and compare and discuss the performance of the original and modified contention request mechanisms. Parameter settings are listed in Table 1.

Fig. 3 shows the $T16_{ib}$ settings upon various numbers of BW-REQs. As the number of requests increases, $T16_{ib}$ also linearly increases. Besides, upon a specific N value, as λ_{packet} increases, $T16_{ib}$ increases, too. The reason is, in average, the number of required time slots increases, and thus a BS can only serves few requests in a UL subframe. Consequently successfully transmitted BW-REQs will be preserved longer before getting grants.

In the following experiment, we set λ_{packet} be 3, and $T16_{ib}$ setting is based on the results in Fig. 3. We investigated the performance of p_c and p_{ib}, as shown in Fig. 4. It is intuitive that both p_c and p_{ib} increase as the number of requests increases. Moreover, we observed that when properly setting W_{min} (e.g., W_{min}=64), p_c is significantly reduced to 1.2×10^{-3}, and p_{ib} maintains at the smallest value among all.

The performance of average number of tries is in Fig. 5 (a) and (b). If a BW-REQ is transmitted successfully to the BS, it may be preserved for future grant. In such a case, the SS does not need to retransmit this request and thus the number of tries per request reduces, compared with the original contention request mechanism. Note that the average number of tries for both original and modified mechanisms of $W_{min} = 8$ is more than that of $W_{min} = 16$. The reason is that a small contention window size results in a high collision probability.

Table 1. Parameter settings

Parameter	Value
W_{min}	8/16/32/64
Maximum backoff stage, r	10
Maximum number of tries, R	16
Number of request slots, m	10
Number of data slots per uplink subframe, d	20
Ratio of data slots for BE, r_{be}	0.5
Time of a request slot, $t_{request}$	0.024 ms (6 slots)
Time for a uplink data slot, t_{data}	0.0376 ms (94 slots)
Guard time duration, t_{guard}	0.004 ms (1 slot)
Frame duration, t_{frame}	1 ms
Packet arrival rate, λ_{packet}	3/5/7

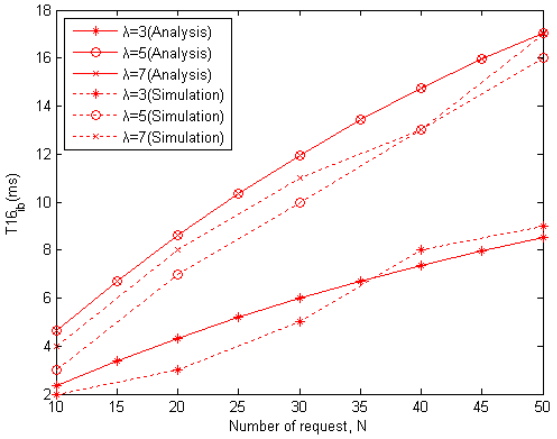


Figure 3. $T16_{ib}$ settings vs. the number of requests N upon various packet arrival rates

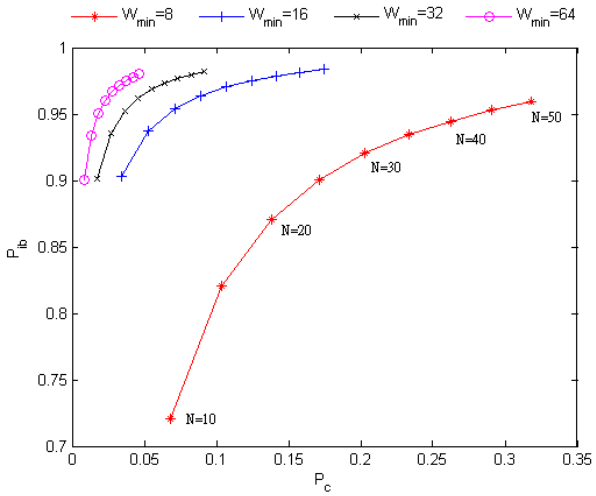
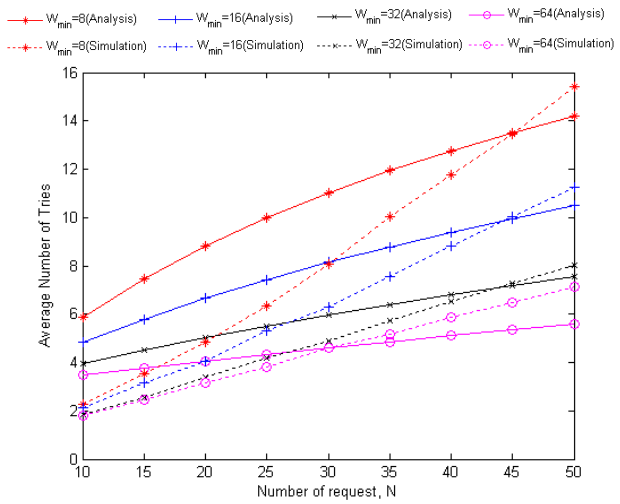
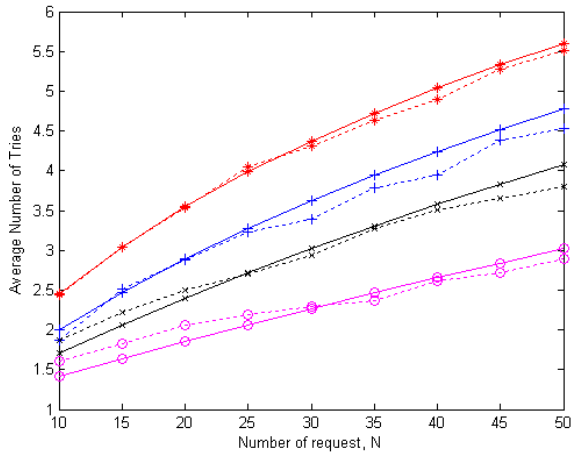


Figure 4 Probabilities of collision and insufficient bandwidth upon various W_{min} settings

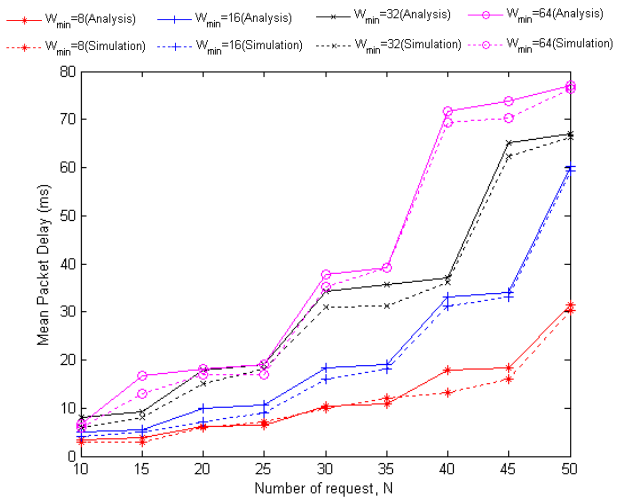


(a) Original

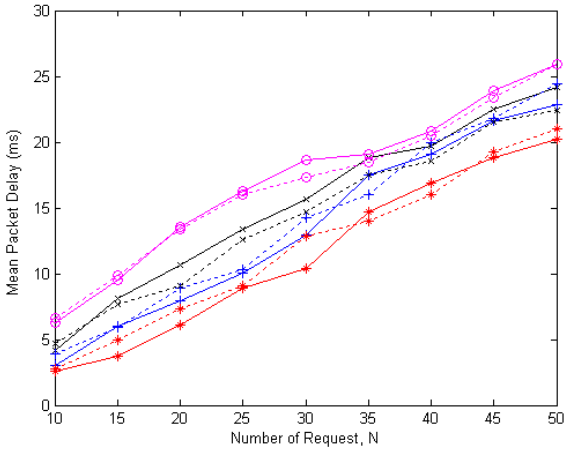


(b) Modified

Figure 5 The performance of average number of tries of the two contention-based bandwidth request mechanisms



(a) Original



(b) Modified

Figure 6 The performance of mean packet delay of the two contention-based bandwidth request mechanisms

Fig. 6 depicts the mean packet delay of both request mechanisms as the number of requests increases from 10 to 50, upon various W_{min} settings. For both mechanisms, when given a W_{min}, a large N value results in long delay due to high collision probability and more retries. On the other hand, for a specific N value, the window size of each backoff stage increases, and the average packet delay increases accordingly. The reason is that when collision occurs, the range of the backoff value becomes larger (0 to W_i -1). An SS is delayed much more frames when using a larger backoff value. The mean packet delay of the modified mechanism is significantly smaller than that of the original mechanism. The reason is that the modified request mechanism preserves successfully transmitted BW-REQs at most (n+1) frames without performing binary exponential backoff process and thus the contention window size is intact. Therefore, it has rather small delay, compared to the original mechanism.

IV. Conclusion

In this paper, focused on BE service class and contention-based request mechanism, we developed an analytical model to derive a theoretical $T16_{ib}$ timeout. Dissimilar to the original contention-based request mechanism that all unsuccessfully transmitted BW-REQs must perform the truncated binary exponential backoff process, the modified mechanism achieves reduction of collisions and tries by adjusts timeout properly for those successfully transmitted BW-REQs while cannot get grants in the next frame. The modeled timeout is a function of (1) number of BE connections, (2) traffic load, (3) retransmission, (4) collision probability, and (5) bandwidth insufficient probability. Numerical results showed that a suitable timeout does reduce the number of tries, and the average packet delay. Since the failure probability of transmitting BW-REQ decreases and the probability of a BW-REQ being hold increases, the number of tries is reduced. In addition, the range of the backoff value grows exponentially when retry occurs. An SS does not need to wait for the backoff counter counting down to zero for BW-REQ transmission when the BW-REQ is hold by the BS. The average packet delay is lower accordingly. From the numeral and simulation results, when the size of initial contention window approaches the number of contention slots, we could get better average packet delay performance. In our case, we suggest that the contention window size is 8.

Acknowledgment

This work was supported in part by NCTU-MTK Research Center under grant 99Q583, in part by National Science Council under grant NSC 99-2219-E-009-013- and in part by Ministry of Economic Affairs and Industrial Technology Research Institute under grant 99-EC-17-A-03-01-0620.

REFERENCES

[1] IEEE Std. 802.16-2004, "Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems".

[2] IEEE 802.16e-2005, IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, 2006.

[3] Taleb T., Fernandez J.C., Hashimoto K., Nemoto Y., Kato N., "A Bandwidth Aggregation-aware QoS Negotiation Mechanism for Next-Generation Wireless Networks", *IEEE Global Telecommunications Conference*, November 2007, pp.1912-1916.

[4] Lidong Lin, Bo Han and Lizhuo Zhang, "Performance Improvement using Dynamic Contention Window Adjustment for Initial Ranging in IEEE 802.16 P2MP Networks", IEEE Wireless Communications & Networking Conference (WCNC), 2007, pp.11-15.

[5] Jianhua He, Ken Guild, Kun Yang, and Hsiao-Hwa Chen, "Modeling Contention Based Bandwidth Request Scheme for IEEE 802.16 Networks", *IEEE Communications Letters*, Volume 11, August 2007 pp.689-700.

[6] Vinel A., Ying Zhang, Qiang Ni, Lyakhov A., "Efficient Request Mechanism Usage in IEEE 802.16", *Global Telecommunications Conference*, December 2006, pp.1-5.

[7] Wenyan Lu, Weijia Jia, Wenfeng Du, Lizhuo Zhang, "Performance analysis of the contention resolution scheme in IEEE 802.16". Journal of Software, Volume 18, No. 9, pp.2259-2270, 2007.

[8] Sung-Min Oh, Jae-Hyun Kim, "The Analysis of the Optimal Contention Period for Broadband Wireless Access Network", *Pervasive Computing and Communications Workshops*, March 2005, pp.215-219..

[9] Giuseppe Bianchi, Luigi Fratta, and Matteo Oliveri, "Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs," in Proc. IEEE PIMRC, Taipei, Taiwan, Sept. 1996, pp. 392–396.

[10] Hai L. Vu, Sammy Chan, and Lachlan L. H. Andrew, "Performance analysis of Best-Effort Service in Saturated IEEE 802.16 Networks," *Proc. IEEE Vehicular Technology*, Volume 59, No. 1, January 2010, pp.460-472.

[11] Q. Ni, L. Hu. "An Unsaturated Model for Request Mechanisms in WiMAX". IEEE Communications Letters, Vol. 14, No. 1, Jan 2010, pp. 45-47.

[12] Q. Ni, A. Vinel, Y. Xiao, A. Turlikov, T. Jiang. "Investigation of Bandwidth Request Mechanisms under Point-to-Multipoint Mode of WiMAX Networks". IEEE Communications Magazine, Vol. 45, No. 5, May 2007, pp. 132-138.

國科會補助計畫衍生研發成果推廣資料表

日期:2011/03/30

國科會補助計畫	計畫名稱: 異質無線多網安全檢測平台建置計畫(Ⅱ)		
	計畫主持人: 謝續平		
	計畫編號: 99-2219-E-009-013- 學門領域: 通訊軟體及平台(網通國家型)		
研發成果名稱	(中文) 惡意執行檔案檢測系統		
	(英文) Malicious Executable Analyzer		
成果歸屬機構	國立交通大學	發明人(創作人)	謝續平, 王繼偉, 卓政逸, 劉晏如
技術說明	(中文) 惡意執行檔案檢測系統是用來檢測惡意執行檔的鑑識工具，結合多項分析技術來達成完整且精確的檢測報告。其技術大致可包含如下：載入函式庫檢測和資訊熵分析以檢測加殼加密惡意程式。惡意執行檔大多依賴外部函式來讓自身程式碼精簡，故檢測載入函式庫用來檢查出該執行檔是否引用敏感核心函式，例如：創建程序、創建檔案和寫入記憶體等。為了避免被分析，惡意執行檔可採用不同的加殼技術以混淆分析人員的判斷。因此，傳統特徵值比對的方式並不能適用在新穎的惡意執行檔之上。資訊熵利用了統計學的原理來判斷該執行檔是否有混淆內容的企圖，國外學者也有發表相關的研究論文指出該方式的可用性。經過以上的技術分析，該系統將會產出一個詳盡的分析結果，並且提醒使用者該檔案是否為可疑，以避免開啟惡意執行檔。		
	(英文) Malicious Executable Analyzer is a analysis tool for bot executable file and general documents. For files with PE executable format, the tool uses entropy analysis to distinguish packed or encrypted ones from ordinary ones. Also, suspicious APIs imported are listed. These information are reported to users in a clean format so that analysts could be warned before executing malicious documents or executables.		
產業別	其他專業、科學及技術服務業		
技術/產品應用範圍	在2010年，我們提供即時性的線上檢測服務，受惠者除了資安人員、產業界，更包括一般社會大眾		
技術移轉可行性及預期效益	本技術與資策會進行產學合作－惡意軟體行為分析與檢測技術 合作項目：針對「惡意執行檔案檢測系統」進行客製化，提供資策會進行惡意軟體行為分析與檢測		

註：本項研發成果若尚未申請專利，請勿揭露可申請專利之主要內容。

99 年度專題研究計畫研究成果彙整表

計畫主持人：謝續平			計畫編號：99-2219-E-009-013-				
計畫名稱：異質無線多網安全檢測平台建置計畫(Ⅱ)							
成果項目			量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）
			實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比		
國內	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		

		研討會論文	4	0	100%		1. Chia-Wei Hsu, Shiuhpyng Shieh, ’FREE: A Fine-grain Replaying Executions by Using Emulation,’ The 20th Cryptology and Information Security Conference (CISC 2010), Taiwan, 2010. (Best Student Paper Award) 2. B.T. Chen and Y.L. Huang, ’The Design and Implementation of a Multi-core Supported Network Intrusion Detection System’, The 20th Cryptology and Information Security Conference (CISC 2010), Taiwan, 2010. 3. 蔡欣宜、王繼偉、陳柏廷、黃育綸、謝續平,平基於虛擬裝置之無線網路安全測試平台’, The 20th Cryptology and Information Security Conference (CISC 2010), Taiwan, 2010. 4. 王繼偉、王嘉偉、許家維、謝續平,’基於虛擬機器外部觀察與映像檔比對的惡意程式分析，對 The 20th Cryptology and Information Security Conference (CISC 2010), Taiwan, 2010.
		專書	0	0	100%		

	專利	申請中件數	3	0	100%	件	1. 劉家隆、邱碧貞、趙禧綠、周詩梵，’ 長程演進技術網路的量測回報機制’，臺灣專利申請中。 2. 黃士一、謝續平、王繼偉，’輕量網路安全認證機制及秘密資料擷取方法與其應用’，臺灣專利申請中。 3. 黃士一、謝續平，’無線感測器網路中安全資料聚合的方法和系統’，臺灣專利申請中。
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（本國籍）	碩士生	21	0	100%	人次	
		博士生	9	0	100%		
		博士後研究員	0	0	100%		
		專任助理	5	0	100%		

國外	論文著作	期刊論文	7	0	100%	篇	1. H.Y. Lin and W.G. Tzeng, ’A Secure Decentralized Erasure Code for Networked Storage Systems,’ IEEE Transactions on Parallel and Distributed Systems, (accepted), 2010. 2. T. Klove, T.T. Lin, S.C. Tsai, and W.G. Tzeng, ’Permutation Arrays Under the Chebyshev Distance, ’ IEEE Transactions on Information Theory 56(6), pp.2611-2617, 2010. 3. C.L. Hou, C. Lu, S.C. Tsai, and W.G. Tzeng, ’An Optimal Data Hiding Scheme with Tree-Based Parity Check,’ IEEE Transactions on Image Processing, (accepted), 2010. 4. Ming Hour Yang, Shiuhpyng Shieh, ’Tracing Anonymous Mobile Attackers in Wireless Network,’ JDCTA: International Journal of Digital Content Technology and its Applications, Vol. 4, No. 4, pp. 161-174, 2010. 5. Shih-I Huang and Shiuhpyng Shieh, ’Secure Encrypted-Data Aggregation for Wireless Sensor Networks,’ accepted for publication, ACM Journal of Wireless Networks. 6. Chi-Wei Wang and

		研究報告/技術報告	0	0	100%		

		研討會論文	5	0	100%		1. Shih-Fan Chou, Jen-I Liu, I-Lu Chao, Tzu-Chi Guo, Chia-Lung Liu, and Feng-Jie Tsai, ’Analytical Modeling of Timeout for Contention-Based Bandwidth Request Mechanism in IEEE 802.16 WiMAX Networks,’ IEEE LCN, 2010. 2. Shih-Fan Chou, Jen-I Liu, I-Lu Chao, Tzu-Chi Guo, Chia-Lung Liu, and Feng-Jie Tsai, ’Performance Enhancement of Contention-Based Bandwidth Request Mechanism in IEEE 802.16 WiMAX Networks,’ IEEE PIMRC, 2010. 3. Ming-Pei Hsu and I-Lu Chao, ’Positioning with Reusability Improvement for Millimeter Wave Based Wireless Personal Area Networks,’ IEEE ICC, 2010. 4. Shuhua Jiang and I-Lu Chao, ’Linear Cooperative Detection for Alarm Messages in Vehicular Ad Hoc Networks,’ IEEE WCNC, 2010. 5. Wei Shi-Sue, Shiuhpyng Shieh, Chin-Wei Tien, ’A Framework Using Fingerprinting for Signal Overlapping-Based Method in WLAN,’ accepted for

		專書	0	0	100%	章/本	
	專利	申請中件數	3	0	100%	件	1. S.I. Huang, S.P. Shieh, and C.W. Wang, ' Light-Weight Authentication and Secret Retrieval Scheme and Its Applications,' USA patent pending. 2. S.I. Huang and S.P. Shieh, ' Method and System for Secure Data Aggregation in Wireless Sensor Networks,' USA patent pending. 3. S.I. Huang and S.P. Shieh, ' 無線感測器網路中安全資料聚合的方法和系統,' 大陸專利申請中。
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（外國籍）	碩士生	2	0	100%	人次	
		博士生	1	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		
其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)		1.本計畫榮獲網路通訊國家型計畫 99 年優良研究計劃 2.主辦 2010 年暑期資安課程,邀請國內資安學者 13 人,國外學者 6 人授課,吸引國內大專院校資工相關系所學生 126 人參予修課 3.辦理第二十屆全國資訊安全會議.					

	成果項目	量化	名稱或內容性質簡述
科教處計	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	

畫加填項目	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與（閱聽）人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標

□未達成目標（請說明，以 100 字為限）

□實驗失敗

□因故實驗中斷

□其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 □撰寫中 □無

專利：□已獲得 ■申請中 □無

技轉：□已技轉 ■洽談中 □無

其他：(以 100 字為限)

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）(以 500 字為限)

本計畫主要目的在於建置一異質多網安全檢測平台，並在此平台下開發完整的安全檢測工具與系統，以提供使用者安全的網路使用環境。異質多網安全檢測平台下開發的工具可分為四大檢測類別：(1)系統安全檢測、(2)網路安全檢測、(3) 軟體安全檢測以及(4)人員安全意識檢測。系統安全檢測提供了遠端系統安全漏洞檢測及網站伺服器的安全漏洞檢測等工具；網路安全檢測提供了應用於 WiMAX 掃描系統及無線網路金鑰的強度檢測等工具：軟體安全檢測提供了目前行動裝置經常使用的 Android 及 Java 應用軟體的檢測以及病毒與惡意程式的工具；人員安全意識檢測則提供了檢驗一般使用者安全意識的網路釣魚檢測及無線網路安全意識檢測工具。藉由本計畫所建置之安全檢測平台，可滿足國內目前對於不同層面的安全檢測需求。