Journal of Computer Science and Educational Technology
2016 VOL.6 No.1

應用模糊理論與類神經網路於偵測視訊會議遭受攻擊

Uses Fuzzy theory and Neuron Networks Detecting Attacks on Video Conference

[1] 劉仲鑫　　[2] 李祐陞

[1] Chung-Hsin Liu　　[2] Yu-Sheng Li

[1] 文化大學資訊工程學系

[1] Department of Computer Science and Information Engineering, Chinese Culture University

[2] 中國文化大學資訊安全產業研發碩士專班

[2] Graduate Institute of R&D Master Program in Information Security Industry, Chinese Culture University

摘要

視訊會議(Video Conference)是指提供語音和影像雙向即時傳送之服務，視訊會議提供比 Public Switched Telephone Network (PSTN)更好的服務品質與更低的價格、有善的介面以及方便的通訊系統。但是方便隨之來的安全議題也極需重視。

本研究量測分析視訊會議時的影像以及 DDoS 攻擊視訊會議之通訊品質狀況，我們使用模糊理論分析系統，使用類神經網路偵測 DDoS 攻擊並產生報告讓系統管理員做參考。並以 ISA Server 防火牆進行防護，期盼在基本且簡易的防火牆網路環境中提供視訊會議通訊影像品質正常運作之參考。

關鍵字：視訊會議、DDoS、模糊理論、類神經網路

Abstract

Video Conference provides two-way real-time voice and video transmission of services. Video Conference provides better quality than Public Switched Telephone Network (PSTN) at less cost. There are convenient and user friendly. But convenience usually accompanies security issues. That is what we need to pay much more attentions to.

This study measures and analyzes the images of video conference and few common video communications applications under the DDoS attacks. The image quality impacts during DDoS attacks are measured. We use fuzzy analysis system and neural network detection of DDoS, generate analysis reports for system administrators. We use ISA Server protect the video communications. The results provide a qualified video conference with an add-in basic firewall security environment.

Keywords: Video Conference, DDoS, Fuzzy, Neural Networks

1. 前言

資訊技術爆性的成長，擴展了人類視野及更方便的生活，過去從飛鴿書信到傳統電話進而發展到利用網路電話通訊，網路電話更縮短了人類的距離。但便利使得有心人士利用此弱點來，竊取、攻擊、阻斷，藉此取得利益。其中以 DDoS 攻擊最不易防範，嚴重的打擊網路電話的可用性。

本論文提出使用模糊理論控制防火牆，在 DDoS 攻擊時，能做最有效的防護措施以及提供有效的系統資訊，我們紀錄其系統的狀況，利用倒傳遞類神經網路，學習分析系狀況，進而可提供一個 DDoS 攻擊時之系統負荷之指標。我們實測分析 VoIP 與視訊會議通訊遭受 DDoS 攻擊時狀況，建構一套通訊品質量測架構，並以中小企業為基礎建立一套環境，我們希望提供一個良好且經濟的參考方案，使用 ISA Server 2006 及 HoneyPot 阻擋分析惡意攻擊。

2. 文獻探討

2.1 視訊會議

視訊會議是指提供語音和影像雙向即時傳送之服務，結合檔案傳輸、文件共享、電子白板等實用的多媒體即時網路交流工具，使雙方在無時空背景的限制下可以隨時隨地的舉行會議(徐悟梵，2010)。

為了提高語音影像傳輸時的安全性，我們透過加解密來保護語音視訊封包，卻降低了視訊會議的服務品質(Quality of service，QoS)，視訊會議 QoS 的評估關係到傳統電話用戶使用者，使用視訊會議之意願；了解及提高視訊會議 QoS 需求是相當重要的工作(陳宏宇，2005)。

由於 ~~VoIP 與~~視訊會議對於封包遺失率，容忍程度很低，故在建立通話後必需不受網路傳路傳輸的干擾，維持平穩語音品質。良好的 ~~VoIP 與~~視訊會議之 QoS 需支援每小時數以萬計的通話，當網路負載過大，要有良好通話拒絕機制，及有效的處理，必需保留特殊電話，並制定通話優先權，支援先佔式(Preemption)通話。且通話遲滯(Latency)不可多於 TDM 網路，也需要有足夠的安全性，並且預先設定通話配置設定(Needham, 1994)。

視訊品質量測指標包括平均意見分數(Mean Opinion Score, MOS)與峰值信號雜訊比(Peak Signal-to-Noise Ratio, PSNR)。平均意見分數 (MOS)是一種 QoS 的量測指標，由大量用戶以主觀的意見來評定的指標值，是最直接最具感官效果的評量法，一般需要具有公信

的組織來進行。峰值信號雜訊比(PSNR)則是一種評價圖像的客觀標準。通常影像壓縮之後或傳輸網路頻寬不穩定,都會讓輸出影像失真。為了量測影像的品質,我們通常會參考 PSNR 值來探討影像的品質

2.2 DDoS 攻擊

分散式阻斷服務(Distributed Denial of Service, DDoS) 目的在於癱瘓目標主機，為傳統 DoS 攻擊的延伸 (嚴芬、王佳佳、趙金鳳、 殷新春，2008) 。採用多對一的攻擊方式，被感染的主機數以指數方式成長，從多個源頭發起攻擊，威力急速增加。近年來更興起了一種反射式分散阻斷服務 DrDoS(Distributed Reflector Denial of Service，DrDoS)，它最優於 DDoS 的主因是它不需在攻擊前佔領大量的殭屍電腦，利用 TCP 三方交握規則，向源 IP 送出 SYN+ACK，如同 Smurf，使目標主機將忙於回應而被拒絕服務。

DDoS 攻擊過程一般可區分為三階段(李德全，2007) (1)資料收集(2)占領傀儡機(3)實施攻擊。

2.3 模糊理論

模糊控制，模擬人類的思考邏輯，是一種典型的智慧型控制系統，主要的特點是不需要依賴於數學模型，它是基於人類的知識、操作經驗以及推理技術，將控制系統的訊息對應出相對控制動作；模糊控制是以推論機為核心，並把知識和經驗，以「若…則」規則表示的知識庫，依據被控目標的現狀推論相對應的操控策略；模糊理論用在不完全的資料或模糊的訊息，不需經過繁複數學計算過程，仍可正確判斷出答案(馮國臣，2007)。

模糊控制器，通常由五大部份所構成，請參見下圖 1(張振宏，2007)。模糊化介面(Fuzzification interface)將輸入資料格式化成被模糊集合表現的語言數值，接收量測資料擷面的值，進行量化工作，以便將觀測量的範圍轉換到語言變量對等的論域。知識庫為模糊理論之資料庫(data base)，提供變數論域、語言項，歸屬函數及子集合的規劃等，以便提供語言控制規則模糊資料管理。規則庫為語言控制規則庫(rule base)，用來描述控制目標和領域專家的控制策略。解模糊化介面(Defuzzitication interface)將輸出變數值的範圍轉換到對等的論域，由推論出來的控制動作，產生出明確實際動作控制。決策邏輯(Decision making logic)為模糊推論機構，模擬人類判斷決策能力。根據特有的相近推理方式，實作出來的計算機構。

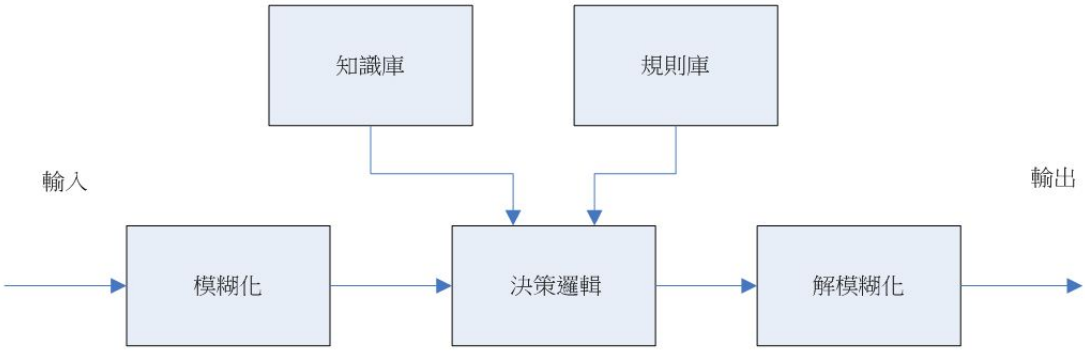

圖 1 模糊控制器

資料來源：類神經網路與模糊控制理論入門與應用

2.4 類神經網路(Neural Network)

類神經網路具有容錯、平行處理、記憶、學習、聯想等功能，基於類神經網路之推論，可分為正向推論、逆向推論、混合正逆向推論(陳杏圓、王焜潔，2007)。類神經網路，模擬人類大腦神經元運作之過程，包含訊息資料，加工、處理、儲存、搜索。

類神經的基本架構可分為兩大類：回歸型網路(recurrent net) 與前授型網路(feed-forward net)。

回歸型網路，請參見下圖 2。最具代表性的為霍普菲爾(Hopfield)網路，它的人工神經元彼此是相連的，每個神經元輸出連結到所有其它神經元，它的輸入神經元是由其它人的輸出所組成；每個神經元平行的接受全部的神經的輸入，在將其平行輸出到其它的神經元上，V1 代表神經元狀態，X1 表示輸入值啟始狀態，X1’ 表示輸出收斂值。

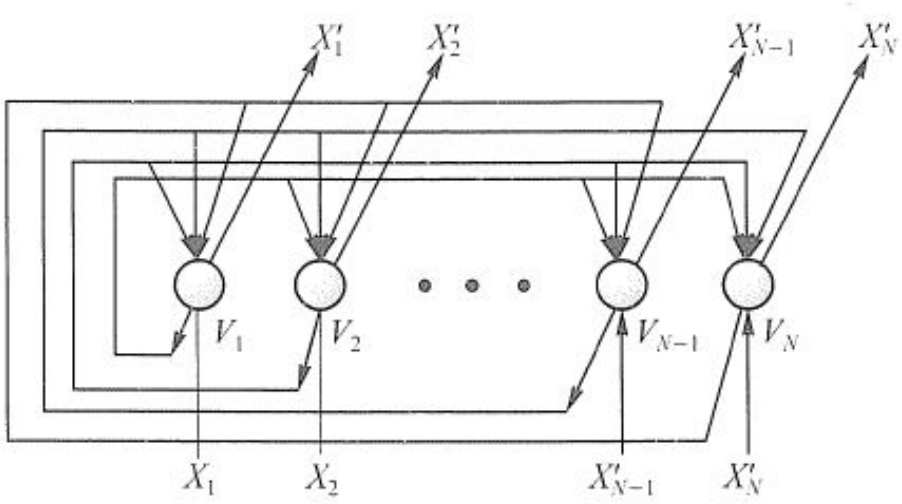

圖 2 回歸型類神經

資料來源：王進德(2003)，類神經網路與模糊控制理論入門與應用

前授型網路(feed-forward net)，請參見下圖 3。是一種階層式網路，輸入層、隱藏層、輸出層，每層皆由神經元組成，每一階層都不互相連接，輸出方向為單向，方向由輸入層到輸出層，最具代表性為倒傳遞網路(Back-Propagation net) (王進德，2007)：

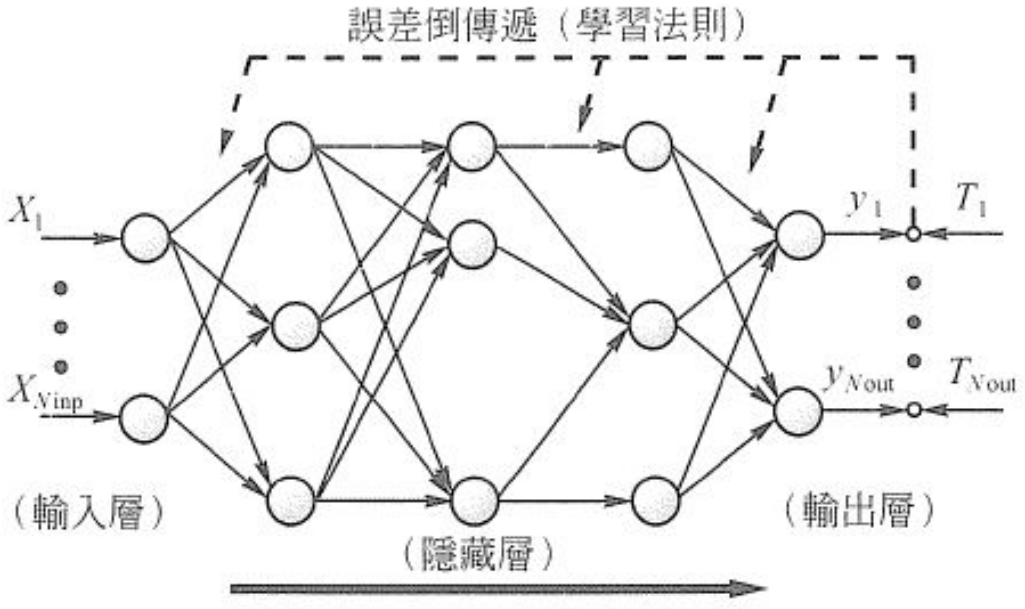

圖 3 前授型類神經網路

資料來源：王進德(2007)，類神經網路與模糊控制理論入門與應用

3. 實驗內容

請參見下圖 4，我們建置了一套中小型企業之環境，並以視訊會議為例，搭配 ISA Sever、Honey Pot 、卡巴斯基主控台……等安全元件，配合 DDoS 攻擊情境，實測量測其遭受攻擊之視訊會議之情況。在此依據實驗之流程，將每一步驟逐一以流程圖方式表示。

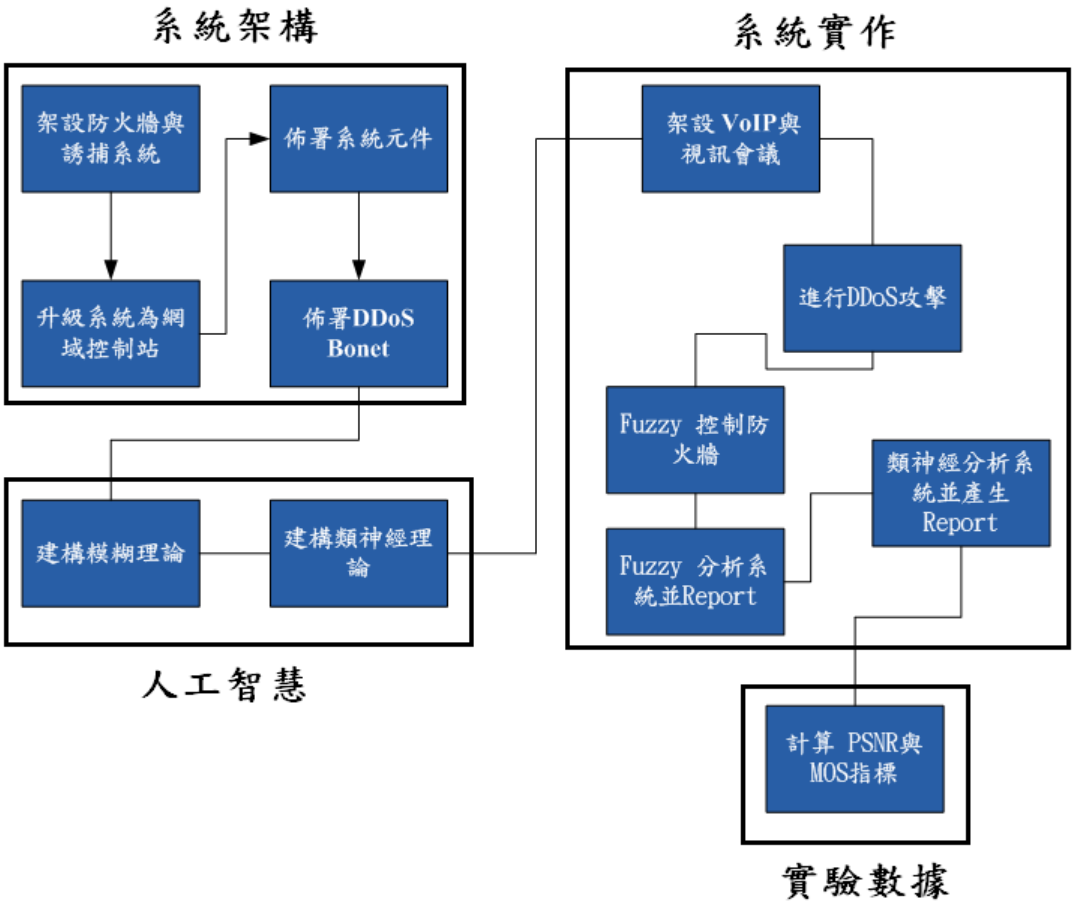

圖 4 系統流程圖

3.1 系統架構

本研究以實際的企業環境為基礎架構，在此建立其實驗環境。如下圖 5 之內部企業網路架構，包含卡巴斯基防毒主控台伺服器、檔案伺服器、列印伺服器、郵件伺服器、系統

管理員、一般使用者；防禦系統包含 ISA Sever 2006、HoneyPot；外部網路即惡意的攻擊來源。我們使用 Windows Server 2003 Active Directory 做為我們的網域控制站，在此並安裝 ISA Server、Honey Pot。透過 ISA Server 可將其組態配置於網域內電腦，稱為防火牆用戶端，提高網域內電腦之安全。

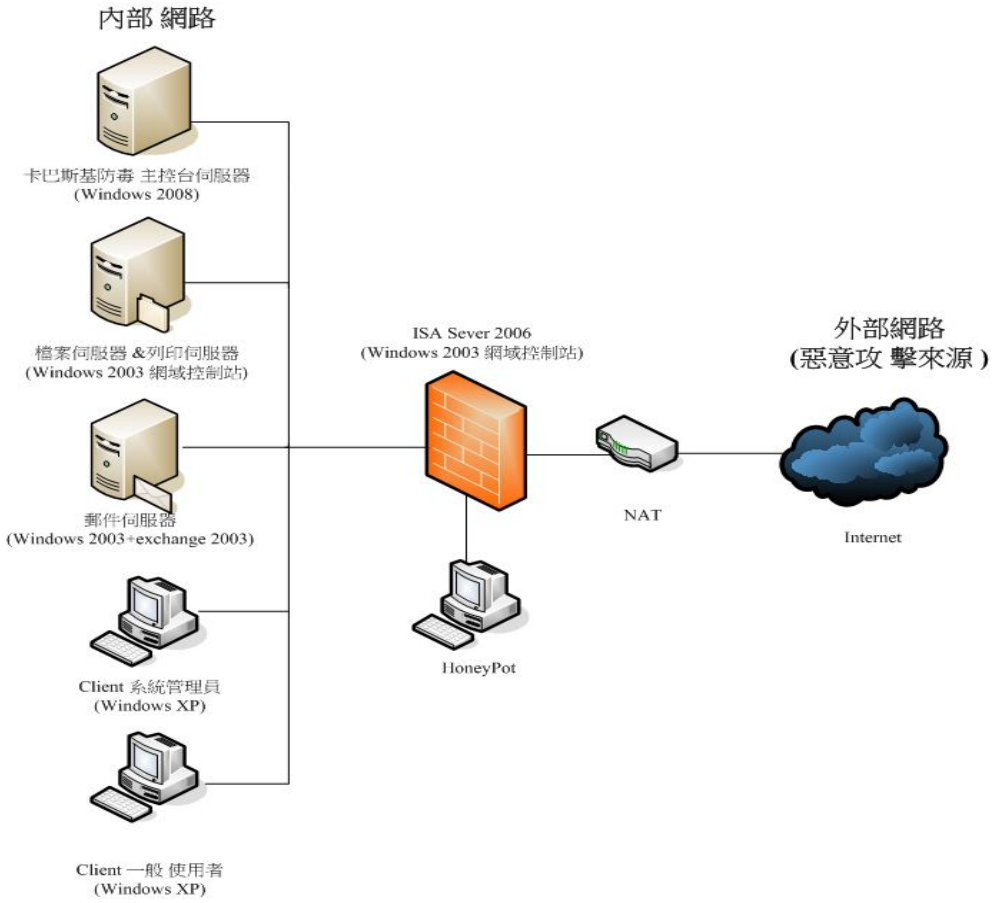

圖 5 系統架構圖

3.2 模糊理論系統架構

我們可以藉著以入侵系統的平均次數與惡意攻擊系統的平均次數為基準，當高於此次數過於多數，我們可以判斷系統疑似遭到大量的惡意攻擊及入侵，反之，當低於此次數，我們可以判定為系統低威脅，因為還在我們可以容許範圍內。

我們將系統攻擊比率與惡意攻擊系統比率，當作模糊規則輸入；完成推論後，經過解模糊化，得到一個明確的輸出信號，我們依此信號為自動判斷依據，亦或評估系統受威脅程度的重要指標。[系統入侵比率]是我們依照 ISA Server 偵測到惡意入侵之次數，如下圖 6 所示，例如：掃描所有連接埠攻擊、掃描知名連接埠攻擊、IP 半掃描攻擊、降落攻擊、死亡之 PING 攻擊、UDP 炸彈攻擊、Windows 出局攻擊……等攻擊，我們統計這些攻擊次數，

當成”入侵次數”，我們統計一季(三個月)每天的總攻擊次數將其取平均值為”平均攻擊次數”，將(入侵次數/平均攻擊次數)*100%，輸出結果當成模糊輸入的第一個輸入參數。

另外，我們亦統計像 IP 詐騙、DNS 干擾、POP 干擾、SYN 攻擊、超過規則的連線限制、超過來自於一個 IP 位址的 HTTP 要求、超過來自於一個 IP 位址的同時 TCP 連線限制、超過來自於一個 IP 位址的非 TCP 工作階段限制、超過每分鐘來自於一個 IP 位址的 TCP 連線限制、超過每分鐘來自於一個 IP 位址的被拒絕連線限制……等惡意的攻擊，也依照上述的方式輸入將(惡意攻擊系統次數/平均惡意攻擊系統次數次數)*100%，輸出結果當成模糊輸入的第二個輸入參數。

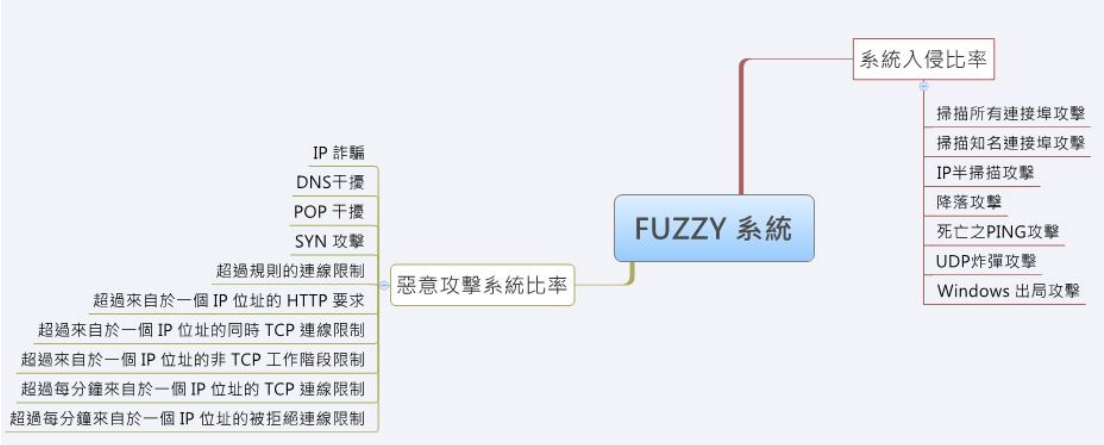

圖 6 惡意攻擊參數

3.3 類神經網路系統架構

類神經網路的優點在於，運作時使用者並不需要瞭解系統的數學模型，請參見下圖 7，而可直接以神經網路模型得到輸入值與輸出值間的關係。我們可以把類神經網路當成黑箱子，僅要依其輸入輸出參數設定，它將會模擬人類的思考模式做運算。我們利用倒傳遞類神經網路學習能力，將系統容易取得的四種參數，CPU 佔用率、記憶體佔用率、網路頻寬消耗率、平均往返時間當成輸入學習參數，將 DDoS 攻擊時的四個參數紀錄下來，用以偵測疑似 DDoS 徵狀，讓系統管理員能依此判斷來做系統調整。

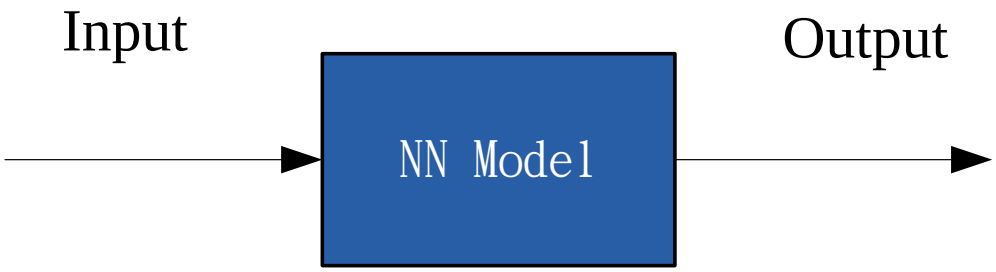

圖 7　類神經方塊圖

請參見下圖 8，在類神經網路學習前我們建立訓練樣本(training pattern)，訓練的樣本之數量為 150 筆，輸入的參數值為 CPU 佔用率、記憶體佔用率、網路頻寬消耗率、平均往返時間共四類，我們收集的訓練樣本是由我們自行建制之環境所收集。我們使用五台機器，安裝之系統為 Windows XP，針對我們架設的 ISA Sever 進行攻擊，將系統遭受 DDoS 攻擊時的狀況紀錄。

DDoS攻擊量	每秒攻擊kbps	攻擊時間min	Cpu佔用率%	記憶體佔用率%	網路頻寬消耗率	磁碟使用率	PING來回時間(平均往返時
不攻擊	0	0	2%~5%	14%	0%	64k	MAX=0,MIN=0,AVG=0 /r
單機攻擊	100000	10MIN	12%~30%	26%	62%	60k	02,03,02
	200000	10MIN	33%~38%	39%	96%	63K	03,03,03
	300000	10MIN	33%~49%	56%	97%	61k	04,06,04
雙機攻擊	100000	10MIN	35%~51%	52%	97.60%	62k	05,08,06
	200000	10MIN	38%~60%	66%	98%	60k	06,08,06
	300000	10MIN	39%~61%	75%	98.10%	60k	06,09,07
三機攻擊	100000	10MIN	40%~60%	67%	98.10%	66k	07,27,17
	200000	10MIN	40%~65%	80%	98.15%	63k	16,27,23
	300000	10MIN	41%~64%	75%	98.19%	65k	16,27,21
四機攻擊	100000	10MIN	40%~66%	85%	98.20%	64k	10,27,18
	200000	10MIN	33%~46%	87%	98.20%	64k	18,26,23
	300000	10MIN	32%~44%	90%	98.30%	59k	18,18,18
五機攻擊	100000	10MIN	34%~47%	89%	99%	61k	0,21,09 25%Miss
	200000	10MIN	35%~50%	93%	99.10%	62k	23,24,23 50%Miss
	300000	10MIN	34%~49%	95%	99.30%	65k	08,08,08 75%Miss
防火牆阻擋	0	0	20%~39%	45%	0%	70k	0 , 0 ,0

圖 8　DDoS 攻擊之實測

請參見下圖 9，我們每秒攻擊頻寬為 100000Kbps，攻擊時間為 10min，我們逐次增加攻擊端機器數量，量測其 CPU 佔用率%、記憶體佔用率%、網路消耗頻寬、磁碟使用率、PING

來回時間(單位 ms)；我們發現 CUP 佔用率，在 DDoS 攻擊量為四機攻擊，每秒攻擊 Kbps 為 200000 時，呈現一個穩定狀態，磁碟使用率，在此壓力測試中，並不會影響太大，CPU 佔用率、記憶體佔用率、網路消耗頻寬則是與 DDoS 攻擊數成正比，Ping 的往返時間亦隨著攻擊機數量成長，到五機攻擊時則開始 Miss。我們將上面記錄之參數，將其正規化為 0~1 間的輸入值，取出四個參數由左到右為 CPU 佔用率、記憶體佔用率、網路頻寬消耗率、平均往返時間。除了惡意 DDoS 攻擊的樣本，我們亦加入未攻擊的樣本共 70 筆。

116	0.1350	0.2510	0.7620	0.7610
117	0.6110	0.2150	0.1180	0.4350
118	0.1960	0.1560	0.5710	0.5860
119	0.3060	0.1250	0.9990	0.9810
120	0.8560	0.4890	0.9850	0.9630
121	0.4560	0.1590	0.9640	0.3650
122	0.1230	0.4510	0.2350	0.3650
123	0.1290	0.2310	0.1110	0.1560
124	0.9650	0.2350	0.7890	0.4890
125	0.4960	0.8880	0.8590	0.8740
126	0.2000	0.1500	0.0500	0.0300
127	0.6500	0.3800	0.0500	0.0300
128	0.6700	0.4000	0.0500	0.0300
129	0.7000	0.5600	0.0600	0.0300
130	0.7400	0.6100	0.1000	0.0312
131	0.8000	0.6300	0.1100	0.0300
132	0.7100	0.5300	0.0500	0.0332
133	0.8200	0.6100	0.0800	0.0365
134	0.9000	0.6600	0.1000	0.0345
135	0.9800	0.7200	0.1200	0.0322
136	0.9800	0.7500	0.1500	0.0478
137	0.8800	0.6800	0.3000	0.0357
138	0.9500	0.7400	0.3000	0.0445
139	0.9900	0.8000	0.3500	0.0412
140	0.9900	0.8800	0.3500	0.0456
141	0.9900	0.9500	0.3500	0.0496
142	0.2300	0.0960	0.0860	0.0235
143	0.0200	0.0250	0.0350	0.0480
144	0.0980	0.0870	0.0780	0.0896
145	0.2500	0.0250	0.0256	0.0150
146	0.0236	0.1560	0.1230	0.0560
147	0.1540	0.2560	0.0960	0.0780
148	0.0880	0.0120	0.0890	0.0960
149	0.2650	0.0114	0.0123	0.0880
150	0.4780	0.0160	0.0147	0.0456

圖 9 輸入之訓練樣本資料第 115 筆~150 筆

4. 實驗及量測方式

4.1 進行 DDoS 攻擊

請參見下表 1，本研究測試視訊會議，選用 Skype、Windows Live MSN 、Polycom PVX 等，它們皆具備 ITU-T H.264 編解碼標準。

表 1 選用視訊會議軟體

Item	Image Size	Pixels
SKYPE 3.8.0.139	143*107	15,301
Windows Live Message2009	320*240	76,800
Polycom PVX 8.0.16	366*277	101,382

DDoS 攻擊採用 DDoS 壓力測試工具與頻寬壓力測試工具 tfgen；壓力測試工具與頻寬壓力測試工具可進行下列型態的攻擊:

1. UDP flood 攻擊
2. TCP/SYN flood 攻擊
3. ICMP/PING flood 攻擊
4. ICMP/SMURF flood 攻擊
5. ICMP+TCP mix flood 攻擊
6. By Pass firewall flood 攻擊

請參見下圖 10，本實驗先將壓力測試工具植入受駭的 Botnet 內，五台電腦中，以組成殭屍網路；接下來以 Attacker 操作殭屍網路發動 DDoS 攻擊接收端之視訊會議主機。

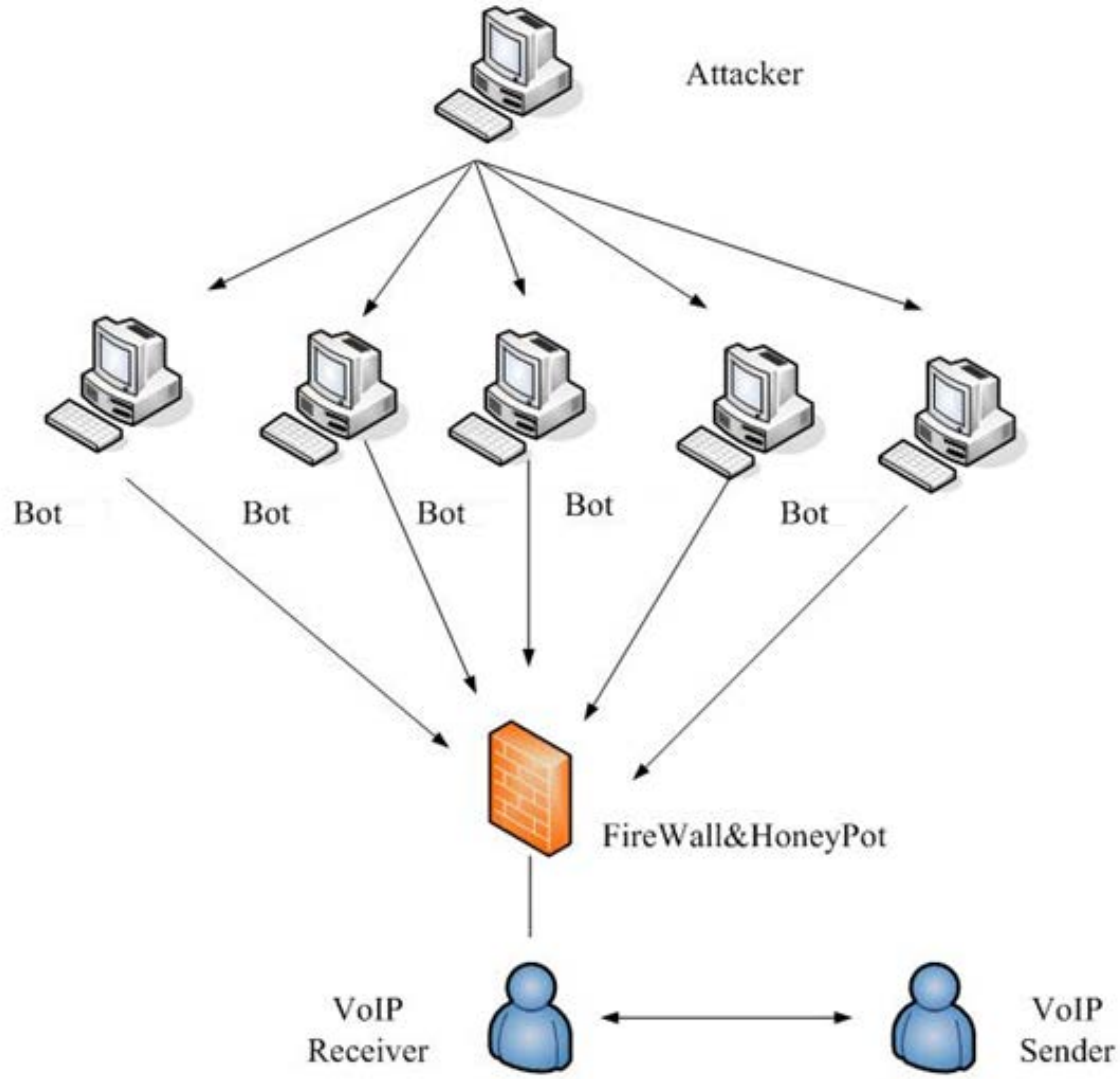

圖 10 壓力測試；DDoS 攻擊 VoIP Receiver

4.2 實驗結果與數據

請參見下圖 10，經過 DDoS 攻擊後，可知道接收端有嚴重頻寬佔用，接收端影像模糊不清。

未攻擊影像　　DDoS 攻擊之影像

圖 10　DDoS 攻擊之影像比較圖

請參見下圖 11，為了圖像內容之一致性以方便計算 PSNR 值，本實驗之視訊會議通訊在攻擊前後皆以固定場景拍攝，首先在 DDoS 攻擊時我們先截取 10 張圖片，再攻擊瞬間再截取 10 張圖片，將圖像使用 Adobe Proemiere 6.5 工具轉換成 avi 檔，再以 MSU Video Quality Measure Tool 轉換成我們所需的 PSNR 值如下圖

未攻擊 PSNR 值　　DDoS 攻擊之 PSNR 值

圖 11　DDoS 攻擊之 PSNR 值比較圖

4.4 計算 PSNR 及 MOS 指標

請參見下表 2，我們使用 PSNR 與 MOS 來評估影音及圖像品質好壞；PSNR 是一種良好的影像品質檢測方式，其單位為 dB，PSNR 值越大代表影像失真度越小，PSNR 若是為 30 左右表示兩張圖相當接近，PSNR 為 40 以上，肉眼幾乎無法分辨出差異(Ohm, 1999)；MOS(Mean Opinion Score)是依照人類的觀感來判定語音品質的指標，MOS 指標 1~5 如下表。

表 2 Mean Opinion Score(MOS) 與 PSNR 對照

PSNR(dB)	MOS
>37	5(Excellent)

31~37	4(Good)
25~31	3(Fair)
20~25	2(Poor)
<20	1(Bad)

資料來源：Ohm(1999). Bildsignalverarbeitung Fuer Multimedia-systeme

請參見下表 3，實測的結果，VoIP 遭受 DDoS 攻擊時，語音品質降低，MOS 指標達到了 2(Poor)和 1(Bad)。

表 3 VoIP 遭受 DDoS 攻擊；PSNR 及 MOS 指標

	Item	PSNR	MOS
1	SKYPE 3.8.0.139	20.77312	2(Poor)
2	Windows Live Message 2009	11.91757	1(Bad)
3	Polycom PVX 8.0.16	20.77440	2(Poor)

請參見下表 4，經過類神經網路評估系統及模糊控制 ISA Server 後，阻擋 DDoS，影像品質達到 4(good)。

表 4 ISA Server 阻擋 DDoS；PSNR&MOS 指標

	Item	PSNR	MOS
1	SKYPE 3.8.0.139	33.19732	4(Good)
2	Windows Live Message 2009	31.56891	4(Good)
3	Polycom PVX 8.0.16	32.58796	4(Good)

4.5 模糊理論與類神經網路之分析比較

請參見下圖 12，在未使用任何的防護之前，VoIP 遭受 DDoS 攻擊時，系統呈現低可用度，比較 MOS：SKYPE 與 Polycom 為 2(Poor)，MSN 為 1(Bad)；使用 Fuzzy 控制防火牆，可讓防火牆即時阻擋一些惡意攻擊，並透過 Fuzzy 依目前系統之威脅程度產生報告。

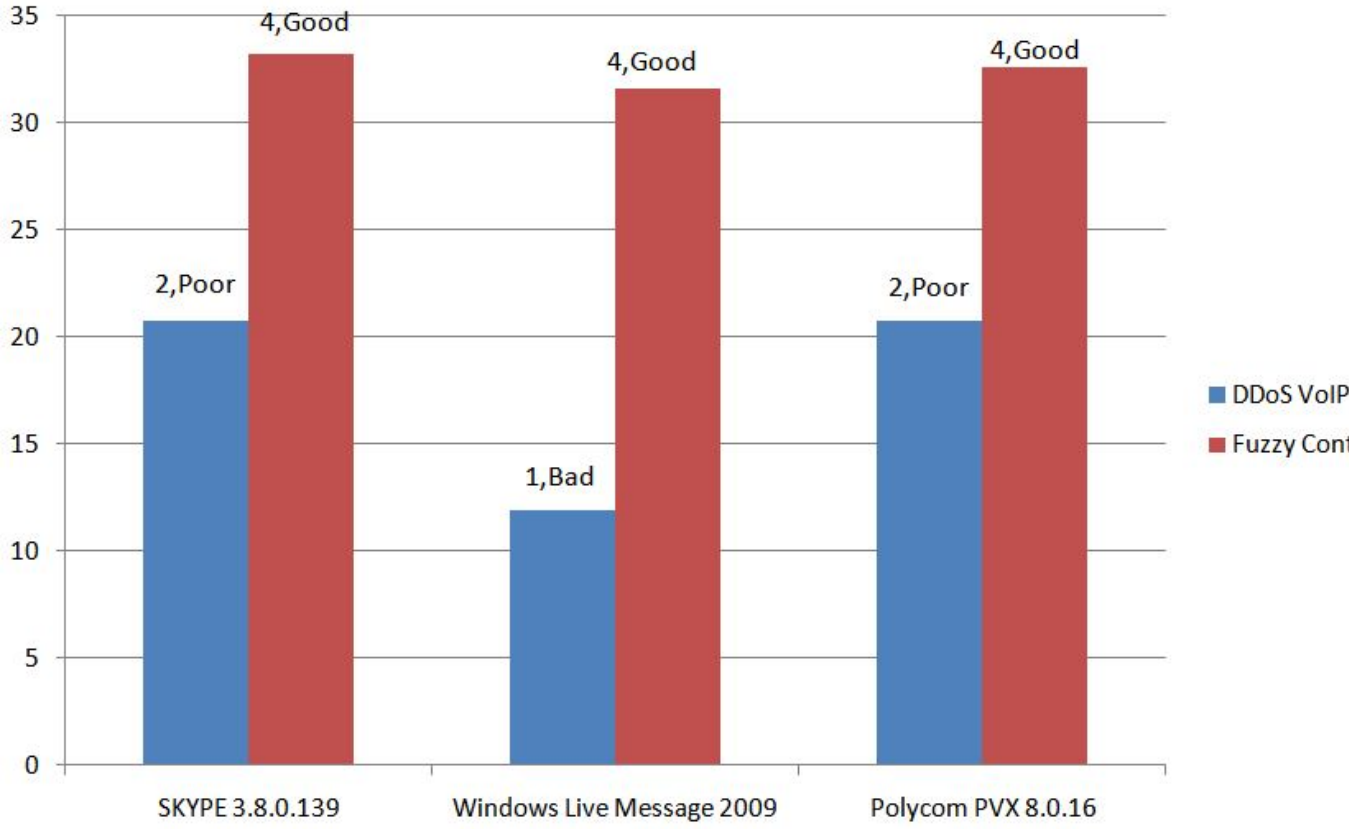

圖 12　模糊控制 ISA Server ,PSNR & MOS

請參見下圖 13，使用類神經網路(NN)評估系統可讓系統管理員隨時時地掌握系統之情況，檢測 DDoS，NN 亦依目前負荷之程度產生報告。

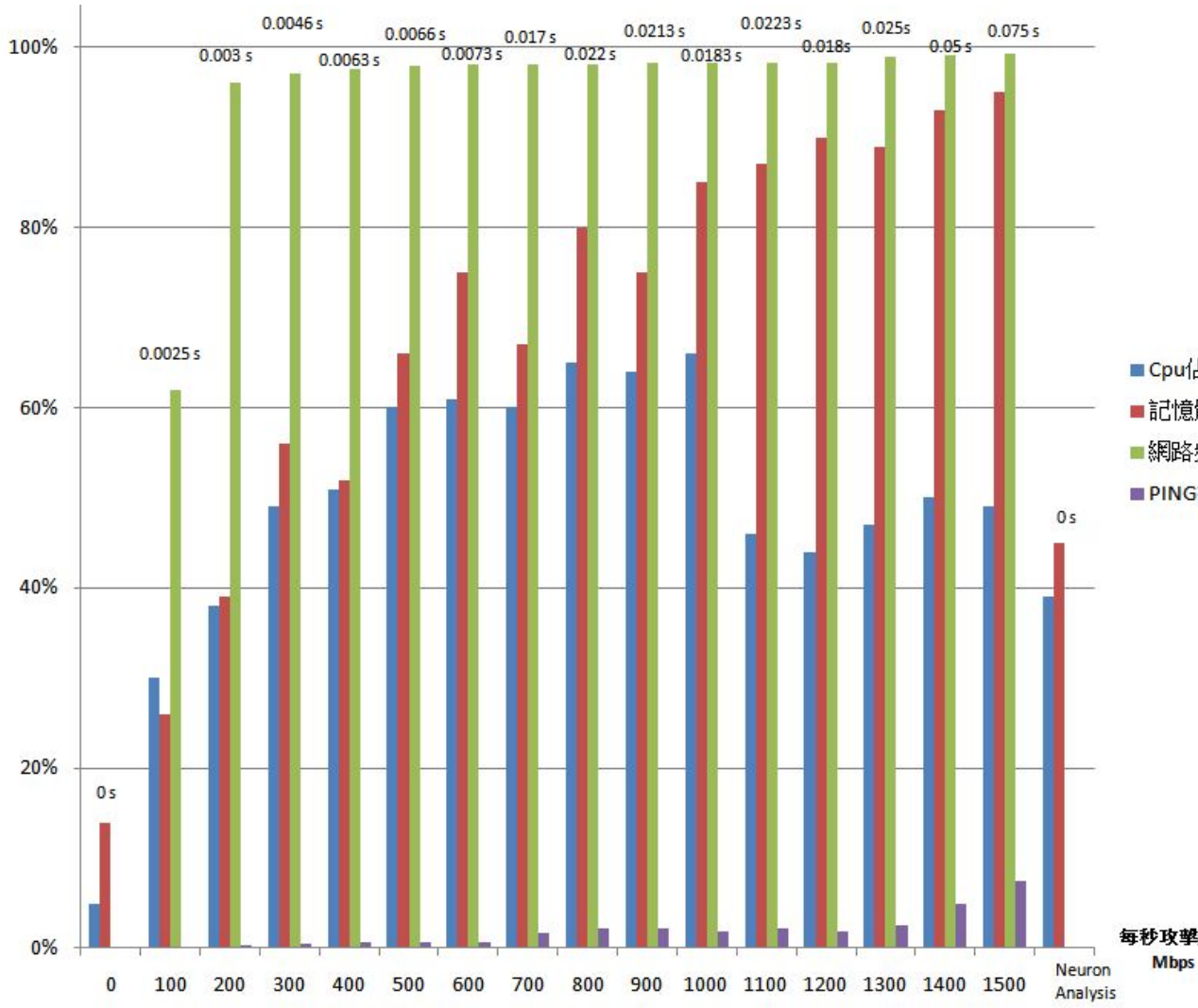

圖 13　類神經評估 DDoS 攻擊系統時之情況

系統管理員可以使用兩種方式可以有效的控制防火牆，並可交叉分析系統之威脅與負荷，使系統達到高可用度。如圖 12，經 Fuzzy 控制 ISA Server 進行防護後，其 MOS：SKYPE、MSN、Polycom 皆為 4(Good)。如圖 13，經過 NN 評估時，可以查覺系統遭受其大量的負荷，我們讓系統管理員依狀況啟動服務防護系統。

在系統遭受到 DDoS Botnet 每秒 100Mbps 攻擊頻寬下之負荷，從圖 13，我們可以很清楚的看到系統的負擔是隨著攻擊的頻寬大小逐次增加，在頻寬 1000Mbps~1500Mbps 間，系統呈現低可用度，此時的系統無法提供良好的服務，我們透過倒傳遞類神經網路，學習分析之能力，透過上面之學習訓練，在 DDoS 攻擊時，我們便能即時的使系統產生報告，讓系統管理員能啟動防護防止 DDoS，透過類神經的判斷分析後，並且啟動防護之後系統達到了一個穩定的狀態。經過類神經網路以及模糊控制器之交互使用更能精確的判斷及防護系統。

5. 結論

本論文針對視訊會議遭受 DDoS 攻擊時建立了一套分析攻擊架構，並架設視訊會議系統。另外，對 VoIP 與視訊會議做 DDoS 攻擊，以 ISA 2006 防火牆搭配誘捕系統，進行安全防護實測，紀錄影像尺寸及品質，並以 PSNR 與 MOS 做為評估標準。並且透過模糊理論來控制 ISA 2006；類神經網路評估系統，使得網管人員能依控制數據做最有效的調整。從本研究的結果証實了 ISA 2006 防火牆的防禦效果。未來，可參照此模型擴增電腦數量，探討不同數量攻擊損害程度。

6. 參考文獻

[1] 王進德(2007)，類神經網路與模糊控制理論入門與應用，全華圖書股份有限公司。
[2] 李勁(2003)，Windows Server 2003 系統建置篇，文魁出版社。
[3] 李德全(2007)，拒絕服務攻擊，第二版，電子工業出版社。
[4] 姜民遂、張思源(1998)，設計網路的錦囊妙計-採用防火牆的隔岸觀火計，網路通訊雜誌 70 期。
[5] 姚步慎(1991)，人工智慧與專家系統導論，碁峯資訊出版。
[6] 高超群(2006)，人工智慧－現代方法，第二版，全華圖書。
[7] 徐悟梵(2010) ，DDoS 攻擊及防火牆之研究：以 VoIP 與視訊會議為例，中國文化大學數位機電科技研究所碩士論文。
[8] 張振宏(2007)，利用統計式流量控制防止分散式阻斷服務攻擊，國立成功大學電腦與通訊工程研究所碩士論文。
[9] 張思源(1998)，揭開防火牆的神祕面紗，網路通訊雜誌 75 期。
[10] 馮國臣(2007)，模糊理論基礎與應用，新文京開發股份有限公司。
[11] 傅奎(2009)，神出鬼沒！教你怎樣駭，上奇資訊。
[12] 趙紅禮(2006)，網路安全，新文京出版社。
[13] 陳宏宇(2005)，VoIP 網路電話技術，松崗。
[14] 陳文生(2005) ，網路電話(IP 電信)系統規劃與建置，松崗。
[15] 陳杏圓、王焜潔(2007)，人工智慧，高立圖書有限公司。
[16] 陳彥升、吳文濱(2007)，人工智慧:智慧型系統導論，第二版，全華圖書。
[17] 蔡均璋(1998) ，網路防火牆的保全之道(一)，網路資訊雜誌 76 期。
[18] 蔡均璋(1998)，揭開防火牆面紗，光碟月刊 48 期。
[19] 駱俊霖(2009)，VoIP 可用性之研究模擬，中國文化大學數位機電科技研究所碩士論文。
[20] 戴有煒(2007)，ISA Server 2006 防火牆安裝與管理指南，碁峰。
[21] 魏慎廷(2007)，應用倒傳遞類神經網路技術建置學習方式分類模型，國立屏東教育大學資訊科學系碩士論文。

[22] 嚴芬、王佳佳、趙金鳳、 殷新春(2008)，DDoS 攻擊檢測綜述，計 算機應用研究。

[23] CEHv6(2007), CEHv6 Module 23 Evading IDS Firewall and Honeypot，EG-Conncil

[24] Dittrich, Dava (2003)，Distributed Denial of Service (DDoS) Attacks/tools[EB/OL]. http://staff.washington.edu/dittrich/misc/ddos/

[25] Microsoft(2006)，ISA Server 2006: A School Guide，Microsoft ISA Server 2006，Microsoft Ltd.

[26] Stamp, Mark (2003)，Packet Filtering CS265 Project Report，Deepali Holankar，CS265 Security Engineering.

[27] Needham, R. (1994)，Denial of Service :An Example[C], volume 37.Communications of ACM.

[28] Stallings, W. (1999)，CRYPTOGRAPHY AND NETWORK SECURITY，Prentice Hall.

[29] Russell, Stuart & Norvig, Peter (2003)，Artifical Intelligence: A Modern Approach, 2/e，Prentice Hall.