以網路流量資料探勘進行阻斷服務攻擊偵測之研究

蕭漢威
高雄大學資訊管理學系

楊錦生
中山大學資訊管理學系

魏志平
清華大學科技管理研究所

馬淑貞
台灣電力公司大林發電廠

摘要

隨著網際網路與電子商務的蓬勃發展，網路安全的議題日趨重要，在眾多網路安全事件中，阻斷服務攻擊(Denial of Service)為近年來造成網路傷害的主要原因之一。阻斷服務攻擊主要是由攻擊者對特定目標傳送大量封包來進行攻擊，使得被攻擊者無法提供服務給正常的使用者，其影響範圍除造成正常使用者無法使用網路服務外，更可能造成進一步的商業損失。在這樣的環境下，如何有效的偵測出阻斷服務攻擊事件，並進行適當的防禦，對於網路管理人員而言是一項迫切且必須的工作。阻斷服務攻擊經常會使用 IP Spoof 的技術，以偽造的來源 IP 來進行攻擊，使得網路管理者無法輕易的找出攻擊來源，並使以網路第三層資訊為基礎的入侵偵測系統無法有效進行防禦。為能有效地偵測網路中的阻斷服務攻擊事件，並克服 IP Spoof 可能造成的偵測困難，本研究以網路設備的 SNMP 流量為基礎，運用資料探勘中的分類分析技術，提出了一個阻斷服務攻擊偵測及防禦系統，並以實際企業網路和學校宿舍網路來評估系統的偵測效能。評估結果顯示，本研究所提偵測系統可以達到相當好的預測準確率，在企業和學校宿舍網路環境下，其準確率分別可達到 99.78%與 98.59%以上，且遺漏率與誤報率也控制在相當低的程度。

關鍵詞：網路安全、阻斷服務攻擊、攻擊偵測、資料探勘

Mining Network Traffic Data for Supporting Denial of Service Attack Detection

Han-Wei Hsiao
Department of Information Management, National University of Kaohsiung

Chin-Sheng Yang
Department of Information Management, National Sun Yat-sen University

Chih-Ping Wei
Institute of Technology Management, National Tsing Hua University

Shu-Chen Ma
Talin Power Station, Taiwan Power Company

Abstract

With the advances in networking technologies, organizations have increasingly participated in or shifted to the Internet environment to conduct business transactions. According to prior research on E-business, network security is one of the key factors for E-business success. Denial of service (DoS) attack, which aims at rendering a computer or network incapable of providing normal services, is a major cause of current network insecurity. Existing DoS attack defense mechanisms (e.g., firewalls and intrusion detection systems) typically rely on packet information gathered from gateways of network systems. Because such packet information is on the IP-layer or above, existing defense mechanisms are incapable of detecting internal attacks or attackers who disguise themselves by spoofing source IP addresses. To address the aforementioned limitations of existing DoS attack defense mechanisms, we propose a classification-based DoS attack detection technique to induce a DoS detection model on the basis of the SNMP data. The constructed DoS detection model is then used for predicting whether a network traffic flowing through a network interface is a DoS attack. To empirically evaluate our proposed classification-based DoS attack detection technique, we collect network traffic data from two different environments, including an enterprise network and a university campus network. Our empirical evaluation results show that the detection accuracy of the proposed technique reaches 99.78% and 98.59% or above in both network environments respectively.

Keywords: Network Security, Denial of Service (DoS), Attack Detection, Data Mining

壹、緒論

由於網際網路科技及其應用蓬勃發展，相關的電子商務和網路服務已逐漸成為企業經營或日常生活中重要的一環。根據經濟部技術處每年定期委託資策會 ACI-FIND 所進行的大型抽樣調查結果顯示，在 2004 年我國整體企業連網普及率已達 81.1%，區域網路(LAN)的建置普及率達 55%，企業網站的建置普及率達 35.7%，以及企業內網路(Intranet)的建置普及率達 33.6%。這份調查結果也顯示，超過四成企業表示電子化對於企業間業務流程帶來明顯的效益(鄭仁富, 2005)。

根據 Kim et al. (2002)與 Ranganathan & Ganapathy (2002)的研究指出，網路安全是影響電子商務成功與否的最重要因素之一。然而根據電腦網路危機處理暨協調中心(Computer Emergency Response Team/Coordination Center, CERT/CC)的統計顯示，2003 年之網路安全事件回報件數即高達 137,529 件(CERT/CC 2004)。此外 Computer Security Institute 在 2004 年所進行電腦犯罪與安全調查報告中指出，在 486 家受訪企業中，有 53%的企業表示組織內的電腦系統曾發生未經授權使用的情形，且其中 269 家企業回報因網路安全所造成的金錢損失高達 1 億 4 千多萬美元 (Lawrence et al., 2004)。上述的統計資料意味著在現今的網際網路環境中，網路安全仍面臨著許多重大的考驗。

網路安全相關研究指出，導致 2004 年網路安全損失的主因，涵蓋了程式漏洞、蠕蟲、間諜程式、阻斷服務(Denial of Service, DoS)攻擊、網路犯罪等手法(徐國祥, 2005)。而 2005 年網路威脅還是跳脫不了 DoS 攻擊、網路傳輸等攻擊模式，而且 DoS 攻擊威脅可能會倍數地增長。由此可知，阻斷服務攻擊是一項影響鉅大的網路安全議題。根據 CERT/CC (2001c)的定義，DoS 攻擊為試圖讓某個網路服務的合法使用者，無法正常地使用該服務的一種行為。DoS 攻擊的發生，除了造成合法使用者無法正常地使用服務外，更可能造成進一步的商業損失。以發生於 2000 年 2 月的 DoS 攻擊事件為例，著名網路巨擘雅虎公司(Yahoo!) 2 月 8 日遭駭客襲擊，Yahoo!的搜尋引擎和入口網站因此停頓將近三小時，是 Yahoo!有史以來最嚴重的當機，當機期間有數百萬網友無法由雅虎獲取資訊服務。在 Yahoo!遭駭客攻擊後二十四小時內，美國另二個著名網站 buy.com 和 eBay 也遭受類似手法的襲擊。此外，著名的購書網站 amazon.com、知名新聞網站 CNN.com、網路券商 E-Trade 和 Datek，以及科技新聞網站 ZDNet 也在此後數天內相繼遭受攻擊。這起網路攻擊事件，除了造成多家知名網路服務公司及其顧客的權益受損外，美國道瓊工業平均指數也因為一週來的駭客攻擊事件而重挫 258.44 點，以及那斯達克指數也下跌了 64.26 點。

針對 DoS 攻擊之防禦，現有的技術主要著重在消除 DoS 攻擊程式所利用的網路弱點、不安全設計或其形成原因，使 DoS 攻擊存在的客觀環境範圍縮小，以達到避免或減低 DoS 攻擊發生的機會(CERT/CC, 2001c)。CERT/CC (2001c)建議的防禦方式主要有幾項，包括利用過濾機制來預防 DoS 攻擊之發生、 隨時修補網路設備或主機的漏洞、關閉不必要的網路服務、啟用作業系統的資源限制功能、安裝必要的入侵偵測

系統、防火牆或防毒軟體等。這些防禦措施若徹底地執行，或許可以防範大部分已知的 DoS 攻擊方式，然而並無法完全防止新類型 DoS 攻擊事件的發生。此外，上述防禦措施的施行，需依賴網路管理者與使用者的高度網路安全管理動機方可達成。然而現實情況中，並非所有管理者或使用者都具有高度的網路安全管理動機與施行所需的資源與能力，例如組織對於資訊安全可能有不同的認知、處理能力及預算，因而不一定會建構防火牆、入侵偵測系統設備，或建置其他封包過濾系統。而對非商用的個人電腦或校園電腦網路使用者而言，可能更難達成上述的防禦措施，例如要求使用者安裝防毒軟體或修補程式等，可能會因使用者的安全認知及資訊能力的差異而無法順利進行。有鑒於防禦 DoS 攻擊發生的各項方案之發揮成效可能有限的情形下，阻斷服務攻擊仍將繼續存在(W3C, 2003)。在這樣的背景下，發展有效的偵測技術，將可協助系統不幸遭遇阻斷服務攻擊時，可以早期的發現，以利進行相關的處置，減少受攻擊主機或其所在網段的影響。

現有 DoS 攻擊偵測技術主要可分成幾類：以封包內容(Packet Content)為基礎、以伺服主機日誌(Server Log)為基礎及以網路流量(Network Traffic)為基礎等三種偵測方法，分別說明如下。1) 以封包內容為基礎的偵測方法：其使用網路封包的內容作為偵測資訊來源，藉由檢查封包內是否包含事先定義的 DoS 攻擊特徵值，來進行 DoS 攻擊之偵測(Rahmani et al., 2004; Wang et al., 2004; Mukkamala & Sun, 2003)。該技術存在一些缺點，例如若以監測設備來進行封包之蒐集，則只能偵測到監測設備所在的網段，若是攻擊事件並不發生在監測設備的網段中，則無法進行偵測。假若採用網路設備來檢查流經的封包，因為進行封包內容(或流量狀態模型)的比對需要進行大量的運算，因此若是比對方式過於複雜，或是流經的封包數量過大時，就會使得網路安全設備所在的位置形成流量瓶頸，因而降低網路的傳輸效能。2) 以伺服主機日誌為基礎的偵測方法：其主要是藉由檢查提供服務的伺服主機或應用程式之系統日誌，來判定是否發生 DoS 攻擊。此類技術的缺點在於偵測範圍較為侷限，無法偵測到伺服主機以外的網路範圍。同時對於 TCP SYN Flood 這類不會產生完整連線的攻擊方式，因日誌中不會留下紀錄，所以也無法進行阻斷服務攻擊之偵測。3) 以網路流量為基礎的偵測方法：其利用網路傳輸設備(例如路由器、交換器)所提供的流量傳輸資訊(例如 SNMP、NetFlow 等)來進行 DoS 偵測。相較於以封包內容與以伺服主機日誌為基礎之 DoS 攻擊偵測技術，利用網路流量來偵測 DoS 攻擊，可以避免上述的大部分缺點。然而現有以網路流量為基礎的偵測方法，大多必須定義正常網路行為以進行偵測，可是在快速演進的網路環境下，經常會有不同的攻擊事件發生，並且在不同的網路環境中，所謂的正常網路使用行為可能存在著相當大的差異(例如，在商業公司網路與大學校園網路，正常網路行為可能是很不相同的)。因此，要定義有代表性的正常網路行為，是具有相當的挑戰性與困難度。

基於上述對 DoS 攻擊偵測系統的需求與現有偵測技術的優缺點之分析，本研究試圖以網路流量資料，配合資料探勘中的分類分析技術，建構一個有效的 DoS 攻擊偵測系統。本研究並實際蒐集企業網路與校園網路環境內的相關流量資料，以驗證所提偵

測系統的效能。本文後續章節的內容簡述如下，第二章將針對 DoS 攻擊偵測及防禦的相關文獻進行探討，第三章將詳述本文所提出的 DoS 攻擊偵測及防禦系統之架構，第四章說明所提系統架構中的 DoS 攻擊預測模式效能之實證評估工作與結果，最後將於第五章中描述本研究結論與未來研究方向。

貳、文獻探討

本章透過國內外文獻之蒐集與分析，探討阻斷服務攻擊(DoS)的相關研究。內容包括 DoS 攻擊之定義與分類，DoS 攻擊之偵測技術，以及不同偵測技術存在的缺點與限制。

一、阻斷服務攻擊 (Denial of Service, DoS)

根據 CERT/CC (2001c)及 Mirkovic & Reiher (2004)的定義，“A *denial of service* attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service”，意指試圖讓某個網路服務的合法使用者，無法正常地使用該服務。如圖 1 所示，在 DoS 攻擊之分類上，主要可以依攻擊的對象、攻擊的弱點與攻擊的架構來進行分類。

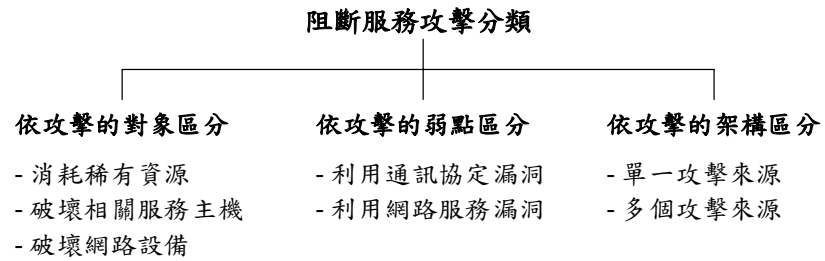

圖 1：阻斷服務(DoS)攻擊分類

1. 依攻擊對象之阻斷服務攻擊分類

依攻擊對象而言，可以將 DoS 攻擊分為三種模式，分別為消耗稀有資源、破壞相關服務主機或破壞網路設備(CERT/CC, 2001c) 以消耗稀有資源為目標的 DoS 攻擊方式，主要是試圖消耗電腦或網路賴以執行的稀有資料(例如網路頻寬、記憶體或磁碟空間、CPU 運算能力等)，以達到影響網路服務合法使用者的目的。常受到攻擊的稀有資源包括網路連線服務能力與網路頻寬：

(1) 網路連線服務：DoS 攻擊針對服務提供者必須對每一個連線保留一些系統資源(包括記憶體、執行程序等)的特性，傳送大量非正常連線要求到服務提供者，藉以消耗服務提供者的系統資源，當系統資源耗盡時，則服務提供者無法提供連線服務給正常的連線要求。這類攻擊的典型範例是 TCP SYN Flood 攻擊，該攻擊方式為發送大

量要求連線的 SYN Request 到攻擊目標，當攻擊目標送回 SYN-ACK Response 後，攻擊端卻不發送最後的 Acknowledgment 回應，讓三向交握(3-way Handshaking)無法完成，使得攻擊目標的 SYN Queue 儲存太多正在等待連結的資訊而超過其容許量，導致服務暫停(CERT/CC 2000)。

(2) 網路頻寬：此類 DoS 攻擊藉由產生大量的封包，耗盡網路頻寬，使一般封包無法正常傳送，以達到影響正常服務的目的。典型的攻擊範例是 ICMP DoS 攻擊或 UDP Flood DoS 攻擊。其方式是假冒來源 IP，對網段內發出 Broadcast ICMP Request 或 UDP Request 封包，使網段內被回應封包塞滿，且導致網路系統無法傳送正常資訊封包。

以破壞相關服務主機為目標的 DoS 攻擊方式並不直接攻擊目標主機，而是藉由破壞與攻擊目標相關的其他服務主機，使被攻擊的目標無法正常運作。例如破壞 DNS 主機，使得網路上的使用者無法順利以網域名稱(Domain Name)查詢到提供服務的 IP 位址，藉此間接攻擊的方式，造成被攻擊的目標無法提供正常的網路服務。最後，以破壞網路設備為目標的 DoS 攻擊方式，採用攻擊目標主機對外連線必經的網路設備，使其無法正常運作，進而造成被攻擊的主機中斷對外連線，影響其正常運作。例如攻擊網路上的路由器，使其無法運作，則所有連接到這個路由器上各網段內的主機都無法與外界連線，藉以達成攻擊的目的。

2. 依攻擊弱點之阻斷服務攻擊分類

若依 DoS 攻擊利用的弱點，則可分成二類，分別為利用通訊協定(Protocol)漏洞與利用網路服務漏洞之 DoS 攻擊。

利用通訊協定漏洞之 DoS 攻擊方式，主要是利用 TCP/IP 網路上各種通訊協定的設計缺失，來進行阻斷服務行為(Paxson, 2001)。依通訊協定的不同，主要可以分為 TCP、UDP 與 ICMP DoS 攻擊三類：

(1) TCP DoS 攻擊：主要是藉由攻擊主機發送大量的正常或不正常的 TCP 網路封包，造成被攻擊的目標主機當機、重新啟動，或是目標網段的交通壅塞，致使該主機無法繼續進行服務。目前常見的 TCP DoS 攻擊主要有三種攻擊途徑，分別為 Land 攻擊、Teardrop 攻擊與 TCP SYN Flood 攻擊。Land 攻擊是由攻擊者發送一假冒的 Connection Request (SYN)封包到被攻擊端，並刻意將此封包的來源端和目的端的 IP 位址設定為相同，而且來源端和目的端的通信埠亦設定為相同，如此將會使得被攻擊目標誤以為是它本身送此封包給自己，進而造成被攻擊端電腦當機。Teardrop 攻擊基本上是利用封包分割和重組間的漏洞，而產生的攻擊方式。根據在 IP 層中定義的封包分割和重組的規則：「分割後的封包大小必須小於傳輸介面的 MTU (Maximum Transfer Unit，最大傳送單位)，並且符合以 8 byte 為單位的倍數」。因此，正常的 TCP 封包片段應該是一個個以互相接續的方式傳入目標主機，再由主機的 IP 層將其重組回原資料段。但如果有經過刻意製造的不正常封包序列(如，封包大小改變等)，則有可能會造成某些作業系統的當機或暫停服務(CERT/CC, 1997)。最後，TCP SYN Flood 的攻擊方法是以發送大量要求連線的 SYN Requests 到攻擊目標，而當該伺服器送回 SYN-ACK Response 後，攻擊端卻不發送最後的 Acknowledgment 回應，讓三向交握(3-way

Handshaking)無法完成，藉此消耗用來記錄新連線的緩衝區(Buffer)之記憶空間，造成伺服器超載或當機(CERT/CC, 2000)。

(2) UDP DoS 攻擊：UDP DoS 攻擊又稱為 Fraggle 攻擊，主要是透過 UDP Protocol 送出假造來源端資訊的 UDP Broadcast 封包至目標網路，當目的網域中有眾多主機回應之後，將產生放大的資料流，以造成網路的壅塞。

(3) ICMP DoS 攻擊：ICMP DoS 攻擊包含 Ping of Death 攻擊與 Smurf 攻擊兩種攻擊方式。首先，Ping of Death 攻擊方法主要是利用網路程式 Ping，將過長的資料送到攻擊目標後，假如接收資料的主機系統(TCP/IP Stack)並沒有對所接收的資料做好長度限制，而使得在處理資料時，把過多的資料覆蓋到系統其它部份的資料，那麼就有可能會造成主機系統發生錯誤，進而造成當機或是重新開機。其次， Smurf 攻擊方式主要是直接對網路進行廣播，造成網路很快地充滿垃圾封包而中斷。Smurf 會不斷地將小量偽造的 ICMP Request 封包送給 IP 廣播位址(IP Broadcast)，然後廣播位址會傳回大量 ICMP Response 封包給目標電腦。這種 Smurf 的攻擊方式除了攻擊特定目標主機，也能在網路上塞滿 ICMP 的 Request 與 Response 封包，而造成網路中斷。

利用網路服務漏洞之 DoS 攻擊方式，主要是利用網際網路上各種服務程式的漏洞來進行攻擊行為。網路服務主要經由伺服主機上的服務程式來完成，這些服務程式在設計上若存在漏洞，就可能成為入侵者進行入侵動作的最佳入口，同時也是許多網路蠕蟲病毒(例如紅色警戒(CERT/CC, 2001a)與娜坦病毒(CERT/CC, 2001b))的攻擊目標。這類的蠕蟲病毒若成功侵入一個服務程式的漏洞後，便不斷地發送封包，試圖感染網路上其他的主機。蠕蟲病毒攻擊常會造成大量的病毒封包在網路上傳遞，這樣的封包傳送雖非針對某一特定主機，但往往會造成阻斷服務的效果。

3、依攻擊架構之阻斷服務攻擊分類

以攻擊架構的角度來看，可分為單一攻擊來源與多個攻擊來源的 DoS 攻擊。首先，單一攻擊來源之攻擊架構是由單一的攻擊主機來發起，利用上述的任一種通訊協定攻擊方式，在瞬間以大量的攻擊封包壓迫被攻擊主機，耗損其網路資源，使得合法使用者無法正常地使用該服務。其次，多個攻擊來源之攻擊方式又稱為分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)。DDoS 攻擊是利用許多分散各處的 DoS Agent(攻擊代理人)，在某一時間點，同時對特定目標主機前述任一種攻擊技術或混和方式，將大量封包傳入目標網域，以阻斷被攻擊者的服務功能。其手法特別之處是必須先選定一定數目的主機，入侵並植入 DoS Agent 程式，並在攻擊發起時遠端操控它們的行為。

二、阻斷服務攻擊之偵測

本節針對現有 DoS 攻擊之偵測技術進行探討，藉以了解現有 DoS 攻擊偵測技術之進行方式，並且分析現有偵測技術存在的缺點，以作為本研究發展新的 DoS 攻擊偵測架構的參考依據。阻斷服務攻擊之偵測屬於入侵偵測(Intrusion Detection)之一種。依照偵測時使用的資訊來源而言，主要可以分成三種：(1) 以封包內容(Packet Content)

為基礎的偵測方法、(2) 以伺服主機日誌(Server Log)為基礎的偵測方法與(3) 以網路流量(Network Traffic)為基礎的偵測方法。

以封包內容為基礎的偵測方法，是利用封包的內容來偵測網路上是否發生 DoS 攻擊。封包的來源主要有二：一為在網路上架設監測設備，以擷取網路上的封包來進行偵測。例如利用網路上所架設的 Sniffer 或是 Tcpdump 的資料來做為 DoS 偵測的基礎；另一為利用網路安全設備來進行偵測，例如利用網路上的防火牆或是 NAT (Network Address Translation)伺服器，來檢查所有流經此安全設備的封包。使用此類偵測資料的偵測技術，主要包括傳統入侵偵測系統(Intrusion Detection Systems, IDS)所採用的特徵值比對(Signature-based)偵測技術(Rahmani et al., 2004; Wang et al., 2004)。這類型的偵測技術主要是檢查監測設備或網路安全設備所擷取到的完整封包，比對封包內容是否含有事先定義好的 DoS 攻擊特徵值，以作為判別是否為 DoS 封包。

以封包內容為基礎之偵測方法存在一些缺點，例如若以監測設備來進行封包之蒐集，只能偵測到監測設備所在的網段，若是攻擊事件並不發生在監測設備的網段中，則無法進行偵測。假如採用網路安全設備來檢查流經的封包，因為進行封包內容(或流量狀態模型)的比對需要進行大量的運算，因此若是比對方式過於複雜，或是流經的封包數量過大時，就會使得網路安全設備所在的位置形成流量瓶頸，因而降低網路的傳輸效能。此外 Signature-based 偵測方式有個嚴重的缺點，此類型的偵測系統需要事先定義好 DoS 攻擊的特徵值，因此當出現新的攻擊方式時，因為在特徵資料庫中並不存在新攻擊方式的特徵值，所以無法有效的偵測出新的攻擊方式。

以伺服主機日誌為基礎的偵測方法，主要是利用提供服務的伺服主機之系統日誌與應用程式日誌資料為基礎，使用 Signature-based 偵測技術，來判定是否發生 DoS 攻擊或其他攻擊事件。例如利用網頁伺服主機(Web Server)日誌中的記錄，可以發現是否發生 Code Red 病毒的發作，以及已經中毒的主機。由於此類 DoS 攻擊偵測技術使用伺服主機日誌來進行，因此僅能針對該伺服主機進行偵測工作，無法偵測到伺服主機以外的網路範圍。此外，對於某些特定類型的 DoS 攻擊，本類偵測技術亦無法有效偵測。例如利用通訊協定漏洞來進行的 TCP SYN Flood 攻擊，因這類攻擊方式並不會產生完整連線，所以不會在伺服主機日誌中留下紀錄，因此以伺服主機日誌為基礎的偵測方法，並無法有效地偵測此類型的 DoS 攻擊。

最後，以網路流量為基礎的偵測方法，主要是利用網路傳輸設備(例如路由器、交換器)所提供的流量傳輸資訊(例如 SNMP、NetFlow、SFlow、RMON 等)作為偵測的基礎。在偵測技術上，主要可以利用異常偵測中之 Anomaly-based 技術來偵測流量狀態是否正常。這種技術主要是藉由蒐集過去的正常使用資料，利用統計方法來建立網路的正常狀態模型，然後比較監控中的網路狀態與正常狀態模型的差異，以差異是否超過了正常狀態的某一門檻值，來判定是否有 DoS 攻擊發生(Yau et al., 2005)。另外，也可以建立 DoS 攻擊模型，若監控中的網路狀態與 DoS 攻擊模型相似時，則可判定發生 DoS 攻擊(Rahmani et al., 2004)。例如，Barford 等人(2002) 利用 SNMP 及 NetFlow 的資料，以 Wavelet Analysis 的方法，分析網路上異常狀況的發生。

現有以網路流量為基礎之偵測方法的缺點在於，Anomaly-based 偵測技術的重點在於定義什麼是正常網路行為，然而在快速演進的網路環境下，經常會有不同的攻擊事件以及新的蠕蟲病毒感染，並且在不同的網路環境中，所謂的正常網路使用行為是非常不相同的(例如，在商業公司網路與大學校園網路的環境下，因為使用者行為是非常不相同的，所以其網路的正常狀態模型也不盡相同)，因此，要定義有代表性的正常網路行為，並以同一種的統計方法，在不同的網路環境中，建立一個有效的正常狀態模型，是相當具有挑戰性的。

考量上述現有 DoS 偵測的缺點與限制，本研究決定採用網路流量資料作為偵測基礎，輔以資料探勘的分類分析技術，來進行 DoS 攻擊偵測。使用網路流量資料的原因，在於網路流量資料可以避免封包內容或伺服主機日誌為基礎之偵測方法所產生的缺點；而採用資料探勘的分類技術之原因，在於可以避免 Anomaly-based 偵測方式在建立正常狀態模型時所面臨的困難。

參、阻斷服務攻擊之偵測與防禦系統架構

根據文獻中所探討對於各種 DoS 攻擊類型的了解與歸納，以大量連線要求攻擊稀有資源的 DoS 攻擊，均會產生大量網路流量的特徵，亦即在內部網路中成為 DoS 攻擊對象或跳板的電腦主機，在攻擊發起時，將有比平常大量的網路流量進入網路交換器實體介面。因此本研究假設，發生 DoS 攻擊的交換器實體介面網路流量，與其他正常使用之交換器實體介面網路流量有差異。然而每一個正常使用之交換器實體介面，也可能因為網路使用行為的差異，而有不同的正常網路流量水準。因此在本研究中，必須要建立能分辨正常網路流量與 DoS 網路流量的機制。資料探勘的分類分析方法是利用已知類別的訓練資料，分析訓練資料之屬性值與其類別的關係，以建立分類模式，並以此分類模式，對新的資料進行類別的判定(Elson, 2000; Mukkamala et al., 2003)。本研究將分辨正常網路流量與 DoS 網路流量的機制視為一分類問題，也就是利用已知分類的正常網路流量與 DoS 網路流量，建立分類模式，據以預測新的網路流量是否為 DoS 攻擊的網路流量。圖 2 為本研究所提出的 DoS 攻擊偵測與防禦系統架構。

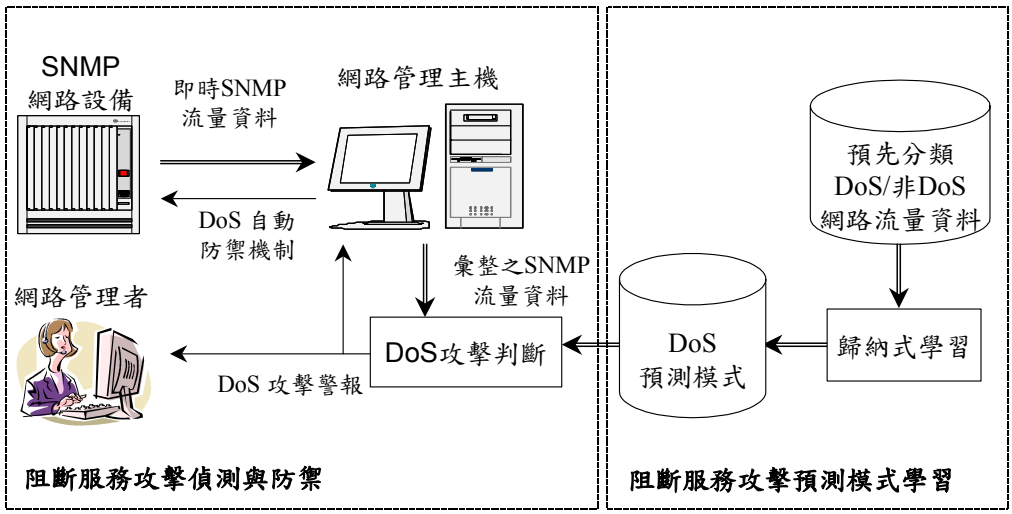

圖 2：阻斷服務(DoS)攻擊偵測與防禦系統架構

一、阻斷服務攻擊預測模式之學習

如圖 2 所示，阻斷服務攻擊預測模式學習包括預先分類 DoS/非 DoS 網路流量資料、歸納式學習及 DoS 預測模式。本研究使用的 DoS/非 DoS 網路流量資料蒐集自網路設備的 SNMP 流量資料。SNMP 為簡易網路管理協定(Simple Network Management Protocol)之簡稱，是管理 IP 網路上各種裝置的 Internet 標準協定(Mauro et al., 2001)。它讓網路上不同的設備，產生具有共通標準，且可提供網路管理的資料。這些資料，可進一步由網管應用程式來讀取或是進行監控；也就是說，只要網路設備上擁有 SNMP 代理人(Agent)之機制，我們就可以使用網路管理軟體，透過這些代理人，檢視或監控其設備上的相關網管資訊。SNMP 適用於各類型的網路設備，但隨著不同的網路及設備，SNMP 所管理的資訊及對資料的表達方式而有所不同。為將這些資訊納入同一套管理系統中，SNMP 定義了網管資訊庫(Management Information Base，簡稱 MIB)，階層性地描述所有受管理資訊的屬性，並稱這些受管理的資訊為 SNMP 物件。

本研究使用的 SNMP 流量資料來自於 MIB-2 下的 Interfaces 類別。如表 1 所示，我們自 Interfaces 類別中選取 12 個與流量相關的變數，作為本研究所提 DoS 攻擊預測模式之學習變數。

表 1：SNMP 流量資料變數及說明

變數名稱	說明
ifInOctets	流入的 bytes 數
ifInUcastpkts	流入的 unicast 封包數
ifInNUcastpkts	流入的非 unicast 封包數
ifInDiscards	流入的 discard 封包數

ifInErrors	流入的 error 封包數
ifInUnknownProtos	流入的不確定通訊協定封包數
ifOutOctets	流出的 bytes 數
ifOutUcastpkts	流出的 unicast 封包數
ifOutNUcastpkts	流出的非 unicast 封包數
ifOutDiscards	流出的 discard 封包數
ifOutErrors	流出的 error 封包數
IfOutQlen	外送佇列的長度(封包數)

根據 SNMP 的標準定義,“IfInOctets”表示在實體介面所接收的 Byte 數,包括 MAC 層的訊框 Byte 數量。“ifInUcastpkts”表示實體介面所接收到且將傳送給上層(如 IP 層)通訊協定的子網路內部單點廣播封包數。“ifInNUcastpkts”表示實體介面所接收到且將傳送給上層(如 IP 層)通訊協定的子網路內部非單點廣播(包括子網路內部廣播或子網路內群播)封包數。“ifInDiscards”表示進入實體介面而被丟棄的封包數量(包含並無任何錯誤但被丟棄的封包)。造成實體介面丟棄封包的可能原因之一是實體介面的暫存區已滿(例如，當攻擊發生時，即有可能造成封包流量大於實體介面的暫存區)，無法再接收新的封包。 “IfInErrors”表示進入實體介面含有錯誤(利用 IP Checksum 判斷是否有錯誤)而未被往上層通訊協定傳送的封包量。“ifInUnknownProtos”表示進入實體介面，因為無法解讀或不支援而被丟棄的封包數量。

當某一個網路節點產生 DoS 攻擊時，攻擊程式所產生的大量通訊流量(如 TCP Acknowledgement、UDP Broadcast、ICMP Broadcast 等)會被包裝成 IP Datagram(通常使用偽造來源 IP 位址)，再以 Ethernet 訊框包裝，並經由網路交換器實體介面傳入網路系統，實體介面 SNMP Agent 上 MIB-2 變數會記錄這些傳入網路系統的流量資訊，而反應出在短時間內產生大量傳出流量資訊的事實或網路行為，例如，TCP SYN Flood 攻擊會在瞬間產生大量的短 IP 封包(即 TCP SYN 封包)，此時實體介面的流量變數“IfInOctets”及“ifInUcastpkts”與正常流量的相同變數相比，將呈現極大差異。這些傳入網路系統的流量資訊即是被記錄於上述六項變數，因此將其列入描述網路流量的相關屬性變數。

而 “ifOutOctets”表示經由實體介面傳送出去至資訊節點的 Byte 數量，包含 MAC 層的訊框 Byte 數量。“ifOutUcastpkts”表示上層(如 IP 層)通訊協定要求實體介面傳送出去至子網路內部單點廣播封包數，包含被丟棄或沒有送出的封包數。“ifOutNUcastpkts”表示上層(如 IP 層)通訊協定要求實體介面傳送至子網路內部非單點廣播封包數，包含被丟棄或沒有送出的封包數。“ifOutDiscards”表示未被實體介面傳出而丟棄的封包數，造成實體介面丟棄封包的可能原因之一，是實體介面的暫存區已滿，無法再傳送新的封包。例如被攻擊點所連接的實體介面，若在短時間內回應大量封包流量且大於實體介面的暫存區時，某些封包即被丟棄，而被丟棄的封包量會被記錄於此變數。“ifOutErrors”表示因封包錯誤而沒有被實體介面傳送出去給資訊節點的封包數。“IfOutQlen”表示要透過實體介面送出的封包佇列(Queue)長度(封包數量)，DoS 攻擊流量可能使此變數的封包佇列長度一直保持上限。

當網路上某些資訊節點遭受 DoS 攻擊時，資訊節點所連接的網路交換器實體介面，極可能反應大量傳送出的網路流量，所以可以假設若被 DoS 攻擊時的網路行為，會對上述六項實體介面外傳資料流量的相關變數有所影響。因此可將其列入描述網路流量的相關屬性變數中。

在完成變數的選擇與定義後，本步驟的另一個重點在於歸納學習。本研究利用表 1 的 12 個預測變數，以資料探勘中分類分析的技術，來進行阻斷服務攻擊預測模式之學習。分類分析是從已知類別的訓練樣本(Training Examples)集合中，依據其屬性值(也就是可能影響樣本類別之變數值)建立一個分類模式來描述屬性值與類別之關係。常使用的分類分析技術，包括決策樹歸納學習法(Quinlan 1986; 1993; 1996)與倒傳遞類神經網路(Backpropagation Neural Network) (Rumelhart et al., 1986)。考量本研究所需處理的資料大小與即時性的要求，我們採用了 C4.5 決策樹歸納學習技術來建構 DoS 攻擊流量預測模式。

針對給定的訓練樣本集合，決策樹歸納學習技術是利用歸納的方式，來產生樹狀結構的分類模式。在構建決策樹的過程中，C4.5 以資訊獲利(Information Gain)或獲利率(Gain Ratio)為衡量依據，選擇最具區分力的屬性做為決策樹的節點。然後在此節點下，依據所選擇的分類屬性之值域，適當地建立多個子節點，並將原本屬於母節點的所有訓練樣本，分配至適當的子節點中。接著針對每一個子節點重複執行上述過程，直到每一子節點中所包含的訓練樣本皆屬於某一類別，或者子節點已滿足 C4.5 之預設終止條件。當完成預測模式的建立後，C4.5 決策樹可以產生如表 2 的預測法則，以作為 DoS 攻擊流量辨別之用。表 2 中的預測法則 Rule 29 表示，當流出的 bytes 數大於 29,706，流出的 unicast 封包數大於 2,351,072，且流入的 unicast 封包數小於等於 9,608 時，有 99.1%的機率是 DoS 攻擊所產生的流量。而 Rule 30 則表示，在流出的非 unicast 封包數大於 327，流入的 unicast 封包數小於等於 89,290，且流入的非 unicast 封包數小於等於 268 時，有 95.79%的機率是非 DoS 攻擊所產生的流量。

表 2：決策樹所產生的 DoS 攻擊預測法則

```
Rule 29:
        ifOutOctets > 29,706 and ifOutUcastpkts > 2,351,072 and
        ifInUcastpkts <= 9,608
        → class DoS [99.1%]
Rule 30:
        ifOutNUcastpkts > 327 and ifInUcastpkts <= 89,290 and
        ifInNUcastpkts <= 268
        → class notDoS [95.79%]
……..
```

二、阻斷服務攻擊偵測及防禦

在上一節中阻斷服務攻擊流量預測法則學習的目的，在於進行實際網路流量資料是否為 DoS 攻擊所產生的流量之判定。實際進行辨別時，僅需將網路管理系統管轄範圍內，所有支援 SNMP 的設備之各個網路介面，即時在某一時間間隔內，彙整上述 12 個預測變數的變數值，然後用前一步驟產生的分類法則來判別該流量資料是否為 DoS 攻擊。當判定某一流量為 DoS 攻擊時，網路管理主機則須適當地執行某些防禦措施，以減低 DoS 攻擊對正常使用者的影響。

彙整 DoS 攻擊防禦的相關研究發現，目前主要有兩類 DoS 攻擊的防禦方式：(1)中斷攻擊者或感染者的網路介面：當防禦系統可以明確地確認攻擊者或受病毒感染者的網路實體位置，並且可以確定中斷該網路介面不會對網路服務造成重大影響時，可以選擇直接中斷這個網路介面的使用，以隔絕攻擊主機對整個網路的影響(楊子翔與蔡錫鈞, 2000)。(2)減低攻擊者的影響：當無法判定攻擊者的網路位置，例如攻擊者使用 IP Spoof 技術來偽造來源 IP (Savage et al., 2001)，或攻擊者(被攻擊者)是網路上重要伺服主機，冒然關閉攻擊端網路介面可能會造成嚴重影響時，則可以利用設定網域對外路由器的 ACL (Access Control List)或降低攻擊來源介面的某些 QoS (Quality of Service)設定，以阻斷或減低攻擊者所造成的影響(林子傑, 2004)。

依據上述的 DoS 攻擊防禦文獻，本研究制定一套以 DoS 攻擊發生位置為基礎的防禦措施。(1) 若 DoS 攻擊發生在網路管理主機直接管理的範圍，且攻擊者是一般的使用者，則系統可透過 SNMP 來中斷最靠近 DoS 攻擊的來源介面，以避免網路上充斥大量攻擊封包，影響其他使用者效能，同時也可以防止蠕蟲病毒式 DoS 攻擊對外擴散傳染。(2) 若是攻擊端位在網路管理主機直接管理的範圍，且是重要的伺服主機，此時我們不應採取直接中斷其網路連線的處理方式，而是改採修定路由器或是最靠近攻擊端的交換器之設定，禁止這台主機 DoS 攻擊使用的 TCP/UDP 通訊埠(port)的封包傳送，如此可以在不中斷重要伺服主機其他服務的情況下，將 DoS 攻擊的影響減低。(3)若是攻擊端不在網路直接管理的範圍，而攻擊來源確定是某個固定 IP 位址(例如沒有使用 IP Spoof 技術的 SYN Flood 攻擊或是 Ping of Death 的攻擊)，網路管理主機可以在網域對外的路由器中設定 ACL，限制這個 IP 位址的傳輸。(4) 若是攻擊端不在網路直接管理的範圍，且攻擊來源也無法確定是某個固定 IP 位址時，則只能透過設定網域對外的路由器，降低 DoS 攻擊來源網域的 QoS，以減緩攻擊事件對網域可能造成的影響。

此外，本系統也會發佈 DoS 攻擊警報給予網路管理者，快速地提醒管理者 DoS 攻擊事件的發生和 DoS 攻擊的來源介面，以利採取適當的處理措施。例如攻擊來源不在管理的範圍內時，網路管理者可以配合其他網域的網路管理人員，儘速的解決其他網域的攻擊事件。藉由本系統的協助，可有效的減低 DoS 攻擊所產生的影響層面與範圍。

三、阻斷服務攻擊之偵測及防禦系統之建置成本與特性

本研究利用目前業界普遍採用的網路管理協定 SNMP 做為蒐集網路流量的基礎，輔以資料探勘的決策樹歸納學習技術，來進行 DoS 攻擊之偵測及防禦。本研究所提系統之建置成本主要有二：一是 SNMP 網路流量蒐集與 DoS 攻擊預測模式學習。(1)在 SNMP 網路流量蒐集成本方面，因目前的網路設備普遍支援 SNMP 協定，且本研究使用的為彙整過後的 SNMP 網路流量，因此所提方法僅對網路傳輸設備進行少量的 SNMP 網路流量查詢，並不會對於實際的網路傳輸造成嚴重的影響。此外，本研究所使用的網路管理主機，僅須對查詢所得之 SNMP 網路流量進行彙整，不同於以封包內容為基礎的偵測方法，需要一一比對流經的封包內容特徵值。因此，本研究所提出之偵測系統對網路管理主機效率之需求，遠低於以封包內容為基礎的偵測方法。(2)在 DoS 攻擊預測模式學習方面，因本研究採用決策樹歸納學習技術(C4.5)，其學習速率相當高。以一個 5,000 筆樣本的訓練資料為例，當我們在一台使用 Intel Pentium 4 2.4GHz CPU、512 MB RAM、執行 Windows XP Professional 的主機上進行學習時，所需之訓練時間僅為 0.92 秒。整體而言，本研究所提 DoS 攻擊偵測及防禦系統之建置成本相當低，僅需一台一般的主機來進行 SNMP 網路流量資料的蒐集與 DoS 攻擊預測模式的學習，並不需要任何額外的網路設備，且對網路實際資料傳輸之影響也相當低。

針對本研究所提 DoS 攻擊偵測與防禦系統及現有偵測及防禦技術之差異，說明如下：目前普遍用來偵測及防禦 DoS 攻擊的機制(如：防火牆、入侵偵測系統(IDS)、入侵防禦系統(IPS)等)，大多是以封包內容為基礎的偵測方法。這類方法所需的系統硬體規格要求較高，且這類的防禦系統只能偵測封包所流經的網段，無法針對區域網路內各不同網段同時進行監測。而本研究所提出的 DoS 偵測系統是利用 SNMP 網路流量作為偵測的基礎，因使用的是彙整的流量資料，系統硬體規格的要求遠低於防火牆、入侵偵測系統或入侵防禦系統，且一台偵測及防禦系統可以對多個網段的網路設備，進行 SNMP 流量查詢，達到同時監測多個網段的能力。此外當偵測到 DoS 攻擊後，可以選擇在最靠近 DoS 攻擊主機的網路介面進行防禦。這樣的特性對於新一代以蠕蟲病毒配合 DoS 攻擊這一類病毒的防禦特別有效，除了可以阻斷 DoS 的攻擊外，同時可以避免這一類病毒的擴散感染，此特性是傳統防禦系統較難達到的成果。然而本研究所提出的 DoS 攻擊偵測及防禦系統所使用的是經彙整的 SNMP 網路流量資料，所以在偵測即時性上不如目前普遍應用的防禦機制。只是它應仍能在幾分鐘內完成偵測(此需視蒐集流量資料彙整的時間間隔而定)及防禦，對於現階段的網路設備而言，承受數分鐘的 DoS 攻擊應不致於產生嚴重的系統故障。

肆、阻斷服務攻擊預測模式之實證評估

針對所提阻斷服務攻擊預測模式之學習，本文進行了實證評估，以驗證所提出 DoS 攻擊預測模式之效能。本評估主要包括三項實證實驗：首先，我們針對 DoS 攻擊流量的預測效能進行評估，這項評估實驗的主要目的，在於了解預測模式分辨 DoS 攻擊流量與正常流量的能力；其次，我們也針對預測模式在區分不同類型 DoS 攻擊事件的效能進行評估，藉以了解本文提出的網路流量為基礎的預測模式，是否除了預測 DoS 攻擊事件的發生外，也能提供是哪一類 DoS 攻擊方式的相關資訊，若能正確地辨別出 DoS 攻擊的類別，相信將能提供網路安全管理工作更多的協助；最後，我們評估所提 DoS 攻擊預測系統對於新的 DoS 攻擊類別之偵測效能。以下針對實證評估相關的流量資料蒐集、評估指標、評估流程與實證評估結果進行更詳細的說明。

一、流量資料蒐集

本實證評估共需要兩種類別的流量資料，分別為正常流量資料與 DoS 攻擊流量資料。在正常流量的資料蒐集方面，本文分別蒐集企業網路與學校網路環境下的正常流量。企業網路流量資料蒐集自某國營企業的內部網路；而學校宿舍網路流量資料則是蒐集自南部某國立大學的兩棟學生宿舍。另外，為了解不同時間間隔網路流量資料，對於本研究所提出之 DoS 攻擊偵測系統效能之影響，本研究將分別以 t 分鐘為取樣時間間隔週期(t = 1, 3, 5)進行網路交換器實體介面流量之蒐集。本研究分別在上述之企業網路及校園網路下，依 1、3 與 5 分鐘為取樣時間間隔週期，分別蒐集 9,000 筆以上網路流量資料，作為實證評估之用。

至於 DoS 攻擊網路流量資料之蒐集，由於在實際網路環境中進行含攻　行為的資料蒐集，將影響正常網路運作，而且恐有無法控制的後果，因此本研究在獨立的實驗網路環境中進行 DoS 攻擊網路流量之蒐集。為考量不同 DoS 攻擊可能會產生不同的流量資料，本研究將使用四類不同的 DoS 攻　程式(包括 TCP SYN Flood、Land、Angry Ping 與 Fake Ping)，分別以此四類 DoS 攻　程式攻　某一特定電腦，並實地蒐集網路交換器實體介面流量資料。利用此一實驗攻擊環境所蒐集的攻擊流量資料(如表三所示)，將作為訓練攻擊預測模式之用。本研究同樣分別以 t 分鐘(t = 1, 3, 5)為取樣時間間隔週期，蒐集 DoS 攻擊的網路流量資料。

表 3：DoS 攻擊流量資料筆數

攻擊類型	取樣時間間隔		
	一分鐘	三分鐘	五分鐘
TCP SYN Flood	1,311	1,726	494
Land	1,440	748	545
Angry Ping	1,425	1,404	925
Fake Ping	874	962	735

二、評估指標與流程

在評估指標方面，我們採用分類分析常用的三項指標：遺漏率(Missing Rate)、誤報率(False rate)及準確率(Accuracy Rate)作為我們效能評估的依據。假設總共有 k 個類別，其中 C_i 代表第 i 類別，而 n_{ij} 代表在測試資料集合中實際為 C_i 類別而本研究偵測系統預測為 C_j 類別之資料總數。很清楚地，n_{ii} 代表正確預測為 C_i 類別之資料個數。因此針對某一特定 C_i 類別，其相關的遺漏率與誤報率定義如下：

$$\text{遺漏率}(C_i) = \frac{\sum_{j=1,i\neq j}^{k} n_{ij}}{\sum_{j=1}^{k} n_{ij}}\text{，而誤報率}(C_i) = \frac{\sum_{j=1,i\neq j}^{k} n_{ji}}{\sum_{j=1}^{k} n_{ji}}$$

最後，整體的準確率定義為：

$$\text{準確率} = \frac{\sum_{i=1}^{k} n_{ii}}{\sum_{i=1}^{k}\sum_{j=1}^{k} n_{ij}}$$

在實證評估流程方面，為避免資料集大小不一可能造成的偏差，本研究首先比照五分鐘 DoS 攻擊的流量資料筆數，分別自一分鐘及三分鐘 DoS 攻擊流量資料集中，隨機取出 494、545、925 及 735 筆 TCP SYN Flood、Land、Angry Ping 與 Fake Ping 所產生的流量資料。緊接著，本研究也對正常流量資料集進行隨機取樣的過程，以使 DoS 攻擊與正常流量資料達到相同筆數。取樣後的 DoS 攻擊流量與正常流量資料將作為後續 DoS 攻擊預測模式實證評估之用。此外，本研究採用十摺交叉驗證法(Weiss & Kulikowski, 1991)來進行實證評估工作，係指將上述 SNMP 流量資料集合隨機分成資料個數相同大小的十組子集合，以其中一組作為測試資料，其餘九組則作為訓練資料，如此形成一摺資料組，且 10 組子集合依序作為測試資料，故總共有 10 摺資料組。最後，以十摺實驗結果的平均值作為最終的結果。

三、阻斷服務攻擊偵測實證評估結果

首先，我們針對所提出之 DoS 攻擊偵測系統，在區分 DoS 攻擊流量與正常流量的效能進行實證評估。在這個評估實驗中，我們並不特別區分不同類別的 DoS 攻擊，而是將這些流量資料都視為 DoS 攻擊流量。因此，預測模式的目的在於區分哪些流量是 DoS 攻擊，哪些流量是正常流量，也就是將預測問題視為一個 DoS 攻擊/非 DoS 攻擊的二分類問題。由表 4 所示的實證評估結果可以發現，本文所提出的 DoS 攻擊偵測系統，在企業網路環境下，其取樣時間間隔為 1, 3 與 5 分鐘其準確率分別可達到 99.78%, 99.91%與 99.83%；而在校園網路環境相同的取樣時間間隔下，也分別有 99.21%, 99.31%與 98.59%的高準確率表現。在預測遺漏率方面，企業網路環境在不同取樣時間間隔下都低於 0.19%；而校園網路環境的遺漏率最高也僅有 1.82%，亦即在 100 個確實為 DoS 攻擊的流量中，分別僅有 0.19 與 1.82 個遭誤判為非 DoS 攻擊流量。同時，企業網路與學校宿舍網路的誤報率亦控制在 0.33%與 1.10%以內。整體而言，本研究

所提的 DoS 攻擊預測模式，在不同的環境下(企業網路與學校宿舍網路)皆可以達到相當好的預測結果。

表 4：DoS 攻擊預測實驗結果

五分鐘取樣資料	遺漏率	誤報率	準確率
企業網路環境	0.19%	0.15%	99.83%
校園網路環境	1.82%	1.01%	98.59%
三分鐘取樣資料	遺漏率	誤報率	準確率
企業網路環境	0.04%	0.15%	99.91%
校園網路環境	0.52%	0.85%	99.31%
一分鐘取樣資料	遺漏率	誤報率	準確率
企業網路環境	0.11%	0.33%	99.78%
校園網路環境	0.48%	1.10%	99.21%

此外，比較不同網路環境下的 DoS 攻擊預測結果，可以發現在企業網路內的預測效能優於學校宿舍網路。造成此現象的可能原因，在於學校宿舍網路的使用者在使用行為上較為多樣化，因此產生的流量較難預測。例如，企業網路大多只用於某些特定的目的，或是可能會有許多的使用限制(不能架設個人 FTP 伺服器、不能使用 P2P、不能觀看 Web TV 等)，因此，產生的流量資料變化較少。相反地，學校網路使用者的行為較為多樣化，且所受的限制較少，反映在流量資料上則是較大的變異。

最後，依取樣時間間隔來比較 DoS 攻擊預測效能，可以發現取樣時間間隔的大小對預測效能的影響並不大，因此若考量預測的時效性，本研究建議以較短的時間間隔來進行資料取樣，如此可以更快速地偵測出區域網路內發生的 DoS 攻擊。相對地，若考量所需的計算資源，則可以以五分鐘的較長時間間隔來進行網路流量取樣，以減低在大型區域網路內的計算資源需求，增加系統的建置可行性。

四、阻斷服務攻擊類別偵測實證評估結果

如同本章開始的說明，除了預測 DoS 攻擊事件的發生外，若能同時提供是哪一類 DoS 攻擊方式的相關資訊，將能提供網路安全管理工作更多的協助。因此本研究也對 DoS 攻擊類別的預測進行實證評估。在這個評估實驗中，我們將 4 種 DoS 攻擊方式 TCP SYN Flood、Land、Angry Ping 及 Fake Ping 所產生的流量資料視為不同的類別，再加上正常流量的資料，所以本預測工作為一個 5 類別的分類問題。

如表 5 所示，無論所處的網路環境與流量的取樣時間間隔為何，本研究建立的預測模式都可達到 98.54%以上的整體預測準確率。根據上述準確率之定義，即有 98.54%以上的機率正確地預測出 TCP SYN Flood、Land、Angry Ping、Fake Ping 以及非 DoS 攻擊流量資料所屬的類別，顯示本研究所提出的預測模式對於這四類不同的 DoS 攻擊均能相當準確地辨認。考量網路環境與取樣時間間隔的個別影響，所得結論與前一節相似，亦即企業網路環境的預測準確率略優於校園網路環境，而取樣時間間隔的大小對預測效能的影響並不大。另外，比較單純對 DoS 攻擊/非 DoS 攻擊流量進行預測與

對 DoS 攻擊類別進行預測的準確率，可以發現單純判斷哪些流量是 DoS 攻擊的準確率略優於更近一步判斷屬於哪一種 DoS 攻擊所產生的流量，不過差異並不是很大(最大的差異為校園網路環境下，以五分鐘進行流量取樣時的 0.78%)。由此可知，在較複雜的 DoS 攻擊類別預測模式下，本研究仍達到相當好的預測準確率。

表 5：DoS 攻擊類別預測實驗結果(準確率)

五分鐘取樣資料	準確率
企業網路環境	99.89%
校園網路環境	98.55%
三分鐘取樣資料	準確率
企業網路環境	99.78%
校園網路環境	98.54%
一分鐘取樣資料	準確率
企業網路環境	99.63%
校園網路環境	98.61%

接下來，我們針對 DoS 攻擊類別預測之遺漏率進行說明，如表 6 所示，TCP SYN Flood 攻擊的預測擁有最低的預測遺漏率，在不同網路環境及不同流量的取樣時間間隔下之遺漏率均為 0%，也就是本研究所提的 DoS 攻擊預測模式可以百分之百地辨識 TCP SYN Flood 攻擊流量與正常流量或其他攻擊流量的差異。另外三種攻擊類型(Land, Angry Ping 與 Fake Ping)的遺漏率則隨著網路環境與流量取樣時間間隔的差異而有不同的表現。Land 攻擊在校園網路環境中均有較高的偵測遺漏率，分別為 6.07% (t = 5 分鐘)、4.40% (t = 3 分鐘)及 3.67% (t = 1 分鐘)，顯示 Land 攻擊在校園網路環境中的某些流量特性與正常流量或其他攻擊流量特性相近，而導致某些 Land 攻擊流量無法被正確辨識，造成較高的遺漏率。但是 Land 攻擊在企業網路環境中，在不同取樣時間間隔下，其偵測遺漏率均很低，分別只有 0.18% (t = 5 分鐘)、0.37% (t = 3 分鐘)及 0.73% (t = 1 分鐘)。因此根據遺漏率指標，顯示在校園網路環境中偵測 Land 攻擊之效能最差，但其在企業網路環境中亦可達到不錯的偵測效能。

表 6：DoS 攻擊類別預測實驗結果(遺漏率)

網路環境	DoS 攻擊類型	五分鐘取樣資料	三分鐘取樣資料	一分鐘取樣資料
企業網路環境	TCP SYN Flood	0%	0%	0%
	Land	0.18%	0.37%	0.73%
	Angry Ping	0.54%	0.11%	0.11%
	Fake Ping	0%	0.41%	0.27%
校園網路環境	TCP SYN Flood	0%	0%	0%
	Land	6.07%	4.40%	3.67%
	Angry Ping	0.86%	0.11%	0.43%
	Fake Ping	2.31%	3.54%	1.63%

偵測 Fake Ping 攻擊在校園網路中亦有偏高的遺漏率，分別有 2.31% (t = 5 分鐘)、3.54% (t = 3 分鐘)及 1.63% (t = 1 分鐘)，其遺漏率僅次於 Land 攻擊，但比 TCP SYN Flood 攻擊及 Angry Ping 攻擊高。Fake Ping 攻擊在企業網路環境中，在不同取樣時間間隔下，其偵測遺漏率均很低，分別只有 0% (t = 5 分鐘)、0.41% (t = 3 分鐘)及 0.27% (t = 1 分鐘)。因此根據遺漏率指標，Fake Ping 攻擊在校園網路環境的偵測效能僅優於 Land 攻擊，但在企業網路環境中仍有相當不錯的偵測效能。另一方面，Angry Ping 攻擊在兩種網路環境中，在不同取樣時間間隔下之偵測結果，均有很低的遺漏率，亦即 Angry Ping 攻擊流量幾乎完全被辨識出來，僅有很少數的 Angry Ping 流量被誤判為其他類別資料。以遺漏率指標而言，Angry Ping 攻擊在不同網路環境與不同取樣時間間隔下，均有很低的遺漏率，因此本研究所提出之 DoS 攻擊偵測系統對於 Angry Ping 攻擊有很好的偵測效能。

最後，考慮流量的取樣時間間隔對遺漏率的影響，可以發現 Land 攻擊於校園網路及 Angry Ping 攻擊於企業網路，以 1 分鐘流量取樣時間間隔所建立的預測模式，明顯優於 3 分鐘及 5 分鐘流量取樣時間間隔的預測結果。Land 攻擊於企業網路反而以 1 分鐘流量取樣時間間隔的遺漏率最高(0.73%)；Fake Ping 於企業網路利用 5 分鐘流量取樣時間間隔的遺漏率為 0%，但在 1 分鐘流量取樣時間間隔的遺漏率稍高(0.27%)，3 分鐘流量取樣時間間隔的遺漏率最高(0.41%)，而 Fake Ping 於校園網路的遺漏率反而是 1 分鐘流量取樣時間間隔最低(1.63%)，3 分鐘流量取樣時間間隔最高(3.54%)。從上述結果看來，由不同時間週期(t=1, 3, 5 分鐘)所建立的 DoS 攻擊預測模式，對於遺漏率的影響會隨著網路環境與攻擊類型而異。

如表 7 所示之 DoS 攻擊類別預測的誤報率，TCP SYN Flood 攻擊與 Angry Ping 攻擊在校園網路與企業網路以不同取樣時間間隔所建立之預測模式，其偵測的誤報率均很低(0.60%以下)，顯示將正常流量或其他攻擊流量誤認為是這兩種攻擊的機率不高。因此根據誤報率指標，利用本研究之偵測系統對於 TCP SYN Flood 攻擊與 Angry Ping 攻擊，在二個實驗網路環境中均有很好的偵測能力。偵測 Land 攻擊及 Fake Ping 攻擊的誤報率在校園網路環境均高於企業網路環境，顯示在校園網路中的某些實體介面之正常網路流量近似於這兩種 DoS 攻擊，因此導致 DoS 攻擊預測模式在校園網路中有較高的誤報率。但在企業網路環境除了以 1 分鐘流量取樣時間間隔之誤報率(1.81%)偏高外，Land 攻擊及 Fake Ping 攻擊的誤報率均相當低(0.81%以下)。因此根據誤報率指標，在企業網路中對 Land 攻擊及 Fake Ping 攻擊亦有不錯的偵測效能。從表 7 結果看來，由不同時間週期(t = 1, 3, 5 分鐘)所建立的 DoS 攻擊預測模式對於誤報率的影響會隨著網路環境與攻擊類型而異，且似乎並沒有一致的關聯性。

表 7：DoS 攻擊類別預測實驗結果(誤報率)

網路環境	DoS 攻擊類型	五分鐘取樣資料	三分鐘取樣資料	一分鐘取樣資料
企業網路環境	TCP SYN Flood	0.40%	0.20%	0.20%
	Land	0.37%	0.18%	1.81%
	Angry Ping	0.11%	0.11%	0.22%
	Fake Ping	0.14%	0.81%	0.27%
校園網路環境	TCP SYN Flood	0.20%	0.20%	0.60%
	Land	1.54%	3.07%	4.37%
	Angry Ping	0.22%	0.11%	0.22%
	Fake Ping	2.05%	3.54%	2.95%

整體而言，企業網路環境下的 DoS 攻擊類別預測效能優於校園網路環境，而流量的取樣時間間隔的影響則會隨著網路環境與 DoS 攻擊類別的影響而改變，沒有一致性。另外，在不同 DoS 攻擊類型下的預測效能，以 TCP SYN Flood 的效能最佳，Angry Ping 的效能次之，而 Fake Ping 與 Land 在校園網路環境下的效能最差。

五、新阻斷服務攻擊類別偵測實證評估結果

本研究進行另一項評估實證，以驗證所提出之 DoS 攻擊偵測系統在面對新攻擊類別時之偵測效能。為模擬新 DoS 攻擊類別之偵測，我們自訓練資料中移除某一 DoS 攻擊類別之資料，然後驗證測試資料中該類 DoS 攻擊之預測效能。例如，當移除訓練資料中的 TCP SYN Flood 攻擊時，因 DoS 攻擊預測模式學習時並沒有使用 TCP SYN Flood 攻擊流量資料，因此可以將 TCP SYN Flood 視為新 DoS 攻擊類別。當我們以學習得到的 DoS 攻擊預測模式，來預測測試資料中的 TCP SYN Flood 攻擊流量時，便可評估本研究所提 DoS 攻擊預測系統在面臨新 DoS 攻擊類別時之預測效能。

本研究分別移除訓練資料中的 TCP SYN Flood、Land、Angry Ping、Fake Ping，所得該新 DoS 類別之預測準確率如表 8 所示(該表中之準確率未包括已知 DoS 攻擊類別與非 DoS 攻擊流量之預測結果)。由表 8 可以發現，在不同的網路環境與流量的取樣時間間隔下，TCP SYN Flood 與 Angry Ping 攻擊類別仍保有相當高的預測準確率，但 Land 與 Fake Ping 的預測準確率卻相當不理想(企業網路環境下 5 分鐘取樣資料的 Land 和 Fake Ping 與 3 分鐘取樣資料的 Fake Ping 攻擊除外)。造成能夠準確預測 TCP SYN Flood 與 Angry Ping 攻擊類別的原因，在於 TCP SYN Flood 與 Angry Ping 攻擊類別的攻擊形態類似。TCP SYN Flood 與 Angry Ping 攻擊都是對攻擊目標單方向地傳送大量的封包(差別僅在於 TCP SYN Flood 傳送的是 TCP 封包，而 Angry Ping 傳送的是 ICMP 封包)，其 SNMP 流量資料的特性都是有大量的流入資料，但流出資料相對地少。因此雖然自訓練資料中移除 TCP SYN Flood (或 Angry Ping)攻擊流量資料時，仍可藉由 Angry Ping (或 TCP SYN Flood)攻擊流量資料所建立的分類模式來進行預測。

表 8：新 DoS 攻擊類別預測準確率

網路環境	新 DoS 攻擊	五分鐘取樣資料	三分鐘取樣資料	一分鐘取樣資料
企業網路環境	TCP SYN Flood	100.00%	100.00%	100.00%
	Land	100.00%	0.73%	0.00%
	Angry Ping	100.00%	99.89%	100.00%
	Fake Ping	100.00%	93.61%	2.31%
校園網路環境	TCP SYN Flood	99.39%	100.00%	100.00%
	Land	2.02%	3.30%	1.10%
	Angry Ping	96.97%	99.24%	98.38%
	Fake Ping	1.90%	5.03%	3.54%

Fake Ping 雖與 Angry Ping 同為 ICMP 封包的攻擊類別，但 Fake Ping 傳送完 ICMP 封包後會等待被攻擊端的回應(但 Angry Ping 並不等待回應)，因此其 SNMP 流量資料特徵為流入與流出資料大致對稱，且流量雖較正常流量大，但卻小於 TCP SYN Flood 與 Angry Ping 攻擊產生的封包數量。整體而言，Fake Ping 的流量特性與 TCP SYN Flood 及 Angry Ping 攻擊有小許的相似性(大量的流入資料)，因此在取樣時間間隔較大時(加大取樣時間間隔可擴大 Fake Ping 攻擊流量與正常流量間的差異)，仍有可能準確地預測 Fake Ping 攻擊流量。

本研究使用的 4 種 DoS 攻擊中，Land 的攻擊方式與另外 3 種有著顯著的差異。TCP SYN Flood、Angry Ping 與 Fake Ping 都是以大量封包壓迫被攻擊主機，造成其無法正常提供服務，但 Land 攻擊卻是以假冒被攻擊端 IP 位置的 TCP SYN 封包來進行攻擊，讓被攻擊端對自己傳送 TCP SYN ACK 訊息，達到消耗被攻擊端連線資源的效果。Land 攻擊的 SNMP 流量資料並沒有產生任何大量流入或流出的特性，因此當移除訓練資料中的 Land 攻擊資料後，本研究之 DoS 攻擊預測模式便無法區分 Land 攻擊與正常流量。

由上述實驗得到的一個重要結論是，如果訓練資料中存在有與新 DoS 攻擊類別相似流量特性的攻擊資料，本研究之 DoS 攻擊預測模式仍可準確地預測該新 DoS 攻擊。相反地，若訓練資料中完全沒有相似流量特性的攻擊資料，本研究之 DoS 攻擊預測模式便較難預測出該新 DoS 攻擊。此時衍生的另一個重要議題是，DoS 攻擊預測模式是否能在少量額外的付出(時間、人力等)下，偵測出該新 DoS 攻擊。為此，我們額外設計了一個實驗來回應這個議題。針對某一新 DoS 攻擊類別，我們隨機加入 10 筆該類 DoS 攻擊的流量資料至訓練資料中，藉由此一實驗，我們可以評估所提出之 DoS 攻擊預測模式，是否能夠迅速地建構出預測新 DoS 攻擊所需的預測法則，實驗結果如表 9 所示。比較表 8 與表 9 可以發現，雖然僅僅加入 10 筆新 DoS 攻擊類別的訓練資料，卻可以顯著地提升新 DoS 攻擊的預測準確率。以 Land 攻擊為例，在校園網路環境的 5、3、1 分鐘取樣資料下，分別由 2.02%、3.30%、1.10%提高到 80.70%、83.30%、85.14%；在企業網路環境下，也分別將 3、1 分鐘取樣資料的預測準確率由 0.73%與 0.00%改善為 97.61%與 68.62%。在 Fake Ping 攻擊類別下，也有類似於 Land 攻擊的顯著改善。根據以上的實驗結果，可知本文之 DoS 攻擊預測模式可以在付出少許的努力(例如蒐

集 10 筆新 DoS 攻擊類別的流量資料與重新學習 DoS 攻擊預測模式)後，達到不錯的新 DoS 攻擊類型預測能力。

表 9：DoS 攻擊類別預測準確率(訓練資料中含有 10 筆新 DoS 攻擊資料)

網路環境	新 DoS 攻擊	五分鐘取樣資料	三分鐘取樣資料	一分鐘取樣資料
企業網路環境	TCP SYN Flood	100.00%	100.00%	100.00%
	Land	100.00%	97.61%	68.62%
	Angry Ping	100.00%	100.00%	100.00%
	Fake Ping	100.00%	93.74%	98.78%
校園網路環境	TCP SYN Flood	99.59%	100.00%	100.00%
	Land	80.70%	83.30%	85.14%
	Angry Ping	97.08%	99.35%	98.92%
	Fake Ping	95.37%	84.22%	91.56%

伍、結論與未來研究方向

Dos 攻擊會造成網路服務的中斷，甚至進一步的商業損失。因此，如何偵測及防禦 DoS 攻擊是目前網路管理中一項重要研究問題。此外，隨著攻擊方式與技術的不斷推陳出新，造成了網路管理者在偵測及防禦上的許多困難。本研究以網路設備普遍支援的 SNMP 流量資料為基礎，提出一個 DoS 攻擊的自動偵測及防禦系統，以減低 DoS 攻擊對網路可能造成的影響。本研究所提出的阻斷服務攻擊與防禦系統主要包括：(1) 阻斷服務攻擊預測模式之學習與(2) 阻斷服務攻擊偵測及防禦機制。此外，本研究更針對阻斷服務攻擊預測模式之學習，進行了實證評估。根據實證結果顯示，利用 SNMP 的網路流量資料，以決策樹 C4.5 的分類方法，對於阻斷服務攻擊的分類有相當好的效能顯示，在企業網路環境中的準確率、遺漏率與誤報率皆優於 99.78%, 0.19%與 0.33%；而在學校宿舍網路中則分別優於 98.59%、1.82%、1.11%。若進一步考量不同網路環境與流量資料取樣時間間隔的影響，可以發現本研究所提阻斷服務偵測技術，皆可以發揮相當好的預測效能，擁有有相當高的預測穩定度。在新 DoS 攻擊類型的偵測方面，如果訓練資料中存在有與新 DoS 攻擊類別相似流量特性的攻擊資料，本研究的偵測技術依然可以達到相當好的偵測效能，但在面對具有獨特流量特性的新 DoS 攻擊類型時，也可以藉由蒐集少量(本研究中僅僅加入了 10 筆)該攻擊的流量資料，而大幅改善偵測的能力。

本研究有下列幾點研究限制與未來研究方向：(1) 本文使用的 DoS 攻擊流量資料為實驗環境下產生的，後續研究可以嘗試收集真實的攻擊流量，以便獲得更真實的驗證結果。(2) 本文僅針對 TCP SYN Flood、Land、Angry Ping 與 Fake Ping 等四種攻擊技術進行資料收集與實證評估，後續可以收集更多樣化的 DoS 攻擊模式的流量資料，以建構一個更全面的 DoS 攻擊偵測及防禦系統。(3) 本研究因受限於實驗的環境為區域網路內，對於在其他跨越廣域網路(WAN)的攻擊並沒有辦法評估偵測結果，未來可

建構更完整的實驗環境，來觀察在不同區域網路間的攻擊行為的偵測效能。(4) 對於其他可能出現特殊網路流量或異常網路行為的網路攻擊(如蠕蟲、病毒等)，均可以嘗試以本論文所提之架構進行偵測，以擴大本研究架構在網路安全方面的應用。

誌謝

本研究承蒙國科會的補助，專題計畫編號： NSC 93-2416-H-390-010，特此致謝。

參考文獻

1. Barford, P., Kline, J., Plonka, D., and Ron, A., "A Signal Analysis of Network Traffic Anomalies," *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement*, Marseille, France, 2002, pp. 71-82.
. CERT/CC, "CERT Advisory CA-1996-01 UDP Port Denial-of-Service Attack," September 24, 1997a, http://www.cert.org/advisories/CA-1996-01.html.
3. CERT/CC, "CERT Advisory CA-1997-28 IP Denial-of-Service Attacks," 1997b, http:// www.cert.org/advisories/CA-1997-28.html.
4. CERT/CC, "CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks," November 29, 2000, http://www.cert.org/advisories/CA-1996-21.html.
5. CERT/CC, "CERT Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow in IIS Indexing Service DLL," 2001a, http://www.cert.org/advisories/CA-2001-19.html.
6. CERT/CC, "CERT Advisory CA-2001-26 Nimda Worm," 2001b, http://www.cert.org/advisories/CA-2001-26.html.
7. CERT/CC, "Denial of Service Attack," June 4, 2001c, http://www.cert.org/tech_tips/denial_of_service.html.
8. CERT/CC, "CERT/CC Statistics 1988-2003," 2004, http://www.cert.org/stats/cert_stats.html.
9. Elson, D., "Intrusion Detection, Theory and Practice," March 27, 2000, http://www.securityfocus.com/infocus/1203.
10. Kargl, F., Marier, J., Schlott, S., and Weber, M., "Protecting Web Servers from Distributed Denial of Service Attacks," *Proceedings of the International WWW Conference (WWW 10)*, Hong Kong, May 1-5, 2001.
11. Kim, J., Lee, J., Han, K., and Lee, M., "Business as Buildings: Metrics for the Architectural Quality of Internet Businesses," *Information Systems Research* (13:3) 2002, pp. 239-254.

12. Lawrence, A.G., Martin, P.L., William, L., and Robert, R., "2004 CSI/FBI Computer Crime and Security Survey," Computer Security Institute, June 2004, http://www.gocsi.com/ press/20040609.jhtml.
13. Mauro, D., Schmidt, K., and Schmidt, K. J., *Essential of SNMP*, O'Reilly, 2001.
14. Mirkovic, J. and Reiher, P. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communication Review* (34:2) 2004, pp. 39-54.
15. Mukkamala, S. and Sung, A.H., "Detecting Denial of Service Attacks Using Support Vector Machines," *Proceedings of the 12th IEEE International Conference on Fuzzy Systems*, 2003, pp.1231-1236.
16. Paxson, V. "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks," *ACM SIGCOMM Computer Communication Review* (31:3) 2001, pp. 38-47.
17. Quinlan, J.R., "Induction of Decision Trees," *Machine Learning* (1:1) 1986, pp.81-106.
18. Quinlan, J.R., *C4.5: Programs for Machine Learning*, Morgan Kaufmann, San Mateo, CA, 1993.
19. Quinlan, J.R., "Improved Use of Continuous Attributes in C4.5," *Journal of Artificial Intelligence Research* (4) 1996, pp.77-90.
20. Rahmani, C., Sharifi, M., and Tafazzoli, T., "An Experimental Analysis of Proactive Detection of Distributed Denial of Service Attacks," *Proceedings of the IIT Kanpur Hackers' Workshop 2004 (IITKHACK04)*, February 2004.
21. Ranganathan, C. and Ganapathy, S., "Key Dimensions of Business-to-Consumer Web Sites," *Information & Management* (39:6) 2002, pp. 457-465.
22. Rumelhart, D.E., Hinton, G.E., and Williams, R.J., "Learning Internal Representations by Error Propagation," In *Parallel Distributed Processing: Explorations in the Microstructures of Cognition*, Vol. 1, Rumelhart, D.E. and McClelland, J.L. (Eds.), MIT Press, Cambridge, MA, 1986, pp. 318-362.
23. Savage, S., Wetherall, D., Karlin, A., and Anderson, T., "Network Support for IP Traceback," *IEEE/ACM Transactions on Networking* (9:3) 2001, pp. 226-237.
24. Wang, H., Zhang, D., and Shin, K.G., "Change-Point Monitoring for the Detection of DoS Attacks," *IEEE Transactions on Dependable and Secure Computing* (1:4) 2004, pp. 193-208.
25. Weiss, S. M. and Kulikowski, C. A., *Computer Systems That Learn: Classification and Prediction Methods from Statistics, Neural Nets, Machine Learning, and Expert Systems*, Morgan Kaufmann, 1991.
26. World Wide Web Consortium (W3C), "The World Wide Web Security FAQ," 2003, http://www.w3.org/Security/Faq/wwwsf6.html.

27. Yau, D., Lui, J., Liang, F., and Yam Y., “Defending Against Distributed Denial-of-Service Attacks with Max-Min Fair Server-Centric Router Throttles,” *IEEE/ACM Transactions on Networking* (13:1) 2005, pp.29-42.
28. 林子傑，2004，基於監控網路效能所提出之追蹤與緩和分散式阻斷服務攻擊的新方法，國立成功大學資訊工程學系碩士論文。
29. 徐國祥，2005，『2005 年網路安全威脅大追緝--國際資安大廠為 2005 危機尋找最佳出口』，http://www.informationsecurity.com.tw/feature/view.asp?fid=371。
30. 楊子翔，蔡錫鈞，2000，『Network DoS/DDoS 攻擊及預防方法研究』，TANET 研討會。
31. 鄭仁富，2005，『2004 年我國企業連網及應用程度調查分析報告』，資策會電子商務研究所 FIND 研究組。